ROAR

Manual de Formação:

Apoio Especializado a Vítimas de Cibercrime

.

Training Manual:

Specialised Support to Victims of Cybercrime

.

Manual de Formare:

Asistență Specializată pentru Victimele Criminalității Informatice

ROAR
empowering victims of cybercrime

APAV
associação portuguesa de Apoio à Vítima

This Manual was funded by the European Union's Internal Security Fund – Police

Promotor:
Associação Portuguesa de Apoio à Vítima (APAV) | Portugal

Parceiros:
Ministério da Administração Interna (MAI) | Portugal
Procuradoria-Geral da República (PGR) | Portugal
PT Portugal | Portugal
Weisser Ring | Alemanha
ACTEDO | Roménia

ISBN: 978-989-54855-9-8
Depósito Legal:

Título:
Manual de Formação ROAR:
Apoio Especializado a Vítimas de Cibercrime

Morada:
APAV – Associação Portuguesa de Apoio à Vítima
Rua José Estêvão, 135 A
1150-201 Lisboa
Portugal

Tel.: +351 213 587 900
Email: apav.sede@apav.pt
Website: www.apav.pt
Facebook: www.facebook.com/APAV.Portugal

ÍNDICE

Introdução 05

a. Apresentação da Formação 07
a.1 Finalidade do curso 07
a.2 Estrutura e distribuição temporal do curso 07
a.3 Duração total do curso 09
a.4 Formadores/as 09
a.5 Avaliação e certificação da formação 09

b. Organização da Formação 11
b.1. Recursos 11
b.2. Notas para o(a) Formador(a) 12

Apêndices 15

PARTE 1 - COMPREENDER O CIBERCRIME 37

MÓDULO 1 - COMPREENDER OS FENÓMENOS DO CIBERCRIME 37
Tipologias de cibercrime 37
Conceitos e definições 37
Fatores de risco e vulnerabilidades comportamentais relacionadas com a cibervitimação 40

MÓDULO 2 - ENQUADRAMENTO LEGAL DO CIBERCRIME 47
O cibercrime na Lei Internacional e na *acquis* da União Europeia 47
O enquadramento jurídico do cibercrime a nível nacional 47
Principais desafios na investigação e na aplicação da Lei 48

MÓDULO 3 - VITIMOLOGIA E IMPACTO DO CIBERCRIME 55
Prevalência do cibercrime 55
Impacto nas vítimas particulares 55
- Consequências na saúde física, psicológica e emocional 56
- Impacto financeiro 56
- Receio do cibercrime e perceções sobre cibersegurança 56

PARTE 2 - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME 63

MÓDULO 4 - ASPETOS CENTRAIS NO APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME 63
Estruturar o apoio especializado a vítimas de cibercrime 63
- Empatia, técnicas de comunicação e apoio emocional 63
- Recolha de informação 64
- Avaliação do risco e desenvolvimento de planos de segurança 64
- Identificação das necessidades de apoio 65
- Intervenção em crise 66

MÓDULO 5 - APOIO ESPECIALIZADO A VÍTIMAS DE CRIMES CIBERDEPENDENTES 73
Modi operandi e natureza do crime 73
Estratégias de prevenção 74
Estratégias de intervenção 75
- Estratégias para preservação de prova digital 75
- A quem e como reportar/denunciar 76
- Estratégias para superar a vitimação e seus impactos 76

MÓDULO 6 - APOIO ESPECIALIZADO A VÍTIMAS DE BURLAS ONLINE 83
Tipos, *modi operandi* e natureza do crime 83
- Burlas no comércio eletrónico (*e-commerce*) 83
- Burla bancária 83
- Burlas nos relacionamentos íntimos (*romance scams*) 84

Estratégias de prevenção 85
Estratégias de intervenção 86
- Estratégias para preservação de prova digital 86
- A quem e como reportar/denunciar 86
- Estratégias para superar a vitimação e seus impactos 86

MÓDULO 7 - APOIO ESPECIALIZADO A VÍTIMAS DE FURTO DE IDENTIDADE ONLINE 99
Modi operandi e natureza do crime 99

ÍNDICE

Estratégias de prevenção 101
Estratégias de intervenção 101
- Estratégias para preservação de prova digital 101
- A quem e como reportar/denunciar 102
- Estratégias para superar a vitimação e seus impactos 102

MÓDULO 8 - APOIO ESPECIALIZADO A CRIANÇAS E JOVENS VÍTIMAS DE ABUSO SEXUAL ONLINE 113
Tipos, *modi operandi* e natureza dos crimes 113
- Disseminação de conteúdos de abuso sexual de crianças (CSAM) 113
- Conteúdos de abuso sexual de crianças gerados *online* 113
- Auto produção de conteúdos 114
- Transmissão em direto de abuso sexual de crianças 114
- Aliciamento (*grooming online*) 114
- Aliciamento nas redes sociais e em jogos de vídeo *online* 115

Estratégias de prevenção 115
Estratégias de intervenção 115
- Estratégias para preservação de prova digital 115
- A quem e como reportar/denunciar 116
- Estratégias para superar a vitimação e seus impactos 116

MÓDULO 9 - APOIO ESPECIALIZADO A VÍTIMAS DE CIBER-BULLYING 127
Modi operandi e natureza do crime 127
Estratégias de prevenção 128
Estratégias de intervenção 128
- Estratégias para preservação de prova digital 128
- A quem e como reportar/denunciar 128
- Estratégias para superar a vitimação e seus impactos 129

MÓDULO 10 - APOIO ESPECIALIZADO A VÍTIMAS DE VIOLÊNCIA ONLINE NAS RELAÇÕES INTERPESSOAIS: CIBER-STALKING E PARTILHA NÃO-CONSENSUAL DE IMAGENS 139
Tipos, *modi operandi* e natureza dos crimes 139
- Ciber-*stalking* 139
- Partilha não-consensual de imagens 139

Estratégias de prevenção 140
Estratégias de intervenção 140
- Estratégias para preservação de prova digital 140
- A quem e como reportar/denunciar 141
- Estratégias para superar a vitimação e seus impactos 141

INTRODUÇÃO

SOBRE O MANUAL

Aos dias de hoje, aproximadamente 90% dos/as cidadãos/ãs da União Europeia tem acesso à internet[1], a par do aumento do uso diário de internet pelos/as utilizadores/as.[2] Num mundo cada vez mais globalizado, em que se diluem não só fronteiras físicas, como virtuais, os riscos associados ao uso da internet encontram-se exponenciados. Não é, por isso, surpreendente que a vitimação por furto ou por burla de dados constitua o sexto risco global e, logo a seguir, enquanto sétimo risco mais provável de se experienciar, surja a vitimação por qualquer outro ataque cibernético.[3]

A cibercriminalidade tem-se alastrado a todas as áreas do crime, sendo os ataques dirigidos não só contra pessoas e o património, mas também contra Estados, impactando estruturas críticas, a economia e, fundamentalmente, a segurança e coesão da malha social.

As crianças são apontadas como um grupo particularmente vulnerável à cibervitimação, dada a natural limitação de capacidades de resiliência cibernética e a parca consciencialização para os riscos associados ao uso da internet, aliada ao facto de o acesso à internet ter lugar cada vez mais cedo, devido à massificação do acesso a *smartphones* e *tablets*.[4] Atente-se, por isso, ao surgimento de conteúdos sexuais explícitos autoproduzidos, i.e., criados pelas próprias crianças ou jovens. Por outro lado, crimes relacionados com conteúdos de abuso e exploração sexual de menores e de aliciamento de menores com vista à prática de atos sexuais, através do recurso à internet, encontram maior possibilidade de sucesso nos meandros da internet.[5]

Igualmente, as pessoas acima dos 55 anos de idade têm também sido associadas a uma maior exposição aos riscos inerentes ao uso da internet, sendo-lhes mais difícil estarem informados/as sobre esses riscos e, em consequência, mais improvável a adoção de medidas pessoais de segurança digital.[6]

A Resolução do Parlamento Europeu de 3 de outubro de 2017, sobre a luta contra a cibercriminalidade (2017/2068(INI)),[7] expressa importantes considerações sobre o impacto na segurança das pessoas, integridade dos seus dados pessoais, bem como na proteção da privacidade e das liberdades fundamentais, devido ao aumento significativo de ataques de *ransomware*, *botnets* e de interferência não autorizada em sistemas informáticos, sublinhando a necessidade de harmonizar as disposições legais referentes ao cibercrime e ao abuso e exploração sexual de crianças *online* nos diferentes Estados-Membros. Para tal, o reforço da cooperação entre todos os *stakeholders* e entre Estados mostra-se essencial.

Por sua vez, as vítimas de cibercrime devem beneficiar plenamente de todos seus direitos,[8] devendo os Estados-Membros apostar na prevenção e sensibilização e no apoio especializado, em caso de vitimação.

Assim, é premente melhorar o entendimento sobre cibercriminalidade, particularmente no que respeita à população em geral, a profissionais e decisores políticos, e promover respostas concertadas no combate ao cibercrime. Para o efeito, destaca-se a necessidade de união de esforços e competências de Estados, indústria, órgãos de polícia criminal, autoridades judiciárias, *media* e organizações da sociedade civil, de modo a garantir investigações eficazes e assegurando uma abordagem centrada nos direitos das vítimas.

Deste modo, objetivando a criação de ferramentas úteis à sensibilização e formação no combate ao cibercrime, na perspetiva das vítimas, pelo meio da elaboração de procedimentos e treino especializado para o apoio e capacitação destas vítimas, foi desenvolvido, no âmbito do Projeto ROAR, o **"ROAR - Manual de Formação: Apoio Especializado a Vítimas de Cibercrime** (***Project ROAR – Training Manual: Specialised Support to Victims of Cybercrime***),

[1] *EUROSTAT*, https://ec.europa.eu/eurostat/databrowser/view/tin00134/default/bar?lang=en

[2] No contexto europeu, ver *Special Eurobarometer 499 Report - Europeans' attitudes towards cyber security*, European Commission, pp. 9-14.

[3] Global Risks Report 2020, World Economic Forum http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

[4] *Internet Organised Crime Threat Assessment (IOCTA) Report 2019*, Europol, pp. 32-33. Ver também *Special Eurobarometer 499 Report - Europeans' attitudes towards cyber security*, European Commission, pp. 15-21.

[5] *IOCTA Report 2019*, Europol, pp. 29-34.

[6] *Special Eurobarometer 499 Report - Europeans' attitudes towards cyber security*, European Commission, pp. 46-47. Ver também *Barómetro APAV / INTERCAMPUS, Perceção da População sobre Cibersegurança*, Março 2020, pp. 11-12.

[7] P8_TA(2017)0366, Resolução do Parlamento Europeu, de 3 de outubro de 2017, sobre a luta contra a cibercriminalidade (2017/2068(INI)).

[8] Consagrados na Diretiva 2012/29/EU.

coordenado pela APAV (Associação Portuguesa de Apoio à Vítima), em parceria com a Guarda Nacional Republicana, Procuradoria-Geral da República e Altice Portugal, e com a parceira internacional da *Weisser Ring* (Alemanha) e *Equality and Human Rights Action Centre* (Roménia). Este Projeto, cofinanciado pelo Fundo de Segurança Interna - Polícia da União Europeia, procura sensibilizar a sociedade civil no geral e, em particular, as potenciais vítimas para este tipo de crimes, contribuindo para um aumento da ciber-resiliência, do número de cibercrimes reportados às autoridades e da procura de serviços especializados de apoio.

O presente Manual de Formação vem estabelecer uma série de recomendações formativas para um público bem definido e essencial no apoio às vítimas de cibercrimes – técnicos/as de apoio à vítima (TAV) -, focando-se também na prevenção e combate ao fenómeno em análise, oferecendo exemplos e materiais úteis, pragmáticos e atualizados à realidade europeia.

Este Manual de Formação não pretende encerrar-se sobre o conteúdo que transporta, mas sim estabelecer orientações para a organização de atividades de formação para o público-alvo supra mencionado, ambicionando, para além de oferta de sugestões de procedimentos para um melhor e mais eficaz apoio a vítimas de cibercrimes, potenciar uma reflexão partilhada junto dos/as formandos/as em matéria de conceitos tão essenciais como "vítimas de crime", "cibercrime", "cibersegurança" ou "ciber-resiliência".

Deste modo, o Curso "Apoio Especializado a Vítimas de Cibercrime" organiza-se da forma que em seguida se apresenta.

a. Apresentação da formação
b. Organização da formação
c. Desenvolvimento do curso de formação
d. Sessões formativas
e. Recursos didáticos

INTRODUÇÃO
a. Apresentação da formação

O Curso de Formação "Apoio Especializado a Vítimas de Cibercrime" pretende familiarizar e capacitar técnicos/as de apoio à vítima (TAV) para o fenómeno da cibercriminalidade, bem como para realidades que lhes estão associadas e o seu impacto nas vítimas, o seu enquadramento legal e para aspetos importantes na comunicação e interação com as vítimas destes crimes.

Pretende-se que os/as TAV compreendam as singularidades dos crimes ocorridos em meio digital e o impacto que geram nas vítimas, no sentido de melhor perceberem as suas necessidades particulares ao nível de informação e apoio para, dessa forma, introduzir melhorias na forma como apoiam e comunicam com estas vítimas.

É ainda objetivo deste Curso de Formação promover a sensibilização e capacitação das vítimas de cibercrime, nomeadamente através da criação de mecanismos de ciber-resiliência e promovendo o aumento dos crimes reportados, e garantir que as respostas do sistema de justiça penal e dos serviços de apoio à vítima sejam adequadas, adaptadas e centradas na vítima e nas suas particulares necessidades.

FINALIDADE DO CURSO

No final da formação, os/as formandos/as deverão ser capazes de reconhecer, de forma correta, as diferentes tipologias e conceitos associados ao cibercrime, bem como outras matérias igualmente importantes para a intervenção com vítimas de cibercrime, nomeadamente: o enquadramento legal do cibercrime; os fatores de risco e o impacto do cibercrime; os aspetos centrais no apoio especializado a vítimas de cibercrime; o apoio especializado a vítimas de diferentes tipos de cibercrime, nomeadamente *modi operandi*, estratégias de intervenção e de prevenção específicas.

ESTRUTURA E DISTRIBUIÇÃO TEMPORAL DO CURSO

	INTRODUÇÃO E CONTEXTUALIZAÇÃO	DURAÇÃO
	Apresentação do/a formador[a] Apresentação dos/as formandos/as Apresentação dos objetivos e conteúdos da intervenção formativa	5 Minutos
	PARTE 1 - COMPREENDER O CIBERCRIME	
Módulo 1	**Compreender os fenómenos do cibercrime**	
	Tipologias de cibercrime Conceitos e definições Fatores de risco e vulnerabilidades comportamentais relacionadas com a cibervitimação	30 Minutos
Módulo 2	**Enquadramento legal do cibercrime**	
	O cibercrime na Lei Internacional e na acquis da União Europeia O enquadramento jurídico do cibercrime a nível nacional Principais desafios na investigação e na aplicação da Lei	45 Minutos
Módulo 3	**Vitimologia e impacto do cibercrime**	
	Prevalência do cibercrime Impacto nas vítimas particulares Consequências na saúde física, psicológica e emocional Impacto financeiro Receio do cibercrime e perceções sobre cibersegurança	20 Minutos
	PARTE 2 - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME	
Módulo 4	**Aspetos centrais no apoio especializado a vítimas de cibercrime**	80 Minutos
	Estruturar o apoio especializado a vítimas de cibercrime Empatia, técnicas de comunicação e apoio emocional Recolha de informação Avaliação do risco e desenvolvimento de planos de segurança Identificação das necessidades de apoio Intervenção em crise	

Módulo 5 — **Apoio especializado a vítimas de crimes ciberdependentes** — 40 Minutos

Modi operandi e natureza dos crimes
Estratégias de prevenção
Estratégias de intervenção
- Estratégias para preservação de prova digital
- A quem e como reportar/denunciar
- Estratégias para superar a vitimação e seus impactos

Módulo 6 — **Apoio especializado a vítimas de burlas *online*** — 40 Minutos

Tipos, *modi operandi* e natureza dos crimes
- Burlas no comércio eletrónico [*e-commerce*]
- Burlas bancárias;
- Burlas nos relacionamentos íntimos [*romance scams*]

Estratégias de prevenção
Estratégias de intervenção
- Estratégias para preservação de prova digital
- A quem e como reportar/denunciar
- Estratégias para superar a vitimação e seus impactos

Módulo 7 — **Apoio especializado a vítimas de furto de identidade *online*** — 40 Minutos

Modi operandi e natureza do crime
Estratégias de prevenção
Estratégias de intervenção
- Estratégias para preservação de prova digital
- A quem e como reportar/denunciar
- Estratégias para superar a vitimação e seus impactos

Módulo 8 — **Apoio especializado a crianças e jovens vítimas de abuso sexual *online*** — 40 Minutos

Tipos, *modi operandi* e natureza dos crimes
- Disseminação de conteúdos de abuso sexual de crianças [CSAM]
  - Conteúdos de abuso sexual de crianças gerados *online*
  - Auto produção de conteúdos
  - Transmissão em direto de abuso sexual de crianças
- Aliciamento [*grooming online*]
  - Aliciamento nas redes sociais e em jogos de vídeo online

Estratégias de prevenção
Estratégias de intervenção
- Estratégias para preservação de prova digital
- A quem e como reportar/denunciar
- Estratégias para superar a vitimação e seus impactos

Módulo 9 — **Apoio especializado a vítimas de ciber-*bullying*** — 40 Minutos

Modi operandi e natureza do crime
Estratégias de prevenção
Estratégias de intervenção
- Estratégias para preservação de prova digital
- A quem e como reportar/denunciar
- Estratégias para superar a vitimação e seus impactos

Módulo 10 — **Apoio especializado a vítimas de violência *online* nas relações interpessoais: ciber-*stalking* e partilha não-consensual de imagens** — 40 Minutos

Tipos, *modi operandi* e natureza dos crimes
- *Ciber-stalking*
- Partilha não-consensual de imagens

Estratégias de prevenção
Estratégias de intervenção
- Estratégias para preservação de prova digital
- A quem e como reportar/denunciar
- Estratégias para superar a vitimação e seus impactos

Cada módulo é inicialmente apresentado com um **breve enquadramento teórico/conceptual** e apresenta-se seguidamente esquematizado através de um **plano de sessão**, organizado da seguinte forma:

- Tema
- Destinatários/as
- Duração da sessão
- Objetivo geral
- Objetivos específicos
- Conteúdos programáticos
- Metodologia
- Recursos pedagógicos/didáticos
- Avaliação | Exercícios
- Observações

DURAÇÃO TOTAL DO CURSO

A duração total deste Curso de Formação é de 7 horas (420 minutos).

O curso deve ser ministrado durante um dia.

FORMADORES/AS

Aconselha-se que os/as formadores/as possuam Certificado de Competências Pedagógicas (CCP, antigo CAP) e sejam da área das ciências sociais e humanas.

AVALIAÇÃO E CERTIFICAÇÃO DA FORMAÇÃO

Avaliação da Formação

A avaliação dos resultados da formação é efetuada:

- Pelos/as formadores/as mediante o Relatório de Avaliação dos/as Formandos/as (ver modelo no apêndice deste Manual);
- Pelos/as formandos/as, mediante o Relatório de Avaliação da Formação (ver modelo no apêndice deste Manual).

Certificação dos/as formandos/as:

- Emissão de Certificado de Frequência de Formação Profissional – documento emitido por uma entidade formadora que comprova que o/a formando/a frequentou uma ação de formação (ver em apêndice o modelo de certificado);
- A avaliação dos/as formandos/as realiza-se de forma contínua e interativa, incidindo na observação do desempenho nos exercícios propostos.

Este Manual inclui na sua estrutura: exercícios, materiais para a apresentação, como diapositivos em *PowerPoint*, material para distribuição e para servir de apoio à dinamização das sessões formativas.

Recursos

Para o desenvolvimento do Curso de Formação, há que ter em consideração os diferentes recursos que iremos enunciar de seguida.

Recursos espaciais e materiais

Os recursos espaciais e materiais desempenham um papel essencial na organização de um curso de Formação e o/A formador(a) deverá considerar de antemão o local em que o curso se vai desenvolver, os recursos materiais utilizados e o inventário dos materiais. O número de formandos/as por curso deverá idealmente ser entre 10 e 18.

Assim, sugerimos que seja verificada a seguinte *checklist*:

CRITÉRIOS	*CHECKLIST*
A sala tem acústica e iluminação apropriadas	
A sala está em condições de perfeita higiene e limpeza	
Existem tomadas em número suficiente	
As condições e a disposição das mesas e cadeiras são adequadas	
Existe um computador com software adequado (*Office PowerPoint*)	
Existe *data show*, colunas e tela para projeção	
Existem folhas brancas e canetas para distribuir pelos/as formandos/as	
Existem materiais didáticos para distribuir pelos/as formandos/as	
Existe um quadro branco e marcadores	

Os/as formandos/as devem ser informados/as sobre os locais onde poderão realizar as suas refeições durante o curso e a localização de transportes públicos que poderão utilizar, como paragens de autocarro, estações de metro e pontos de táxi mais próximos.

DICAS PARA O/A FORMADOR[A]

PREPARAÇÃO DO CURSO DE FORMAÇÃO

- **Ler, compreender e apreender o conteúdo do *ROAR* – Manual de Formação: Apoio especializado a vítimas de cibercrime.**
- **Familiarizar-se com os recursos disponíveis no referido Manual, incluindo suportes visuais propostos (apresentações em PowerPoint), assim como com os exercícios e materiais a distribuir**
- **Complementar e leitura do Manual de Formação com a consulta do conteúdo do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas***
- **Conhecer os objetivos e o programa do curso de formação**
- **Preparar todos os documentos (programas, fichas de inscrição, materiais didáticos, etc.) em número suficiente para distribuir pelos/as formandos/as**
- **Preparar folhas brancas de papel e canetas em número suficiente para distribuir pelos/as formandos/as**
- **Verificar a ficha de presença, as folhas de Avaliação de Satisfação da Formação e a folha de Avaliação Individual dos/as formandos/as**
- **Verificar as condições da sala, tendo em conta o número de formandos/as que vão participar na formação**
- **Verificar as condições do *software*, do *data show*, das colunas e do ecrã**

NO INÍCIO DO CURSO DE FORMAÇÃO

- **Realizar um bom acolhimento dos/as formandos/as**
- **Reforçar a importância do curso – expressar a importância da ação e dos resultados que se esperam alcançar**
- **Apresentar os objetivos e o programa do curso de formação**

DURANTE O CURSO DE FORMAÇÃO

- **Interagir e comunicar com os/as formandos/as e promover um clima de proximidade**
- **Recolher *feedback* intermédio relativamente à formação, dado que é sempre possível realizar correções ou alterar estratégias de dinamização**
- **Validar e reforçar as mensagens**
- **Perguntar se há dúvidas**

NO FIM DO CURSO DE FORMAÇÃO

- **Preencher o Relatório de Avaliação dos/as formandos/as**
- **Avaliar a reação dos/as formandos/as ao curso, distribuindo as folhas de Avaliação de Satisfação da Formação**

Os *slides PowerPoint* devem guiar e apoiar o desenvolvimento/dinamização deste Curso de Formação, mas não devem ser apenas lidos. Deverá acrescentar-se oralmente outra informação adicional e/ou complementar que enriqueça a apresentação de conteúdos.

Aquando da apresentação dos slides, deve prestar-se atenção à imagem e garantir que está focada e centrada e que pode ser vista em qualquer ponto da sala em que a formação tem lugar. Deve ajustar-se o brilho da imagem, de modo a que os/as formandos/as consigam ler os *slides*, sem os escurecer.

O/A formador(a) deverá preocupar-se com o modo como expõe os conteúdos programáticos previstos, pelo que deve atender aos seguintes aspetos:

- O tom de voz;
- Os gestos;
- As atitudes/posturas corporais;
- A expressão do rosto;
- A citação dos nomes dos/as participantes;

- As imagens;
- Os exemplos;
- O sentido de humor;
- O uso de analogias.

Deverá, ainda, ter em atenção ao modo como promove a participação do grupo e ao modo como utiliza os suportes audiovisuais para explicar, mostrar e ilustrar.

Deve também o/a formador(a) ter presente que toda a exposição tem:

O/A formador(a) deverá igualmente não esquecer que é responsável:

Durante a formação, o/a formador(a) deve procurar:

- Reunir os factos;
- Selecioná-los e valorizá-los;
- Obter a compreensão do grupo;
- Assumir várias funções: organizar, orientar, dirigir, informar, interpretar, reformular, animar, estimular, referir, moderar e conciliar, sempre que necessário. Deve fazê-lo sem que os/as participantes o sintam, o que implica:
  - Apresentar-se capaz e com tato para lidar com pessoas, nomeadamente com os/as formandos/as presentes;
  - Ser capaz de pensar com clareza e de forma rápida;
  - Ser capaz de se exprimir com facilidade;
  - Manter-se imparcial;
  - Procurar ser analítico/a;
  - Não demonstrar ser influenciável;
  - Apresentar autocontrolo;
  - Revelar-se paciente.

Deverá realizar o papel e as técnicas de animador(a), através da:

- Reformulação das opiniões individuais, o que facilita a expressão, dá importância a quem as emite e incita os/as outros/as participantes a escutar as ideias emitidas, estimulando as interações;
- Síntese, que é de importância fundamental e executa-se em todos os níveis: reformulação e síntese de uma intervenção que seja mais longa ou a síntese de duas ou mais opiniões:
  - Síntese por frase;
  - Síntese parcial em cada ponto do plano de sessão;
  - Síntese final.

Deve o/a formador(a) ter em conta um conjunto de técnicas:

A PERGUNTA TESTE	Utilizada para definir uma palavra ou um conceito que os/as participantes utilizam com conotações diferentes. Também é utilizada para definir uma palavra desconhecida que um[a] participante tenha utilizado.
APELO DIRETO À PARTICIPAÇÃO	Utilizada para promover a partilha/participação por um[a] participante que durante muito tempo permaneça silencioso/a ou para dar a palavra a um[a] participante que manifesta o seu interesse em participar
A PERGUNTA ECO	Pergunta realizada ao/à formador[a] por um[a] participante e devolvida sob a mesma forma, pedindo-lhe que partilhe a sua própria resposta
A PERGUNTA REVEZAMENTO	Repetição da questão colocada ao/à formador[a] por um[a] participante a um[a] outro[a] participante
A PERGUNTA ESPELHO	Repetição da questão colocada ao/à formador[a] por um[a] participante, devolvendo-a ao grupo
O RELANÇAMENTO	Repetição de uma pergunta realizada anteriormente e à qual o grupo ainda não havia respondido

Para lá das técnicas anteriores, o/a formador(a) pode tornar a ação de formação mais atrativa e agradável, expondo as suas ideias sob a forma de perguntas, ao invés de realizar afirmações diretas.

A conclusão da sessão/módulo e/ou do dia de formação é um momento de extrema importância. Uma boa conclusão é fundamental, por isso, deverá o/a formador(a):

- Ser breve;
- Salientar as fases e/ou conceitos mais importantes e referir os pontos-chave significativos;
- Promover a partilha de opiniões e feedback dos/as participantes face à ação;
- Sintetizar.

APÊNDICES

- Programa
- Cronograma
- Ficha de Inscrição
- Presenças e Sumários
- Registo de ocorrências e desistências
- Avaliação de satisfação da formação - formandos/as internos/as
- Avaliação de satisfação da formação - formandos/as externos/as
- Avaliação individual dos/as formandos/as
- Pauta final

DATA/S		CÓD. REF.	ÁREA DE EDUCAÇÃO E FORMAÇÃO
INTERVENÇÃO FORMATIVA	INTERNA	INTEREMPRESA	INTRAEMPRESA
DESIGNAÇÃO	Apoio Especializado a Vítimas de Cibercrime		
FORMADORES/AS			
HORÁRIO		Nº DE HORAS	7 Horas
LOCAL			
PRÉ-REQUISITOS	Trabalhar diretamente ou indiretamente com vítimas de cibercrime(s).		
DESTINATÁRIOS/AS	Técnicos/as de Apoio à Vítima (TAV).		
MODALIDADE DE FORMAÇÃO	Outra formação profissional	FORMA DE ORGANIZAÇÃO	Presencial
METODOLOGIAS	Expositiva, interrogativa e ativa.		
OBJETIVO GERAL	No final da formação, os/as formandos/as deverão ser capazes de reconhecer, de forma correta, as diferentes tipologias e conceitos associados ao cibercrime, bem como outras matérias igualmente importantes para a intervenção com vítimas de cibercrime, nomeadamente: o enquadramento legal do cibercrime; os fatores de risco e o impacto do cibercrime; os aspetos centrais no apoio especializado a vítimas de cibercrime; o apoio especializado a vítimas de diferentes tipos de cibercrime, nomeadamente *modi operandi*, estratégias de intervenção e de prevenção específicas.		
OBJETIVOS ESPECÍFICOS	No final da formação, os/as formandos/as deverão ser capazes de: • Distinguir, de forma correta, crimes ciberdependentes e crimes facilitados/possibilitados pela internet e pelas TIC; • Reconhecer, de modo correto, diferentes conceitos e definições associadas ao cibercrime, nomeadamente tipos de cibercrime; • Identificar, corretamente, os fatores de risco de cibervitimação relacionados com as características sociodemográficas; • Assinalar, sem erros, as vulnerabilidades comportamentais relacionadas com a cibervitimação, nomeadamente os fatores de risco relativos aos comportamentos de utilização da internet e das TIC; • Reconhecer, de forma correta, o enquadramento legal do cibercrime, à luz da lei internacional e do enquadramento jurídico nacional; • Identificar adequadamente, pelo menos, metade dos desafios abordados relativamente à investigação do cibercrime e à aplicação da lei; • Reconhecer, corretamente, o impacto do cibercrime em diferentes domínios da vida das vítimas de cibercrime; • Identificar, de modo adequado, as consequências do cibercrime nas perceções sobre cibersegurança e no receio relativamente ao cibercrime; • Enumerar, corretamente, todos os aspetos e etapas centrais na estruturação do apoio especializado a vítimas de cibercrime; • Distinguir, corretamente, a natureza e *modi operandi* de diferentes tipos de cibercrime; • Enumerar, de forma correta, estratégias de intervenção propostas para o apoio especializado a vítimas de diferentes tipos de cibercrime; • Reconhecer, de forma correta, estratégias de prevenção da revitimação propostas para a intervenção junto de vítimas de diferentes tipos de cibercrime.		

Estrutura programática	Carga horária	Formadores/as
INTRODUÇÃO E CONTEXTUALIZAÇÃO	5'	
• Apresentação do/a formador(a) • Apresentação dos/as formandos/as • Apresentação dos objetivos e conteúdos da intervenção formativa		
PARTE 1 – COMPREENDER O CIBERCRIME		
Módulo 1 – Compreender os fenómenos do cibercrime	30'	
• Tipologias de cibercrime • Conceitos e definições • Fatores de risco e vulnerabilidades comportamentais relacionadas com a cibervitimação		
Módulo 2 – Enquadramento legal do cibercrime	45'	
• O cibercrime na Lei Internacional e na *acquis* da União Europeia • O enquadramento jurídico do cibercrime a nível nacional • Principais desafios na investigação e na aplicação da Lei		

Módulo 3 – Vitimologia e impacto do cibercrime 20'

- Prevalência do cibercrime
- Impacto nas vítimas particulares
  - Consequências na saúde física, psicológica e emocional
  - Impacto financeiro
  - Receio do cibercrime e perceções sobre cibersegurança

PARTE 2 – APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME

Módulo 4 – Aspetos centrais no apoio especializado a vítimas de cibercrime 80'

- Estruturar o apoio especializado a vítimas de cibercrime
  - Empatia, técnicas de comunicação e apoio emocional
  - Recolha de informação
  - Avaliação do risco e desenvolvimento de planos de segurança
  - Identificação das necessidades de apoio
  - Intervenção em crise

Módulo 5 – Apoio especializado a vítimas de crimes ciberdependentes 40'

- *Modi operandi* e natureza dos crimes
- Estratégias de prevenção
- Estratégias de intervenção
  - Estratégias para preservação de prova digital
  - A quem e como reportar/denunciar
  - Estratégias para superar a vitimação e seus impactos

Módulo 6 – Apoio especializado a vítimas de burlas *online* 40'

- Tipos, *modi operandi* e natureza dos crimes
  - Burlas no comércio eletrónico (*e-commerce*)
  - Burlas bancárias
  - Burlas nos relacionamentos íntimos (*romance scams*)
- Estratégias de prevenção
- Estratégias de intervenção
  - Estratégias para preservação de prova digital
  - A quem e como reportar/denunciar
  - Estratégias para superar a vitimação e seus impactos

Módulo 7 – Apoio especializado a vítimas de furto de identidade *online* 40'

- *Modi operandi* e natureza do crime
- Estratégias de prevenção
- Estratégias de intervenção
  - Estratégias para preservação de prova digital
  - A quem e como reportar/denunciar
  - Estratégias para superar a vitimação e seus impactos

Módulo 8 – Apoio especializado a crianças e jovens vítimas de abuso sexual *online* 40'

- Tipos, *modi operandi* e natureza dos crimes
  - Disseminação de conteúdos de abuso sexual de crianças (CSAM)
    - Conteúdos de abuso sexual de crianças gerados *online*
    - Auto produção de conteúdos
    - Transmissão em direto de abuso sexual de crianças
  - Aliciamento (*grooming online*)
    - Aliciamento nas redes sociais e em jogos de vídeo *online*
- Estratégias de prevenção
- Estratégias de intervenção
  - Estratégias para preservação de prova digital
  - A quem e como reportar/denunciar
  - Estratégias para superar a vitimação e seus impactos

Módulo 9 – Apoio especializado a vítimas de ciber-*bullying* 40'

- *Modi operandi* e natureza do crime
- Estratégias de prevenção
- Estratégias de intervenção
  - Estratégias para preservação de prova digital
  - A quem e como reportar/denunciar
  - Estratégias para superar a vitimação e seus impactos

Módulo 10 – Apoio especializado a vítimas de violência *online* nas relações interpessoais: ciber-*stalking* e partilha não-consensual de imagens 40'

- Tipos, *modi operandi* e natureza dos crimes
  - Ciber-*stalking*

- Partilha não-consensual de imagens
- Estratégias de prevenção
- Estratégias de intervenção
  - Estratégias para preservação de prova digital
  - A quem e como reportar/denunciar
  - Estratégias para superar a vitimação e seus impactos

RECURSOS DIDÁTICOS E EQUIPAMENTOS

Computador com o *software Office* (*PowerPoint*) e *Media Player* (ou outro programa similar) instalado, retroprojetor| *Datashow*, colunas, televisão ou tela, cadeiras, apresentação em *PowerPoint*.

BIBLIOGRAFIA DE SUPORTE

APAV (2021). *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*. Lisboa: APAV.

AVALIAÇÃO DE CONHECIMENTOS

Avaliação diagnóstica através do levantamento de expetativas e nível de conhecimentos dos/as formandos/as sobre o tema.

Avaliação formativa/sumativa realizada através dos exercícios práticos e da verificação de objetivos.

CERTIFICAÇÃO

Após a conclusão do curso com sucesso será emitido um Certificado de Formação Profissional através da plataforma SIGO (Sistema de Informação e Gestão da Oferta Educativa e Formativa) com base nos seguintes critérios:

- Ter assiduidade no curso superior ou igual a 80%;
- Realizar as atividades propostas durante o curso;

A emissão de segundas vias de certificados tem custos associados.

CURSO: **Apoio Especializado a Vítimas de Cibercrime**

LOCAL: HORÁRIO:

DATA DE INICIO: DATA DE TÉRMINO:

MÊS																													
DATA	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
MANHÃ																														
TARDE																														

Módulos	Temática	Formador/a
1. Compreender os fenómenos do cibercrime		
2. Enquadramento legal do cibercrime		
3. Vitimologia e impacto do cibercrime		
4. Aspetos centrais no apoio especializado a vítimas de cibercrime		
5. Apoio especializado a vítimas de crimes ciberdependentes		
6. Apoio especializado a vítimas de burlas *online*		
7. Apoio especializado a vítimas de furto de identidade *online*		
8. Apoio especializado a crianças e jovens vítimas de abuso sexual *online*		
9. Apoio especializado a vítimas de ciber-*bullying*		
10. Apoio especializado a vítimas de violência online nas relações interpessoais: ciber-*stalking* e partilha não-consensual de imagens		

IDENTIFICAÇÃO DO/A FORMANDO/A

Nome Completo [*]:

Morada [*]:

Código Postal [*]: ___-___

Localidade [*]:

Nacionalidade [*]:

Sexo [*]:

País de origem [*]:

Data de nascimento [*]:

Naturalidade - Concelho [*]:

Naturalidade – Distrito [*]:

Telemóvel [*]:

E-mail [*]:

Tipo de documento de identificação [*]:

☐ Autorização de residência
☐ Identificação civil [cartão de cidadão/bilhete de identidade]
☐ Militar
☐ Passaporte

Nº do documento de identificação [*]:

Válido até [*]:

NIF [*]:

HABILITAÇÕES ACADÉMICAS

Habilitações académicas [*]:

Outras habilitações:

SITUAÇÃO PROFISSIONAL

Condição perante o trabalho [*]:

☐ 1. Empregado/a:
☐ 2. Desempregado/a:
☐ 3. Outra. Especifique:
☐ 4. À procura do 1º emprego
☐ 1.1. Trabalhador/a por conta de outrem
☐ 1.2. Trabalhador/a por conta própria
☐ 2.1. Desempregado/a [< 12 meses]
☐ 2.2. Desempregado/a de longa duração [> 12 meses]

DADOS PROFISSIONAIS

Empresa [*]:

Setor de atividade [*]:

Cargo/Função [*]:

DADOS PARA FACTURAÇÃO

Morada:

NIF:

AÇÃO DE FORMAÇÃO

Designação da ação de formação [*]:

Data/s [*]:

Local de realização [*]:

Tomei conhecimento e aceito as condições de inscrição e de frequência desta ação de formação e as condições gerais do funcionamento da formação definidas no Regulamento de Funcionamento da Formação? Se sim, assinale com X no quadrado. ☐

Nos termos da Norma Nacional de Proteção de Dados Pessoais, os dados aqui apresentados apenas poderão ser divulgados para efeitos de acompanhamento e avaliação da formação. Para além das situações referenciadas, autoriza que os seus dados pessoais possam ser utilizados para a comunicação de iniciativas e de informação de natureza associativa ou profissional por parte da APAV - Associação Portuguesa de Apoio à Vítima? Se autoriza, assinale com X no quadrado. ☐

NOTA: São critérios de seleção para as inscrições rececionadas

1. Ordem de chegada da candidatura, caso o número de participantes ultrapasse o limite máximo fixado
2. Limite máximo de formando/as previsto por cada ação de formação
3. Cumprimento dos requisitos pré-definidos para cada ação de formação
4. Respeito pelo prazo de apresentação das inscrições
5. Preenchimento integral da ficha de inscrição

Declaro, sob compromisso de honra, serem verdadeiros todos os elementos constantes nesta ficha.

Data: / /

Assinatura do/a formando/a:

AÇÃO DE FORMAÇÃO

Designação da ação de formação [*]:

Data/s [*]: **Local de realização [*]:**

DADOS PROFISSIONAIS

DATA/S | CÓD. REF. | ÁREA DE EDUCAÇÃO E FORMAÇÃO

DESIGNAÇÃO: Apoio Especializado a Vítimas de Cibercrime

FORMADORES/AS | HORÁRIO

		RÚBRICA		EQUIPA DE COORDENAÇÃO DA FORMAÇÃO	
Nº	NOME COMPLETO	MANHÃ	TARDE	HORAS E TIPO DE FALTA	
				JUSTIFICADAS	INJUSTIFICADA
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

SUMÁRIO

ASSINATURA DO FORMADOR/ES:

ASSINATURA DA COORDENAÇÃO PEDAGÓGICA:

REGISTO DE OCORRÊNCIAS E DESISTÊNCIAS

DESIGNAÇÃO DA
INTERVENÇÃO FORMATIVA

ÁREA DE EDUCAÇÃO
FORMAÇÃO

CÓD. REF.

FORMADOR(A)

DATA

HORÁRIO

LOCAL

FORMANDO/A

CONTACTOS

Ocorrência (assinalar com X)

- ☐ Alteração de cronograma
- ☐ Alteração de formador(a)
- ☐ Avaria do equipamento
- ☐ Problemas de logística
- ☐ Desistência de formando/a *
- ☐ Problemas inerentes aos/às formandos/as
- ☐ Problemas inerentes ao/à formador(a)
- ☐ Problemas inerentes aos colaboradores de apoio à formação
- ☐ Outra. Qual?

*** Motivo de desistência do/a formando/a (assinalar com X)**

- ☐ Motivo de saúde
- ☐ Motivos pessoais
- ☐ Motivos profissionais
- ☐ Problemas com a entidade formadora
- ☐ Outra. Qual?

☐ **Não houve ocorrências e desistências a registar**

DESCRIÇÃO

DATA:

ASSINATURA DA COORDENAÇÃO PEDAGÓGICA:

A PREENCHER PELA GESTÃO DA FORMAÇÃO

Categorização da Gravidade da Ocorrência/ Reclamação (assinalar com X)

POUCO GRAVE

- ☐ Pouco impacto no desenvolvimento da formação
- ☐ Primeira vez

GRAVE

- ☐ Impacto no desenvolvimento de formação
- ☐ Reincidente (2ª vez)
- ☐ Possibilidade de mais do que 2 pessoas afetadas

MUITO GRAVE

- ☐ Elevado impacto no desenvolvimento da formação
- ☐ Reincidência (mais do que 2 vezes)
- ☐ Elevado número de reclamações associado
- ☐ Exige intervenção da coordenação

Resolução da Reclamação

Data de Resolução

Descrição da Solução

Data

Assinatura d@ Coord. Executiv@

Comunicação aos interessados

Modo de comunicação

Data

AVALIAÇÃO DE SATISFAÇÃO DA FORMAÇÃO – FORMANDOS/AS INTERNOS/AS

DATA | CÓD. REF. | ÁREA DE EDUCAÇÃO E FORMAÇÃO

DESIGNAÇÃO DO CURSO/MÓDULO Apoio Especializado a Vítimas de Cibercrime

FORMADORES/AS

LOCAL | DURAÇÃO

A sua opinião é fundamental para a melhoria da qualidade da formação da APAV. Agradecemos a sua sinceridade para nos ajudar a melhorar. Para tal deverá efetuar a sua avaliação de acordo com a seguinte escala:

1 = **Mau** (avaliação entre 0 e 4 valores);
2 = **Insuficiente** (avaliação entre 5 e 9 valores);
3 = **Suficiente** (avaliação entre 10 e 13 valores);
4 = **Bom** (avaliação entre 14 e 17 valores;
5 = **Muito Bom** (avaliação entre 18 e 20 valores).

1. Organização da formação

1 2 3 4 5

- Duração do curso/módulo
- Condições da sala (equipamentos/conforto)
- Coordenação pedagógica

2. Formador(a)

1 2 3 4 5

- Pontualidade
- Clareza das intervenções
- Domínio dos conteúdos (temas)
- Resposta às questões/dúvidas colocadas
- Métodos e técnicas utilizadas
- Cumprimento do programa
- Material de apoio (documentação, exercícios)

3. Conteúdos

1 2 3 4 5

- Relação dos conteúdos aos seus objetivos e expectativas
- Utilidade dos conteúdos para a função que desempenha
- Contribuição dos conteúdos para a sua melhoria profissional/pessoal
- Expectativa de aplicação dos conteúdos num prazo de 3 meses

4. Avaliação Global

1 2 3 4 5

- Do curso/módulo

COMENTÁRIOS E SUGESTÕES DE MELHORIA

SUGIRA-NOS OUTROS CURSOS QUE GOSTARIA DE FREQUENTAR

Nome do/a Formand@:

AVALIAÇÃO DE SATISFAÇÃO DA FORMAÇÃO – FORMANDOS/AS EXTERNOS/AS

DATA | CÓD. REF. | ÁREA DE EDUCAÇÃO E FORMAÇÃO

DESIGNAÇÃO DO CURSO/MÓDULO Apoio Especializado a Vítimas de Cibercrime

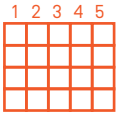
FORMADORES/AS

LOCAL | DURAÇÃO

A sua opinião é fundamental para a melhoria da qualidade da formação da APAV. Agradecemos a sua sinceridade para nos ajudar a melhorar. Para tal deverá efetuar a sua avaliação de acordo com a seguinte escala:

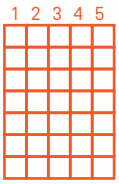
1 = **Mau** (avaliação entre 0 e 4 valores);
2 = **Insuficiente** (avaliação entre 5 e 9 valores);
3 = **Suficiente** (avaliação entre 10 e 13 valores);
4 = **Bom** (avaliação entre 14 e 17 valores;
5 = **Muito Bom** (avaliação entre 18 e 20 valores).

1. Organização da formação



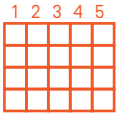
- Duração do curso/módulo
- Condições da sala (equipamentos/conforto)
- Coordenação pedagógica
- Relação Preço/Qualidade

2. Formador(a)



- Pontualidade
- Clareza das intervenções
- Domínio dos conteúdos (temas)
- Resposta às questões/dúvidas colocadas
- Métodos e técnicas utilizadas
- Cumprimento do programa
- Material de apoio (documentação, exercícios)

3. Conteúdos



- Relação dos conteúdos aos seus objetivos e expectativas
- Utilidade dos conteúdos para a função que desempenha
- Contribuição dos conteúdos para a sua melhoria profissional/pessoal
- Expectativa de aplicação dos conteúdos num prazo de 3 meses

4. Avaliação Global

- Do curso/módulo

COMENTÁRIOS E SUGESTÕES DE MELHORIA

SUGIRA-NOS OUTROS CURSOS QUE GOSTARIA DE FREQUENTAR

Nome do/a Formand@:

AVALIAÇÃO INDIVIDUAL DOS/AS FORMANDOS/AS

DATA | **CÓD. REF.** | **ÁREA DE EDUCAÇÃO E FORMAÇÃO**

DESIGNAÇÃO DO CURSO/MÓDULO Apoio Especializado a Vítimas de Cibercrime

FORMADORES/AS

LOCAL | **DURAÇÃO**

A sua opinião é fundamental para a melhoria da qualidade da formação da APAV. Agradecemos a sua sinceridade para nos ajudar a melhorar. Para tal deverá efetuar a sua avaliação de acordo com a seguinte escala:

1 = **Mau** (avaliação entre 0 e 4 valores);
2 = **Insuficiente** (avaliação entre 5 e 9 valores);
3 = **Suficiente** (avaliação entre 10 e 13 valores);
4 = **Bom** (avaliação entre 14 e 17 valores;
5 = **Muito Bom** (avaliação entre 18 e 20 valores).

Nome completo d@ formand@	Assiduidade	Pontualidade	Motivação	Nível de participação	Relacionamento interpessoal	Domínio dos assuntos	Exercícios em grupo ou individuais	Avaliação final

OBSERVAÇÕES

Formador@ | **Coordenação Pedagógica**

PAUTA FINAL

DATA | **CÓD. REF.** | **ÁREA DE EDUCAÇÃO E FORMAÇÃO**

DESIGNAÇÃO DO CURSO/MÓDULO Apoio Especializado a Vítimas de Cibercrime

FORMADORES/AS

LOCAL | **DURAÇÃO**

A sua opinião é fundamental para a melhoria da qualidade da formação da APAV. Agradecemos a sua sinceridade para nos ajudar a melhorar. Para tal deverá efetuar a sua avaliação de acordo com a seguinte escala:

1 = **Mau** (avaliação entre 0 e 4 valores);
2 = **Insuficiente** (avaliação entre 5 e 9 valores);
3 = **Suficiente** (avaliação entre 10 e 13 valores);
4 = **Bom** (avaliação entre 14 e 17 valores;
5 = **Muito Bom** (avaliação entre 18 e 20 valores).

Nome completo d@ formand@	Nota Final

OBSERVAÇÕES

Formador@ | **Coordenação Pedagógica**

PARTE
PART
PARTEA

1

COMPREENDER O CIBERCRIME

UNDERSTANDING CYBERCRIME

SĂ ÎNȚELEGEM CRIMINALITATEA INFORMATICĂ

MOD. 1

APRESENTAÇÃO E ENQUADRAMENTO DO MÓDULO

Tipologias de cibercrime

Procuraremos, neste Módulo, apresentar definições possíveis para o conceito de cibercrime. Para tal, recorremos a diferentes tipologias e categorizações, como meio de demonstrar a complexidade do fenómeno e a miríade de formas ou tipos de atos contemplados.

Estas definições e tipologias são aprofundadas no capítulo 1 - Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*, pelo que, no presente Manual, apresentaremos apenas uma síntese de tais conteúdos, com destaque para os conceitos-chave.

O/A formador(a) deve salientar que o cibercrime pode ser categorizado em:

- **Crimes ciberdependentes**[9] - estão associados a novas formas de criminalidade, cuja ocorrência depende da existência e da utilização das tecnologias de informação e comunicação (TIC), de computadores e de redes de computadores (Leukfeldt, Notté & Malsch, 2020; Maimon & Louderback, 2019). São os chamados cibercrimes *strictu sensu*, uma vez que a sua prática depende de um sistema informático e visam atacar a disponibilidade, o acesso, a integridade, a autenticidade, a confidencialidade, a conservação e a segurança da informação.

- **Crimes possibilitados pela Internet e pelas TIC**[10] - dizem respeito a formas tradicionais de criminalidade nas quais as TIC desempenham um papel importante para a sua prática, incluindo crimes com motivação financeira, mas também formas de violência interpessoal e crimes sexuais. Alguns exemplos são o ciber-*stalking* ou as burlas *online* (Leukfeldt et al., 2020).

Neste último caso, as diferentes formas de cibercriminalidade que são possibilitadas ou ativadas pela internet e pelas TIC podem ainda, por sua vez, ser subdivididas em:

- Cibercrimes financeiramente motivados (e.g., *phishing* [11] e *romance scams*[12]);
- Cibercrimes em relacionamentos interpessoais (e.g., ciber-*stalking*[13]);
- Cibercrimes sexuais (e.g., *revenge porn*[14]).

Conceitos e definições

Comecemos, então, por definir os **crimes ciberdependentes** mais comuns, também conhecidos como cibercriminalidade *strictu sensu*, cuja apresentação conceptual é realizada neste Módulo. No entanto, nos Módulos 5 e seguintes deste Curso de Formação é realizada a desconstrução e aprofundamento da compreensão de muitos destes tipos de cibercrime, sendo ainda apresentadas propostas de intervenção e prevenção específicas.

Hacking ou ***cracking*** são habitualmente definidos como o **acesso não autorizado a sistemas informáticos com intenção criminosa** (Grabosky, 2016 *cit in* Maimon & Louderback, 2019). Associam-se ao *cyber-trespassing*, que implica a passagem não autorizada de barreiras invisíveis do ambiente virtual (Wall, 2001 *cit in* Maimon & Louderback, 2019).

O *hacking* inclui uma série de comportamentos, como o **redesenho de sistemas de *hardware* ou de *software***, para a modificação da sua função inicial, bem como a participação numa subcultura própria (Bachmann, 2010, Holt, 2007, Steinmetz, 2015 *cit in* Maimon & Louderback, 2019).

O ***spamming*** ou ***SPAM***, acrómico da expressão "envio e publicação de publicidade em massa"[15], refere-se ao **envio de**

[9] Traduzido da expressão *cyber-dependent crimes*.

[10] Traduzido da expressão *cyber-enabled crimes*.

[11] Este fenómeno é abordado no Módulo 5 do Curso de Formação.

[12] Este fenómeno é abordado no Módulo 6 do Curso de Formação.

[13] Este fenómeno é abordado no Módulo 10 do Curso de Formação.

[14] Este fenómeno é abordado no Módulo 10 do Curso de Formação.

[15] Traduzido da expressão *Sending and Posting Advertisement in Mass*.

dados e à distribuição massiva de *e-mails* que anunciam produtos, serviços ou esquemas de investimento, que podem ter um carácter fraudulento e inclusivamente conter *malware* ou outro anexo de arquivo executável (Rathi & Pareek, 2013).

Já ***malware*** é o termo utilizado para se referir a uma variedade de *software* de caráter hostil ou intrusivo (e.g., vírus de computador, *worms*[16], *ransomware*[17], *spyware*[18], *adware*[19], *scareware*[20], etc.). Trata-se de ***software* destinado a infiltrar-se, de forma ilícita, em equipamentos**, com o intuito de causar danos, alterações ou furtar informação. O *malware* pode também assumir a forma de código executável, *scripts*, conteúdo ativo e outro *software* (Aycock, 2006 *cit in* Reep-van den Bergh & Junger, 2018).

Um dos esquemas frequentemente utilizados é a publicação de conteúdos com títulos que despertam curiosidade ou apelam a algum tipo de ação "urgente", bem como convites para instalar jogos ou sugestões para visitar perfis novos.

O ***phishing*** traduz-se no envio em massa de mensagens de correio eletrónico - *spamming* -, habitualmente com uma hiperligação (*link*) para uma página da internet, que os/as destinatários/as são persuadidos a aceder, apelando a motivos ou ações urgentes. Por norma, estas mensagens de correio eletrónico solicitam ou apontam para a importância de os/as destinatários/as "atualizarem", "validarem" ou "confirmarem" informações bancárias.

Estas mensagens de correio eletrónico (e as páginas para as quais remetem) são falsas e constituem uma reprodução aproximada da comunicação original efetuada por entidades bancárias, entidades emissoras de crédito ou outras que permitam a realização de pagamentos *online*. Aquando do acesso a tais páginas, é habitualmente solicitada a introdução de informação bancária do/a utilizador/a, sendo possível, a partir desse processo de inserção de dados bancários, a sua captura e posterior utilização indevida.

Por sua vez, o **ataque distribuído de negação de serviço *(DDoS)*** diz respeito a uma tentativa intencional de sobrecarregar um determinado sistema informático, com o propósito de inviabilizar a sua utilização (Overvest & Straathof, 2015).

Já no que toca aos **crimes possibilitados pela internet e pelas TIC**, os mais comuns são as burlas online, o furto de identidade e os crimes relacionados com o abuso e exploração sexual de crianças.

As **burlas *online*** podem assumir várias formas:

- Burlas no comércio eletrónico (*e-commerce*);
- Burlas bancárias;
- Burlas nos relacionamentos íntimos (*romance scams*).

As **burlas no comércio eletrónico** apresentam diferentes graus de complexidade, incluindo esquemas simples em que é prometido ao/à comprador(a) o envio de determinado artigo, mediante transferência bancária prévia, acabando aquele/a por não receber o referido artigo.

Nas **burlas bancárias**, poderemos aludir aos esquemas de *phishing* para acesso a informação bancária da vítima, bem como a burlas com cartão de crédito. Estas referem-se à utilização do cartão de crédito de outra pessoa para uso pessoal, sem o conhecimento do/a proprietário/a do cartão e da entidade emissora (Patel & Singh, 2013).

Quanto às **burlas nos relacionamentos íntimos**, as mesmas ocorrem quando o/a agente procura estabelecer uma relação de confiança e de intimidade, nomeadamente através da internet e das TIC, com um determinado alvo, como prelúdio para obter benefício pessoal, nomeadamente financeiro e patrimonial.

[16] *Worms* são códigos maliciosos que se propagam através de uma rede, com ou sem assistência humana (Kienzle & Elder, 2003).

[17] *Ransomware* é *malware* inserido no sistema por download e cria um arquivo "exe" para execução. O objetivo pode incluir a extorsão da vítima, criptografando as suas informações pessoais (Kansagra, Kumhar & Jha, 2016).

[18] *Spyware* é um programa automático que recolhe informações sobre o/a utilizador/a e sobre os seus hábitos de utilização da internet e transmite essa informação a uma entidade externa, sem o conhecimento e consentimento do/a utilizador/a.

[19] *Adware* é designado como *software* que exibe ou descarrega automaticamente material publicitário (geralmente indesejado) quando o/a utilizador/a está online (Gao, Li, Kong, Bissyandé & Klein, 2019).

[20] *Scareware* é uma forma de *malware* que engana o/a utilizador/a, fazendo-o/a acreditar que o seu computador está infetado quando, na realidade, o sistema está a funcionar (Seifert, Stokes, Lu, Heckerman, Colcernian, Parthasarathy & Santhanam, 2015).

O **furto de identidade** inclui, de forma cumulativa, os seguintes atos:

- Obtenção de informações pessoais e/ou confidenciais sobre outra pessoa, sem o seu conhecimento;
- Posse ou transferência desses dados com a consciência de que serão utilizados para objetivos ilícitos;
- Utilização dos dados inicialmente obtidos para a prática de crimes.

No que toca aos **crimes relacionados com o abuso e exploração sexual de crianças e jovens através da internet**:

- **O abuso sexual *online*** pode ser definido enquanto conceito abrangente, contemplando **qualquer forma de abuso sexual de crianças em contexto *online***. Neste conceito lato incluem-se diferentes manifestações de abuso e exploração, desde o abuso sexual sem contacto, facilitado pelas TIC e pela internet, redes sociais ou outras plataformas, como o assédio e o aliciamento (*grooming online*), até à partilha de conteúdos na *darkweb* (imagem e/ou áudio) de abuso e exploração sexual de crianças, previamente recolhidos em fotografia ou vídeo.

- No âmbito do abuso e exploração de crianças online, destacamos o **abuso sexual de crianças em direto**: prática de atos sexuais com crianças e a sua transmissão em direto, nomeadamente através de serviços de *live streaming*, sendo, deste modo, possível a sua visualização por outras pessoas.

- Destacamos ainda o ***grooming online***, que pode ser definido como um **processo de manipulação** e uma **forma de aliciamento**. Inicia-se geralmente através de uma abordagem não-sexual, nomeadamente através da internet e das TIC, incluindo jogos *online* e redes sociais, de forma a estabelecer uma relação de confiança com a criança e a convencê-la a encontrar-se pessoalmente com outra pessoa, para que esta última possa consumar o abuso sexual. O estabelecimento de relação de confiança com a criança, mediado pela internet e pelas TIC, pode ainda visar a **persuasão da criança à produção e partilha de conteúdo sexual**.

- Na sequência desta forma de abuso e exploração sexual, pode a criança ser sujeita a **ameaças e chantagem de divulgação ou partilha dos conteúdos sexuais auto produzidos**, tendo o/a aliciador/a em vista a obtenção de favores sexuais, dinheiro ou outros benefícios. Este fenómeno designa-se por **extorsão sexual de crianças**.

Na exploração dos conceitos e fenómenos de abuso e exploração sexual de crianças online, é também abordada neste Módulo uma questão terminológica importante:

- as expressões **material de abuso sexual de crianças** e **material de exploração sexual de crianças**[21] procuram substituir, pelo menos em contextos não legais ou jurídicos, o conceito de pornografia infantil (terminologia ainda constante em legislação nacional e internacional).

No âmbito de agressões online nas relações interpessoais, elucidaremos os casos mais comuns, nomeadamente o ciber-*bullying*, ciber-*stalking* e a partilha não-consensual de imagens.

O **ciber-*bullying*** emerge da utilização das TIC e da internet e alguns dos comportamentos que operacionalizam esta forma de agressão *online* poderão incluir: a disseminação de informação negativa/falsa com intenção de difamar a vítima (pelo recurso a telefonemas, mensagens de texto, mensagens de vídeo, *e-mail*, *chat room*, *websites*, redes sociais); importunação da vítima (pelo recurso aos mesmos meios) (APAV, 2011; Jahankhani et al., 2014). Poderemos ainda destacar as situações de ciber-*bullying* com cariz sexual, tais como a partilha *online* de boatos ou mentiras sobre o comportamento sexual da vítima ou a partilha de informação *online*, de forma não consensual, referente à intimidade da vítima.

O ciber-*bullying* distingue-se das modalidades mais convencionais de *bullying*:

- pela possibilidade de ser praticado em qualquer altura do dia, independentemente da necessidade de contacto direto entre vítima e agressor/a;
- pelo potencial de anonimato que garante ao/à agressor/a;
- pelo elevado potencial de "publicidade" e audiência a que está associado;
- pela dificuldade de remoção do conteúdo criado (Stopbullying. Gov, 2017).

[21] Traduzido das expressões *child sexual abuse material* (CSAM) e *child sexual exploitation material* (CSEM).

Já o **ciber-*stalking*** pode ser definido como uma forma de *stalking* que, mantendo o carácter intrusivo, repetitivo e persistente que causa medo à vítima e que caracteriza esta forma de perseguição e assédio persistente, é praticado com recurso à internet e às TIC, com o objetivo de ameaçar e assediar a vítima (Maran & Begotti, 2019).

As práticas de ciber-*stalking* poderão incluir diferentes comportamentos de perseguição: efetuar várias e indesejadas tentativas de contacto com a vítima, via telefone, *e-mail* e redes sociais; instalar *spyware* no computador da vítima; aceder, sem autorização da vítima, ao seu *e-mail* e/ou conta das redes sociais, para monitorizar informação privada e o quotidiano da vida da vítima e/ou para agir em seu nome (Martellozzo & Jane, 2017).

Ainda no âmbito da violência online no contexto de relações interpessoais, poderemos destacar, para além do ciber-*bullying* e do ciber-*stalking*, a **partilha não-consensual de imagens e vídeos**.

As motivações para a divulgação deste conteúdo podem ser:

- **A extorsão ou coação sexual da vítima**.
- A **vingança**, frequentemente designada por *revenge porn*, que implica a divulgação não-consensual de imagens íntimas de um/a companheiro/a, habitualmente após o término do relacionamento, enquanto forma de retaliação.

Fatores de risco e vulnerabilidades comportamentais relacionadas com a cibervitimação

Os **fatores de risco** dizem respeito a características, condições ou variáveis associadas a uma determinada pessoa que aumentam a probabilidade de ocorrência de resultados negativos ou indesejáveis (Reppold et al., 2002 *cit in* Maia et al., 2016).

Deste modo, os **fatores de risco associados à cibervitimação** são características ou condições que podem aumentar a probabilidade ou a vulnerabilidade de uma determinada pessoa face ao cibercrime.

No caso do cibercrime, as características individuais podem não revelar-se tão significativas para a ocorrência de vitimação, uma vez que o cibercrime envolve uma menor (ou até inexistente) interação direta entre vítima e autor/a do crime. Por exemplo, no caso de *malware*, é difícil determinar quem será a vítima em concreto da infeção pelo *software* malicioso, uma vez que qualquer computador pode ser potencialmente infetado, independentemente de características individuais dos/as intervenientes (Ngo & Paternoster, 2011).

A investigação não é particularmente extensa neste domínio, como em muitos outros associados à compreensão do cibercrime. Ainda assim, destacam-se os seguintes:

- **Fatores de risco associados às características sociodemográficas**

Fatores como o **sexo**, a **idade** e o nível de **escolarização** serão abordados neste Módulo. O *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*, no seu capítulo 3 – Parte I, explora os resultados e conclusões de alguns estudos nos quais os fatores de risco de vitimação por cibercrime foram abordados e/ou em que tais variáveis foram medidas, tendo em vista a caracterização de um perfil sociodemográfico das respetivas vitimas de diferentes formas de cibercrime.

- **Fatores de risco associados à utilização da internet e das TIC**

Alguns conceitos, como literacia tecnológica e efeito de desinibição, são explorados neste Módulo, enquanto fatores que podem aumentar ou reduzir a vulnerabilidade à cibervitimação:

- A **literacia tecnológica** diz respeito à consciência, conhecimento e competências que permitem a uma determinada pessoa a movimentação em ambientes digitais e a utilização eficaz da internet, das TIC e dos equipamentos e ferramentas associadas (Holt & Bossler, 2013 *cit in* Maimon & Louderback, 2019). A literacia tecnológica parece reduzir o risco de cibervitimação (Holt & Bossler, 2008).

- O **efeito de desinibição** refere-se ao processo ou efeito de desinibição que resulta do modo como a distância física a que a interação ou comunicação através das TIC ocorre, da ausência de contacto direto no processo de comunicação, do maior anonimato e da perceção de maior controlo sobre o processo de interação. O efeito de desinibição poderá contribuir para a exposição a situações e/ou para a adoção de comportamentos *online* que aumentam a vulnerabilidade à cibervitimação (Agustina, 2015).

Além destes conceitos, neste Módulo exploramos ainda outros fatores de risco de cibervitimação, como os **níveis de utilização** da internet e das TIC e o **tipo de atividades realizadas** na internet ou através da internet e das TIC.

Como referido para os fatores de risco sociodemográficos, o *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*, no seu capítulo 3 – Parte I, aborda também, em maior profundidade, cada um destes **fatores de risco de cibervitimação associados ao comportamento dos/as utilizadores/as da internet e das TIC**.

Posto isto, para um entendimento mais aprofundado relativamente aos conteúdos abordados neste Módulo, sugerimos, para além da leitura atenta dos conceitos-chave supra e do suporte audiovisual proposto (*PowerPoint*), a consulta do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*, nomeadamente dos seus capítulos 1 e 3 – Parte I.

Formação para TAV -

Apoio Especializado a Vítimas de Cibercrime

Apoio Especializado a Vítimas de Cibercrime

PARTE I - COMPREENDER O CIBERCRIME

Módulo 1 - Compreender os fenómenos do cibercrime

1. Compreender os fenómenos do cibercrime

Cibercrime - Definição

Quando falamos de cibercrime podemos estar a falar de duas realidades distintas:

- **1º** Crimes ciberdependentes / crimes informáticos / Cibercrime em sentido estrito
- **2º** Crimes possibilitados pela Internet e pelas TIC / Cibercrime em sentido lato

1. Compreender os fenómenos do cibercrime

Tipologias de cibercrime

Crimes ciberdependentes - ocorrência depende da existência e da utilização das tecnologias de informação e comunicação (TIC), de computadores e de redes de computadores. A sua prática depende de um sistema informático e visam atacar a disponibilidade, o acesso, a integridade, a autenticidade, a confidencialidade, a conservação e a segurança da informação.

Crimes possibilitados pela Internet e pelas TIC – formas de criminalidade tradicionais nas quais as TIC possibilitam, facilitam e auxiliam a sua prática.

Cibercrime - Definição

1º - Crime informático:

Dentro do cibercrime só algum é crime informático - crimes em que as tecnologias de informação, processamento e comunicação são meio e fim para o crime acontecer e em que esse crime atinge sempre uma ou mais das condições de operacionalidade da segurança da informação: a **confidencialidade**, a **integridade**, a **disponibilidade** e o **não repúdio da informação**. Estas práticas são punidas pela Lei do Cibercrime.

Cibercrime - Definição

2º - Cibercrime em sentido lato:

Tipos de crimes comuns cujo o uso de tecnologias de informação facilita o seu cometimento ou alcance. Ex: Injuriar alguém através das redes sociais. Neste tipo de situações ao contrário da primeira nunca está em causa o comprometimento da **confidencialidade, integridade, disponibilidade** ou **não repúdio** de sistema informático.

1. Compreender os fenómenos do cibercrime

Conceitos e definições

Crimes ciberdependentes:

- Hacking ou cracking; acesso não autorizado a sistemas informáticos com intenção criminosa
- Spamming ou SPAM;
- Malware (e.g., vírus de computador, worms, ransomware, spyware, adware, scareware, etc.)
- Phishing
- DDoS

Crimes possibilitados pelas TIC:

- Vários tipos de burlas online (Burlas no comércio eletrónico (e-commerce); Burlas bancárias; Burlas nos relacionamentos íntimos (romance scams).
- Furto de identidade

1. Compreender os fenómenos do cibercrime

Conceitos e definições

Crimes possibilitados pelas TIC (continuação)

- Crimes relacionados com o abuso e exploração sexual de menores através da internet
  - Qualquer forma de abuso online
  - Grooming online
  - Ameaça e chantagem de divulgação ou partilha de conteúdos sexuais autoproduzidos
    - ❑Material de abuso e exploração sexual de crianças → diferenças e relação com conceito pornografia infantil?
    - ❑Conteúdos auto-gerados

- Crimes relacionados com agressões online
  - Ciber-bullying
  - Ciber-stalking
  - Divulgação não consensual de imagens e vídeos
    - ❑E.g. revenge porn

1. Compreender os fenómenos do cibercrime

Fatores de risco e vulnerabilidades comportamentais relacionadas com a cibervitimação

- Características individuais não parecem ser tão significativas para a ocorrência de vitimação - cibercrime envolve uma menor (ou até inexistente) interação direta entre vítima e autor/a do crime
- Fatores de risco associados às características sociodemográficas - o **sexo**, a **idade** e o nível de **escolarização**
- Fatores de risco associados à utilização da Internet e das TIC
  - Literacia tecnológica
  - Efeito de desinibição
  - Níveis de utilização da internet e das TIC
  - Tipo de actividades realizadas

Ver mais em *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*, nomeadamente dos seus capítulos 1 e 3 – Parte I

PLANO DE SESSÃO Nº 1

1. Identificação da Ação

Designação Curso de Formação Apoio Especializado a Vítimas de Cibercrime

Módulos/ temas Introdução e Contextualização
Compreender os fenómenos do cibercrime

Data da Sessão **Horário** **Duração da Sessão** 35 minutos

Formadores/as

2. Objetivos Específicos

No final da sessão, os/as formandos/as deverão ser capazes de:

- Reconhecer corretamente os/as outros/as formandos/as e o/a formador[a];
- Reconhecer de forma correta os objetivos e os conteúdos da intervenção formativa;
- Distinguir, de forma correta, crimes ciberdependentes e crimes facilitados/possibilitados pela internet e pelas TIC;
- Reconhecer, de modo correto, diferentes conceitos e definições associadas ao cibercrime, nomeadamente tipos de cibercrime;
- Identificar, corretamente, os fatores de risco de cibervitimação relacionados com as características sociodemográficas;
- Assinalar, sem erros, as vulnerabilidades comportamentais relacionadas com a cibervitimação.

3. Estrutura da Sessão

	Conteúdos Programáticos	Metodologia	Recursos Pedagógicos/ Didáticos	Avaliação | Exercícios	Tempo (minutos)
Introdução	Introdução e contextualização: Apresentação e levantamento de expectativas Apresentação do/a formador[a] Apresentação dos/as formandos/as Apresentação dos objetivos e conteúdos programáticos da intervenção formativa	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
Desenvolvimento	Tipologias de cibercrime: • Crimes ciberdependentes *vs* crimes possibilitados pela internet e pelas TIC	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
	Conceitos e definições: • *Hacking*, *spamming*, *malware*, *phishing* e *DDoS* [ataque distribuído de negação de serviço] • Burlas *online*: burlas no comércio eletrónico [*e-commerce*], burlas bancárias e burlas nos relacionamentos íntimos [*romance scams*] • Furto de identidade online • Abuso e exploração sexual de crianças *online*: abuso sexual de crianças em direto, aliciamento [*grooming online*] e conteúdos de abuso sexual de crianças • Ciber-*bullying* • Ciber-*stalking* e partilha não-consensual de imagens	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	10
	Fatores de risco e vulnerabilidades comportamentais relacionadas com a cibervitimação: • Fatores de risco associados às características sociodemográficas • Fatores de risco associados à utilização da internet e das TIC	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	10
Conclusão	Síntese conclusiva e esclarecimento de questões	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5

OBSERVAÇÕES

Destionatários/as:
Técnicos/as de Apoio à Vítima [TAV]

Data: / / **Formador[a]:**

INSTRUÇÕES E INFORMAÇÕES ESSENCIAIS PARA O/A FORMADOR(A)

CORRESPONDÊNCIA DE CONTEÚDOS

Plano de Sessão	*Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*	
	PARTE	CAPÍTULO
Introdução e contextualização	Sem correspondência Utilizar Programa do Curso de Formação (ver Apêndices)	
Tipologias de cibercrime	Parte I – Compreender	Capítulo 1 – 1.2.
Conceitos e definições	Parte I – Compreender	Capítulo 1 – 1.3.
Fatores de risco e vulnerabilidades comportamentais relacionadas com a cibervitimação	Parte I – Compreender	Capítulo 3 – 3.2.
Síntese conclusiva e esclarecimento de questões	Sem correspondência	

MOD. 2

MOD. 2

APRESENTAÇÃO E ENQUADRAMENTO DO MÓDULO

Neste Módulo, o/a formador(a) apresentará, em linha com o capítulo 2 - Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*, o enquadramento legal do cibercrime.

Para o efeito, e num registo marcadamente expositivo, será explorado o cibercrime na **Lei Internacional e na *acquis* da União Europeia**, nomeadamente:

- A Convenção sobre o Cibercrime do Conselho da Europa, de 23 de Novembro de 2001[22];
- A Convenção sobre Proteção de Crianças contra Exploração e Abuso Sexual, conhecida como Convenção de Lanzarote[23];
- A Estratégia da União Europeia para a Cibersegurança[24];
- A resolução do Parlamento Europeu sobre a luta contra o crime informático, no dia 3 de outubro de 2017[25].

Neste Módulo são também apresentadas, em traços gerais, algumas Diretivas da União Europeia:

- Diretiva 2011/93/UE – Relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho[26];
- Diretiva 2013/40/UE – Relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho[27];
- Diretiva (UE) 2019/713 – Relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho[28];
- Diretiva 2000/31/CE – Relativa ao comércio eletrónico[29];
- Regulamento 679/2016 – Implementou o regulamento geral de proteção de dados pessoais (RGPD)[30].

Este Módulo apresenta ainda algumas das iniciativas encetadas a nível Europeu e internacionalmente, tendo em vista o combate ao cibercrime, de entre as quais a Associação INHOPE[31]

O Módulo prossegue com a apresentação do **enquadramento jurídico do cibercrime a nível nacional**.

O caso de Portugal

É apresentada a Lei n.º 109/2009 de 15 de setembro, a Lei do Cibercrime (LC), que transpõe para o ordenamento português a Decisão-Quadro 2005/222/JAI (que veio a ser substituída pela Diretiva 2013/40/EU) e adapta o direito interno à Convenção de Budapeste (CCCE).

No ordenamento jurídico Português, para além da LC, é ainda possível encontrar previsões de crimes cujo cometimento se pode dar com recurso a meios eletrónicos, ainda que não exclusivamente, também chamados de crimes facilitados por sistema informático (*cyber-enabled offenses*). Nesse sentido, o presente Módulo explorará ainda o Código Penal Português e disposições em matéria de Cibercrime.

[22] Council of Europe Convention on Cybercrime, Budapest, 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

[23] Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, https://rm.coe.int/protection-of-children-against-sexual-exploitation-and-sexual-abuse/1680794e97.

[24] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; Cybersecurity Strategy of the European Union: An Open, Safe And Secure Cyberspace, Brussels, 7.2.2013, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN.

[25] European Parliament Resolution of 3 October 2017 on the Fight Against Cybercrime (2017/2068 (INI)), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0366&from=EN.

[26] Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32011L0093&from=PT.

[27] Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0040&from=DE.

[28] Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L0713&from=PT.

[29] Diretiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico»), https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000L0031&from=EN.

[30] Regulamento 679/2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504.

[31] Veja-se https://www.inhope.org/EN.

Este Módulo termina, por fim, com a apresentação e reflexão relativamente aos **principais desafios na investigação da cibercriminalidade e na aplicação da Lei**:

- Os principais desafios na investigação e na aplicação da Lei, em matéria de cibercrime, são transversais aos estados europeus, sendo particularmente sentidos pelos órgãos de polícia criminal e pelo Ministério Público:

    - A rápida movimentação de conteúdos *online*, o anonimato que algumas plataformas oferecem e as técnicas de encriptação[32] dificultam ou até impossibilitam o rastreamento da origem dos conteúdos ilícitos *online*;
    - A dificuldade em harmonização de mecanismos de bloqueio de conteúdos ilícitos possibilita o reaparecimento dos mesmos conteúdos em domínios situados em outros países:
    - A complexidade das ferramentas e instrumentos capazes de processar grandes quantidades de dados em pouco tempo;
    - Os apertados prazos de preservação de prova pelos prestadores de serviços de internet - ISP (*Internet Service Providers*);
    - A cooperação com países terceiros que alojem conteúdo ilegal;
    - O dilema entre privacidade e a previsão de métodos ocultos de investigação.

[32] Veja-se, por exemplo, os Módulos 8, 9 e 10 deste Curso de Formação, em que a encriptação ponta a ponta é explorada.

Apoio Especializado a Vítimas de Cibercrime

PARTE I - COMPREENDER O CIBERCRIME

Módulo 2 - Enquadramento Legal

2. Enquadramento Legal do Cibercrime

- ❑Legislação Internacional e da União Europeia;
- ❑A Lei do Cibercrime;
- ❑Cibercrime no Código Penal Português.
- ❑Legislação avulsa

Saber mais em capítulo 2 - Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*, o enquadramento legal do cibercrime.

2. Enquadramento Legal do Cibercrime

Lei Internacional e da União Europeia

A Convenção sobre o Cibercrime do Conselho da Europa, de 23 de Novembro de 2001;
A Convenção sobre Proteção de Crianças contra Exploração e Abuso Sexual, conhecida como Convenção de Lanzarote;

Diretiva 2011/93/UE – Relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho;
Diretiva 2013/40/UE – Relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho;
Diretiva (UE) 2019/713 – Relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho;
Diretiva 2000/31/CE – Relativa ao comércio eletrónico.;
Regulamento 679/2016 – Implementou o regulamento geral de proteção de dados pessoais (RGPD) .

2. Enquadramento Legal do Cibercrime

Lei Internacional e da União Europeia

O instrumento internacional de maior relevo na área do cibercrime é a **Convenção sobre o Cibercrime do Conselho da Europa**, de **23 de Novembro de 2001**, destinada a «proteger a sociedade do cibercrime, através da adoção de legislação adequada e da melhoria da cooperação internacional», de modo a «tornar mais eficazes as investigações e os processos penais respeitantes às infrações penais relacionados com sistemas e dados informáticos, bem como permitir a recolha de prova, em formato eletrónico».

2. Enquadramento Legal do Cibercrime

Lei Internacional e da União Europeia

Com este fim, a Convenção impõe aos Estados signatários que adequem o seu Direito Penal substantivo e adjetivo interno às especificidades destes crimes, tendo como objetivo a harmonização de legislações, incluindo instrumentos processuais e de produção de prova adequados e simplificar a cooperação internacional de modo a facilitar e agilizar a deteção, a investigação, a recolha de prova e a perseguição.

2. Enquadramento Legal do Cibercrime

A Lei do Cibercrime

No que à lei nacional diz respeito, o quadro de referência resulta, em primeiro lugar, da **Lei nº 109/2009 de 15 de setembro**, a Lei do Cibercrime (LC), que transpõe para o nosso ordenamento a Decisão - Quadro 2005/222/JAI e adapta o direito interno à CCCE.

Os tipos legais de crime previstos na LC encontram-se nos arts.º 3º a 8º desta lei.

2. Enquadramento Legal do Cibercrime

A Lei do Cibercrime

Artigo 3.º - *Falsidade informática*

Pratica o crime de Falsidade Informática quem «introduzir, modificar, apagar ou suprimir dados informáticos ou interferir, por qualquer modo, no tratamento informático de dados» até aqui o crime de falsidade Informática aparenta ser idêntico ao de dano informático – art. 4º (LC). No entanto para a falsidade informática ainda se exigem algumas condutas típicas, no **caso a produção de dado ou documento não genuíno com intenção de provocar engano nas relações jurídicas**.

Exemplo de caso de Falsidade Informática: *Josefina cria, no seu computador, documento com a aparência de comprovativo de transferência bancária e envia-o a vendedor de telemóveis, para demonstrar que pagou o preço combinado.*

2. Enquadramento Legal do Cibercrime

A Lei do Cibercrime

Artigo 4.º - *Dano relativo a programas ou outros dados informáticos*

É punido quem sem autorização legal ou sem autorização, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afetar a capacidade de uso.

Em causa estão apenas as atuações ilegítimas. O que exclui do tipo testes de segurança a determinado sistema, desde que autorizados pelo dono desse sistema.

O bem jurídico protegido neste tipo de crimes é a integridade e fiabilidade dos dados e o bom funcionamento dos programas informáticos. Ao contrário do crime de Dano (art. 212 CP) não se pretende apenas proteger a propriedade, o dano informático, além da integridade patrimonial dos dados informáticos como propriedade do lesado, tutela ainda a integridade funcional desses dados no que respeita à disponibilidade e utilização eficaz dos dados informáticos.

Exemplo: O computador do João é infetado por vírus que codifica/encripta todos os dados nele guardados, impedindo-o de a eles aceder

2. Enquadramento Legal do Cibercrime

A Lei do Cibercrime

Artigo 5.º *Sabotagem informática*

A distinção entre o dano informático e a sabotagem informática não é fácil, contrapondo os dois tipos de crime podemos dizer que no dano informático punem-se atos relacionados com dados informáticos, quanto à sabotagem o que está em causa é a perturbação do funcionamento de sistemas informáticos ou da comunicação de dados.

O tipo legal também pune a difusão de vírus e de outros programas maliciosos, destinados a provocar sabotagem informática artg. 5º Nº 2 da LC, nestes casos estamos perante uma antecipação da tutela penal para a fase dos atos preparatórios do crime de sabotagem.

Exemplo: A montagem de *botnets* destinados a permitir o controlo malévolo de redes, por via do estabelecimento de uma rede de computadores «zombie» cujo uso posterior provocará falhas técnicas conhecidas por DoS e DDoS.

2. Enquadramento Legal do Cibercrime

A Lei do Cibercrime

Artigo 6.º - *Acesso ilegítimo*

O crime de acesso ilegítimo pretende tutelar a segurança do sistema informático, máxime, a sua confidencialidade. Trata-se de um crime de perigo abstrato destinado a funcionar como barreira para evitar a prática de outros ilícitos de maior gravidade.

Assim sendo para que a conduta típica se verifique basta estar consumado o acesso não autorizado.

Exemplo: Comete o crime de acesso ilegítimo alguém que não estando autorizado para tal acede a grupo privado da rede social Whatsapp criado por grupos e alunos do 7º ano de escolaridade, e aí começa a partilhar links de venda de dinheiro falso.

2. Enquadramento Legal do Cibercrime

A Lei do Cibercrime

Artigo 7.º - *Interceção ilegítima*

Constitui crime a interceção de qualquer forma de transferência eletrónica de dados, por telefone, fax, correio eletrónico ou ficheiro. Para a consumação do crime não se exige a efetiva obtenção de informações, basta proceder de forma a captar essas informações.

O termo "não-públicas" delimita a natureza da comunicação e não a natureza dos dados transmitidos. Os dados comunicados poderão constituir informação disponível ao público, mas as partes desejarem comunicar confidencialmente. Ou os dados poderão ser mantidos em sigilo, para fins comerciais, até que o serviço seja remunerado. Desta forma, o termo "não-públicas" não exclui as redes públicas.

Exemplo: Pedro instala um *software* no telefone de Maria que lhe permite ter acesso a todas as suas comunicações telefónicas.

2. Enquadramento Legal do Cibercrime

A Lei do Cibercrime

Artigo 8.º - *Reprodução ilegítima de programa protegido*

Embora o bem protegido seja um direito privado, entendeu-se que existe um interesse essencial do Estado em proteger os criadores intelectuais e se justificava o interesse do Estado em agir criminalmente contra a violação de direitos desta natureza.

Assim, este crime não depende de queixa, sendo um crime público.

2. Enquadramento Legal do Cibercrime

Cibercrime no Código Penal Português

O Código Penal Português e disposições em matéria de Cibercrime

Quando se fala no conceito **estrito** de Cibercriminalidade, também encontramos incriminações no próprio Código Penal que prevê tipos de crime que atacam disponibilidade, o acesso, a integridade, a autenticidade, a confidencialidade, a conservação e a segurança da informação, são estes:

- ***Artigo 193.º - Devassa por meio de informática***
- ***Artigo 194.º - Violação de correspondência ou de telecomunicações***
- ***Artigo 221.º - Burla informática e nas comunicações***

2. Enquadramento Legal do Cibercrime

Cibercrime no Código Penal Português

Além desta Cibercriminalidade, outros crimes comuns podem ser praticados e os seus efeitos potenciados fazendo uso das tecnologias. São crimes cujo tipo não contempla como elemento constitutivo do crime a utilização do meio tecnológico.

Exemplos (lista não exaustiva):

Crimes contra a honra cometidos através da inclusão das expressões ou acusações injuriosas em páginas online, blogs ou difundindo-as por correio eletrónico. A única relevância do meio eletrónico respeita à utilização desse meio para a divulgação da expressão injuriosa ou difamatória e à superior potencialidade de dano para o bem jurídico protegido (cfr. Art. 183º/1 a) CP: ofensa praticada através de meios que facilitem a sua divulgação; e n.º3 CP: meio de comunicação social, v.g. redes sociais).

2. Enquadramento Legal do Cibercrime

Cibercrime no Código Penal Português

❖ **Gravação e fotografias ilícitas** (art. 199º CP) - O direito à imagem abrange dois direitos autónomos: o direito a não ser fotografado e o direito a não ver divulgada a fotografia. O visado pode autorizar ou consentir que lhe seja tirada uma fotografia e pode não autorizar que essa fotografia seja usada ou divulgada. Contra vontade do visado não pode ser fotografado nem ser usada uma sua fotografia. É suscetível de preencher o tipo legal de crime de Gravações e fotografias ilícitas, do art. 199.º nº 2, do Cód. Penal, a arguida que, contra a vontade do fotografado, utiliza uma fotografia deste, ainda que licitamente obtida e a publicita no Facebook. (Ac. TRP de 5-06-2015)

2. Enquadramento Legal do Cibercrime

Cibercrime no Código Penal Português

❖ **Devassa da vida privada** (arts. 192º e 197 CP)

❖ **Discriminação e incitamento ao ódio e à violência** (art. 240.º CP)

❖ **Extorsão** (art. 223.º CP). Está, normalmente, associado às práticas de ransomware. Com efeito, normalmente associado ao bloqueio de um determinado sistema, pela encriptação dos dados nele armazenados ou dos respetivos ficheiros operativos, vem comunicação exigindo, em troca do seu desbloqueio, elevada quantia (normalmente, a ser paga em Bitcoins).

2. Enquadramento Legal do Cibercrime

Cibercrime no Código Penal Português

❖ **Pornografia infantil** (176.º CP)

❖ **Aliciamento de Menores para fins sexuais** (176.º - A CP) Neste caso o agente (que tem de ter 18 ou mais anos) que, por intermédio do uso das tecnologias de informação e de comunicação, alicie menor (até aos 18 anos) para encontro que vise a prática de atos sexuais de relevo (simples ou qualificados) ou para a utilização do menor em espetáculo pornográfico, fotografia, filme ou gravação pornográfica, é punido com pena de prisão de 1 mês até 1 ano. No entanto, as penas previstas para este crime são agravadas de um terço, nos seus limites mínimo e máximo, se o crime for cometido conjuntamente por duas ou mais pessoas.

2. Enquadramento Legal do Cibercrime

Cibercrime no Código Penal Português

❖ **Violência Doméstica** (alínea b) do n.º 2 do art. 152.º do CP) – preceito foi introduzido pela Lei n.º 44/2018 protege-se particularmente os dados pessoais (designadamente imagem ou som, o que inclui vídeos, filmes, fotos) sobre a intimidade (nomeadamente a sexualidade) e a reserva da vida privada de qualquer vítima (dados privados que são sensíveis), quando são difundidos (divulgados/espalhados) através da Internet ou de outros meios de difusão pública generalizada (como, por exemplo, através das redes sociais), sem o consentimento da vítima.

❖ **Perseguição** (154-A.º CP)

2. Enquadramento Legal do Cibercrime

Cibercrime no Código Penal Português

É também o combate do *cyberstalking* particularmente na área da violência doméstica (entendido este como as condutas que consistem sobretudo, como "enviar mensagens de correio eletrónico, mensagens de texto e mensagens instantâneas ofensivas ou ameaçadoras, publicar comentários ofensivos sobre a vítima na internet, partilhar fotografias ou vídeos íntimos da mesma através da internet", que são vividas como "mais intrusivas para as vítimas" e que lhes "provocam mais efeitos psicológicos adversos") que se visou censurar de forma acrescida com esta agravação/qualificação especial.

2. Enquadramento Legal do Cibercrime

Legislação avulsa

❖ **Decreto Lei n.º 7/2004, de 07 de Janeiro** transpôs a Diretiva 2000/31/CE

Regra geral: princípio da irresponsabilidade dos prestadores intermediários de serviços em rede face à eventual ilicitude das mensagens/informação que disponibilizam. **EXCEPÇÕES**:

- Obrigação de informação/comunicação imediata ao MP sempre que tenham conhecimento que a disponibilização de conteúdos por meio dos serviços que prestam, ou o acesso aos mesmos, possa constituir crime;
- Bloqueio ou remoção de conteúdo de natureza **manifestamente** ilegal nos casos assim que tomar conhecimento dos mesmos;
- Obrigação de remoção, num prazo de 48 horas, de conteúdos de abuso ou exploração sexual de menores.

2. Enquadramento Legal do Cibercrime

Legislação avulsa

❖ **Lei n.º 32/2008, de 17 de Julho,** conhecida como a lei da retenção de dados

- prevê o **prazo de um ano para armazenamento dos dados de tráfego e localização** no setor das comunicações eletrónicas.

❖ **Lei n.º 46/2018, de 13 de Agosto** que estabelece o **Regime Jurídico da Segurança do Ciberespaço**

- Equipa de Resposta a Incidentes de Segurança Informática Nacional – CERT.PT

❖ **Resolução do Conselho de Ministros n.º 92/2019** que aprovou a primeira **Estratégia Nacional de Segurança do Ciberespaço**

Encaminhamento das Situações de Cibercrime
Autoridades

Algumas notas práticas sobre Encaminhamento de situações de Cibercrime:

Todos os Crimes previstos na Lei 109/09 Lei do Cibercrime, a saber:

- Falsidade Informática (art. 3º)
- Dano relativo a programas ou outros dados informáticos (art.4º)
- Sabotagem Informática (art.5º)
- Acesso Ilegítimo (art. 6º)
- Intercepção Ilegítima (art. 7º)
- Reprodução ilegítima de programa protegido (art. 8º)

Devem ser denunciados ou encaminhados para a **Polícia Judiciária (PJ)**

Encaminhamento das Situações de Cibercrime
Autoridades

Todos os Crimes contra a autodeterminação sexual, nomeadamente:

- Abuso sexual de Crianças (art. 171º Nº3)
- Pornografia de Menores (art.176º)
- Aliciamento de menores para fins sexuais (art. 176º - A)
- Todos do Código Penal

Sempre que praticados com recurso às tecnologias de informação, de processamento e comunicação.

Devem ser denunciados ou encaminhados para a **Polícia Judiciária (PJ)**

Encaminhamento das Situações de Cibercrime
Autoridades

Não devem ser encaminhados para a Polícia Judiciária os crimes que não sendo da competência reservada da PJ (os que vimos anteriormente), o agente se socorra tão somente de mecanismos ou instrumentos informáticos acessíveis à generalidade das pessoas, em que a sua ação não se rodeie de especiais conhecimentos de informática ou em que o recurso à tecnologia informática se resuma à simples e comum utilização de uma plataforma de comunicação – como sucede por exemplo, nos crimes de **ameaças, injúrias, burlas simples praticados com o uso da internet**.

PLANO DE SESSÃO Nº 2

1. Identificação da Ação

Designação Curso de Formação Apoio Especializado a Vítimas de Cibercrime

Módulos/ temas Enquadramento legal do cibercrime

Data da Sessão **Horário** **Duração da Sessão** 45 minutos

Formadores/as

2. Objetivos Específicos

No final da sessão, os/as formandos/as deverão ser capazes de:

- Reconhecer, de forma correta, o enquadramento legal do cibercrime, à luz da lei internacional;
- Reconhecer, de forma correta, o enquadramento jurídico do cibercrime a nível nacional;
- Identificar adequadamente, pelo menos, metade dos desafios abordados relativamente à investigação do cibercrime e à aplicação da Lei.

3. Estrutura da Sessão

	Conteúdos Programáticos	Metodologia	Recursos Pedagógicos/ Didáticos	Avaliação | Exercícios	Tempo (minutos)
Introdução	O cibercrime na Lei Internacional e na *acquis* da União Europeia	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
Desenvolvimento	O cibercrime na Lei Internacional e na *acquis* da União Europeia: • Convenção sobre o Cibercrime do Conselho da Europa • Convenção sobre Proteção de Crianças contra Exploração e Abuso Sexual • Estratégia da União Europeia para a Cibersegurança • Resolução do Parlamento Europeu sobre a luta contra o crime informático • Diretiva 2011/93/UE – Relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil • Diretiva 2013/40/UE – Relativa a ataques contra os sistemas de informação • Diretiva (UE) 2019/713 – Relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário • Diretiva 2000/31/CE – Relativa ao comércio eletrónico • Regulamento 679/2016 – regulamento geral de proteção de dados pessoais (RGPD)	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	15
	O enquadramento jurídico do cibercrime a nível nacional	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	20
Conclusão	Principais desafios na investigação e na aplicação da Lei	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	3
	Síntese conclusiva e esclarecimento de questões	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	2

OBSERVAÇÕES

Destionatários/as:
Técnicos/as de Apoio à Vítima (TAV)

Data: / / **Formador(a):**

INSTRUÇÕES E INFORMAÇÕES ESSENCIAIS PARA O/A FORMADOR(A)

CORRESPONDÊNCIA DE CONTEÚDOS

Plano de Sessão	*Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*	
	PARTE	CAPÍTULO
O cibercrime na Lei Internacional e na *acquis* da União Europeia	Parte I – Compreender	Capítulo 2 – 2.1. e 2.2.
O enquadramento jurídico do cibercrime a nível nacional	Parte I – Compreender	Capítulo 2 – 2.3.
Principais desafios na investigação e na aplicação da Lei	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Síntese conclusiva e esclarecimento de questões	Sem correspondência	

MOD. 3

MOD. 3

APRESENTAÇÃO E ENQUADRAMENTO DO MÓDULO

Prevalência do cibercrime

Apesar do crescente conhecimento relativamente aos diversos fenómenos de cibercriminalidade, **ainda é insipiente a informação acerca da real dimensão da vitimação pelos diferentes tipos de cibercrimes**, desconhecendo-se, portanto, quais as proporções reais da sua prevalência na população (Reep-van den Bergh & Junger, 2018).

Não sendo conteúdo programático do presente Curso, sugerimos, ainda assim, a consulta do tema *As cifras negras associadas ao cibercrime no Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas* (capítulo 1 – Parte I), em que são explorados os motivos e dificuldades associadas ao conhecimento da real dimensão dos diferentes fenómenos de cibercriminalidade.

Em seguida, são sumariamente apresentados alguns dos dados estatísticos explorados e detalhados no suporte audiovisual (*PowerPoint*) deste Módulo e que procuram fornecer uma leitura possível da dimensão de diferentes tipos de cibercrimes em Portugal:

- No contexto português, o *phishing* e a infeção por *malware* (incluindo *ransomware*) foram os tipos de incidentes mais registados, em 2019, pelo CERT.PT e pela RNCSIRT (Equipa de Resposta a Incidentes de Segurança Informática Nacional e Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática, respetivamente)[33];
- Os crimes mais frequentes registados pela Linha Internet Segura, em 2019, foram a burla, o furto de identidade e o *phishing* (APAV, 2019);
- Entre 2009 e 2018, segundo a Direção-Geral da Política de Justiça[34] , verificou-se um aumento constante da percentagem, entre todos os crimes registados no país, de crimes informáticos, crime de devassa por meio informático e de crime de burla informática/comunicações;
- Alguns aspetos sociodemográficos relevantes relativos aos incidentes de cibersegurança registados em Portugal, em 2019, são os seguintes:
  - Género - Sem diferenças relevantes entre géneros;
  - Idade - Indivíduos com idades compreendidas entre os 25 e os 34 anos tendem a reconhecer mais ter sido alvo de incidentes de cibersegurança (35%) do que indivíduos com idades entre os 65 e os 74 anos (18%);
  - Educação - Em geral, indivíduos entre os 25 e os 64 anos, com uma educação formal superior, tendem a identificar ter sido vítima de mais incidentes de cibersegurança (40%) do que aqueles que, na mesma faixa etária, têm uma educação formal inferior (17%);

Sugere-se, ainda assim, a consulta do capítulo 1 – Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*, que remete, nos diversos campos de DESTAQUE | ESTATÍSTICAS EM FOCO, para um conjunto de estudos, inquéritos e relatórios dedicados à prevalência ou incidência destes fenómenos.

Impacto nas vítimas particulares

Neste ponto do Módulo, é sobretudo explorado o conteúdo do capítulo 4 - Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*. Para aprofundar o conhecimento relativamente às consequências de diferentes tipos de cibercrime, deverá ser consultado o referido capítulo.

Em todo o caso, nos Módulos 5 a 10 deste Curso de Formação, nos quais são trabalhadas *estratégias para superar a vitimação e seus impactos*, as consequências das experiências de cibervitimação serão novamente exploradas, desta feita em função do tipo de cibercrime.

Como referido no Manual ROAR, considera-se, genericamente, que as consequências experienciadas pelas vítimas de cibercrime não se distinguem, pelo menos de forma significativa, das consequências experienciadas por vítimas de crimes *tradicionais*.

[33] Relatório *Cibersegurança em Portugal, Riscos e Conflitos*, Junho 2020, Observatório de Cibersegurança.

[34] Consultar informação detalhada em https://estatisticas.justica.gov.pt/sites/siej/pt-pt

Importa destacar que o impacto do cibercrime na vítima é muito variável, sendo agravado ou atenuado em função de um conjunto de:

- Variáveis individuais, nomeadamente características sociodemográficas e competências e comportamentos de utilização da internet;
- Variáveis associadas ao cibercrime propriamente dito, como o tipo de cibercrime, a duração da cibervitimação, o nível de publicitação da cibervitimação e a (eventual) relação com o/a autor/a do cibercrime;
- Variáveis associadas à rede de suporte formal e informal.

Consequências na saúde física, psicológica e emocional

Como ponto de partida, importará salientar que, grosso modo, as consequências emocionais e psicológicas do cibercrime são normalmente subestimadas, sendo o cibercrime entendido como uma categoria da criminalidade com baixo impacto (Button, Lewis, & Tapley, 2014a cit in Jansen & Leukfeldt, 2018).

Algumas das consequências e reações frequentemente apontadas são (Leukfeldt et al., 2019; Cross et al., 2016; De Kimpe et al., 2020; Jansen & Leukfeldt, 2018; Cross et al., 2016):

- perda de confiança;
- culpa;
- vergonha;
- raiva e frustração;
- ansiedade e re-experienciação dos incidentes;
- medo e tristeza;
- angústia;
- sentimentos de insegurança, impotência e desilusão;
- redução nos níveis de autoconfiança e nos níveis de confiança relativamente a outras pessoas;
- isolamento social;
- depressão e ideação suicida;
- declínio no rendimento/produtividade;
- sintomas físicos, como perturbações de sono, cansaço ou fraqueza excessiva, problemas de apetite, cefaleias e náuseas.

Impacto financeiro

As **consequências financeiras do cibercrime** podem incluir (Leukfeldt et al., 2019):

- custos suportados pelas vítimas como consequência do ato de que foram alvo, incluindo custos com despesas acrescidas de saúde, custos com deslocações, telecomunicações e/ou com a necessidade de substituição de equipamentos;
- consumo de tempo e perda de horas de trabalho e eventual perda subsequente de rendimentos;
- custos adicionais associados à necessidade de alterar as rotinas e estilo de vida, incluindo a adoção de medidas de segurança e a implementação de mecanismos mais eficazes de cibersegurança, a mudança de casa e/ou a alteração de local de trabalho/estudo, entre outros.

Receio do cibercrime e perceções sobre cibersegurança

No que diz ainda respeito ao impacto do cibercrime nas vítimas particulares, o *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas* explora também o receio do cibercrime e o risco percebido de cibervitimação. Esta temática será também abordada neste Módulo. Deve, por isso, o/a formador(a) consultar o capítulo 4 – Parte I do Manual e atender aos seguintes conceitos-chave:

- O **medo do crime** pode ser definido enquanto reação emocional ao crime e/ou a símbolos a ele associados.
- O **risco percebido** constitui um julgamento cognitivo no qual as pessoas avaliam o seu próprio risco ou probabilidade de vitimação, em função das suas experiências pessoais, do contexto/ambiente social e das circunstâncias, o que, por sua vez, se reflete no medo relativamente ao crime (Ferraro, 1995, Rontree, 1998 *cit in* Yucedal, 2010).

Assim:

A **perceção de risco de cibervitimação**, como resultado de processos cognitivos que contemplam a análise das experiências pessoais de cibervitimação (caso existam) e das pistas de vitimação/crime que advêm do estilo de vida *online*, poderá derivar em **respostas comportamentais orientadas para uma maior proteção**, nas quais se inclui a implementação de medidas/mecanismos de cibersegurança e a alteração dos comportamentos de utilização da Internet e das TIC (Yucedal, 2010).

Alguns estudos dedicam-se à medição do receio face ao cibercrime[35].

[35] Veja-se o caso do Special *Eurobarometer 423: Cyber security*, disponível em https://www.europeandataportal.eu/data/datasets/s2019_82_2_423_eng?locale=en.

Apoio Especializado a Vítimas de Cibercrime

PARTE I - COMPREENDER O CIBERCRIME

Módulo 3 – Vitimologia e Impacto do Cibercrime

3. Vitimologia e impacto do Cibercrime

Prevalência do Cibercrime em PT

- Phishing, malware e ransomware
- Burla
- Furto de Identidade
- Crime de devassa por meio informático

Dados de 2019; CERT.PT, RNCSIRT, Linha Internet Segura

3. Vitimologia e impacto do Cibercrime

Impacto nas vítimas singulares

De modo geral, as consequências experienciadas pelas vítimas de cibercrime não se distinguem de forma significativa das consequências experienciadas por vítimas de crimes *tradicionais*.

Impacto do cibercrime pode variar em função de:

- Variáveis individuais: características sociodemográficas, competências e comportamentos de utilização da Internet;
- Variáveis associadas ao cibercrime propriamente dito, como o tipo de cibercrime, a duração da cibervitimação, o nível de publicitação da cibervitimação e a (eventual) relação com o/a autor/a do cibercrime;
- Variáveis associadas à rede de suporte formal e informal.

Para aprofundar conhecimentos sobre as necessidades das vítimas de cibercrime, consultar capítulo 4 - Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*.

3. Vitimologia e impacto do Cibercrime

Impacto nas vítimas singulares

- **Consequência na saúde física, psicológica e emocional:** perda de confiança; culpa; vergonha; raiva e frustração; ansiedade e re-experienciação dos incidentes; medo e tristeza; angústia; sentimentos de insegurança, impotência e desilusão; redução nos níveis de autoconfiança e de confiança nas outras pessoas; isolamento social; depressão e ideação suicida; declínio no rendimento/produtividade; sintomas físicos, como perturbações de sono, cansaço ou fraqueza excessiva, problemas de apetite, cefaleias e náuseas.
- **Impacto financeiro:** custos suportados pelas vítimas como consequência do ato criminoso, consumo de tempo e perda de horas de trabalho e eventual perda de rendimentos subsequente, custos adicionais associados à necessidade de alterar as rotinas e estilo de vida.
- **Receio do cibercrime e perceções sobre cibersegurança:** pode originar respostas comportamentais orientadas para uma maior proteção. Por outro lado, **experiências pessoais de vitimação** podem aumentar o risco percebido de (re)vitimação e, consequentemente, o medo face ao crime.

PLANO DE SESSÃO Nº 3

1. Identificação da Ação

Designação	Curso de Formação Apoio Especializado a Vítimas de Cibercrime		
Módulos/ temas	Vitimologia e impacto do cibercrime		
Data da Sessão	**Horário**	**Duração da Sessão**	20 minutos
Formadores/as			

2. Objetivos Específicos

No final da sessão, os/as formandos/as deverão ser capazes de:

- Reconhecer, corretamente, o impacto do cibercrime em diferentes domínios da vida das vítimas de cibercrime;
- Identificar adequadamente as consequências do cibercrime nas perceções sobre cibersegurança e no receio relativamente ao cibercrime.

3. Estrutura da Sessão

	Conteúdos Programáticos	Metodologia	Recursos Pedagógicos/ Didáticos	Avaliação | Exercícios	Tempo (minutos)
Introdução	Prevalência do cibercrime	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
Desenvolvimento	Impacto nas vítimas particulares: • Consequências na saúde física, psicológica e emocional • Impacto financeiro • Receio do cibercrime e perceções sobre cibersegurança	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	13
Conclusão	Síntese conclusiva e esclarecimento de questões	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	2

OBSERVAÇÕES

Destionatários/as:
Técnicos/as de Apoio à Vítima (TAV)

Data: / / **Formador(a):**

INSTRUÇÕES E INFORMAÇÕES ESSENCIAIS PARA O/A FORMADOR(A)

CORRESPONDÊNCIA DE CONTEÚDOS

Plano de Sessão	*Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*	
	PARTE	CAPÍTULO
Prevalência do cibercrime	Parte I – Compreender	Capítulo 2 – 2.1. e 2.2. Ver campos DESTAQUE | ESTATÍSTICAS EM FOCO
Impacto nas vítimas particulares	Parte I – Compreender	Capítulo 2 – 2.3.
Síntese conclusiva e esclarecimento de questões	Sem correspondência	

PARTE
PART
PARTEA

2

APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME

SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MOD. 4

MOD. 4

PARTE 2 - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME
MÓDULO 4 - ASPETOS CENTRAIS NO APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME

APRESENTAÇÃO E ENQUADRAMENTO DO MÓDULO

Estruturar o apoio especializado a vítimas de cibercrime

Este Módulo propõe uma primeira abordagem deste Curso de Formação ao apoio e atendimento a vítimas de cibercrime. Tem, por isso, como objetivo a apresentação de um conjunto de orientações centrais e domínios-chave a considerar na intervenção junto de vítimas de cibercrime, independentemente do(s) tipo(s) de cibercrime dos quais a vítima tenha sido alvo. Nos Módulos seguintes, procuraremos, por seu turno, aprofundar o conhecimento dos/as formandos/as relativamente a estratégias de prevenção e de intervenção específicas para cada tipo de cibercrime (dos crimes ciberdependentes aos crimes possibilitados ou facilitados pela internet e pelas TIC), tendo em vista a superação da experiência de cibervitimação e seus impactos por parte da vítima apoiada.

Assim, este Módulo abordará as seguintes temáticas:

- As competências - pessoais e técnicas - essenciais a um(a) profissional de apoio – Técnico/a de Apoio à Vítima (TAV), nomeadamente a empatia e as competências de comunicação;
- O apoio emocional;
- A recolha de informação;
- A avaliação do risco de revitimação e o desenvolvimento de planos de segurança;
- A identificação das necessidades de apoio;
- A intervenção em crise.

Refira-se, no entanto, que, no presente enquadramento deste Módulo, é apresentada uma síntese dos conteúdos dos capítulos 1, 2 e 3 – Parte II do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*. Para o aprofundamento do conhecimento relativamente às temáticas abordadas, sugerimos a leitura atenta dos capítulos citados.

Empatia, técnicas de comunicação e apoio emocional

O apoio a vítimas de cibercrime exige ao/à profissional de apoio (TAV) um conjunto de competências essenciais e imprescindíveis:

- **Empatia**: diz respeito à capacidade para se colocar na perspetiva da vítima de crime, de ser sensível à situação por ela vivenciada e de intuir e compreender os sentimentos e significados que atribui ao crime; é uma competência fundamental para o estabelecimento de uma relação de apoio e de confiança.

- **Outras competências pessoais são**:

  - Vocação;
  - Capacidade de autogestão emocional e de estabelecimento de relações interpessoais positivas;
  - Gestão positiva de *stress* e capacidade de resolução pacífica de problemas interpessoais e/ou interinstitucionais;
  - Respeito pela dignidade humana e tolerância e respeito pelas diferenças e diversidade cultural.

Já no que diz respeito às **competências técnicas**, além da necessidade de formação específica para a intervenção junto de vítimas de cibercrime e da literacia tecnológica[36], são fundamentais as **competências comunicacionais** no contacto e apoio a vítimas de cibercrime, nomeadamente, saber ouvir/escutar, mas também ter a capacidade para transmitir informação e mensagens claras e inteligíveis, no âmbito do processo de apoio (Pessoa et al., 2011).

A comunicação e a empatia são fundamentais ao longo de toda a intervenção e processo de apoio junto da vítima de cibercrime e, concretamente, no apoio emocional.

Sinteticamente, o **apoio emocional** a prestar junto de uma vítima de cibercrime é suportado pelas dimensões e atitudes do/a profissional de apoio (TAV), entre as quais:

[36] Veja-se desconstrução deste conceito no Módulo 1 deste Curso de Formação.

- **Comunicação empática** e escuta ativa;
- **Linguagem não-verbal**;
- **Valorização da denúncia e respeito pelos ritmos** de partilha da vítima;
- Promoção da **expressão emocional da vítima e validação** da experiência de cibervitimação.

Recolha de informação

A **recolha de informação** é um processo central para o apoio e intervenção.

À partida, o primeiro contacto com a vítima será dedicado a este processo de recolha e reunião de informação, sendo certo tratarem-se de etapas circulares e constantes, que alimentam regularmente qualquer processo de apoio e de intervenção com a vítima.

Sinteticamente, o processo de recolha de informação procura responder a 3 domínios:

1. História pessoal e de pré-vitimação;
2. Experiência de cibervitimação;
3. História pós-vitimação.

A recolha de informação junto da vítima de cibercrime permitirá:

- Obter informação sobre a situação de cibercrime experienciada;
- Aferir os impactos e consequências;
- Avaliar o risco e definir medidas de segurança;
- Identificar as necessidades da vítima;
- Acionar os recursos e serviços mais adequados para responder a tais necessidades.

Avaliação do risco e desenvolvimento de planos de segurança

A avaliação do grau de risco procura aferir a **probabilidade de ocorrência de novas situações de cibervitimação contra a vítima**.

O processo de avaliação resulta da:

- **Informação partilhada pela vítima** relativamente à sua experiência de cibervitimação;
- Utilização dessa mesma informação para **identificar (de forma mais ou menos estruturada) os fatores de risco de revitimação** presentes em cada caso (e que merecerão atenção particular, no que respeita à intervenção e planificação dos comportamentos de proteção pessoal *online* e de medidas de cibersegurança, tendo em vista a prevenção da revitimação);
- **Experiência e julgamento do/a profissional** de apoio (TAV).

De forma genérica, poderemos dizer que a avaliação do risco de revitimação se deverá centrar em 3 **domínios de risco**:

1. Características de vítima;
2. Características, especificidades e dinâmicas do cibercrime;
3. Características do/a autor(a) do cibercrime.

Neste Módulo, exploraremos algumas **variáveis e fatores de risco associados a cada um dos domínios de risco** supra e que poderão ser considerados pelo/a profissional (TAV) na sua intervenção. O *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*, no capítulo 3 - Parte I e no capítulo 3 – Parte II, detalha os fatores de risco que poderão ser considerados.

Este Módulo visa ainda sensibilizar os/as profissionais/formandos/as para a necessidade de os mecanismos e estratégias de avaliação do risco junto da vítima serem sempre acompanhados pelo desenvolvimento de **planos de segurança**:

- Estratégias de prevenção da revitimação, acordadas e definidas entre vítima e profissional (TAV), no qual se incluem medidas e comportamentos de proteção face a novas situações de crime, bem como estratégias e instruções práticas para lidar e atuar, perante a eventual re-ocorrência de cibervitimação.

Identificação das necessidades de apoio

No seguimento da recolha de informação efetuada junto da vítima e considerando os resultados da avaliação do risco de revitimação, é importante que o/a profissional (TAV) identifique as **necessidades de apoio da vítima de cibercrime**.

De uma forma geral, poderá afirmar-se que as necessidades das vítimas de cibercrime são semelhantes às necessidades das vítimas de outras formas mais *tradicionais* de criminalidade (Leukfeldt et al., 2020).

Assim, podem ser identificadas (Cross et al., 2016; Leukfeldt et al., 2020):

- **Necessidades emocionais e psicológicas**, com destaque para o reconhecimento enquanto vítima de crime, para a valorização e validação da experiência de cibervitimação, para o acesso a apoio e para a recuperação/reparação das consequências do crime sofrido;
- **Necessidades de informação e necessidades relacionadas com o processo-crime**, nomeadamente sobre os serviços de apoio existentes, sobre os direitos, sobre a denúncia e o estado do processo-crime;
- **Necessidades práticas e financeiras**, como a remoção online de conteúdos, a articulação com entidades e a compensação financeira.

No capítulo 4 – Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas* é disponibilizada informação detalhada, para uma melhor compreensão das necessidades identificadas nas (e pelas) vítimas de cibercrime.

No caso concreto das **necessidades relacionadas com os direitos e com o processo-crime**, é fundamental assegurar que, em qualquer fase do processo-crime, a vítima tenha acesso a informação sobre os seus direitos, para que deles possa usufruir:

- O/A profissional de apoio (TAV) deve estar familiarizado com o enquadramento legal do cibercrime, abordado no Módulo 2 deste Curso de Formação;
- O/A profissional de apoio (TAV) também deverá conhecer as etapas do processo-crime e os direitos das vítimas de crime legalmente previstos, no sentido de ajudar a compreendê-los e a exercê-los, de entre os quais:
  - Direito à informação;
  - Direito a receber comprovativo de denúncia;
  - Direito a tradução;
  - Direito a acesso a serviços de apoio à vítima;
  - Direito a ser ouvida;
  - Direitos em caso de não acusação do/a arguido/a;
  - Direito a serviços de mediação;
  - Direito a informação ou proteção jurídica;
  - Direito a compensação por participação no processo e a reembolso de despesas;
  - Direito à restituição de bens;
  - Direito a indemnização;
  - Direito a proteção;
  - Direitos das vítimas com necessidades especiais de proteção;
  - Direito a ser esquecido[37].

Estes direitos são apresentados em maior detalhe no *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*, capítulo 3 – Parte II. Veja-se também o texto integral da Diretiva 2012/29/EU[38].

[37] Este direito, ao contrário dos anteriores, não integra a Diretiva 2012/29/EU. Consta no artigo 17.º do Regulamento Geral de Proteção de Dados Pessoais.

[38] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32012L0029.

Também no capítulo 3 – Parte II do mesmo Manual são propostas algumas estratégias que podem auxiliar a identificação das necessidades de apoio na prática e no decurso do processo de intervenção.

Na sequência da identificação das necessidades de apoio, informação e proteção, poderá ser necessário o **encaminhamento (interno ou externo)** da vítima de cibercrime para serviços/respostas especializadas, nomeadamente a nível jurídico, psicológico e social ou de outra natureza.

Neste Módulo, é ainda identificado e definido o fenómeno de **vitimação secundária**: segunda forma de vitimação, provocada pela resposta inadequada providenciada pelos sistemas e estruturas e pela sua discrepância face aos interesses, necessidades e direitos das vítimas.

Intervenção em crise

A experiência de cibervitimação poderá constituir um acontecimento gerador de uma **situação de crise** para a vítima, sendo observável, por exemplo, através de reações psicológicas intensas na vítima.

A intervenção em crise (ou primeiros socorros psicológicos) é uma **atuação intensiva, focalizada e limitada no tempo**, orientando-se para a resolução de problemas atuais e respondendo a objetivos específicos. Trata-se de uma resposta de apoio inicial, de cuidados práticos, não invasivos, em situações de crise ou emergência.

Este Módulo explora os objetivos e etapas da intervenção em crise, podendo ser esta intervenção ser sintetizada em aspetos-chave como:

- A avaliação da segurança da vítima e dos recursos (pessoais e sociais) para responder adequadamente a uma situação;
- A operacionalização de intervenção orientada para a recuperação e reorganização da vítima.

No *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*, capítulo 3 – Parte II, as etapas da intervenção em crise são abordadas em detalhe.

Apoio Especializado a Vítimas de Cibercrime

PARTE II - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME

Módulo 4 - Aspetos centrais no apoio especializado a vítimas de cibercrime

Estruturar o apoio especializado a vítimas de cibercrime

Este Módulo abordará as seguintes temáticas:

a. As competências - pessoais e técnicas - essenciais a um(a) profissional de apoio – Técnico(a) de Apoio à Vítima (TAV), nomeadamente a empatia e as competências de comunicação;
b. A recolha de informação;
c. A avaliação do risco de revitimação;
d. A identificação das necessidades de apoio;
e. A intervenção em crise.

Estruturar o apoio especializado a vítimas de cibercrime

a. As competências pessoais essenciais ao TAV:

- Empatia
- Vocação;
- Capacidade de autogestão emocional e de estabelecimento de relações interpessoais positivas;
- Gestão positiva de *stress* e capacidade de resolução pacífica de problemas interpessoais e/ou interinstitucionais;
- Respeito pela dignidade humana e tolerância e respeito pelas diferenças e diversidade cultural.

Competências técnicas essenciais ao TAV: formação específica para a intervenção , literacia tecnológica , competências comunicacionais no contacto e apoio a vítimas de cibercrime

Estruturar o apoio especializado a vítimas de cibercrime

a. Competências do TAV

O apoio emocional a prestar junto de uma vítima é suportado pelas dimensões e atitudes do TAV, e.g.:

- **Comunicação empática** e escuta ativa;
- **Linguagem não-verbal**;
- **Valorização da denúncia** e **respeito pelos ritmos** de partilha da vítima;
- Promoção da **expressão emocional da vítima e validação** da experiência de cibervitimação.

Estruturar o apoio especializado a vítimas de cibercrime

b. A recolha de informação;

- História pessoal e de pré-vitimação;
- Experiência de cibervitimação;
- História pós-vitimação.

Que permitirá:

- Obter informação sobre a situação de cibercrime experienciada;
- Aferir os impactos e consequências;
- Avaliar o risco e definir medidas de segurança;
- Identificar as necessidades da vítima;
- Acionar os recursos e serviços mais adequados para responder a tais necessidades.

Estruturar o apoio especializado a vítimas de cibercrime

c. Avaliação do risco e desenvolvimento de planos de segurança

Procurar aferir a **probabilidade de ocorrência de novas situações de cibervitimação contra a vítima**.

Através de:

- **Informação partilhada pela vítima** relativamente à sua experiência de cibervitimação;
- Utilização dessa mesma informação para **identificar (de forma mais ou menos estruturada) os fatores de risco de revitimação** presentes em cada caso (e que merecerão atenção particular, no que respeita à intervenção e planificação dos comportamentos de proteção pessoal *online* e de medidas de cibersegurança, tendo em vista a prevenção da revitimação);
- **Experiência e julgamento do(a) profissional** de apoio (TAV).

c. Avaliação do risco e desenvolvimento de planos de segurança

Avaliação de risco deve ser acompanhada pelo desenvolvimento de **planos de segurança**:

- Estratégias de prevenção da revitimação, acordadas e definidas entre vítima e o(a)profissional (TAV), no qual se incluem medidas e comportamentos de proteção face a novas situações de crime, bem como estratégias e instruções práticas para lidar e atuar, perante eventual re-ocorrência de cibervitimação.

d. Identificação das necessidades de apoio

- **Necessidades emocionais e psicológicas**, com destaque para o reconhecimento enquanto vítima de crime, para a valorização e validação da experiência de cibervitimação, para o acesso a apoio e para a recuperação/reparação das consequências do crime sofrido;
- **Necessidades de informação e necessidades relacionadas com o processo-crime**, nomeadamente sobre os serviços de apoio existentes, sobre os direitos, sobre a denúncia e o estado do processo-crime;
- **Necessidades práticas e financeiras**, como a remoção *online* de conteúdos, a articulação com entidades e a compensação financeira.

d. Identificação das necessidades de apoio

No caso das **necessidades relacionadas com o processo-crime**, é fundamental assegurar que, em qualquer fase do processo-crime, a vítima tenha acesso a informação sobre os seus direitos.

Para tal:

- ✓ O(a) TAV deve estar familiarizado com o enquadramento legal do cibercrime, abordado no Módulo 2 deste Curso de Formação;
- ✓ O(a) TAV também deverá conhecer as etapas do processo-crime e os direitos das vítimas de crime legalmente previstos, no sentido de ajudar a compreendê-los e a exercê-los, nomeadamente: Direito à informação; Direito a receber comprovativo de denúncia; Direito a tradução; Direito a acesso a serviços de apoio à vítima; Direito a ser ouvida; Direitos em caso de não acusação do/a arguido/a; Direito a serviços de mediação; Direito a informação ou proteção jurídica; Direito a compensação por participação no processo e a reembolso de despesas; Direito à restituição de bens; Direito a indemnização; Direito a proteção; Direitos das vítimas com necessidades especiais de proteção; Direito a ser esquecido.

d. Identificação das necessidades de apoio

Especial atenção ao fenómeno de **vitimação secundária**, provocada pela resposta inadequada providenciada pelos sistemas e estruturas e pela sua discrepância face aos interesses, necessidades e direitos das vítimas.

Deverá ainda, se identificada tal necessidade, ser feito um **encaminhamento (interno ou externo)** da vítima de cibercrime para serviços/respostas especializadas, nomeadamente a nível jurídico, psicológico e social ou de outra natureza.

e. Intervenção em crise

A experiência de cibervitimação poderá gerar reações psicológicas intensas na vítima.

Intervenção em crise = ou primeiros socorros psicológicos = é uma **atuação intensiva, focalizada e limitada no tempo**, orientando-se para a resolução de problemas atuais e respondendo a objetivos específicos. Trata-se de uma resposta de apoio inicial, de cuidados práticos, não invasivos, em situações de crise ou emergência.

Etapas:

- A avaliação da segurança da vítima e dos recursos (pessoais e sociais) para responder adequadamente a uma situação;
- A operacionalização de intervenção orientada para a recuperação e reorganização da vítima.

PLANO DE SESSÃO Nº 4

1. Identificação da Ação

Designação Curso de Formação Apoio Especializado a Vítimas de Cibercrime

Módulos/ temas Aspetos centrais no apoio especializado a vítimas de cibercrime

Data da Sessão **Horário** **Duração da Sessão** 80 minutos

Formadores/as

2. Objetivos Específicos

No final da sessão, os/as formandos/as deverão ser capazes de:

- Enumerar, corretamente, todos os aspetos e etapas centrais na estruturação do apoio especializado a vítimas de cibercrime, nos quais se devem incluir:
  - Empatia e técnicas de comunicação;
  - Apoio emocional;
  - Recolha de informação;
  - Avaliação do rico e desenvolvimento de planos de segurança;
  - Identificação das necessidades de apoio;
  - Intervenção em crise.

3. Estrutura da Sessão

	Conteúdos Programáticos	Metodologia	Recursos Pedagógicos/ Didáticos	Avaliação | Exercícios	Tempo (minutos)
Introdução	Estruturar o apoio especializado a vítimas de cibercrime	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
Desenvolvimento	Estruturar o apoio especializado a vítimas de cibercrime: • Empatia, técnicas de comunicação e apoio emocional • Recolha de informação • Avaliação do risco e desenvolvimento de planos de segurança • Identificação das necessidades de apoio • Intervenção em crise	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	60
Conclusão	Exercício n.º 1	Ativa	Quadro/*flipchart*, marcador e Regras do Exercício n.º 1	Observação	10
	Síntese conclusiva e esclarecimento de questões	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5

OBSERVAÇÕES

Destionatários/as:
Técnicos/as de Apoio à Vítima (TAV)

Data: / / **Formador(a):**

INSTRUÇÕES E INFORMAÇÕES ESSENCIAIS PARA O/A FORMADOR(A)

CORRESPONDÊNCIA DE CONTEÚDOS

Plano de Sessão	*Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*	
	PARTE	CAPÍTULO
Estruturar o apoio especializado a vítimas de cibercrime		
Empatia, técnicas de comunicação e apoio emocional	Parte II - Proceder	Capítulo 1 – 1.1. e 1.2. Capítulo 2 – 2.1. e 2.2.
Recolha de informação	Parte II - Proceder	Capítulo 2 – 2.3.
Avaliação do risco e desenvolvimento de planos de segurança	Parte I - Compreender Parte II - Proceder	Capítulo 3 – 3.2. Capítulo 3 – 3.2.
Identificação das necessidades de apoio	Parte I – Compreender Parte II - Proceder	Capítulo 4 – 4.2. Capítulo 3 – 3.3.
Intervenção em crise	Parte II - Proceder	Capítulo 3 – 3.1.
Exercício n.º 1	Sem correspondência Ver Regras do Exercício n.º 1	
Síntese conclusiva e esclarecimento de questões	Sem correspondência	

REGRAS DO EXERCÍCIO N.º 1

Módulo/Tema	Aspetos centrais no apoio especializado a vítimas de cibercrime	CÓD. REF.	ÁREA DE EDUCAÇÃO E FORMAÇÃO

Objetivos

Este exercício tem como objetivo consolidar os aspetos centrais a considerar no apoio especializado a vítimas de cibercrime, procurando, em concreto, promover a reflexão dos/as formandos/as relativamente a um conjunto de práticas e atitudes do/a profissional de apoio (TAV) que poderão beneficiar ou prejudicar a intervenção e apoio a prestar junto de uma vítima.

Execução

Partindo do Quadro 3 (disponível no ponto 2.1. do capitulo 2 – Parte II do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*), o/a formador(a) deverá escrever no quadro/*flipchart* disponível na sala de formação um conjunto de atitudes e práticas que podem ter lugar no âmbito do contacto com vítimas de cibercrime.

Estas práticas e atitudes poderão ou não ser positivas para o sucesso da intervenção a realizar.

Podendo outras práticas listadas no referido Quadro ser selecionadas, algumas das que sugerimos pra reflexão do grupo são as seguintes:

a) *Minimizar o problema ou o impacto da experiência de cibervitimação relatada pela vítima.*
b) *Oferecer soluções para o problema apresentado pela vítima ou para as necessidades identificadas.*
c) *Prometer à vítima a resolução do problema apresentado ou a resposta às necessidades identificadas.*
d) *Incentivar a vítima a partilhar a sua experiência de cibervitimação, bem como os seus pensamentos, sentimentos e reações.*
e) *Partilhar com a vítima experiências pessoais ou situações próximas em matéria de cibervitimação.*

Depois de disponibilizadas no quadro/*flipchart*, deve o/a formador(a) perguntar junto do grupo, para cada afirmação, em que medida cada uma das atitudes/práticas pode ou não ser adequada, promovendo a reflexão dos/as formandos/as.

Da discussão promovida sobre cada afirmação, deve resultar a seguinte solução:

a) Prática/atitude não adequada.
É importante o reconhecimento e validação da vítima e da sua experiência enquanto forma de crime e de vitimação. Como tal, é importante explicar à vítima que, no contexto do apoio, o seu relato e a sua experiência importam e que o/a profissional/TAV acredita no que está a ser dito. Importa explicar ainda que existem outras pessoas a viver situações semelhantes à sua, quebrando a noção de "caso único", e enquadrar eventuais reações, emoções, sentimentos e pensamentos no âmbito da experiência de cibervitimação vivida.

b) Prática/atitude não adequada.
Respeitar as decisões e a autonomia da vítima é fundamental. Muito embora a exploração de possíveis soluções possa ser efetuada em conjunto entre vítima e profissional/TAV, este/a não deve substituir a vítima no processo decisório ou oferecer soluções à vítima, sem a envolver no processo de decisão. Deverá, ao invés, apresentar e explorar as vantagens e desvantagens de cada possível decisão, para que a vítima possa tomar decisões informadas.

c) Prática/atitude não adequada.
Oferecer à vítima uma falsa sensação de segurança e/ou promover expectativas irrealistas quanto ao seu papel e/ou quanto à resolução da situação e/ou das necessidades pode ser contraproducente, podendo levar a uma quebra na relação de confiança entre vítima profissional/TAV e/ou à frustração da vítima pelo insucesso/insatisfação de tais necessidades.

d) Prática/atitude adequada.
Todavia, importa garantir que os *timings* e vontades da vítima são respeitados, não forçando a partilha de informação em momentos em que a vítima não se encontra preparada ou em condições para o fazer.

e) Prática/atitude não adequada.
A partilha por parte do/a profissional de informação/experiências pessoais, como meio de aproximação à vítima, pode ser contraproducente, podendo levar à quebra da relação profissional que se pretende entre vítima e profissional/TAV. A desconstrução de crenças de vulnerabilidade única deve, ao invés, ser realizada através da apresentação de informação factual, como é o caso da prevalência associada ao cibercrime sofrido pela vítima ou do número de vítimas apoiadas que tenham sido alvo de situações de vitimação semelhantes.

Notas

Consultar capítulo 2 (ponto 2.1.) da Parte II do Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas.

MOD. 5

MOD. 5

PARTE 2 - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME
MÓDULO 5 - APOIO ESPECIALIZADO A VÍTIMAS DE CRIMES CIBERDEPENDENTES

APRESENTAÇÃO E ENQUADRAMENTO DO MÓDULO

Os conceitos centrais associados aos crimes ciberdependentes são exploradas no Módulo 1 deste Curso de Formação. No entanto, o presente Módulo, no seguimento do Módulo anterior em que foram exploradas as orientações centrais e aspetos-chave na intervenção junto de vítimas de cibercrime, visa aprofundar o conhecimento dos/as formandos/as quanto à intervenção concreta a realizar no caso de crimes ciberdependentes. Para o efeito, serão exploradas as estratégias de intervenção e de prevenção da revitimação, bem como os modi operandi e natureza dos crimes em apreço.

Modi operandi e natureza do crime

Os **crimes ciberdependentes** podem ser definidos como qualquer crime que **só pode ser cometido por meio de computadores, redes de computadores ou outras formas de TIC**. Como já foi referido, são crimes que sem a internet não poderiam ser praticados.

Assim, incluem atividades como a criação e disseminação de ***malware*** e ***hacking*** para roubar dados pessoais ou industriais confidenciais e/ou **ataques de negação de serviço** (DDoS) para causar danos financeiros e/ou reputacionais.

As vítimas deste tipo de crime podem ser distintas:

- pessoas coletivas (como empresas e organizações);
- pessoas singulares (i.e., qualquer cidadão/ã).

No cometimento deste tipo de criminalidade são usados vários tipos de ataque, dos quais destacaremos o ***ransomware***, o **furto de informação confidencial** (*data compromise*) e os **ataques de negação de serviço** (DDoS).

O ***ransomware*** é um tipo de *software* malicioso, ou *malware*, desenhado para **negar o acesso a um sistema ou dados de computador até que um resgate seja pago**. O *ransomware*, geralmente, é disseminado por *e-mails* de *phishing* ou ao visitar um *website* infetado.

A forma mais comum de cometer ataques de *ransomware* continua a decorrer pela **Engenharia Social** e pelo **envio de *e-mails* de *phishing***, muitas vezes já direcionados para aquela pessoa ou empresa (***spear phishing***), como forma de ter acesso ao computador/rede de computadores daquela entidade e, assim, proceder à encriptação dos dados.

Outro vetor de ataque utilizado é a **exploração de vulnerabilidades nos protocolos de acesso remoto dos computadores**: nestes casos, o/a atacante tenta explorar vulnerabilidades do próprio software para, dessa forma, ter acesso remoto ao computador.

O *ransomware*, bem como os tipos de ataques que iremos analisar, constituem crime, encontrando a sua previsão e punição na Lei do Cibercrime. Assim, pratica o **crime de dano informático** aquele que infeta o computador de outrem, de forma a não permitir o acesso a certos ficheiros pela vítima, localizados no seu computador pessoal.

O **furto de informação pessoal *online*** é também outro tipo de cibercriminalidade comum. Prende-se sobretudo com a obtenção ilegal de informação financeira, nomeadamente credenciais de cartão de crédito, dados bancários ou carteiras de cripto-moedas. O acesso a esta informação tem muito valor, uma vez que permite a venda dessa informação ou a sua utilização para furto do património das vítimas.

Para além da informação bancária, existem ainda outros tipos de informação pessoal das vítimas com elevado valor. Neste sentido, o acesso a informação pessoal das vítimas permite ao/à atacante a criação de *e-mails* de *phishing* especificamente direcionados para aquelas vítimas (*spear phishing*). A vantagem deste ataque é ser mais preciso e, por isso, mais credível para a vítima, uma vez que no *e-mail* constarão dados pessoais da mesma. Alguns exemplos de crimes que utilizam este *modus operandi* são a **burla *online*** e o **acesso Ilegítimo**.

O furto de informação pessoal *online* pode ser caracterizado por **três fases**:

1) **Investigação:** O/a cibercriminoso/a procura as vulnerabilidades do alvo; estas vulnerabilidades podem ser as próprias pessoas (singulares), as infraestruturas de rede ou os dispositivos eletrónicos;

2) **Ataque:** Depois de identificadas as fragilidades, o/a cibercriminoso/a inicia o seu ataque:

   - contra os próprios dispositivos eletrónicos, pela exploração das suas vulnerabilidades, de modo a obter acesso aos mesmos.
   - através da engenharia social, em que as pessoas são a própria vulnerabilidade, sendo enganadas pelos/as atacantes e levadas a revelar informação que permitirá o acesso aos dispositivos eletrónicos ou à rede.

3) **Exfiltração dos dados:** Uma vez conseguido o acesso aos dispositivos eletrónicos, o/a cibercriminoso/a pode procurar os dados relevantes que pretende retirar. Se esses mesmos dispositivos se encontrarem ligados em rede, o/a cibercriminoso/a pode infiltrar-se na rede e atacar outros dispositivos.

Os **ataques de negação de serviço** (DDoS) estão desenhados para **degradar serviços *online***, como ***websites*, *e-mail*** e **serviços DNS** (*Domain Name System*). Para atingir estes objetivos, o/a cibercriminoso/a pode usar diversas **formas de ataque**:

- Usar vários computadores, para direcionar grandes volumes de tráfego aos serviços *online*, de forma a colocá-los temporariamente indisponíveis;
- Desvio dos serviços *online* de uma empresa (ex.: *website*), numa tentativa de redirecionar o/as utilizadores/as para um outro *website* que não o dessa empresa.

Pelas suas características, este tipo de prática criminosa afeta sobretudo as pessoas coletivas, sendo que as pessoas singulares acabam por ser vítimas indiretas, uma vez que o acesso a determinados serviços fica impossibilitado, em virtude do ataque.

Os ataques de negação de serviço são também previstos e punidos pela Lei do Cibercrime, através da disposição relativa à **sabotagem informática**.

Estratégias de prevenção

No que diz respeito a **ataques de *ransomware* e de furto de informação confidencial**, são aplicáveis as seguintes estratégias de prevenção:

- Ativação de filtros de spam fortes, para impedir que *e-mails* de *phishing* entrem nas caixas de correio eletrónico. Também é recomendada a utilização de mecanismos de autenticação de *e-mail* com *Sender Policy Framework* (SPF), relatórios e conformidade de autenticação de mensagens de domínio (DMARC) e *Domain Keys Identified Mail* (DKIM), para impedir a falsificação de *e-mails*;
- Utilização de mecanismos de análise de ficheiros executáveis de *e-mails* enviados ou recebidos, prevenindo que os/as utilizadores/as os recebam;
- Configuração da *firewall* de forma a bloquear o acesso a IPs (*Internet Protocol*) que já se sabem que são uma ameaça;
- Configuração de antivírus e programas de anti-*malware* em todos os computadores e configuração dos mesmos para realizarem análises regulares;
- Implementação de ações de formação e sensibilização sobre os riscos *online*, principalmente junto de funcionários/as e quadros de empresas, pois estes podem ser alvos deste tipo de ataques;
- Aplicação do "Princípio dos Privilégios Mínimos" nas empresas/organizações: a nenhum (a) utilizador(a) deve ser atribuído acesso administrativo superior ao estritamente necessário para o exercício da sua atividade.

No que concerne aos **ataques de negação de serviço** (DDoS), uma vez que ocorrem sobretudo em serviços *online* prestados por pessoas coletivas, estas devem garantir que os seus serviços online se mantêm ativos, mesmo perante o ataque. Para o efeito, podem ser implementados os seguintes mecanismos de prevenção:

- Determinar *a priori* qual o nível de serviço adequado e que deverá ser mantido em permanência para os/as

seus utilizadores/as;
- Definir quais as funcionalidades do serviço *online* que a entidade/pessoa coletiva pode prescindir em caso de ataque;
- Identificar, em conjunto com a equipa de IT (*Information Technology*) da entidade/pessoa coletiva ou com o *Webhost* que foi contratado para alojar os serviços online, quais as medidas que estão implementadas tendentes à proteção de ciber-ataques, nomeadamente:

    - Qual a capacidade de resiliência a um ataque de negação de serviço;
    - Quais os custos (se existem) de sofrer este tipo de ataque;
    - Qual o limite de tráfego a partir do qual o *Webhost* está obrigado/deve notificar a entidade/pessoa coletiva de que os seus servidores devem ser encerrados;
    - Que medidas previstas pelo *Webhost* e pela equipa de IT são automaticamente acionadas, quando existem este tipo de ataques.

- Proteger os domínios da entidade/pessoa coletiva, usando o bloqueio do registo de domínio[39] e confirmando se os detalhes do registo do domínio estão corretos;
- Verificar quais os pontos de contacto responsáveis, para a partilha de informação entre a entidade/pessoa coletiva e o *Webhost*, e se é uma rede de contacto 24/7, isto é, se esses pontos de contacto estão disponíveis todos os dias da semana e em qualquer hora do dia;
- Estabelecer uma rede de contactos fora da rede, caso as demais linhas de contacto falhem;
- Implementar mecanismos de monotorização, em tempo real, de ataques de negação de serviço;
- Efetuar uma segmentação dos diferentes serviços críticos (ex.: *e-mail*) de outros serviços que possam ser mais facilmente atacados (ex.: serviços de *webhosting*);
- Disponibilizar uma versão alternativa do website que possa estar disponível com a informação essencial.

Estratégias de intervenção

Estratégias para preservação de prova digital

Neste tipo de cibercriminalidade, para além das medidas que podem ser tomadas para preservação de prova, mostra-se essencial a adoção de estratégias que permitam mitigar um ataque e reportá-lo a entidades que possam prestar suporte técnico e com competência de investigação criminal.

No que diz respeito a ataques de ***ransomware*** ou qualquer outro que vise a interferência ou sabotagem de sistema informático, devem ser tomadas as seguintes medidas:

- Colocar imediatamente todos os sistemas *offline*;
- Garantir que os *backups* (cópias de segurança) estão livres de *malware*;
- Contactar de imediato o Centro Nacional de Cibersegurança[40] para apoio e reportar o ataque informático às autoridades - Polícia Judiciária;
- Se possível e quando aplicável, recolher e colocar em segurança parte dos dados que não tenham sido infetados pelo vírus;
- Se possível, alterar as palavras-passe da rede e de todas as contas *online*, após o ataque. Após remoção do vírus, alterar novamente dados de acesso de todas as contas;
- Apagar dados de registo e ficheiros que impeçam o vírus de carregar;

Muitas destas medidas são também aplicáveis a situações/ataques que tenham envolvido o **furto *online* de informação confidencial**; tratando-se de um ataque via *malware* aos dispositivos ou rede, todos os dispositivos devem ser colocados *offline*, seguido de alteração de todos os dados de acesso (nome de utilizador e palavra-passe). Deve ainda procurar proceder-se à identificação da origem da fuga de informação e efetuar a correção das vulnerabilidades. Por fim, deve o ataque informático ser reportado às autoridades competentes.

[39] REGISTRAR-LOCK é um código de status que pode ser definido num nome de domínio da Internet pelo/a responsável pelo registo desse mesmo domínio. Geralmente, é efetuado para impedir alterações não autorizadas, indesejadas ou acidentais no nome do domínio.

[40] Veja-se https://www.cncs.gov.pt/.

No que diz respeito aos **ataques de negação de serviço**, podem ser tomadas as seguintes medidas:

- Transferência dos serviços online para um serviço *Cloud* com elevada capacidade de tráfego e com capacidade para alojar um website não dinâmico;
- Contratação de empresa/serviço que ofereça mecanismos de combate a ataques de negação de serviço ou avançar para soluções internas - INHOUSE - através de técnicos/as especializados/as responsáveis por implementar essas medidas;
- Desativar os serviços que permitem que este ataque de negação de serviço seja eficaz (ex.: ter pronto para lançamento uma versão do website).

A quem e como reportar/denunciar

Para denúncia deste tipo de ataques, devem ser contactadas as autoridades com competência para investigação criminal nesta matéria que, à semelhança dos outros casos de cibercriminalidade, é, no caso de Portugal, a Polícia Judiciária.

Estratégias para superar a vitimação e seus impactos

A compreensão das dinâmicas, do impacto e das consequências associadas às experiências de cibervitimação é muito importante para que o/a profissional de apoio (TAV) seja capaz de auxiliar a vítima na superação da experiência de crime.

Nesse âmbito, para além dos conteúdos pedagógicos propostos no Módulo 3, é importante a leitura dos capítulos 3 e 4 – Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*.

Como já referido no Módulo 3, os estudos existentes relativos ao impacto e consequências da cibervitimação são escassos e considera-se que as consequências experienciadas pelas vítimas de cibercrime não se distinguem das consequências sentidas por vítimas de outros crimes.

Para lá das consequências causadas na saúde das vítimas particulares, no impacto financeiro e no receio do cibercrime, no caso específico dos crimes ciberdependentes, não podemos olhar apenas para as consequências per se, mas também para a finalidade que o/a cibercriminoso/a deu aos dados da vítima aos quais teve acesso ilegítimo.

No que respeita às estratégias para auxiliar a vítima na superação da situação de cibercrime, este Módulo explorará os aspetos-chave já abordados no Módulo anterior relativamente à intervenção e apoio junto de vítimas de cibercrime. Aconselha-se ainda, para uma abordagem aprofundada desta matéria, a consulta do capítulo 2 - Parte II *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*.

De entre os objetivos de tal apoio e intervenção, destaca-se:

- A valorização da denúncia/procura de apoio e a validação da experiência;
- O fornecimento de informações sobre o crime e sua prevalência.
- A prevenção de novos crimes, incluindo através do desenvolvimento, em conjunto com a vítima, de planos de segurança.

Apoio Especializado a Vítimas de Cibercrime

PARTE II - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME

Módulo 5 - Apoio especializado a vítimas de crime ciberdependente

5. Apoio especializado a vítimas de crime ciberdependente

***a. Modi operandi* e natureza do crime**

Crimes ciberdependentes – dependem de computadores e redes pelo que sem a internet não poderiam ser praticados.

- Malware e Hacking – comumente utilizados para roubar dados pessoais
- Ataques de negação de serviço (DDoS) – concebidos para degradar serviços online, como websites, e-mail e serviços DNS → danos financeiros e reputaconais (crime de sabotagem informática)
- Ransomware – tipo de malware que nega o acesso a um sistema de dados de computador até que um resgate seja pago (crime de dano informático)

5. Apoio especializado a vítimas de crime ciberdependente

***a. Modi operandi* e natureza do crime**

- Furto de informação confidencial
- Phishing, spear-phishing – e-mails com links maliciosos
- Exploração de vulnerabilidades do software para aceder remotamente ao computador
- Furto de informação pessoal online – financeira, dados bancários, carteiras, etc.
  - Investigação
  - Ataque
  - Exfiltração de dados

5. Apoio especializado a vítimas de crime ciberdependente

b. Estratégias de prevenção

- **Ataques de *ransomware* e de furto de informação confidencial**
  - Ativação de filtros de *spam* fortes; utilização de mecanismos de autenticação de e-*mail* com *Sender Policy Framework* (SPF), relatórios e conformidade de autenticação de mensagens de domínio (DMARC) e *Domain Keys Identified Mail* (DKIM), para impedir a falsificação de *e-mails*;
  - Utilização de mecanismos de análise de ficheiros executáveis de *e-mails* enviados ou recebidos, prevenindo que os/as utilizadores/as os recebam;
  - Configuração da *firewall* de forma a bloquear o acesso a IPs (*Internet Protocol*) que já se sabem que são uma ameaça;

5. Apoio especializado a vítimas de crime ciberdependente

b. Estratégias de prevenção

- **Ataques de *ransomware* e de furto de informação confidencial**
  - Configuração de antivírus e programas de anti-malware em todos os computadores e configuração dos mesmos para realizarem análises regulares;
  - Implementação de ações de formação e sensibilização sobre estes riscos online, principalmente quando falamos de funcionários(as)/quadros de empresas, pois estes podem ser alvos deste tipo de ataques;
  - Aplicação do "Princípio dos Privilégios Mínimos" nas empresas/organizações: a nenhum (a) utilizador(a) deve ser atribuído acesso administrativo superior ao estritamente necessário para o exercício da sua atividade.

5. Apoio especializado a vítimas de crime ciberdependente

b. Estratégias de prevenção

- **Ataques de negação de serviço (DDoS)**
  - Determinar *a priori* qual o nível de serviço adequado e que deverá ser mantido em permanência para os/as seus utilizadores/as;
  - Definir quais as funcionalidades do serviço *online* que a entidade/pessoa coletiva pode prescindir em caso de ataque (ex.: se um *website* da entidade estiver a sofrer um ciber-ataque em tempo de Pandemia, pode ser vedado o acesso a toda a informação do *website*, exceto os contactos, de forma a mitigar a sobrecarga na rede);
  - Proteger os domínios da entidade/pessoa coletiva, usando o bloqueio do registo de domínio e confirmando se os detalhes do registo do domínio (por exemplo, detalhes do contacto) estão corretos;

5. Apoio especializado a vítimas de crime ciberdependente

b. Estratégias de prevenção

- **Ataques de negação de serviço (DDoS)**

- Identificar, em conjunto com a equipa de IT (*Information Technology*) da entidade/pessoa coletiva ou com o *Webhost* que foi contratado para alojar os serviços *online*, quais as medidas que estão implementadas tendentes à proteção de ciber-ataques, nomeadamente:
  - Qual a capacidade de resiliência a um ataque de negação de serviço;
  - Quais os custos (se existem) de sofrer este tipo de ataque;
  - Qual o limite de tráfego a partir do qual o *webhost* está obrigado/deve notificar a entidade/pessoa coletiva de que os seus servidores devem ser encerrados;
  - Que medidas previstas pelo *Webhost* e pela equipa de IT são automaticamente acionadas quando existem este tipo de ataques.

5. Apoio especializado a vítimas de crime ciberdependente

b. Estratégias de prevenção

- **Ataques de negação de serviço (DDoS)**

- Verificar quais os pontos de contacto responsáveis, para a partilha de informação entre a entidade/pessoa coletiva e o *Webhost*, e se é uma rede de contacto 24/7, isto é, se esses pontos de contacto estão disponíveis todos os dias da semana e em qualquer hora do dia;
- Estabelecer uma rede de contactos fora da rede (ex.: existência de uma lista de contactos telefónicos rápida e, em última análise, ponderar a utilização de *e-mails* que não os da entidade/pessoa coletiva para a troca de informação), caso as demais linhas de contacto falhem;
- Implementar mecanismos de monotorização, em tempo real, de ataques de negação de serviço;
- Efetuar uma segmentação dos diferentes serviços críticos (ex.: *e-mail*) de outros serviços que possam ser mais facilmente atacados (ex.: serviços de *webhosting*);
- Disponibilizar uma versão alternativa do *website* que possa estar disponível com a informação essencial.

5. Apoio especializado a vítimas de crime ciberdependente

c. Estratégias de intervenção

i. Preservação da prova digital

***Ransomware*, furto *online* de informação confidencial, malware,**

- Colocar imediatamente todos os sistemas *offline*;
- Garantir que os *backups* (cópias de segurança) estão livres de *malware*;
- Se possível e quando aplicável, recolher e colocar em segurança parte dos dados que não tenham sido infetados pelo vírus;
- Se possível, alterar as palavras-passe da rede e de todas as contas *online*, após o ataque. Após remoção do vírus, alterar novamente dados de acesso de todas as contas;
- Apagar dados de registo e ficheiros que impeçam o vírus de carregar;
- Identificação da origem da fuga de informação e efetuar a correção das vulnerabilidades;
- Contactar de imediato o Centro Nacional de Cibersegurança para apoio e reportar o ataque informático às autoridades - Polícia Judiciária; https://www.cncs.gov.pt/

5. Apoio especializado a vítimas de crime ciberdependente

c. Estratégias de intervenção

i. Preservação da prova digital

Ataques de negação de serviço:

- Transferência dos serviços *online* para um serviço *Cloud* com elevada capacidade de tráfego e com capacidade para alojar um *website* não dinâmico;
- Contratação de empresa/serviço que ofereça mecanismos de combate a ataques de negação de serviço ou avançar para soluções internas - INHOUSE - através de técnicos(as) especializados(as) responsáveis por implementar essas medidas;
- Desativar os serviços que permitem que este ataque de negação de serviço seja eficaz (ex.: ter pronto para lançamento uma versão do website em que não estejam disponíveis: o mecanismo de procura de conteúdos, conteúdos dinâmicos, ou ficheiros que ocupem muito tráfego da rede).

5. Apoio especializado a vítimas de crime ciberdependente

c. Estratégias de intervenção

ii. A quem e como reportar

Polícia Judiciária.

iii. Orientações práticas para superar a vitimação e seus impactos

Para além dos conteúdos pedagógicos propostos no Módulo 3, é importante a leitura dos capítulos 2, 3 e 4 – Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas.*

De entre os objetivos de apoio e intervenção, **destaca-se:**

- A valorização da denúncia/procura de apoio e a validação da experiência;
- O fornecimento de informações sobre o crime e sua prevalência.
- A prevenção de novos crimes, incluindo através do desenvolvimento, em conjunto com a vítima, de planos de segurança.

PLANO DE SESSÃO Nº 5

1. Identificação da Ação

Designação Curso de Formação Apoio Especializado a Vítimas de Cibercrime

Módulos/ temas Apoio especializado a vítimas de crimes ciberdependentes

Data da Sessão **Horário** **Duração da Sessão** 40 minutos

Formadores/as

2. Objetivos Específicos

No final da sessão, os/as formandos/as deverão ser capazes de:

- Distinguir, corretamente, a natureza e modi operandi dos crimes ciberdependentes;
- Enumerar, de forma correta, estratégias de intervenção propostas para o apoio especializado a vítimas de crimes ciberdependentes;
- Reconhecer, de forma correta, estratégias de prevenção da revitimação propostas para a intervenção junto de vítimas de crimes ciberdependentes.

3. Estrutura da Sessão

	Conteúdos Programáticos	Metodologia	Recursos Pedagógicos/ Didáticos	Avaliação | Exercícios	Tempo (minutos)
Introdução	Exercício n.º 2	Ativa	Regras do Exercício n.º 2, Folha do Exercício n.º 2 e canetas	Observação	5
Desenvolvimento	*Modi operandi* e natureza dos crimes	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
	Estratégias de prevenção	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
	Estratégias de intervenção: • Estratégias para preservação de prova digital • A quem e como reportar/denunciar • Estratégias para superar a vitimação e seus impactos	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	20
Conclusão	Síntese conclusiva e esclarecimento de questões	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5

OBSERVAÇÕES

Destionatários/as:
Técnicos/as de Apoio à Vítima (TAV)

Data: / / **Formador(a):**

INSTRUÇÕES E INFORMAÇÕES ESSENCIAIS PARA O/A FORMADOR(A)

CORRESPONDÊNCIA DE CONTEÚDOS

Plano de Sessão	*Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*	
	PARTE	CAPÍTULO
Exercício n.º 2	Sem correspondência Ver Regras do Exercício n.º 2	
Modi operandi e natureza dos crimes	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Estratégias de prevenção	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Estratégias de intervenção		
Estratégias para preservação de prova digital	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
A quem e como reportar/denunciar	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Estratégias para superar a vitimação e seus impactos	Parte II - Proceder Ver Apresentação e Enquadramento do Módulo	Capítulo 2 – 2.1.
Síntese conclusiva e esclarecimento de questões	Sem correspondência	

REGRAS DO EXERCÍCIO N.º 2

Módulo/Tema	Apoio especializado a vítimas de crimes ciberdependentes	**CÓD. REF.**	**ÁREA DE EDUCAÇÃO E FORMAÇÃO**

Objetivos

Este exercício tem como objetivo, através de uma atividade breve e lúdica, relembrar alguns conceitos-chave abordados no Módulo 1 (relativos a fenómenos e ataques cibernéticos associados à criminalidade ciberdependente) e introduzir o Módulo 5 no qual o apoio a vítimas de crimes ciberdependentes será detalhado.

Execução

O/A formador(a) deve distribuir pelos formandos/as a Folha do Exercício, explicando que a cada definição/frase total/parcial apresentada na Coluna A deve corresponder um fenómeno/conceito listado na Coluna B. Deve também indicar aos/às formandos/as que estes dispõem de 60 segundos para procederem à associação entre definições/Coluna A e fenómenos/Coluna B.

Em seguida, o/a formador(a) deve efetuar a correção em conjunto/grande grupo, esclarecendo dúvidas, caso existam.

Os fenómenos/conceitos (Coluna B) e respetivas definições/frases (Coluna A) são os seguintes:

Hacking: Implica o acesso não autorizado a sistemas informáticos.

Spamming: Diz respeito ao envio e publicação de publicidade em massa.

Malware: É software de caráter hostil ou intrusivo.

Crime ciberdependente: Refere-se ao cibercrime *strictu sensu*.

Phishing: É utilizado para o acesso ilegítimo a informação confidencial.

Ataque de negação de serviço (*DDoS*): É relativo à sobrecarga de um sistema.

Notas

Consultar Apresentação e Enquadramento do Módulo

FOLHA DO EXERCÍCIO N.º 2

Associe, a cada uma das definições apresentadas na Coluna A, o fenómeno correspondente apresentado na Coluna B.

COLUNA A	COLUNA B
É software de caráter hostil ou intrusivo	*Hacking*
Refere-se ao cibercrime strictu sensu.	*Spamming*
Implica o acesso não autorizado a sistemas informáticos	*Malware*
É relativo à sobrecarga de um sistema	Crime ciberdependente
É utilizado para o acesso ilegítimo a informação confidencial	*Phishing*
Diz respeito ao envio e publicação de publicidade em massa	Ataque de negação de serviço

MOD. 6

MOD. 6

PARTE 2 - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME
MÓDULO 6 - APOIO ESPECIALIZADO A VÍTIMAS DE BURLAS *ONLINE*

APRESENTAÇÃO E ENQUADRAMENTO DO MÓDULO

Em Portugal, podemos distinguir dois tipos de crimes de burla: o crime de burla, previsto e punido no artigo 217º do código penal, e o crime de burla informática, previsto e punido no artigo 221º do código penal:

- **Burla** – o elemento essencial do crime de burla materializa-se na indução em erro de alguém, implicando, para tal, a colaboração da vítima a atuar de acordo com uma vontade viciada.
- **Burla informática** – na burla informática, verifica-se um atentado direto ao património levado a cabo por meios informáticos. O computador surge como mecanismo de ação do/a agente, logo, não pode ser alvo de engano. Ao contrário do crime de burla, não é necessário que se verifique um enriquecimento do/a autor(a), bastando o *animus* de enriquecimento. Neste sentido, também não é necessário que se verifique a intenção de induzir alguém em erro, sendo suficiente, para a prática do crime, a verificação de configuração incorreta de programa informático que se concretize na sua total ou parcial reestruturação, no aditamento, na alteração ou supressão de fases do programa e/ou na introdução de novas instruções.

Este Módulo irá explorar os tipos de burlas *online* com maior expressão em termos estatísticos e aquelas que causam maior dano patrimonial às suas vítimas, a saber:

- Burlas no comércio eletrónico (*e-commerce*);
- Burlas bancárias;
- Burlas nos relacionamentos íntimos (*romance scams*).

Em todo o caso, estes fenómenos são explorados no capítulo 1 – Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*.

Tipos, *modi operandi* e natureza do crime

Burlas no comércio eletrónico (e-commerce)

As **burlas no comércio eletrónico** apresentam diferentes graus de complexidade:

- desde esquemas mais simples, nos quais é prometido ao/à comprador(a) o envio de um determinado artigo pelo correio, mediante transferência bancária, o qual acaba por não ser recebido;
- até esquemas mais elaborados, que podem envolver a falsificação de documentos, como comprovativos de transferência bancária, a exploração de vulnerabilidades em websites de compras online que armazenam dados bancários dos/as utilizadores/as (cartões de crédito ou débito), sendo estes acedidos e usados pelo/a cibercriminoso/a para venda na *darkweb* ou para realizar transações bancárias sem o conhecimento da vítima (*card not present fraud*).

Ainda ao nível do comércio eletrónico, também podem ocorrer **burlas em leilões na Internet**, nomeadamente quando os itens comprados são produtos falsos ou obtidos por meios ilícitos ou quando o/a vendedor(a) anuncia ou disponibiliza para venda itens inexistentes (Jahankhani et al., 2014).

Burla bancária

A **burla bancária** centra-se sobretudo em ataques de ***phishing*** de que podem ser alvo as vítimas particulares, mas também entidades coletivas (como empresas e organizações). O modo de funcionamento do *phishing* já foi abordado:

- regra geral, através da receção de *e-mails* ou SMS, a vítima é levada a clicar num link que pensa ser da sua entidade bancária, sendo conduzida a um website que está desenhado para parecer o da sua entidade bancária. O desenho deste website é efetuado através de uma técnica denominada de *pharming*, termo atribuído ao ataque baseado na técnica *DNS cache poisoning* (envenenamento de *cache* DNS), que consiste em corromper o Sistema de Nomes de Domínios - DNS (*Domain Name System*) numa rede de computadores, fazendo com que o Localizador Uniforme de Recursos - URL (*Uniform Resource Locator*) de um website passe a "apontar" para um servidor diferente do original.

A **burla com cartão de crédito** refere-se à utilização do cartão de crédito de outra pessoa para uso pessoal, sem o conhecimento do/a proprietário/a do cartão e da entidade emissora (Patel & Singh, 2013). Existem vários crimes ciberdependentes que poderão ser utilizados para a obtenção de acesso a tais cartões e a detalhes sobre o mesmo, como o *phishing*, o *spamming* ou o *hacking* (Jahankhani et al., 2014).

Destaque também para o ***skimming fraud***, que consiste na cópia da banda magnética de um cartão de pagamento, sem o conhecimento ou consentimento do/a titular do cartão, aquando da utilização do referido cartão numa máquina ATM ou num terminal de ponto de venda.

Recentemente têm vindo a verificar-se outro tipo de ataques a sistemas informáticos, nomeadamente a máquinas ATM, num processo denominado de ***jackpotting***, que visa a emissão de dinheiro existente nas máquinas de multibanco, através do comando do/a criminoso/a. O ataque a máquinas ATM pode ocorrer através da introdução de *malware* no sistema informático do equipamento/ATM ou através da ligação de *hardware*, denominado de "*Black-Box*".

Burlas nos relacionamentos íntimos [romance scams]

As **burlas nos relacionamentos íntimos** acontecem quando o/a agente procura estabelecer uma relação de confiança e de intimidade, nomeadamente através da internet e das TIC, com um determinado alvo, como prelúdio para obter benefício pessoal, nomeadamente financeiro e patrimonial. Os atos fraudulentos podem envolver acesso ao dinheiro da vítima, contas bancárias, cartões de crédito, passaportes, contas de *e-mail* ou números de identificação nacional, ou, ainda, forçando a vítima a cometer crimes em nome do/a agente.

Neste Módulo, exploraremos os *modi operandi* destes três tipos de burlas, bem como estratégias de prevenção e de intervenção que o/a formando/a, enquanto profissional de apoio (TAV), deverá considerar na prestação de apoio a vítimas de burlas *online*.

No que diz respeito às **burlas no comércio eletrónico**, nomeadamente às burlas mais comuns - que não estão associadas à exfiltração dos/as utilizadores/as -, podemos dizer que a maior parte acontece em plataformas de vendas *online* onde é possível a pessoas particulares procederem à compra e venda de bens.

Quando o/a autor(a) da burla se apresenta como vendedor(a):

- Publica anúncios falsos, através de plataformas de compra e venda de artigos variados - imóveis para arrendamento, animais de estimação, carros usados, barcos, bicicletas, etc..
- O anúncio pode incluir fotos e outros detalhes - geralmente copiados de um outro anúncio de um(a) vendedor(a) genuíno -, podendo também indicar a venda do referido artigo a um preço baixo;
- Quando a vítima mostra interesse no artigo, o/a autor(a) pode alegar, por exemplo, que está em viagem ou que se mudou para outra localidade, motivo pelo qual será uma empresa de transporte a entregar a mercadoria, após o recebimento do pagamento. Após o pagamento, a vítima poderá receber um recibo falso via *e-mail*, muito embora não receba o artigo comprado, nem consiga entrar em contacto com o/a vendedor(a);
- No caso dos imóveis, o/a autor(a) fará o papel de proprietário/a ou senhorio/a de um imóvel para compra ou arrendamento. Quando a vítima mostrar interesse no referido imóvel, o/a autor(a) inventará desculpas para não mostrar presencialmente a propriedade ao/à comprador(a) interessado, alegando, por exemplo, que se encontra fora do país/em outra cidade. Se a vítima mantiver interesse em adquirir o imóvel ou arrendá-lo, irão ser pedidos valores a título de sinal.

Quando o/a autor(a) da burla se apresenta como comprador(a):

- O/A vendedor(a) publica um anúncio numa plataforma de compra e venda de artigos e recebe um *e-mail* ou mensagem de uma pessoa potencialmente interessada em comprar o artigo, aparentemente de outro país (tendo em conta os erros ortográficos e gramaticais que o texto contém);
- O/A interessado/a solicita os dados bancários do/a vendedor(a) (número de identificação bancário - NIB - ou dados de pagamento através de *Paypal*®), para proceder ao pagamento, e informa que contactará uma empresa de transportes para proceder à recolha o artigo;

- De seguida, o/a comprador(a) volta a contactar o/a vendedor(a), informando-o/a de que não consegue efetuar o pagamento à transportadora e que, por isso, transferiu para a conta do/a vendedor(a) o valor do artigo acrescido do custo com as despesas do transporte;
- O/A comprador(a) pede ao/à vendedor(a) que proceda ao pagamento à transportadora, através de serviços de envio de dinheiro, fornecendo, para isso, os dados necessários (nome e morada da suposta empresa de transportes). Normalmente, para aumentar a credibilidade do esquema, o(a) comprador(a) anexa a este *e-mail* um (falso) comprovativo da suposta transferência realizada para o(a) vendedor(a).

Na **burla bancária**, o *modus operandi* mais utilizado é o envio de *e-mails* de *phishing*. Veja-se exemplo utilizado no suporte visual deste Módulo (*PowerPoint*):

- O exemplo do *e-mail* típico de *phishing* procura copiar a imagem e o *lettering* de uma comunicação realizada por entidade bancária;
- Por norma, este tipo de *e-mail* convida o/a destinatário/a a fazer o *download* de algum ficheiro ou a clicar num *link* que o/a redireciona para um *website* onde deve introduzir os seus dados pessoais;
- Esses *websites* são desenhados de forma a serem muito semelhantes aos *websites* genuínos das entidades bancárias (Veja-se método explicado no Módulo 5).

Já nas **burlas nos relacionamentos amorosos**, podemos identificar os seguintes *modi operandi*:

- Criação de perfil falso nas redes sociais, nas aplicações de encontros amorosos ou em outras plataformas de *chat* e interação social;
- Estabelecimento de contacto com alvos aparentemente mais vulneráveis, nomeadamente pessoas com perfis públicos (definições de privacidade);
- Criação de vínculo emocional com o alvo previamente identificado, recolhendo sobre este o máximo de informação possível;
- Desenvolvimento de uma narrativa com o intuito de extorquir património pessoal/financeiro ao alvo.

Estratégias de prevenção

Para **prevenir burlas no comércio eletrónico ou burlas bancárias**, neste ponto do Módulo, o/a formador(a) deve transmitir aos/às formandos/as as seguintes estratégias que estes/as, enquanto profissionais de apoio (TAV), poderão utilizar na intervenção com a vítima apoiada:

- Não adquirir bens através de redes Wi-fi não protegidas (Wi-fi público ou redes em não seja necessária *password*).
- Selecionar plataformas e websites de compras *online* conhecidos e fidedignos e que ofereçam métodos de pagamento seguros.
- Verificar e reconhecer *websites* seguros:
  - O website deverá apresentar o símbolo de um cadeado, no lado esquerdo, imediatamente antes do endereço do website;
  - O URL do website deve conter o certificado - 'https://'; contendo o 's' de "seguro" acrescentado ao 'http', devendo sempre verificar-se o URL dos websites, nomeadamente quando os endereços são partilhados por mensagem ou e-mail;
- Não fornecer informação pessoal ou dados pessoais requeridos através de *e-mails*, mensagens, chamadas, *websites* não solicitados;
- Verificar o nome do remetente do *e-mail* – gralhas ou outro tipo de erros significam que o remetente do *e-mail* não é/representa quem diz ser.

Para a **prevenção de burlas nos relacionamentos amorosos**, o/a formador(a) deve transmitir aos/às formandos/as as seguintes estratégias que estes/as, enquanto profissionais de apoio (TAV), poderão utilizar na intervenção com a vítima apoiada:

- Verificar a fotografia do perfil (ex.: através do motor de busca de imagens *Tin Eye* ou do Google Chrome, carregando, para o efeito, no botão do lado direito do rato e escolhendo a opção "pesquisar imagem no Google");

- Efetuar pesquisa no Google®, copiando parágrafos de mensagens recebidas via *chat* ou *e-mail*, de forma a perceber se é uma abordagem/comunicação já conhecida e denunciada por outras pessoas;
- Verificar erros ortográficos que indiciem que a língua em que a pessoa está a comunicar não é a sua língua nativa;
- Verificar se o/a agente realiza vários pedidos para que a comunicação seja efetuada através de plataformas de chat como, por exemplo, Facebook®, WhatsApp®, Kik®, SMS, Messenger® ou Skype®.

Estratégias de intervenção

Estratégias para preservação de prova digital

Ainda neste Módulo, deverá o/a formador(a) apresentar junto dos/as formandos/as estratégias que podem ser explicadas às vítimas em processo de apoio, para a preservação da prova. Em seguida, são identificadas algumas dessas estratégias por tipo de burla *online*.

Como salvaguardar prova, em caso de **burlas no comércio eletrónico e de burlas bancárias**:

- Havendo transferências patrimoniais, guardar registos de tais transferências e contactar a entidade bancária;
- Apresentar queixa-crime junto das autoridades competentes;
- Solicitar apoio junto de estruturas de apoio à vítima, para lidar com o sofrimento emocional causado pela situação de vitimação e garantir acompanhamento ao longo do processo-crime.

Além das estratégias supra, em caso de **burla num relacionamento amoroso**, dever-se-á:

- Guardar todos os registos das comunicações feitas com o/a autor(a) do crime;
- Reportar o perfil do/a autor(a) do crime junto do *website*, rede social ou plataforma de encontros *online*.

É importante que o(a) profissional de apoio (TAV) se mantenha disponível para **auxiliar e/ou acompanhar** a vítima no processo de operacionalização das estratégias supra.

A quem e como reportar/denunciar

As **burlas informáticas** devem ser reportadas junto da Polícia Judiciária ou Ministério Público. As **burlas** podem ser reportadas junto de qualquer órgão de polícia criminal com competência genérica (PSP e GNR), desde que não seja uma **burla qualificada**. No último caso, o órgão de polícia criminal competente é a Polícia Judiciária. Para todos os efeitos, o crime pode ser sempre reportado ao Ministério Público, seja qual for a sua natureza.

Estratégias para superar a vitimação e seus impactos

A **insegurança** gerada pela perda de estabilidade financeira tem impacto negativo nas vítimas de burlas *online*. Para além do **prejuízo financeiro**, a vítima de burla pode manifestar um conjunto diversificado de **sintomas e de consequências** decorrentes da experiência de vitimação, que são comuns a todas as vítimas de crime, entre os quais:

- ***Flashbacks***: pensamentos constantes sobre o que aconteceu;
- **Ansiedade**, que pode ainda associar-se a dificuldades de concentração;
- **Dificuldade em dormir e pesadelos**;
- **Sentimento de culpa**, que pode ainda ser reforçado pelas eventuais reações das pessoas mais próximas, após a revelação da experiência de cibervitimação;
- **Raiva**, por vezes, associada a pensamentos de vingança;
- **Medo** de voltar a ser vítima de crime;
- **Mudanças de humor**;
- **Perturbações de ordem física** como, por exemplo, distúrbios na alimentação, dores no peito, tonturas, dores de cabeça, dores nas costas e no pescoço, problemas digestivos ou suores.

No que respeita às orientações para auxiliar a vítima na superação da situação de cibercrime, este Módulo explorará os aspetos-chave já abordados no Módulo 4 relativamente à intervenção e apoio junto de vítimas de cibercrime. Aconselha-se ainda, para uma abordagem aprofundada desta matéria, a consulta do capítulo 2 - Parte II *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*.

Sem prejuízo das orientações centrais para a intervenção abordadas no Módulo 4, consideram-se particularmente prementes, no caso do apoio a vítimas de burlas *online*, as **estratégias de apoio emocional** seguidamente apresentadas:

- Escutar empaticamente, demonstrando que está a ouvir ativamente e a compreender o que está a ser dito e a valorizar as reações, emoções/sentimentos, comportamentos, pensamentos e significados atribuídos pela vítima à sua experiência de cibervitimação por burla *online*;
- Demonstrar que acredita naquilo que a vítima está a contar sobre o que lhe aconteceu, sem julgamentos ou juízos de valor;
- Normalizar as reações apresentadas, enquadrando/contextualizando as reações da vítima no contexto emocional da situação experienciada;
- Disponibilizar os serviços prestados, explicando de que modo é que estes poderão ajudar a vítima.

Outras estratégias de apoio devem ser também destacadas neste ponto do Módulo:

- Informar, de forma simples, sucinta e clara, transmitindo informação essencial à vítima sobre o que aconteceu e os passos seguintes a adotar, através de linguagem ajustada às características da vítima;
- Não promover expectativas irrealistas quanto ao papel do/a profissional de apoio (TAV) e/ou quanto à resolução da situação;
- Não tomar decisões pela vítima e respeitar as suas escolhas;
- Informar acerca da possibilidade de revitimação, explorando possíveis cenários com que a vítima ainda se poderá deparar;
- Elaborar um plano de recuperação económica com a vítima, com o intuito de facultar estratégias à vítima para esta reestabelecer o controlo sobre a sua vida;
- Prevenir novos crimes, através da consciencialização para a importância de adoção das estratégias de prevenção já descritas neste Módulo.

O caso específico das vítimas das vítimas de burlas nos relacionamentos íntimos (*romance scams*)

Neste ponto do Módulo, deve ainda o/a formador(a) explorar o caso específico da intervenção junto de vítimas de burlas nos relacionamentos íntimos. Partindo do Exercício n.º 3 (Veja-se Plano de Sessão), são detalhadas reações e consequências emocionais e psicológicas desta forma de vitimação, nomeadamente:

- Culpa intensa;
- Sentimento de injustiça e de desconfiança generalizada relativamente a outras pessoas;
- Vergonha por terem sido enganadas;
- Relutância em denunciar o crime às autoridades policiais, sobretudo no caso de terem descoberto que o/a autor(a) é alguém próximo e em quem confiavam, como um(a) familiar ou amigo/a;
- Isolamento social.

Adicionalmente às estratégias supra, o/a formador(a) deverá ainda explorar as seguintes estratégias:

- Recomendar o retomar progressivo de atividades, incluindo hábitos de utilização da internet e TIC;
- Incentivar o reforço do envolvimento em atividades anteriormente apreciadas, nomeadamente atividades *offline*;
- Mobilizar o suporte social e, caso seja vontade da vítima e com a sua autorização, envolver familiares e/ou amigos/as no processo de recuperação, solicitando o seu auxílio para a prevenção do evitamento e isolamento, por exemplo;
- Evitar a hiperproteção por familiares e amigos/as (sem negligenciar a segurança da vítima).

Apoio Especializado a Vítimas de Cibercrime

PARTE II - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME

Módulo 6 - Apoio especializado a vítimas de burlas online

6. Apoio especializado a vítimas de burlas online

Diferença entre...

Burla, art. 217.º CP - indução em erro de alguém, vontade viciada da vítima

Burla online, art. 221.º CP - atentado direto ao património levado a cabo por meios informáticos; o computador é o mecanismo através do qual se opera a prática do crime, pelo que não existe engano ou erro, bastando o *animus* de enriquecimento.

Neste Módulo - burlas *online* com maior expressão em termos estatísticos e maior dano patrimonial às suas vítimas:

1. **Burlas no comércio eletrónico (*e-commerce*);**
2. **Burlas bancárias;**
3. **Burlas nos relacionamentos íntimos (*romance scams*).**

6. Apoio especializado a vítimas de burlas online

a. Tipos e Modi operandi

1. **Burlas no comércio eletrónico (*e-commerce*)**

Esquemas simples: envio/pagamento de bem que acaba por nunca ser pago/recebido

Esquemas mais elaborados: falsificação de documentos (ex. comprovativos de transferência bancária), exploração de vulnerabilidades em *websites* de compras *online* que armazenam dados bancários dos utilizadores, usados pelo(a) cibercriminoso(a) para venda na *darkweb* ou para realizar transações bancárias sem o conhecimento da vítima (*card not present fraud*)

e.g. Burla em leilões na Internet, plataformas de compra e venda online, anúncios falsos, etc.

6. Apoio especializado a vítimas de burlas online

a. Tipos e Modi operandi

2. Burla Bancária

Sobretudo através de ataques de ***phishing*** – SMS ou e-mail com link malicioso – com direcionamento para página que aparenta ser da entidade bancária

E.g.:

Burla com cartão de crédito – utilização de cartão alheio sem conhecimento do proprietário nem do banco

Skimming fraud - cópia da banda magnética de um cartão (utilização numa máquina ATM ou num terminal de ponto de venda)

Jackpotting - emissão de dinheiro existente nas máquinas de multibanco, através do comando do(a) criminoso(a) através de *malware* ou *black-box*

6. Apoio especializado a vítimas de burlas online

a. Tipos e Modi operandi

2. Burla Bancária

Sobretudo através de ataques de ***phishing*** – SMS ou e-mail com link malicioso – com direcionamento para página que aparenta ser da entidade bancária

E.g.:

Burla com MBWAY

Burla com cartão de crédito – utilização de cartão alheio sem conhecimento do proprietário nem do banco

Skimming fraud - cópia da banda magnética de um cartão (utilização numa máquina ATM ou num terminal de ponto de venda)

Jackpotting - emissão de dinheiro existente nas máquinas de multibanco, através do comando do(a) criminoso(a) através de *malware* ou *black-box*

6. Apoio especializado a vítimas de burlas online

a. Modi operandi

Meios Comuns para o cometimento de Burla Informática: SPAM

O termo SPAM pode ser um acrónimo derivado da expressão em inglês "*Sending and Posting Advertisement in Mass*", traduzido em português "Enviar e Postar Publicidade em Massa", ou também *Stupid Pointless Annoying Messages* que significa mensagem ridícula, sem propósito, e irritante.

Fonte: Dezi Technical

6. Apoio especializado a vítimas de burlas online

a. Modi operandi

Meios Comuns para o cometimento de Burla Informática: *Phishing*

O *phishing* deve o seu nome à palavra inglesa *"fishing"*, cujo significado é "pescar". O *phishing* consiste em utilizar métodos tecnológicos que levem o utilizador a revelar dados pessoais e/ou confidenciais.

Fonte: High Wire Networks

6. Apoio especializado a vítimas de burlas online

a. Modi operandi

Exemplo de Email de *Phishing*

Fonte: Scoop

Email que tenta copiar a imagem e o *lettering* de uma entidade legítima (ex: banco, serviços de *streaming online*, entidades governamentais, etc.)

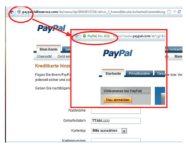
Leva sempre a pessoa a fazer o download de algum ficheiro ou clicar num *link* que redireciona a pessoa para um site onde deve introduzir os seus dados pessoais.

6. Apoio especializado a vítimas de burlas online

a. Modi operandi

Meios Comuns para o cometimento de Burla Informática: *Pharming*

Em informática ***Pharming*** é o termo atribuído ao ataque baseado na técnica DNS cache *poisoning* (envenenamento de cache DNS) que, consiste em corromper o DNS (Sistema de Nomes de Domínio ou *Domain Name System*) numa rede de computadores, fazendo com que o URL (*Uniform Resource Locator* ou Localizador Uniforme de Recursos) de um site passe a apontar para um servidor diferente do original.



Fonte: Quora

Exercício:
Rio da Realidade | Não caias na armadilha

https://beinternetawesome.withgoogle.com/pt-br_br/interland/rio-realidade

6. Apoio especializado a vítimas de burlas online

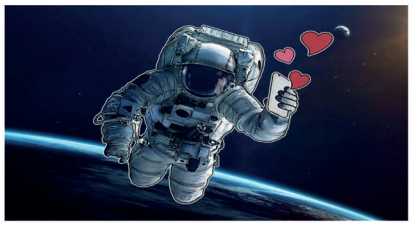
a. Modi operandi

3. Burlas nos relacionamentos íntimos (*Romance scam*)

O(a) agente procura estabelecer uma relação de confiança e de intimidade, nomeadamente através da internet e das TIC, com um determinado alvo, como prelúdio para obter benefício pessoal, nomeadamente financeiro e patrimonial.

Tipo de atos: acesso ao dinheiro da vítima, contas bancárias, cartões de crédito, passaportes, contas de *e-mail* ou números de identificação nacional, ou, ainda, forçando a vítima a cometer crimes em nome do(a) agente.

Relacionamentos *Online*



Fonte: https://www.kaspersky.com/blog/online-dating-report/

a. Modi operandi

3. Burlas nos relacionamentos íntimos (*Romance scam*)

- Criação de perfil falso nas redes sociais, nas aplicações de encontros amorosos ou em outras plataformas de *chat* e interação social;
- Estabelecimento de contacto com alvos aparentemente mais vulneráveis, nomeadamente pessoas com perfis públicos (definições de privacidade);
- Criação de vínculo emocional com o alvo previamente identificado, recolhendo sobre este o máximo de informação possível;
- Desenvolvimento de uma narrativa com o intuito de extorquir património pessoal/financeiro ao alvo.

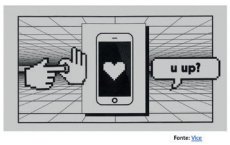
Relacionamentos *Online*

Quais são alguns dos Riscos dos Relacionamentos Online?

Fonte: Pinterest

Exemplo:
Sexting

Resulta das palavras '*sex*' (sexo) e '*texting*' (envio de SMS) e significa a troca de mensagens eróticas com ou sem fotos via telemóvel, chats ou redes sociais.



Fonte: Vice

a. Tipos e Modi operandi

Riscos nos Relacionamentos *Online*

- ❑ Divulgação Não Consensual de Imagens e Vídeos: (abordado no Módulo 10)
  - *Sextortion*
  - *Revenge Porn*
  - *Grooming*
- ❑ Assédio Sexual *Online*:
  - Ameaças e Coação
  - *Bullying* "Sexualizado"
  - "Sexualização Indesejada"

a. Tipos e Modi operandi

Riscos nos Relacionamentos *Online*

Assédio Sexual *Online*

O Assédio Sexual Online pode assumir várias formas, das quais podemos destacar:

- Ameaças e Coação;
- *Bullying* "Sexualizado";
- "Sexualização Indesejada".

a. Tipos e Modi operandi

Riscos nos Relacionamentos *Online*

Ameaças e Coação

Nestes casos a vítima é ameaçada, sendo coagida a ter comportamentos sexuais *online* ou chantageada com conteúdo sexual.

Incluí comportamentos, como:

- ❑ Assediar ou pressionar alguém à partilha de imagens sexuais ou a envolver-se em comportamento sexual *online* (ou *offline*);
- ❑ Ameaçar a publicação de conteúdo sexual (imagens, vídeos, boatos) para ameaçar, coagir ou chantagear alguém ('*sextortion*');
- ❑ Ameaças on-line de natureza sexual (por exemplo, ameaças de violação);
- ❑ Incitar outras pessoas on-line a cometer violência sexual;
- ❑ Incitar alguém a participar de comportamento sexual e depois compartilhar imagens ou vídeos do mesmo.

6. Apoio especializado a vítimas de burlas online

a. Tipos e Modi operandi

Riscos nos Relacionamentos *Online*

Bullying "Sexualizado"

Alguém que é sistematicamente excluído de um grupo ou comunidade com o uso de conteúdo sexual que humilha, perturba ou discrimina.

Incluí comportamentos, como:

- Partilha *Online* de boatos ou mentiras sobre comportamento sexual;
- Uso de linguagem sexual ofensiva ou discriminatória *online*;
- Furto de Identidade da vítima e com isso prejudicar sua reputação partilhando conteúdo sexual ou assediando sexualmente outras pessoas;
- Partilha de informação referente à intimidade de terceiro *online* de forma não consensual para incentivar o assédio sexual contra este;
- Ser intimidado por causa pela identidade de género ou orientação sexual;
- Prática de «*body shamming*» - partilha de comentários depreciativos relativos ao aspeto físico de alguém;
- "*Outing*" – Quando alguém revela publicamente informação relativa à orientação sexual ou identidade de género de certa pessoa sem o conhecimento e autorização da mesma.

6. Apoio especializado a vítimas de burlas online

a. Tipos e Modi operandi

Riscos nos Relacionamentos *Online*

"Sexualização Indesejada"

Alguém que recebe solicitações sexuais indesejadas, comentários e conteúdo.

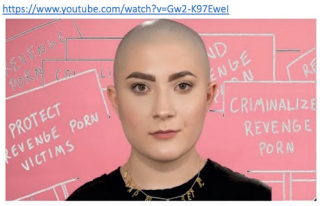
Incluí comportamentos, como:

- Comentários sexualizados (por exemplo, nas fotos publicadas nas redes sociais);
- Desafios "virais" sexualizados que pressionam as pessoas a participar;
- Enviar conteúdo sexual a alguém (imagens, emojis, mensagens) sem que eles consintam;
- Avanços sexuais indesejados ou pedidos de favores sexuais;
- "Piadas" de natureza sexual;
- Classificação de pares em atratividade / atividade sexual;
- Edição de imagens de uma pessoa para torná-la sexual.

Atividade – Debate

"A Victim Of Revenge Porn Tells Their Story" (2018)

https://www.youtube.com/watch?v=Gw2-K97EweI



6. Apoio especializado a vítimas de burlas online

b. Estratégias de prevenção

Prevenir <u>burlas no comércio eletrónico ou burlas bancárias</u>:

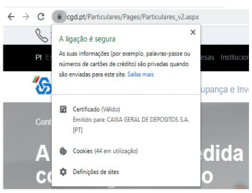
- Não adquirir bens através de redes Wi-fi não protegidas (Wi-fi público ou redes em não seja necessária *password*).
- Selecionar plataformas e *websites* de compras *online* conhecidos e fidedignos e que ofereçam métodos de pagamento seguros.
- Não fornecer informação pessoal ou dados pessoais pedidos através de *e-mails*, mensagens, chamadas, *websites* não solicitados;
- Verificar o nome do remetente do *e-mail* – gralhas ou outro tipo de erros significam que o remetente do *e-mail* não é/representa quem diz ser.

6. Apoio especializado a vítimas de burlas online

b. Estratégias de prevenção

Prevenir <u>burlas no comércio eletrónico ou burlas bancárias</u>:

- Verificar e reconhecer *websites* seguros:
  - O *website* deverá apresentar o símbolo de um cadeado, no lado esquerdo, imediatamente antes do endereço do *website*;
  - O URL do *website* deve conter o certificado - 'https://'; contendo o 's' de "seguro" acrescentado ao 'http', devendo sempre verificar-se o URL dos websites, nomeadamente quando os endereços são partilhados por mensagem ou *e-mail*;



6. Apoio especializado a vítimas de burlas online

b. Estratégias de prevenção

Prevenir <u>burlas nos relacionamentos amorososos:</u>

- Verificar a fotografia do perfil (ex.: através do motor de busca de imagens *Tin Eye* ou do Google Chrome, carregando, para o efeito, no botão do lado direito do rato e escolhendo a opção "pesquisar imagem no Google");
- Efetuar pesquisa no Google®, copiando parágrafos de mensagens recebidas via *chat* ou *e-mail*, de forma a perceber se é uma abordagem/comunicação já conhecida e denunciada por outras pessoas pessoas;
- Verificar erros ortográficos que indiciem que a língua em que a pessoa está a comunicar não é a sua língua nativa;
- Verificar se o(a) agente realiza vários pedidos para que a comunicação seja efetuada através de plataformas de *chat* como, por exemplo, Facebook®, WhatsApp®, Kik®, SMS, Messenger® ou Skype®.

6. Apoio especializado a vítimas de burlas online

c. Estratégias de intervenção

i. Preservação da prova digital

Em caso de **burlas no comércio eletrónico e de burlas bancárias**:

- Havendo transferências patrimoniais, guardar registos de tais transferências e contactar a entidade bancária;
- Apresentar queixa-crime junto das autoridades competentes;
- Solicitar apoio junto de estruturas de apoio à vítima, para lidar com o sofrimento emocional causado pela situação de vitimação e garantir acompanhamento ao longo do processo-crime.

6. Apoio especializado a vítimas de burlas online

c. Estratégias de intervenção

i. Preservação da prova digital

Em caso de **burla num relacionamento amoroso,** dever-se-á:

- Guardar todos os registos das comunicações feitas com o(a) autor(a) do crime;
- Reportar o perfil do(a) autor(a) do crime junto do *website*, rede social ou plataforma de encontros *online*.

É importante que o(a) profissional de apoio (TAV) se mantenha disponível para **auxiliar e/ou acompanhar** a vítima no processo de operacionalização das estratégias supra.

6. Apoio especializado a vítimas de burlas online

c. Estratégias de intervenção

ii. A quem e como reportar/denunciar

Burlas informáticas -Polícia Judiciária ou Ministério Público
Burlas simples- qualquer órgão de polícia criminal com competência genérica (PSP e GNR)
Burla qualificada - Polícia Judiciária.

Para todos os efeitos, o crime pode ser sempre **reportado ao Ministério Público**, seja qual for a sua natureza.

6. Apoio especializado a vítimas de burlas online

c. Estratégias de intervenção

ii. Orientações práticas para superar a vitimação e seus impactos

Aconselha-se a leitura do Módulo 5 relativamente à intervenção e apoio junto de vítimas de cibercrime e, para uma abordagem aprofundada desta matéria, a consulta do capítulo 2 - Parte II *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas.*

Sem prejuízo:

Estratégias de apoio emocional:

- Escutar empaticamente, demonstrando que está a escutar e a compreender o que está a ser dito e a valorizar as reações, emoções/sentimentos, comportamentos, pensamentos e significados atribuídos pela vítima à sua experiência de cibervitimação por burla *online*;
- Demonstrar que acredita naquilo que a vítima está a contar sobre o que lhe aconteceu, sem julgamentos ou juízos de valor;
- Normalizar as reações apresentadas, enquadrando/contextualizando as reações da vítima no contexto emocional da situação experienciada;
- Disponibilizar os serviços prestados, explicando como é que estes poderão ajudar a vítima.

6. Apoio especializado a vítimas de burlas online

c. Estratégias de intervenção

ii. Orientações práticas para superar a vitimação e seus impactos

Além dessas, **outras estratégias de apoio** devem ainda ser consideradas:

- Informar, de forma simples, sucinta e clara, transmitindo informação essencial à vítima sobre o que aconteceu e os passos seguintes a adotar, através de linguagem ajustada às características da vítima;
- Não promover expectativas irrealistas quanto ao papel do(a) profissional de apoio (TAV) e/ou quanto à resolução da situação;
- Não tomar decisões pela vítima e respeitar as suas escolhas;
- Informar acerca da possibilidade de revitimação, explorando possíveis cenários com que a vítima ainda se poderá deparar;
- Elaborar um plano de recuperação económica com a vítima, com o intuito de facultar estratégias à vítima para esta reestabelecer o controlo sobre a sua vida;
- Prevenir novos crimes, através da consciencialização da importância de adoção das estratégias de prevenção anteriormente descritas neste Módulo.

6. Apoio especializado a vítimas de burlas online

c. Estratégias de intervenção

ii. Orientações práticas para superar a vitimação e seus impactos

Relativamente às burlas nos relacionamentos amorosos, adicionalmente às estratégias supra, o(a) profissional deverá ainda:

- Recomendar o retomar progressivo de atividades, incluindo hábitos de utilização da Internet e TIC;
- Incentivar o reforço do envolvimento em atividades anteriormente apreciadas, nomeadamente as atividades *offline*;
- Mobilizar o suporte social e, caso seja vontade da vítima e com a sua autorização, envolver familiares e/ou amigos/as no processo de recuperação, solicitando o seu auxílio para a prevenção do evitamento e isolamento, por exemplo;
- Evitar a hiperproteção por familiares e amigos/as (sem negligenciar a segurança da vítima).

PLANO DE SESSÃO Nº 6

1. Identificação da Ação

Designação	Curso de Formação Apoio Especializado a Vítimas de Cibercrime		
Módulos/ temas	Apoio especializado a vítimas de burlas *online*		
Data da Sessão	**Horário**	**Duração da Sessão**	40 minutos
Formadores/as			

2. Objetivos Específicos

No final da sessão, os/as formandos/as deverão ser capazes de:

- Distinguir, corretamente, a natureza e *modi operandi* das burlas *online*, incluindo as burlas no comércio eletrónico, as burlas bancárias e as burlas nos relacionamentos íntimos;
- Enumerar, de forma correta, estratégias de intervenção propostas para o apoio especializado a vítimas de burlas *online*;
- Reconhecer, de forma correta, estratégias de prevenção da revitimação propostas para a intervenção junto de vítimas de burlas *online*.

3. Estrutura da Sessão

	Conteúdos Programáticos	Metodologia	Recursos Pedagógicos/ Didáticos	Avaliação | Exercícios	Tempo (minutos)
Introdução	Tipos de burlas *online*: • Burlas no comércio eletrónico • Burlas bancárias • Burlas nos relacionamentos íntimos	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	2
Desenvolvimento	*Modi operandi* e natureza dos crimes	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	10
	Estratégias de prevenção	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
	Estratégias de intervenção: • Estratégias para preservação de prova digital • A quem e como reportar/denunciar • Estratégias para superar a vitimação e seus impactos	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	15
Conclusão	Exercício n.º 3	Ativa	Regras do Exercício n.º 3 e Caso do Exercício n.º 3	Observação	5
	Síntese conclusiva e esclarecimento de questões	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	3

OBSERVAÇÕES

Destionatários/as:
Técnicos/as de Apoio à Vítima (TAV)

Data: / / **Formador(a):**

INSTRUÇÕES E INFORMAÇÕES ESSENCIAIS PARA O/A FORMADOR(A)

CORRESPONDÊNCIA DE CONTEÚDOS

Plano de Sessão	*Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*	
	PARTE	CAPÍTULO
Tipos de burlas *online*	Parte I - Compreender	Capítulo 1 – 1.3.
	Ver Apresentação e Enquadramento do Módulo	
Modi operandi e natureza dos crimes	Sem correspondência	
	Ver Apresentação e Enquadramento do Módulo	
Estratégias de prevenção	Sem correspondência	
	Ver Apresentação e Enquadramento do Módulo	
Estratégias de intervenção		
Estratégias para preservação de prova digital	Sem correspondência	
	Ver Apresentação e Enquadramento do Módulo	
A quem e como reportar/denunciar	Sem correspondência	
	Ver Apresentação e Enquadramento do Módulo	
Estratégias para superar a vitimação e seus impactos	Parte II - Proceder	Capítulo 2 – 2.1.
	Ver Apresentação e Enquadramento do Módulo	
Exercício n.º 3	Sem correspondência	
	Ver Regras do Exercício n.º 3	
Síntese conclusiva e esclarecimento de questões	Sem correspondência	

REGRAS DO EXERCÍCIO N.º 3

Módulo/Tema	Módulo 6- Apoio especializado a vítimas de burlas *online*	**CÓD. REF.**	**ÁREA DE EDUCAÇÃO E FORMAÇÃO**

Objetivos

Este exercício tem como objetivo consolidar a informação e conteúdo abordado neste Modulo, nomeadamente no que se refere à natureza dos crimes de burla online e às estratégias de prevenção da revitimaçao e de intervenção.

Execução

O/A formador[a] deve ler o Caso do Exercício n.º 3 [ou pedir a algum dos/as formandos/as presentes para ler em voz alta].

Sugerimos a distribuição deste Caso junto dos/as formandos/as ou a sua projeção no quadro, para leitura.

Depois da leitura, o/a formador[a] deverá apresentar ao grupo as questões que se seguem:

1. Que tipo de burla é identificável neste Caso?
2. Quais as consequências da vitimação evidenciadas pela vítima deste Caso?
3. O que deve o/a TAV contemplar na intervenção/apoio à vítima?

Durante a participação do grupo, deve o/a formador[a] ter presente as seguintes orientações relativamente às questões supra:

1. O relato da Lucinda enquadra-se numa situação de burla nos relacionamentos íntimos.
2. Na situação relatada pela Lucinda, são evidenciados sentimentos de culpa, de vergonha, de desconfiança face às intenções de outras pessoas e de isolamento/evitamento de interações/relações sociais, em linha com as consequências e reações manifestadas por vítimas de *romance scams*. É também evidente a resistência à denúncia, decorrente da existência de relação próxima [de amizade] com a autora da burla.
3. Alguns aspetos-chave na intervenção devem ser salientados: escutar empaticamente; demonstrar que acredita na situação relatada; enquadrar reações no contexto da situação experienciada pela vítima; recomendar o retomar de atividades e o envolvimento em atividades apreciadas [nomeadamente *offline*]; mobilizar pessoas da rede significativa [caso a vítima demonstre vontade nesse envolvimento]; prevenir novos crimes, através da transmissão de medidas de segurança/cibersegurança; apresentar as vantagens e desvantagens associadas à denúncia. Veja-se informação disponibilizada na Apresentação e Enquadramento do Módulo.

Notas

Consultar Apresentação e Enquadramento do Módulo

CASO DO EXERCÍCIO N.º 3

Lucinda, 55 anos, viúva, mãe de três filhos, todos maiores de idade. O mais novo tem 23 anos e saiu de casa o ano passado. Na primeira sessão de apoio, disse o seguinte:

"Eu sei que a culpa foi minha, a culpa foi toda minha, eu já não tenho idade para isto...Mas é que eu sinto-me tão sozinha desde que o meu filho mais novo saiu de casa...E esta minha amiga, ou aliás, achava eu que era minha amiga, a Adelaide... veio-me com esta história de que eu ainda sou nova, que podia arranjar alguém para me fazer companhia, que ela tinha uma colega de trabalho que também arranjou um namorado no Facebook. Ora, nem de propósito – achei eu, burra! –, uns dias depois tenho um pedido de amizade no Facebook de um senhor chamado José, muito bem-apresentado. Com 60 anos, divorciado já há muito, com os filhos já criados. Ele começou a falar comigo e tratava-me tão bem... Já não me davam atenção assim há tanto tempo... Senti que tinha outra vez 20 anos! Ele disse-me que vivia nos Estados Unidos, mas que estava a pensar voltar para Portugal. Eu acreditei em tudo, até vi passagens de avião para ir ter com ele... Enfim... Pouco tempo depois ele começa a dizer que um dos filhos dele estava muito doente e que ele precisava de mandar dinheiro para o filho. Só que ele não estava a conseguir fazer transferências dos Estados Unidos para Portugal - ele explicou-me porquê mas, sinceramente, eu nem liguei à explicação, pois eu só queria era poder ajudá-lo, logo numa coisa tão angustiante como a doença de um filho... - e pediu-me para ser eu a fazer estas transferências. E eu fui fazendo, fui fazendo...Transferi mais de 5 mil euros... E agora descubro que tudo isto foi um esquema da Adelaide...Nunca houve José nenhum... (choro...) Como é que pude ser tão burra?! Que vergonha... A culpa foi toda minha em querer ter alguém... Estou muito bem sozinha, não quero amigas, nem nada! Olhe, eu só queria ter o meu dinheiro de volta, mas não quero fazer queixa dela. Não consigo, não quero que nada de mal lhe aconteça, ela tem filhos pequenos sabe..."

MOD. 7

MOD. 7

PARTE 2 - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME
MÓDULO 7 - APOIO ESPECIALIZADO A VÍTIMAS DE FURTO DE IDENTIDADE *ONLINE*

APRESENTAÇÃO E ENQUADRAMENTO DO MÓDULO

O furto de identidade abrange a obtenção não consentida de dados pessoais e/ou secretos da vítima, a sua posse ou transferência com consciência de que serão utilizados para fins criminosos.

Estes atos correspondem a **furto de identidade *online*** quando os dados pessoais e/ou confidenciais da vítima são obtidos através da internet e/ou quando os dados obtidos, por qualquer meio, são transferidos através da internet e/ou utilizados para a prática de um crime pela internet.

Caso o crime se consubstancie apenas em uma das fases descritas, a conduta correspondente – obtenção, posse ou utilização – tem que ser praticada através da internet, para encaixar no conceito em foco.

Podemos identificar **três fases distintas**:

1. A fase da obtenção de dados pessoais [pela internet];
2. A fase de posse ou transferência dos dados [pela internet], sabendo que estes serão utilizados para a comissão de um crime;
3. A fase de utilização dos dados para a prática de crimes [pela internet].

Podem ser identificados **3 tipos de furto de identidade**:

- Crimes não relacionados diretamente com a vítima mas praticados em seu nome;
- Crimes que visam o enriquecimento do/a autor/a do crime ou de terceiros e que causam danos diretos à vítima;
- Crimes que visam a difamação da vítima.

Neste Módulo, exploraremos os *modi operandi* do furto de identidade *online*, bem como estratégias de prevenção e de intervenção que o/a formando/a, enquanto profissional de apoio (TAV), deverá considerar na prestação de apoio às vítimas deste tipo de cibercrime.

Modi operandi e natureza do crime

O furto de identidade não é, em si, um crime, pretendendo apenas descrever um fenómeno de obtenção não consentida de dados pessoais, tendo em vista o cometimento de uma atividade criminosa. Portanto, quando falamos de furto de identidade, podemos falar de uma multiplicidade de crimes previstos e punidos no Código Penal Português.

Este Módulo do Curso parte de um Exercício (Veja-se Plano de Sessão) para exemplificar os diferentes crimes legalmente previstos que podem ser enquadrados numa situação de furto de identidade *online*, tais como: crime de falsificação de documentos (art.º 256º, n.º1, al. a) do CP); crime de acesso ilegítimo (art. 6º, n.º1 da Lei do Cibercrime); crime de burla informática (art.º 221º, n.º1 do CP).

Relativamente aos *modi operandi* do crime de furto de identidade, podemos identificar dois métodos:

- Os **menos tecnológicos**, recorrendo à chamada **Engenharia Social** para obter informações pessoais das vítimas;
- Os **mais tecnológicos**, em que a interação com a vítima não é elemento fundamental para o cometimento deste crime.

Relativamente aos **métodos de Engenharia Social** como forma do cometimento do furto de identidade, poderão ser identificados os seguintes:

- Exploração do fator humano, enquanto elemento de vulnerabilidade para a cibersegurança;
- Ato de manipulação psicológica tendente a levar alguém a desenvolver determinada ação ou a divulgar informação confidencial;

Os **métodos menos tecnológicos** poderão ser mais fáceis de utilizar do que métodos mais tecnológicos (tais

como *malware* ou *hacking*), sobretudo para cibercriminosos/as com poucas competências técnicas para utilizar determinadas ferramentas e/ou sem recursos para as adquirir na *darkweb*.

Exemplos:

- *Vishing* (obter dados através de contactos telefónicos – cada vez mais, os/as cibercriminosos/as recorrem a *native speakers*);
- *Romance scams*;
- *Sextortion*;
- Aliciamento de menores online;
- Vasculhar no lixo;
- Intercetar correio;
- Furtar documentos que contenham informação pessoal ou financeira da vítima;
- Fazer-se passar por pessoa que possa pedir esse tipo de dados/informação;
- Obter informações junto de pessoas próximas da vítima;
- Contactar a vítima com falsos pretextos para obter informações privilegiadas;
- Comprar estas informações;
- Observar a vítima enquanto ela utiliza a informação a obter;
- Furto de *hardware* ou do telemóvel contendo informações pessoais ou secretas da vítima.

Quanto aos **métodos mais tecnológicos** para obtenção de dados pessoais, destaque para os seguintes:

1. **Furto de identidade através de *Phishing*:**

- Remessa massiva de mensagens de correio eletrónico com um atalho para uma página *web*;
- Vítima fornece ao/à autor(a) do crime, através do acesso à referida página *web*, informação pessoal/palavras-passe/códigos de acesso;
- Autor(a) do crime acede à verdadeira página da instituição bancária, introduzindo os dados da vítima e retirando dinheiro da conta;
- Branqueamento de capitais: processo pelo qual os/as autores(as) de algumas atividades criminosas encobrem a origem dos bens e rendimentos (vantagens) obtidos ilicitamente, transformando a liquidez proveniente dessas atividades em capitais reutilizáveis legalmente, por dissimulação da origem ou do verdadeiro proprietário dos fundos.

2. **Furto de identidade através do uso de Malware:**

- *Malware, software* que pode ser disseminado de várias formas, para permitir a infiltração ilícita em equipamentos, computadores e redes, com o propósito de furtar informação, alterar informação ou causar danos:
  - Através de *link* ou ficheiro recebido via *e-mail*;
  - No *download* de filmes ou jogos;
  - No acesso a *websites* comprometidos;
  - Com a instalação de *apps* comprometidas, etc.

Um exemplo de **furto de identidade que combina métodos de Engenharia Social e métodos tecnológicos** é o ***Spear Phishing***: criação de *e-mails* de *phishing* usando técnicas de Engenharia Social para personalizar mensagens e websites em função do/a destinatário/a, amentando a credibilidade da informação e ludibriando a vítima para aceder a informação privilegiada.

Nas situações mais comuns de furto de identidade *online*, é possível identificar:

1. *Phishing* para obtenção de acesso à conta de *e-mail*:

- Uma vez obtidos os dados pessoais e confidenciais da vítima, através de qualquer um dos métodos mais sofisticados mencionados anteriormente, o/a criminoso/a informático poderá obter acesso à conta de *e-mail* da vítima, com o objetivo de tomar conhecimento do conteúdo da caixa de correio, de estabelecer contacto com o banco da vítima - normalmente

com o/a gestor(a) de conta – para efetuar operações bancárias ou utilizar aquela conta de *e-mail* para credibilizar as mensagens de correio eletrónico que pretende enviar e que serão, normalmente, pedidos de ajuda financeira.

2. *Phishing* para obtenção de acesso à conta bancária:

- Envio em massa de mensagens de correio eletrónico (*spamming*);
- As mensagens contêm um *link* para uma página falsa de uma entidade bancária;
- Na página falsa, é solicitado o preenchimento/envio de dados confidenciais.

3. Difamação nas redes sociais:

- Existem situações de furto de identidade que visam a difamação da vítima numa rede social, ocorrendo geralmente no âmbito das relações de amizade ou namoro:
  - Criação de perfil falso;
  - Utilização do perfil verdadeiro da vítima, utilizando as suas credenciais de acesso:
    - A própria vítima fornece dados ao/à criminoso/a;
    - O/A criminoso/a obtém esses dados através de outros meios.

Estratégias de prevenção

Para **prevenir o furto de identidade *online***, neste ponto do Módulo, o/a formador(a) deve transmitir aos/às formandos/as as seguintes estratégias que estes/as, enquanto profissionais de apoio (TAV), poderão utilizar na intervenção com a vítima apoiada:

- Configuração de antivírus e programas de anti-*malware* nos dispositivos e configuração dos mesmos para realizarem análises regulares;
- Ativação de filtros de *spam*;
- Proteger os dispositivos, através da utilização de métodos de autenticação que usem dados biométricos ou, em alternativa, códigos de bloqueio e instalação de *software* antivírus nos dispositivos;
- Verificar e reconhecer websites seguros (Veja-se informação no Módulo 6 sobre este assunto);
- Não fornecer informação pessoal ou dados pessoais requeridos através de *e-mails*, mensagens, chamadas, *websites* não solicitados;
- Verificar o nome do remetente do *e-mail* – gralhas ou outro tipo de erros significam que o remetente do *e-mail* não é/representa quem diz ser;
- Verificar erros ortográficos que indiciem que a língua em que a pessoa está a comunicar não é a sua língua nativa.

Estratégias de intervenção

Estratégias para preservação de prova digital

Ainda neste Módulo, deverá o/a formador(a) apresentar junto dos/as formandos/as estratégias que podem ser explicadas às vítimas em processo de apoio, para a preservação da prova. Uma vez que o furto de identidade pode ter como objetivo uma multiplicidade de fins criminosos, apresentam-se, em seguida, algumas estratégias genéricas:

- Salvaguardar a prova em redes sociais, através da cópia do URL dos conteúdos ilegais e de capturas de ecrã desses conteúdos (Consultar Módulo 10, para informação adicional sobre a cópia do URL);
- Havendo transferências patrimoniais, guardar registos de tais transferências e contactar a entidade bancária;
- Apresentar queixa-crime junto das autoridades competentes;
- Solicitar apoio junto de estruturas de apoio à vítima, para lidar com o sofrimento emocional causado pela situação de vitimação e garantir acompanhamento ao longo do processo-crime.

É importante que o/a profissional de apoio (TAV) se mantenha disponível para **auxiliar e/ou acompanhar** a vítima no processo de operacionalização das estratégias supra.

A quem e como reportar/denunciar

O furto de identidade não constitui um crime em si. Contudo, poderá ser um meio para a prática de uma multiplicidade de crimes previstos e punidos no Código Penal Português e na Lei do Cibercrime. Nestes casos, os factos devem ser reportados junto de qualquer órgão de polícia criminal com competência genérica (PSP e GNR), junto da Polícia Judiciária ou do Ministério Público, consoante o crime em que se traduzir. Para todos os efeitos, o crime pode ser sempre reportado ao Ministério Público seja qual for a sua natureza.

Estratégias para superar a vitimação e seus impactos

O furto de identidade implica, para a vítima, um sério transtorno e muito tempo despendido para reparar as consequências do crime. Para além do **dispêndio de tempo**, consequência frequentemente apontada pelas vítimas, o **impacto emocional** do furto de identidade é descrito como sendo semelhante às reações das vítimas de crimes violentos. Muitas vítimas sentem a sua privacidade violada, sentem-se desamparadas, impotentes, receosas de que o crime se repita e desconfiadas quanto às intenções das pessoas em seu redor. Se o furto de identidade da vítima for utilizado para a difamação nas redes sociais, o impacto que a **publicitação/audiência** adiciona ao crime praticado exacerba sintomas de mal-estar emocional e psicológico.

Sem prejuízo das orientações centrais para a intervenção abordadas no Módulo 4 deste Curso de Formação, consideram-se particularmente prementes, no caso do apoio a vítimas de furto de identidade *online*, as **estratégias de apoio** seguidamente apresentadas:

- Prestar apoio emocional à vítima, escutando, validando a sua experiência e normalizando/enquadrando reações;
- Explicar à vítima que existem outras pessoas a viver situações semelhantes à sua, quebrando a noção de "caso único";
- Informar, de forma simples, sucinta e clara, transmitindo informação essencial à vítima sobre o que aconteceu e os passos seguintes a adotar, através de linguagem ajustada às características da vítima;
- Explicar os vários tipos de apoio prestados de que pode usufruir, transmitindo a mensagem de que a vítima não está sozinha ao longo deste processo;
- Não promover expectativas irrealistas quanto à resolução da situação;
- Explicar à vítima que, devido à própria natureza das situações de furto de identidade, pode haver lugar à prática de outros crimes contra si, reforçando a disponibilidade para apoiar;
- Prevenir novos crimes, através da consciencialização para a importância de adoção das estratégias de prevenção anteriormente descritas neste Módulo.

Sempre que possível, a apresentação destas estratégias (bem como das seguintes) deve ser acompanhada por exemplos concretos da sua operacionalização, procurando familiarizar os/as formandos/as com a linguagem e forma de comunicação a utilizar com a vítima ao longo do apoio/atendimento. Tais exemplos estão disponíveis no suporte visual (*PowerPoint*).

As vítimas de furto de identidade podem apresentar **relutância em denunciar às autoridades policiais o crime** de que foram alvo, sobretudo no caso de terem descoberto que o/a autor(a) é alguém próximo e em quem confiavam, como um(a) familiar ou amigo/a. Nestes casos, para além das estratégias supra, é importante que o/a profissional de apoio (TAV):

- Reforce a coragem na procura de apoio e na revelação da experiência pessoal de cibervitimação;
- Auxilie a vítima no processo de decisão quanto à denúncia (sem tomar decisões em nome da vítima e/ou a influenciar no processo), demonstrando-lhe as vantagens e desvantagens de cada opção, tendo em vista a tomada de decisões informadas;
- Transmita informação essencial à vítima sobre os seus direitos após a apresentação de queixa, reafirmando que o apoio é independente da mesma.

Por vezes, as vítimas de furto de identidade *online* sentem-se **injustiçadas**, com a necessidade de provarem a sua inocência ou **desiludidas/frustradas** com o resultado do processo criminal. O/A profissional de apoio (TAV) deverá estar consciente da existência deste tipo de pensamentos e atuar sobre eles:

- Reforçar que acredita no relato da vítima;
- Validar a experiência e reconhecer os efeitos causados pela situação de vitimação aos mais diversos níveis (psicologicamente e emocionalmente, socialmente e em outros domínios impactados);
- Valorizar tentativas prévias de proteção/resolução;
- Prevenir a culpabilização;
- Sugerir a partilha de sentimentos e receios com aqueles/as em quem confia, recomendando aos últimos que mantenham uma posição de disponibilidade para a escuta, sem pressionarem à partilha;
- Explicar que a recuperação da vitimação é independente do desfecho do processo-crime;
- Disponibilizar o apoio psicológico.

Apoio Especializado a Vítimas de Cibercrime

PARTE II - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME

Módulo 7 - Apoio especializado a vítimas de furto de identidade online

Furto de identidade

O furto de identidade abrange a obtenção não consentida dos dados pessoais e/ou secretos da vítima, a sua posse ou transferência com consciência de que serão utilizados para fins criminosos e a sua utilização para a prática de crimes.

Quando obtidos através da internet, trata-se da modalidade **online do crime**

- Podemos identificar **três fases distintas**:
- A fase da obtenção de dados pessoais [pela internet];
- A fase de posse ou transferência dos dados [pela internet], sabendo que estes serão utilizados para a comissão de um crime;
- A fase de utilização dos dados para a prática de crimes [pela internet].

a. Tipos e Modi operandi

Furto de identidade

Podem ser identificados **3 tipos de furto de identidade**:

- Crimes não relacionados diretamente com a vítima mas praticados em seu nome;
- Crimes que visam o enriquecimento do(a) autor(a) do crime ou de terceiros e que causam danos diretos à vítima;
- Crimes que visam a difamação da vítima.

a. Modi operandi

Relativamente aos *modi operandi* do crime de furto de identidade, podemos identificar dois métodos:

- Os **menos tecnológicos**, recorrendo à chamada **Engenharia Social** para obter informações pessoas das vítimas;
- Os **mais tecnológicos**, em que a interação com a vítima não é o elemento fundamental para o cometimento deste crime.

Relativamente a **métodos de Engenharia** Social como forma do cometimento do furto de identidade, poderão ser identificadas duas formas:

- Exploração do fator humano, enquanto elo mais fraco da cibersegurança;
- Ato de manipulação psicológica tendente a levar alguém a desenvolver determinada ação ou a divulgar informação confidencial;

a. Modi operandi

Os **métodos menos tecnológicos** poderão ser mais fáceis de utilizar do que métodos mais tecnológicos (tais como *malware* ou *hacking*) sobretudo para cibercriminosos(as) com poucas competências técnicas para utilizar determinadas ferramentas e/ou sem recursos para as adquirir na *darkweb*.

Exemplos:
Vishing (obter dados através de contactos telefónicos – cada vez mais, os/as cibercriminosos(as) recorrem a *native speakers*);
Romance scams; *Sextortion*;
Aliciamento de menores *online*;
Vasculhar no lixo;
Intercetar correio;
Furtar documentos que contenham informação pessoal ou financeira da vítima;
Fazer-se passar por pessoa que possa pedir esse tipo de dados/informação;
Obter informações junto de pessoas próximas da vítima;
Contactar a vítima com falsos pretextos para obter informações privilegiadas;
Comprar estas informações;
Observar a vítima enquanto ela utiliza a informação a obter;
Furto de *hardware* ou do telemóvel contendo informações pessoais ou secretas da vítima.

a. Modi operandi

Quanto aos **métodos mais tecnológicos** para obtenção de dados pessoais, destaque para os seguintes:

Furto de identidade através de *Phishing*:

- Remessa massiva de mensagens de correio eletrónico com um atalho para uma página *web*;
- Vítima fornece ao(à) autor(a) do crime, através do acesso à referida página, informação pessoal/palavras-passe/códigos de acesso;
- Autor(a) do crime acede à verdadeira página da instituição bancária, introduzindo os dados da vítima e retirando dinheiro da conta;
- Branqueamento de capitais: processo pelo qual os/as autores(as) de algumas atividades criminosas encobrem a origem dos bens e rendimentos (vantagens) obtidos ilicitamente, transformando a liquidez proveniente dessas atividades em capitais reutilizáveis legalmente, por dissimulação da origem ou do verdadeiro proprietário dos fundos.

a. Modi operandi

Ainda quanto aos **métodos mais tecnológicos** para obtenção de dados pessoais:

Furto de identidade através do uso de *Malware*:
- *Malware*, *software* no qual se incluem os vírus, *worms* e *spywares,* pode se disseminado de várias formas, para permitir a infiltração ilícita em equipamentos, computadores e redes, com o propósito de furtar informação, alterar informação ou causar danos:
- *Link* ou ficheiro recebido via *e-mail*;
- Clicando no *download* de filmes ou jogos;
- Acesso a *websites* comprometidos;
- Instalação de *apps* comprometidas, etc.

Um exemplo de **furto de identidade que combina métodos de Engenharia Social e métodos tecnológicos** é o ***Spear Phishing***: criação de *e-mails* de *phishing* usando técnicas de Engenharia Social para personalizar mensagens e websites em função do(a) destinatário(a), amentando a credibilidade da informação e ludibriando a vítima para aceder a informação privilegiada.

a. Modi operandi

Situações mais comuns de furto de identidade online:

***1) Phishing* para obtenção de acesso à conta de *e-mail*:**
Uma vez obtidos os dados pessoais e confidenciais da vítima, através de qualquer um dos métodos mencionados anteriormente, o/a criminoso/a acede à conta de *e-mail* da vítima com o objetivo de estabelecer contacto com o banco da vítima - normalmente com o/a gestor(a) de conta – para efetuar operações bancárias ou de utilizar aquela conta de *e-mail* para credibilizar as mensagens de correio eletrónico que pretende enviar e que serão, normalmente, pedidos de ajuda financeira.

***2) Phishing* para obtenção de acesso à conta bancária:**
Através do envio em massa de mensagens de correio eletrónico (*spamming*). Estas mensagens contêm um *link* para uma página falsa de uma entidade bancária. Na página falsa, é solicitado o preenchimento/envio de dados confidenciais.

a. Modi operandi

Situações mais comuns de furto de identidade online:

3) Difamação nas redes sociais:

Existem ainda duas possibilidades de furto de identidade, visando a difamação da vítima numa rede social, ocorrendo geralmente no âmbito das relações de amizade ou namoro:

- Criação de perfil falso;
- Utilização do perfil verdadeiro da vítima, utilizando as suas credenciais de acesso:
  - A própria vítima fornece dados ao/à criminoso/a;
  - Criminoso/a obteve esses dados através de outros meios.

b. Estratégias de prevenção

- Configuração de antivírus e programas de anti-*malware* nos dispositivos e configuração dos mesmos para realizarem análises regulares;
- Ativação de filtros de *spam*;
- Proteger os dispositivos, através da utilização de métodos de autenticação que usem dados biométricos ou, em alternativa, códigos de bloqueio e instalação de *software* antivírus nos dispositivos;
- Verificar e reconhecer *websites* seguros:
  - O *website* deverá apresentar o símbolo de um cadeado, no lado esquerdo, imediatamente antes do endereço do *website*;
  - O URL do *website* deve conter o certificado - 'https://'; contendo o 's' de "seguro" acrescentado ao 'http', devendo sempre verificar-se o URL dos websites, nomeadamente quando os endereços são partilhados por mensagem ou *e-mail*;
- Não fornecer informação pessoal ou dados pessoais pedidos através de *e-mails*, mensagens, chamadas, *websites* não solicitados;
- Verificar o nome do remetente do *e-mail* – gralhas ou outro tipo de erros significam que o remetente do *e-mail* não é/representa quem diz ser;
- Verificar erros ortográficos que indiciem que a língua em que a pessoa está a comunicar não é a sua língua nativa.

b. Estratégias de intervenção

i. Preservação da prova digital

- Salvaguardar a prova em redes sociais, através da cópia do URL dos conteúdos ilegais e de capturas de ecrã desses conteúdos;
- Havendo transferências patrimoniais, guardar registos de tais transferências e contactar a entidade bancária;
- Apresentar queixa-crime junto das autoridades competentes;
- Solicitar apoio junto de estruturas de apoio à vítima, para lidar com o sofrimento emocional causado pela situação de vitimação e garantir acompanhamento ao longo do processo-crime.

Importante o auxílio e acompanhamento do(a) TAV.

b. Estratégias de intervenção

ii. A quem e como reportar/denunciar

O furto de identidade <u>não constitui um crime em si</u>. Contudo, poderá ser um meio para a prática de uma <u>multiplicidade de crimes</u> previstos e punidos no Código Penal Português e na Lei do Cibercrime.

Factos devem ser reportados junto de:
- Qualquer órgão de polícia criminal com competência genérica (PSP e GNR);
- Polícia Judiciária;

<u>Consoante o crime em que se traduzir, **OU**</u>

- Ministério Público (sempre competente independentemente da natureza do crime).

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

Estratégias de apoio: (Sem prejuízo das orientações gerais para a intervenção - Módulo 5)

- Prestar apoio emocional à vítima, escutando, validando a sua experiência e normalizando reações;
- Elucidar a vítima acerca das possíveis reações emocionais com que esta se poderá deparar, normalizando-as;
- Explicar à vítima que existem outras pessoas a viver situações semelhantes à sua, quebrando a noção de "caso único";
- Informar, de forma simples, sucinta e clara, transmitindo informação essencial à vítima sobre o que aconteceu e os passos seguintes a adotar, através de linguagem ajustada às características da vítima;
- Explicar os vários tipos de apoio prestado de que pode usufruir, transmitindo a mensagem de que a vítima não está sozinha ao longo deste processo;
- Não promover expectativas irrealistas quanto à resolução da situação;
- Explicar à vítima que, devido à própria natureza das situações de furto de identidade, pode haver lugar à prática de outros crimes si, reforçando a disponibilidade para apoiar;
- Prevenir novos crimes, através da consciencialização da importância de adoção das estratégias de prevenção anteriormente descritas neste Módulo.

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

As vítimas de furto de identidade podem apresentar **relutância em denunciar às autoridades policiais o crime** de que foram alvo, sobretudo no caso de terem descoberto que o(a) autor(a) é alguém próximo e em quem confiavam, como um(a) familiar ou amigo(a).

Nestes casos, para além das estratégias supra, **é importante que o(a) TAV:**

- Reforce a coragem na procura de apoio e na revelação da experiência pessoal de cibervitimação;
- Auxilie a vítima no processo de decisão quanto à denúncia (sem tomar decisões em nome da vítima e/ou a influenciar no processo), demonstrando-lhe as vantagens e desvantagens de cada opção, tendo em vista a tomada de decisões informadas.
- Transmita informação essencial à vítima sobre os seus direitos após a apresentação de queixa, reafirmando que o apoio é independente da mesma.

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

Por vezes, as vítimas de furto de identidade *online* sentem-se **injustiçadas,** com a necessidade de provarem a sua inocência ou **desiludidas/frustradas** com o resultado do processo criminal.

O(a) TAV deverá estar **consciente** da existência deste tipo de pensamentos **e atuar** sobre eles:

- Reforçar que acredita no relato da vítima;
- Validar a experiência e reconhecer os efeitos causados pela situação de vitimação aos mais diversos níveis (psicologicamente e emocionalmente, socialmente e em outros domínios impactados)
- Valorizar tentativas prévias de proteção/resolução;
- Prevenir a culpabilização;
- Sugerir a partilha de sentimentos e receios com aqueles/as em quem confia, recomendando aos últimos que mantenham uma posição de disponibilidade para a escuta, sem pressionarem à partilha;
- Explicar que a recuperação da vitimação é independente do desfecho do processo-crime;
- Disponibilizar o apoio psicológico.

PLANO DE SESSÃO Nº 7

1. Identificação da Ação

Designação Curso de Formação Apoio Especializado a Vítimas de Cibercrime

Módulos/ temas Apoio especializado a vítimas de furto de identidade *online*

Data da Sessão **Horário** **Duração da Sessão** 40 minutos

Formadores/as

2. Objetivos Específicos

No final da sessão, os/as formandos/as deverão ser capazes de:

- Distinguir, corretamente, a natureza e *modi operandi* do furto de identidade *online*;
- Enumerar, de forma correta, estratégias de intervenção propostas para o apoio especializado a vítimas de furto de identidade *online*;
- Reconhecer, de forma correta, estratégias de prevenção da revitimação propostas para a intervenção junto de vítimas de furto de identidade *online*.

3. Estrutura da Sessão

	Conteúdos Programáticos	Metodologia	Recursos Pedagógicos/ Didáticos	Avaliação | Exercícios	Tempo (minutos)
Introdução	Exercício n.º 4	Ativa	Regras do Exercício n.º 4 e Caso do Exercício n.º 4	Observação	5
Desenvolvimento	*Modi operandi* e natureza do crime	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	10
	Estratégias de prevenção	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
	Estratégias de intervenção: • Estratégias para preservação de prova digital • A quem e como reportar/denunciar • Estratégias para superar a vitimação e seus impactos	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	15
Conclusão	Síntese conclusiva e esclarecimento de questões	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5

OBSERVAÇÕES

Destionatários/as:
Técnicos/as de Apoio à Vítima (TAV)

Data: / / **Formador(a):**

INSTRUÇÕES E INFORMAÇÕES ESSENCIAIS PARA O/A FORMADOR(A)

CORRESPONDÊNCIA DE CONTEÚDOS

Plano de Sessão	*Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*	
	PARTE	CAPÍTULO
Exercício n.º 4	Sem correspondência Ver Regras do Exercício n.º 4	
Modi operandi e natureza do crime	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Estratégias de prevenção	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Estratégias de intervenção		
Estratégias para preservação de prova digital	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
A quem e como reportar/denunciar	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Estratégias para superar a vitimação e seus impactos	Parte II - Proceder Ver Apresentação e Enquadramento do Módulo	Capítulo 2 – 2.1.
Síntese conclusiva e esclarecimento de questões	Sem correspondência	

REGRAS DO EXERCÍCIO N.º 4

Módulo/Tema	Apoio especializado a vítimas de furto de identidade *online*	**CÓD. REF.**	**ÁREA DE EDUCAÇÃO E FORMAÇÃO**

Objetivos

Este exercício tem como objetivo sensibilizar para as particularidades das situações de furto de identidade online e para a natureza deste fenómeno, alertando nomeadamente para a multiplicidade de crimes que podem ser praticados no seu âmbito.

Execução

O/A formador(a) deve ler o Caso do Exercício n.º 4 (ou pedir a algum dos/as formandos/as presentes para ler em voz alta).

Sugerimos a distribuição deste Caso junto dos/as formandos/as ou a sua projeção no quadro, para leitura.

Depois da leitura, o/a formador(a) deverá questionar o grupo sobre os crimes presentes neste Caso.

Durante a participação do grupo, deve o/a formador(a) remeter para *O enquadramento jurídico do cibercrime a nível nacional* (Veja-se Módulo 2) e concretizar que, neste Caso, são vários os crimes identificáveis:

- A conduta de criação de e-mail falso, corresponde o crime de falsificação de documentos (art.º 256º, n.º1, al. A) do CP);
- A conduta de acesso à conta de e-mail da mulher de Júlio, corresponde o crime de acesso ilegítimo (art. 6º, n.º1 da Lei do Cibercrime);
- Corresponde ao crime de burla informática (art.º 221º, n.º1 do CP), na sua forma tentada, as tentativas de obtenção de crédito em nome de Júlio.

Notas

Consultar Apresentação e Enquadramento do Módulo

CASO DO EXERCÍCIO N.º 4

Foram enviadas mensagens para vários endereços de *e-mail* que aparentavam ser do serviço de *webmail* utilizado e que pediam a atualização da palavra-passe.

A mulher de Júlio introduziu os seus dados e, desse modo, o/a criminoso/a teve acesso à sua conta de *e-mail*, ficando a conhecer inúmeros dos seus dados pessoais, assim como da sua família. Júlio foi posteriormente contactado por duas companhias de crédito que pretendiam confirmar se as candidaturas à obtenção de crédito em seu nome eram legítimas. Júlio, que nunca tinha recorrido ao crédito, esclareceu que não se havia candidatado junto de qualquer das empresas. Ficou abismado com a quantidade de dados pessoais seus que o/a criminoso/a conhecia. As candidaturas foram declinadas. Um mês depois, Júlio dirigiu-se ao seu Banco, pretendendo contrair um empréstimo para compra de uma nova habitação. O empréstimo foi recusado, devido às muitas candidaturas à obtenção de crédito realizadas em seu nome nos últimos meses.

MOD. 8

MOD. 8

PARTE 2 - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME
MÓDULO 8 - APOIO ESPECIALIZADO A CRIANÇAS E JOVENS VÍTIMAS DE ABUSO SEXUAL *ONLINE*

APRESENTAÇÃO E ENQUADRAMENTO DO MÓDULO

Neste Módulo, serão exploradas diferentes formas de expressão do abuso sexual de crianças e jovens *online*.

O conceito de abuso sexual *online* é abrangente e contempla **qualquer forma de abuso sexual de crianças em contexto *online***. Inclui, por isso mesmo, diferentes manifestações de abuso e exploração, desde o abuso sexual sem contacto, facilitado pelas TIC e pela internet, redes sociais ou outras plataformas, como o assédio e o aliciamento (*grooming online*), até à partilha de conteúdos na *darkweb* (imagem e/ou áudio) de abuso e exploração sexual de crianças, previamente recolhidos em fotografia ou vídeo.

Particular destaque será dado à compreensão dos fenómenos de **aliciamento** (*grooming online*) e de **disseminação de conteúdos de abuso sexual de crianças *online***.

A quantidade de conteúdos de abuso e de exploração sexual de crianças (CSAM) a ser disseminado *online* continua a aumentar, tendência corroborada pelas autoridades policiais e pelas organizações não-governamentais que se dedicam à análise e reporte de conteúdo de abuso sexual *online*. A disseminação desse conteúdo tem um sério impacto nas vítimas, que sofrem processos de revitimação, de cada vez que as suas fotos ou vídeos são visualizados e/ou compartilhados.

O modo de disseminação deste material continua a ser através das/de Redes "*peer-to-peer*" (P2P) e acesso anónimo, como navegadores de acesso à *Darknet* (por exemplo, Tor).

Paralelamente, tem-se verificado um aumento contínuo na distribuição de CSAM via redes sociais. A dificuldade de salvaguardar a prova em algumas destas redes torna particularmente difícil a investigação por parte das autoridades. Casos existem em que tais conteúdos/materiais são partilhados pelas próprias crianças, sendo depois compartilhados com colegas que, por sua vez, partilham com outros pares até que, eventualmente, esses conteúdos/materiais acabam em plataformas de distribuição de CSAM. Em muitos casos, os/as infratores/as que distribuem CSAM *online* também estão envolvidos em situações de abuso sexual de crianças. A elevada procura por este tipo de material perpetua o abuso e a vitimação contínua de crianças.

Legalmente, em Portugal, as situações de CSAM estão enquadradas no crime de pornografia infantil.

A nível internacional, tem sido defendido o abandono do conceito de "pornografia infantil", já que este (isto é, pessoas adultas envolvidas, de forma consensual, em comportamento erótico em imagens, vídeo e/ou escrita, destinado a causar excitação sexual) não traduz o que está subjacente às situações de abuso sexual de crianças. Por este motivo, é defendido que, quando nos referimos a material de "pornografia infantil", seja utilizada a terminologia "Conteúdo de Abuso Sexual de Menores".

Além destes fenómenos, também o *grooming online* merece especial atenção. Para o efeito, exploraremos os *modi operandi* subjacentes ao *grooming online* nas redes sociais e nos jogos *online*, considerando que estas plataformas ocupam uma dimensão considerável do tempo de utilização da internet e das TIC por parte das crianças e jovens.

Em todo o caso, além da leitura do conteúdo do presente Módulo, sugerimos ainda ao/à formador(a) a consulta do capítulo 1 – Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*.

Tipos, modi operandi e natureza dos crimes

Disseminação de conteúdos de abuso sexual de crianças [CSAM]

Conteúdos de abuso sexual de crianças gerados online

Atualmente, são dois os modos que têm vindo a ganhar destaque, enquanto meios de disseminação de conteúdo de abuso sexual de menores online:

- Conteúdo auto produzido/auto gerado pelos menores;
- A procura de sessões de *live-streaming* de abuso sexual de menores.

Auto produção de conteúdos

O acesso crescente e em idades mais precoces por parte de crianças e jovens a *smartphones* e outros dispositivos, aliado à reduzida perceção do risco relativamente à partilha de conteúdos íntimos, têm estado associados à emergência de situações de auto produção de conteúdos íntimos.

Uma distinção deverá ser realizada entre o **conteúdo íntimo que é (auto)produzido voluntariamente** pela criança ou jovem e o **conteúdo íntimo (auto)produzido sob coação ou extorsão** por parte de outra pessoa:

- A respeito da primeira categoria, há um crescente número de crianças e jovens que partilham fotos ou vídeos, através de redes sociais ou de plataformas de *chat*, com outros pares e amigos/as, tornando-se, por isso, mais vulneráveis a situações de abuso e exploração sexual *online*, tais como o aliciamento (*grooming online*) realizado por pessoas adultas que se fazem passar por pares.

  A este nível, poderemos referir, a título de exemplo, o *sexting*, enquanto forma de auto produção de conteúdos - texto, imagens e/ou vídeos - de natureza sexual e sua partilha, habitualmente de forma consentida e entre pares.

  Apesar de esta produção e partilha ser voluntária, pode precipitar situações subsequentes de extorsão, aliciamento e outras formas de abuso sexual *online*

- Igualmente, os conteúdos auto produzidos podem ser, numa primeira linha, partilhados entre pares, mas eventualmente em redes de abuso sexual *online*. Tais casos podem, subsequentemente, expor as crianças e jovens a situações de coação ou extorsão por parte de terceiros que, recorrendo a ameaça e/ou chantagem, procuram coagir as crianças à (auto)produção de conteúdos sexuais adicionais.

Transmissão em direto de abuso sexual de crianças

Com a melhoria das infraestruturas e da velocidade da conexão à internet, registou-se um aumento da procura de **sessões de *live-streaming* de abuso sexual de crianças**: assistir a conteúdos de abuso sexual de menores em direto.

Estas situações são comuns em países já conotados como locais de destino de turismo sexual para abuso de menores. Estes canais de *streaming* são pagos, sendo, muitas vezes, publicitados em *websites* pornográficos para pessoas adultas. Uma vez encontrado esse serviço/canal de *streaming*, os/as utilizadores/as são direcionados para plataformas encriptadas que permitem a videoconferência. Muitas vezes, aos/às agressores/as que usufruem destes serviços/canais de *streaming* é dada a possibilidade de fornecerem instruções sobre o modo como pretendem que o abuso sexual dos/as menores seja praticado, em tempo real. Os/as utilizadores/as que procuram este tipo de conteúdo podem ainda viajar para os países onde as sessões de *live streaming* decorrem para a prática de abuso sexual, desta feita presencialmente.

Aliciamento [grooming online]

O ***grooming online*** pode ser definido como um **processo de manipulação** e uma **forma de aliciamento** de crianças e jovens. Inicia-se geralmente através de uma abordagem não-sexual, nomeadamente através da internet e das TIC, incluindo jogos *online* e redes sociais, de forma a estabelecer uma relação de confiança com a criança e a convencê-la a encontrar-se pessoalmente com outra pessoa, para que esta última possa consumar o abuso sexual. O estabelecimento de relação de confiança com a criança, mediado pela internet e pelas TIC, pode ainda visar a **persuasão da criança à produção e partilha de conteúdo sexual**.

O *grooming online* permite aos/às autores/as a seleção do tipo de vítima que pretendem manipular e aliciar, podendo escolher especificamente pela idade e/ou pela aparência física. Adicionalmente, o *grooming online* permite o aliciamento de um grande número de vítimas em simultâneo, entre outras vantagens para o/a autor(a) do processo de manipulação e aliciamento *online*, como a possibilidade de "desaparecer", mudando a sua identidade, caso a vítima recuse ou ignore os avanços, reaparecendo com outra identidade, de forma a aproximar-se da mesma vítima, sabendo, desta vez, um pouco mais sobre os seus limites e preferências.

Aliciamento nas redes sociais e em jogos de vídeo online

A abordagem dos meios de aliciamento de crianças e jovens *online* inicia com a apresentação de informação relativa à crescente utilização de plataformas de *online gaming* (Veja-se *PowerPoint*).

Os/as agressores/as aproveitam-se do anonimato providenciado pelas plataformas de videojogos *online* e da reduzida sensibilização das crianças e jovens (consumidores/as destas plataformas) quanto aos riscos online para a prática de processos de aliciamento e manipulação.

Para o efeito, utilizam as plataformas de jogos online para ganhar a confiança destas crianças e jovens e, posteriormente, convencem os alvos à utilização de outras plataformas *online* de comunicação – *Messenger* do *Facebook*®, *Instagram*®, *WhatsApp*®, *Viber*®, *Telegram*®, *Snapchat*®, etc. - para manterem a comunicação e relação com estas crianças e jovens e, desta forma, as aliciarem para fins sexuais.

O surgimento de casos de *grooming online* neste contexto motivou as plataformas de jogos *online* à criação de medidas de prevenção do *grooming online*, incluindo através de políticas de segurança e guias específicos para crianças e famílias.

Estratégias de prevenção

Para **prevenir situações de abuso sexual *online***, neste ponto do Módulo, o/a formador(a) deve transmitir aos/às formandos/as as seguintes estratégias que estes/as, enquanto profissionais de apoio (TAV), poderão utilizar na intervenção com a criança/jovem vítima e a sua família:

- Sensibilizar para a importância da educação da criança ou jovem para uma utilização segura e consciente da internet e das TIC e para a identificação de situações e contextos de risco *online*;
- Sensibilizar para a definição de regras claras de utilização da internet e TIC: por exemplo, colocar videojogos/computador numa área comum da casa e/ou permitir a utilização de dispositivos móveis/eletrónicos apenas em espaços comuns da habitação;
- Reforçar a importância do acompanhamento ou supervisão do comportamento *online* da criança ou jovem a cargo: nomeadamente se recebe chamadas de números desconhecidos, se passa muito tempo *online* e até muito tarde, se demonstra um súbito isolamento relativamente à família e amigos/as, bem como o tipo de pedidos de amizade rececionados e sua origem;
- Configurar, em conjunto com as crianças e jovens a cargo, as definições de privacidade de redes sociais e páginas/perfis, eliminando informação pessoal ou outra que possa identificar a morada de casa, escola, número de telemóvel, etc.;

A **família** desempenha um papel muito importante na proteção de crianças e jovens face aos riscos da utilização da internet e das TIC. Podem encontrar informação sobre a importância da família na prevenção do cibercrime contra crianças e jovens no capítulo 4 - Parte II do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*. Igualmente, o envolvimento da família no apoio e intervenção junto de crianças e jovens vítimas de cibercrime é importante, inclusivamente na educação da criança ou jovem vítima para uma utilização consciente e segura da internet e das TIC. Veja-se capítulo 2 – Parte II do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*.

Estratégias de intervenção

Estratégias para preservação de prova digital

Ainda neste Módulo, para além da abordagem às dinâmicas e *modi operandi* de diferentes formas de abuso sexual de crianças e jovens online e da apresentação de medidas de prevenção da revitimação supra, o/a o formador(a) deve apresentar junto dos/as formandos/as estratégias que podem ser explicadas à criança e jovem vítima (e suas famílias) em processo de apoio, para a preservação da prova. Vejamos algumas delas:

- Cessar toda a comunicação com o/a agressor(a);

- Não bloquear ou desativar a rede social/plataforma de comunicação que o/a agressor(a) utilizou para comunicar com a vítima; esta indicação é mais importante para plataformas de comunicação que usam encriptação ponta a ponta[41] - como o WhatsApp® ou Viber®, entre outras -, o que significa que não é possível aceder a cópias das conversas, uma vez apagadas pelos/as utilizadores/as;
- Guardar todos os registos da comunicação com o/a agressor(a) (por exemplo, tirando capturas de ecrã), incluindo de imagens e/ou vídeos enviados e recebidos;
- Guardar todas as informações que permitam identificar o/a agressor(a), como: nome do/a utilizador(a), URL do perfil da sua rede social (Veja-se estratégias de intervenção propostas no Módulo 10), ID do Skype®, detalhes da transferência bancária (se tiver sido exigida quantia em dinheiro);
- Não ceder às exigências/chantagem do/a agressor(a);
- Apresentar queixa-crime junto das autoridades competentes;
- Solicitar apoio junto de estruturas de apoio à vítima, para lidar com o sofrimento emocional causado pela situação de vitimação e garantir acompanhamento ao longo do processo-crime.

A quem e como reportar/denunciar

No que diz respeito à **visualização de conteúdos de abuso de sexual de menores *online***, quem for confrontado/a com este tipo de conteúdos/material, deverá reportar às autoridades nacionais ou a entidades competentes no seu país, nomeadamente entidades/plataformas destinadas à denúncia de conteúdos ilegais *online*, como é o caso das entidades/*hotlines* pertencentes à INHOPE[42]. Estas entidades não só encaminham os casos denunciados para as autoridades nacionais competentes para subsequente investigação, como dispõem de algumas ferramentas que permitem a remoção rápida destes conteúdos e a preservação da prova.

As suspeitas de **aliciamento de menores ou de coação sexual *online*** devem ser reportadas às autoridades ou a estruturas de apoio à vítima especializadas. Também se reveste da maior importância a denúncia destes casos, assim que se tenha conhecimento dos mesmos, uma vez que, regra geral, podem existir outras crianças/jovens em perigo alvo das situações de abuso e exploração sexual do/a mesmo agressor(a).

Constituindo todas estas condutas crimes sexuais praticados contra menores de 18 anos, estes crimes são da competência reservada da Polícia da Judiciária, devendo os mesmos ser denunciados junto desta entidade ou ao Ministério Público.

Estratégias para superar a vitimação e seus impactos

No já citado capítulo 2 – Parte II do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas* são detalhadas algumas das especificidades associadas à intervenção junto de crianças e jovens vítimas de cibercrime, nomeadamente:

- Atender às características e **estádios de desenvolvimento** da criança ou jovem;
- Contemplar, sempre que possível, o **envolvimento da família**;
- Apresentar um **enfoque na educação** para uma utilização segura e consciente das TIC e da internet, enquanto comportamento de **proteção face à revitimação**.

Deve, por isso, o/a formador(a) distribuir pelos/as formandos/as os Quadros-Anexo *Estádios-chave no processo de desenvolvimento da criança/jovem* e *Abordagem e comunicação com crianças e jovens de diferentes faixas etárias* (Veja-se Plano de Sessão).

Este Módulo abordará precisamente essas especificidades que devem orientar a intervenção de qualquer profissional de apoio (TAV), explorando os **ganhos (aquisições desenvolvimentais) esperados para cada faixa etária** da criança/jovem e, consequentemente, o modo como deve realizar-se a comunicação e a intervenção com a criança/jovem vítima. Aborda ainda os efeitos da cibervitimação da criança/jovem na família.

[41] Trata-se de mecanismo de segurança que protege os dados durante uma troca de mensagens, para que o conteúdo só possa ser acedido pelos dois extremos da comunicação, ou seja, pelo/a remetente e pelo/a destinatário/a.

[42] A INHOPE é uma rede internacional que agrega diversas entidades/hotlines que, em diferentes países, operam serviços de denúncia de conteúdos ilegais online. Veja-se https://www.inhope.org/EN.

Além disso, considera também os **impactos e consequências da experiência de cibervitimação** sexual para a criança ou jovem, em linha com o capítulo 4 – Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas* e com o Módulo 3 deste Curso de Formação. Considera também a síntese de consequências da experiência de cibervitimação sexual apresentada no quadro seguinte:

Consequências na saúde emocional e psicológica	Consequências na saúde física	Alterações no comportamento
• Choque, especialmente quando a violência sexual é cometida por alguém que a criança/jovem conhece ou em quem confiava; • Raiva relativamente ao/à autor(a) do crime e em relação a si própria, por não ter conseguido evitar a situação de vitimação; • Culpa e vergonha; • Ansiedade, incluindo pensamentos e recordações frequentes em relação ao que aconteceu; • Medos diversos, incluindo de que a situação de violência se repita, de estar sozinho/a, de que ninguém acredite no seu relato, das consequências para o/a autor(a) do crime (especialmente se a vítima o/a conhecer); • Empobrecimento da autoestima (deixar de gostar de si próprio/a); • Tristeza profunda.	• Lesões e ferimentos relacionados com a violência ou força física utilizada; • Lesões e ferimentos relacionados diretamente com a violência sexual, como ferimentos nos órgãos sexuais, dor, sangramento, corrimento; • Problemas na saúde sexual e reprodutiva, como infeções sexualmente transmissíveis; • Gravidezes indesejadas; • Diminuição do apetite; • Insónias e pesadelos durante a noite (associados a pensamentos constantes sobre o que aconteceu) ou excesso de sono.	• Mais agressividade em relação a outras pessoas e a si própria (incluindo automutilação); • Comportamentos regressivos (ex.: dormir de luz acesa, voltar a fazer xixi na cama); • Isolamento social face a colegas/pares, amigos/as e familiares; • Desinteresse pela escola e quebra no rendimento escolar; • Desinteresse por atividades anteriormente apreciadas; • Alterações ao nível do comportamento sexual.

Assim, sem prejuízo das orientações centrais para a intervenção abordadas no Módulo 4 deste Curso de Formação, consideram-se particularmente prementes, no caso do apoio a crianças/jovens vítimas de abuso sexual *online* e suas famílias (ou responsáveis legais ou outros prestadores de cuidados que estejam a acompanhar a criança/jovem), as **estratégias de apoio** seguidamente apresentadas:

- Informar, de forma simples, sucinta e clara, transmitindo informação essencial junto do/a responsável legal, prestador(a) de cuidados ou outra pessoa adulta, ou ao próprio jovem, no caso de vir sozinho/a, sobre:

  - **O dever de denunciar**: É fundamental que, perante uma revelação ou suspeita, se denuncie a situação às autoridades policiais ou judiciárias, para que se possa iniciar uma investigação formal e proteger a criança/jovem vítima de novas vitimações.

    A denúncia é obrigatória para qualquer pessoa que tenha conhecimento de situações que coloquem em risco a vida, a integridade física ou psíquica ou a liberdade de uma criança ou jovem com menos de 18 anos.

    Daqui se depreende que, caso a situação ainda não tenha sido denunciada, pode cumprir ao/à profissional de apoio (TAV), após ter tido conhecimento desta situação, denunciá-la junto das autoridades competentes.

    O contacto célere com as autoridades policiais ou judiciárias permite que a investigação se conduza mais rapidamente, se ouça a vítima num menor espaço de tempo e se preservem provas físicas e/ou testemunhais.

  - A importância de a criança ou jovem ser examinada em consulta médica, sobretudo no caso das situações de abuso sexual *online* que resultam na vitimação sexual da criança ou jovem em contexto presencial (*offline*) (veja-se quadro supra e consequências ao nível da saúde física).

- Também a criança ou jovem deve ser informado/a de que o/a profissional de apoio (TAV)/responsável legal/prestador(a) de cuidados irá ter de contactar outras entidades (nomeadamente policiais ou judiciárias), para que melhor o/a possam ajudar.

- Explicar à criança/jovem vítima e família/responsáveis legais os passos subsequentes à denúncia e o funcionamento do processo-crime.
- Disponibilizar apoio ao longo do processo, inclusivamente psicológico, tanto à criança/jovem vítima, como aos/às familiares/responsáveis legais/prestadores de cuidados.
- Reforçar as estratégias de prevenção abordadas anteriormente.

Para além dos aspetos e estratégias centrais supra, no contacto/comunicação com criança ou jovem vítima de abuso sexual *online*, o/a profissional de apoio (TAV) deve reforçar os aspetos e estratégias já abordadas nos Módulos anteriores do Curso. Veja-se também capítulo 2 - Parte II do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*. No caso das crianças e jovens, de entre todas as estratégias, salientamos a importância de transmitir, da forma mais clara possível, que:

- Nada do que está a acontecer é culpa da vítima;
- Nada do que a vítima possa ter dito ou feito justifica que tenha sido forçado/a, enganado/a ou convencido/a a envolver-se sexualmente com outra pessoa;
- Ninguém tem o direito de obrigar a vítima a ter uma interação sexual contra a sua vontade (nem as pessoas que lhe são próximas têm esse direito);
- O/a autor(a) do crime é a única responsável pelo que lhe aconteceu.

Igualmente, no contacto/comunicação com familiares/responsáveis legais/prestadores de cuidados, o/a profissional de apoio (TAV) deve:

- Salientar que a revelação da cibervitimação pela criança/jovem deve ser reforçada positivamente, credibilizada e validada pelas pessoas significativas/pessoas adultas de confiança;
- Reforçar, junto de familiares/responsáveis legais/prestadores de cuidados, que é fundamental que se mantenham disponíveis para apoiar a criança/jovem vítima e para a escutar, sem que haja lugar condutas de hiperproteção ou de pressão para a partilha de pensamentos/emoções e/ou de recordações sobre o acontecimento de cibervitimação;
- Sensibilizar para a necessidade de não serem partilhadas com a criança/jovem vítima promessas irrealistas ou resultados mágicos face ao que pode a vir a acontecer, tanto no processo de recuperação psicológica e emocional, como no processo-crime.

No caso de profissionais que tenham acompanhado a criança/jovem vítima, deve o/a profissional de apoio (TAV):

- Informar da necessidade de cumprimento de procedimentos internos definidos, salvaguardando a privacidade da criança/jovem e restringindo ao essencial a partilha intra e inter institucional de informação sobre a situação de vitimação.

Apoio Especializado a Vítimas de Cibercrime

PARTE II - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME

Módulo 8 - Apoio especializado a crianças e jovens vítimas de abuso sexual online

Conceito de abuso sexual *online* é abrangente e contempla **qualquer forma de abuso sexual de crianças em contexto *online***.

CSEM/CSAM

Inclui, por isso, diferentes manifestações de abuso e exploração, desde o **abuso sexual** sem contacto, facilitado pelas TIC e pela internet, redes sociais ou outras plataformas, como o **assédio** e o **aliciamento** (*online grooming*), até à **partilha de conteúdos na *darkweb*** (imagem e/ou áudio) de abuso e exploração sexual de crianças, previamente recolhidos em fotografia ou vídeo.

O modo de disseminação comum é por Redes "***peer-to-peer***" (P2P) e acesso anónimo, como navegadores de acesso à ***Darknet*** (por exemplo, Tor). Mas, distribuição de CSAM/CSEM via **redes sociais** tem vindo a aumentar.

Quanto ao *grooming* - redes sociais e nos jogos *online*

Em Portugal, as situações de **CSEM** e **CSAM** estão enquadradas no crime de **Pornografia Infantil**, artigo 176.º CP

- Problemas com a terminologia: conceito de pornografia (isto é, pessoas adultas envolvidas, de forma consensual, em comportamento erótico em imagens, vídeo e/ou escrita, destinado a causar excitação sexual) não traduz o que está subjacente às situações de abuso sexual de crianças

a. Tipos e Modi operandi

1. **Disseminação de conteúdos de abuso sexual de crianças (CSAM)**
   - i. **Conteúdos de abuso sexual de crianças gerados *online***
   - ii. **Auto produção de conteúdos**
   - iii. **Transmissão em direto de abuso sexual de crianças**

2. **Aliciamento (grooming online)**

a. Tipos e Modi operandi

1. **Disseminação de conteúdos de abuso sexual de crianças (CSAM)**
   - i. **Conteúdos de abuso sexual de crianças gerados *online***

   - Conteúdo auto produzido/auto gerado pelos menores;
   - A procura de sessões de *live-streaming* de abuso sexual de menores.

a. Tipos e Modi operandi

1. **Disseminação de conteúdos de abuso sexual de crianças (CSAM)**
   - ii. **Auto produção de conteúdos**

Conteúdo íntimo que é (auto)produzido voluntariamente pela criança ou jovem – partilhado por fotos ou vídeos, através de redes sociais ou de plataformas de *chat*, com outros pares. E.g. *sexting;* forma de auto produção de conteúdos de natureza sexual - texto, imagens e/ou vídeos.
Autor dos conteúdos torna-se mais vulnerável a situações de abuso online (aliciamento, *online grooming*) realizado por pessoas adultas que se fazem passar por pares.

≠

Conteúdo íntimo (auto)produzido sob coação ou extorsão por parte de outra pessoa.
A partilha de conteúdos de natureza sexual, habitualmente de forma consentida e entre pares, pode levar a situações subsequentes de extorsão, aliciamento e outras formas de abuso sexual *online*, nomeadamente pela divulgação em redes de abuso sexual de crianças e jovens.

a. Tipos e Modi operandi

1. Disseminação de conteúdos de abuso sexual de crianças (CSAM)

iii. Transmissão em direto de abuso sexual de crianças

Aumento da procura de **sessões de *live-streaming* de abuso sexual de crianças**: assistir a conteúdos de abuso sexual de menores em direto.

Como? Canais de *streaming* são pagos, sendo, muitas vezes, publicitados em *websites* pornográficos para pessoas adultas, onde os/as utilizadores/as são direcionados para plataformas encriptadas que permitem a videoconferência.

Turismo sexual para abuso de menores **-** Os/as utilizadores/as que procuram este tipo de conteúdo podem ainda viajar para os países onde as sessões de *live streaming* decorrem para a prática de abuso sexual, desta feita presencialmente.

a. Tipos e Modi operandi

2. Aliciamento (*grooming*)

Consiste no **processo de manipulação** e uma **forma de aliciamento** de crianças e jovens.

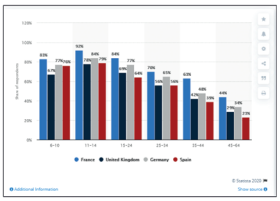
Inicia-se geralmente através de uma abordagem não-sexual, através da internet, incluindo jogos *online* e redes sociais, com vista a estabelecer uma relação de confiança com a criança e a convencê-la a encontrar-se pessoalmente com outra pessoa, para que esta última possa consumar o abuso sexual.

O estabelecimento de relação de confiança com a criança, pode ainda visar a **persuasão da criança à produção e partilha de conteúdo sexual**.

a. Tipos e Modi operandi

2. Aliciamento (*grooming*)

Percentagem de Jogadores Online (*gamers*) por faixa etária em 4 países Europeus, no primeiro trimestre de 2018.



b. Estratégias de prevenção

O/A TAV deve transmitir à criança/jovem vítima e sua família para **prevenir situações de abuso sexual *online***, as seguintes estratégias:

- Sensibilizar para a importância da educação da criança ou jovem para uma utilização segura e consciente da internet e das TIC e para a identificação de situações e contextos de risco *online*;
- Sensibilizar para a definição de regras claras de utilização da internet e TIC: por exemplo, colocar videojogos/computador numa área comum da casa e/ou permitir a utilização de dispositivos móveis/eletrónicos apenas em espaços comuns da habitação;

b. Estratégias de prevenção

- Reforçar a importância do acompanhamento ou supervisão do comportamento *online* da criança ou jovem a cargo: nomeadamente se recebe chamadas de números desconhecidos, se passa muito tempo *online* e até muito tarde, se demonstra um súbito isolamento relativamente à família e amigos/as, bem como o tipo de pedidos de amizade rececionados e sua origem;
- Configurar, em conjunto com as crianças e jovens a cargo, as definições de privacidade de redes sociais e páginas/perfis, eliminando qualquer tipo de informação pessoal ou outra que possa identificar a morada de casa, escola, número de telemóvel, etc.;

b. Estratégias de prevenção

A **família** desempenha um papel muito importante na proteção de crianças e jovens face aos riscos da utilização da internet e das TIC.

Sobre a importância da família na prevenção do cibercrime contra crianças e jovens: Consultar capítulo 4 - Parte II do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas.*

Sobre importância da família no apoio e intervenção junto de crianças e jovens vítimas de cibercrime, inclusivamente na educação da criança ou jovem vítima para uma utilização consciente e segura da internet e das TIC: Consultar capítulo 2 – Parte II do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas.*

c. Estratégias de intervenção

i. Preservação da prova digital

- parar imediatamente toda a comunicação com o/a agressor(a);
- não bloquear ou desativar a rede social/plataforma de comunicação que o/a agressor(a) utilizou para comunicar com a vítima; esta indicação é mais importante para plataformas de comunicação que usam encriptação ponto a ponto - como o WhatsApp® ou Viber®, entre outras -, o que significa que não é possível aceder a cópias das conversas, uma vez apagadas pelos/as utilizadores/as;
- Trata-se de mecanismo de segurança que protege os dados durante uma troca de mensagens, para que o conteúdo só possa ser acedido pelos dois extremos da comunicação: remetente e destinatário/a.

b. Estratégias de intervenção

- guardar todos os registos da comunicação com o/a agressor(a) (por exemplo, tirando capturas de ecrã), incluindo de imagens e/ou vídeos enviados e recebidos;
- guardar todas as informações que permitam identificar o/a agressor(a), como: nome do/a utilizador(a), URL do perfil da sua rede social (ver estratégias de intervenção no módulo 10), ID do Skype®, detalhes da transferência bancária (se tiver sido exigida quantia em dinheiro);
- não ceder às exigências/chantagem do/a agressor(a);
- apresentar queixa-crime junto das autoridades competentes;
- solicitar apoio junto de estruturas de apoio à vítima, para lidar com o sofrimento emocional causado pela situação de vitimação e garantir acompanhamento ao longo do processo-crime.

b. Estratégias de intervenção

ii. A quem e como reportar/denunciar

Visualização de conteúdos de abuso de sexual de menores *online* – autoridades nacionais ou entidades/plataformas destinadas à denúncia de conteúdos ilegais *online*, como é o caso das *hotlines* pertencentes à INHOPE

Aliciamento de menores ou de coação sexual *online* – autoridades nacionais ou a estruturas de apoio à vítima especializadas

As autoridades nacionais: competência reservada da Polícia da Judiciária, ou Ministério Público.

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

Sem prejuízo das orientações centrais para a intervenção abordadas no Módulo 4 deste Curso de Formação

- Informar, de forma simples, sucinta e clara, transmitindo informação essencial junto do/a responsável legal, prestador(a) de cuidados ou outra pessoa adulta, ou ao próprio jovem, no caso de vir sozinho/a, sobre:
  - **O dever de denunciar**: É fundamental que, perante uma revelação ou suspeita, se denuncie a situação às autoridades policiais ou judiciárias, para que se possa iniciar uma investigação formal e proteger a criança/jovem vítima de novas vitimações.
  - **A denúncia é obrigatória** para qualquer pessoa que tenha conhecimento de situações que coloquem em risco a vida, a integridade física ou psíquica ou a liberdade de uma criança ou jovem com menos de 18 anos.

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

Sem prejuízo das orientações centrais para a intervenção abordadas no Módulo 4 deste Curso de Formação

- A importância de a criança ou jovem ser examinada em consulta médica, sobretudo no caso das situações de abuso sexual *online* que resultam na vitimação sexual da criança ou jovem em contexto presencial (*offline*) (veja-se quadro supra e consequências ao nível da saúde física).
- Que o(a) TAV/responsável legal/prestador(a) de cuidados irá ter de contactar outras entidades (nomeadamente policiais ou judiciárias), para que melhor o/a possam ajudar.
- Explicar à criança/jovem vítima e família/responsáveis legais os passos subsequentes à denúncia e o funcionamento do processo-crime.
- Disponibilizar apoio ao longo do processo, inclusivamente psicológico, tanto à criança/jovem vítima, como aos/às familiares/responsáveis legais/prestadores de cuidados.
- Reforçar as estratégias de prevenção abordadas anteriormente.

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

Para além dos aspetos e estratégias centrais acima sintetizadas, no contacto/comunicação com criança ou jovem vítima de abuso sexual *online*, o(a) TAV deve:

- Reforçar a coragem da procura de apoio e da revelação da experiência de cibervitimação.
- Demonstrar que acredita naquilo que a vítima está a contar sobre o que lhe aconteceu, sem julgamentos ou juízos de valor.
- Respeitar e promover a ventilação emocional, bem como momentos de maior fragilidade e emocionalidade associados à partilha da experiência de cibervitimação.
- Normalizar as reações apresentadas.

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

- Transmitir, da forma mais clara possível, que:
  - Nada do que está a acontecer é culpa da vítima.
  - Nada do que a vítima possa ter dito ou feito justifica que tenha sido forçado/a, enganado/a ou convencido/a a envolver-se sexualmente com outra pessoa.
  - Ninguém tem o direito de obrigar a vítima a ter uma interação sexual contra a sua vontade (nem as pessoas que lhe são próximas têm esse direito).
  - O/a autor(a) do crime é a única responsável pelo que lhe aconteceu.
- Sugerir a partilha de sentimentos e receios com aqueles/as em quem confia.
- No caso de a vítima ser jovem, caso seja vontade da vítima e com a sua autorização, envolver familiares e/ou amigos/as no processo de recuperação.

8 - Apoio especializado a crianças e jovens vítimas de abuso sexual online

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

Igualmente, no contacto/comunicação com familiares/responsáveis legais/prestadores de cuidados, o(a) TAV deve:

- Salientar que a revelação da cibervitimação pela criança/jovem deve ser reforçada positivamente, credibilizada e validada pelas pessoas significativas/pessoas adultas de confiança;
- Reforçar, junto de familiares/responsáveis legais/prestadores de cuidados, que é fundamental que se mantenham disponíveis para apoiar a criança/jovem vítima e para a escutar, sem que haja lugar condutas de hiper proteção ou de pressão para a partilha de pensamentos/emoções e/ou de recordações sobre o acontecimento de cibervitimação;
- Sensibilizar para a necessidade de não ser partilhadas com a criança/jovem vítima promessas irrealistas ou resultados mágicos face ao que pode a vir a acontecer, tanto no processo de recuperação psicológico e emocional, como no processo-crime.

PLANO DE SESSÃO Nº 8

1. Identificação da Ação

Designação	Curso de Formação Apoio Especializado a Vítimas de Cibercrime		
Módulos/ temas	Apoio especializado a crianças e jovens vítimas de abuso sexual *online*		
Data da Sessão	**Horário**	**Duração da Sessão**	40 minutos
Formadores/as			

2. Objetivos Específicos

No final da sessão, os/as formandos/as deverão ser capazes de:

- Distinguir, corretamente, a natureza e *modi operandi* das diferentes formas de abuso sexual de crianças *online* abordadas, nomeadamente a disseminação de conteúdos de abuso sexual de crianças e o *grooming online*;
- Enumerar, de forma correta, estratégias de intervenção propostas para o apoio especializado a crianças e jovens vítimas de abuso sexual *online*;
- Reconhecer, de forma correta, estratégias de prevenção da revitimação propostas para a intervenção junto de crianças e jovens vítimas de abuso sexual *online*.

3. Estrutura da Sessão

	Conteúdos Programáticos	Metodologia	Recursos Pedagógicos/ Didáticos	Avaliação | Exercícios	Tempo (minutos)
Introdução	Tipos de abuso sexual de crianças *online*: • Disseminação de conteúdos de abuso sexual de crianças: conteúdos de abuso sexual de crianças gerados *online*; auto produção de conteúdos; transmissão em direto de abuso sexual de crianças • Aliciamento (*grooming online*): aliciamento nas redes sociais e em jogos de vídeo *online*	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	10
Desenvolvimento	*Modi operandi* e natureza dos crimes	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
	Estratégias de prevenção	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
	Estratégias de intervenção: • Estratégias para preservação de prova digital • A quem e como reportar/denunciar • Estratégias para superar a vitimação e seus impactos	Expositiva e ativa	Computador: Datashow e tela para projeção; Quadros - Anexo[43]	Observação	15
Conclusão	Síntese conclusiva e esclarecimento de questões	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5

OBSERVAÇÕES

Destionatários/as:
Técnicos/as de Apoio à Vítima (TAV)

Data: / / **Formador(a):**

[43] Os Quadros - Anexo *Estádios-chave no processo de desenvolvimento da criança/jovem e Abordagem e comunicação com crianças e jovens de diferentes faixas etárias, do Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*, estão disponíveis nas páginas seguintes.

INSTRUÇÕES E INFORMAÇÕES ESSENCIAIS PARA O/A FORMADOR(A)

CORRESPONDÊNCIA DE CONTEÚDOS

Plano de Sessão	*Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*	
	PARTE	CAPÍTULO
Tipos de abuso sexual de crianças *online*	Parte I - Compreender	Capítulo 1 – 1.3.
	Ver Apresentação e Enquadramento do Módulo	
Modi operandi e natureza do crime	Sem correspondência	
	Ver Apresentação e Enquadramento do Módulo	
Estratégias de prevenção	Sem correspondência	
	Ver Apresentação e Enquadramento do Módulo	
Estratégias de intervenção		
Estratégias para preservação de prova digital	Sem correspondência	
	Ver Apresentação e Enquadramento do Módulo	
A quem e como reportar/denunciar	Sem correspondência	
	Ver Apresentação e Enquadramento do Módulo	
Estratégias para superar a vitimação e seus impactos	Parte II - Proceder	Capítulo 2 – 2.1. e 2.4.
	Ver Apresentação e Enquadramento do Módulo	
Síntese conclusiva e esclarecimento de questões	Sem correspondência	

Quadro - Anexo: Estádios-chave no processo de desenvolvimento da criança/jovem

	desenvolvimemto físico	desenvolvimento emocional e cognitivo (incluindo linguagem)	desenvolvimento social e moral
3-6 anos	• É capaz de desenhar e de outras manualidades • É capaz de escrever o seu próprio nome • O corpo desenvolve-se, assumindo as formas do corpo adulto • A destreza e capacidade de coordenação aumentam	• Lembra-se de experiências familiares • Possui algum vocabulário • É capaz de ajustar o discurso de acordo com as características do/a interlocutor(a) (como idade, sexo e estatuto social)	• É capaz de interpretar, prever e influenciar as reações de outras pessoas • Estabelece as primeiras amizades • Surgem as emoções autoconscientes (como vergonha e culpa) • em um controlo relativo sobre as suas emoções
6-12 anos	• Aumenta progressivamente de peso e de altura • A caligrafia torna-se mais pequena e legível • Os desenhos são mais estruturados • Os jogos e brincadeiras que envolvam correrias, confusão e competição são comuns • Desenvolve-se a capacidade de resposta rápida ao nível da destreza motora • Podem evidenciar-se indicadores púberes, particularmente no caso das raparigas	• Os pensamentos e a capacidade de atenção são mais focalizados • Raciocínio indutivo • É capaz de estabelecer a relação entre experiências e ocorrências específicas • Aumento de vocabulário	• Torna-se mais independente e mais responsável • Faz a distinção entre ser bem-sucedido e mal-sucedido • Tem consciência dos seus esforços *vs* acaso/sorte na obtenção de um dado resultado • É capaz de se colocar no lugar do outro (empatia)
12-18 anos	• Puberdade • Menstruação e aumento do tecido adiposo, no caso das raparigas • Voz torna-se mais grave e há aumento de massa muscular, no caso dos rapazes • Maior interesse pela sexualidade	• É capaz de discutir eficazmente • É mais autoconsciente e concentrado/a • Desenvolvimento do raciocínio hipotético-dedutivo • É capaz de ajustes subtis no discurso • É capaz de fazer planos e de tomar decisões	• Aumento da conflitualidade com pais/família • Aproximação ao grupo de pares e surgimento de situações de pressão de pares • Procura da própria identidade • Desenvolvimento de relacionamentos íntimos

Quadro - Anexo: Abordagem e comunicação com crianças e jovens de diferentes faixas etárias

	1-6 anos	6-12 anos	12-18 anos
Apresentação	Fundamentalmente dirigida à criança. É ainda demasiadamente nova para poder compreender a informação prestada.	A criança demonstra mais interesse na informação prestada e maior capacidade para a compreender.	Compreende a informação prestada, mas pode demonstrar relutância quanto à participação num programa de intervenção ou num processo de apoio à vítima.
Descrição do acontecimento	Expressa-se preferencialmente através de desenhos ou de jogos, preterindo a expressão verbal.	Apresenta mais detalhes do que as crianças mais novas. As crianças mais velhas preferem expressar-se verbalmente recusando, por vezes, o recurso a desenhos e jogos.	A descrição do acontecimento é detalhada. Verificam-se sentimentos de auto-culpabilização.
Psico-educação	Fundamentalmente dirigida à família/pais. No entanto, a criança assimilará informações simples, como o reconhecimento da situação, pelo que poderá simular uma maneira de lidar com ela.	Dirigida à criança, integrando a família/pais no processo de psico-educação.	Dirigida à/através da criança.

MOD. 9

MOD. 9

PARTE 2 - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME
MÓDULO 9 - APOIO ESPECIALIZADO A VÍTIMAS DE CIBER-*BULLYING*

APRESENTAÇÃO E ENQUADRAMENTO DO MÓDULO

Este Módulo dedica-se à compreensão do fenómeno de ciber-*bullying*, assim como à intervenção junto das respetivas vítimas, tendo em vista a superação dos impactos da cibervitimação e a prevenção da revitimação.

Além da leitura do conteúdo do presente Módulo, sugerimos ainda ao/à formador(a), como temos feito para os demais módulos deste Curso, a consulta do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*.

Modi operandi e natureza do crime

O ciber-*bullying* constitui uma extensão do *bullying*. Se o *bullying* implica agressão "cara-a-cara", no ciber-*bullying* a agressão e a ofensa são realizadas *online*, através da internet e das TIC.

O ciber-*bullying* manifesta-se através da partilha de textos, fotos e/ou vídeos agressivos ou humilhantes para com outra pessoa, colocando a sua identidade em causa e afetando a sua autoestima. O facto de o ciber-*bullying* ser praticado através da internet - nas redes sociais e/ou através de aplicações de mensagens como o WhastApp® - possibilita que o/a agressor(a) não tenha de confrontar diretamente a vítima, sentindo-se menos inibido no momento de agredir, com menos medo de vir a ser punido/a e, por isso, mais poderoso/a.

O ciber-*bullying* pode ser praticado:

- de um para um (apenas entre vítima e agressor(a));
- de um para muitos (por exemplo, um(a) agressor(a) publica algo *online* que muitas pessoas podem ver);
- de muitos para muitos (quando muitos/as agressores/as partilham algo que muitas pessoas vão poder ver).

O ciber-*bullying* possibilita que os/as agressores/as atuem de forma anónima, muitas vezes recorrendo a identidades falsas (que lhes permitem dissociar-se da moralidade dos seus atos) e a esquemas de pensamento que justificam as suas condutas, como:

- Obscurecer ou minimizar o seu próprio papel, "deslocando" ou diluindo a sua responsabilidade;
- Distorcer ou desvalorizar o impacto do comportamento;
- Culpar e desumanizar a vítima.

As formas comuns de violência no ciber-*bullying* são:

- *Flaming* – discussões *online*, utilizando mensagens eletrónicas com linguagem vulgar e enraivecida;
- *Harassement* – enviar repetidamente mensagens inadequadas, hostis e insultuosas;
- *Impersonation* – fazer passar-se por outra pessoa e enviar/publicar material ou conteúdo que visa prejudicar a sua reputação ou amizades;
- *Outing* – partilhar informação pessoal, embaraçosa ou imagens *online* de outra pessoa, sem o seu consentimento;
- *Trickery* – levar alguém a revelar informação pessoal/confidencial ou embaraçosa e, posteriormente, partilhá-la *online*;
- *Exclusion* – excluir alguém, intencionalmente e de forma cruel, de um grupo *online*;
- *Cyberstalking* – assédio repetido e intenso, que inclui ameaças ou gera um medo significativo;
- *Happy slapping* – agressões cara-a-cara que são cometidas por uma pessoa (ou várias) contra a vítima, estando a agressão física a ser gravada por terceiros que, mais tarde, partilham o episódio nas redes sociais.

Há também práticas de ciber-*bullying* com componente sexual, com o objetivo de atacar a dignidade e a esfera da vida privada da vítima, tais como:

- Partilha *online* de boatos ou mentiras sobre o comportamento sexual da vítima;
- Uso de linguagem sexual ofensiva ou discriminatória *online* contra a vítima;
- Furto de identidade da vítima e subsequente partilha de conteúdo sexual envolvendo a vítima ou assediando sexualmente outras pessoas;

- Recurso a ameaças e intimidação por causa da identidade de género ou orientação sexual da vítima;
- Prática de *body shamming* - partilha de comentários depreciativos relativos ao aspeto físico da vítima.

Estratégias de prevenção

Para **prevenir situações de *ciber-bullying***, neste ponto do Módulo, o/a formador(a) deve transmitir aos/às formandos/as as seguintes estratégias que estes/as, enquanto profissionais de apoio (TAV), poderão utilizar na intervenção com a vítima:

- Parar toda a comunicação com o/a agressor(a);
- Não bloquear ou desativar a rede social/plataforma de comunicação que o/a agressor(a) utilizou para comunicar com a vítima, uma vez que plataformas como WhatsApp® ou Viber® usam encriptação ponta a ponta (Veja-se Módulo 8);
- Não fornecer informação pessoal ou dados pessoais pedidos através de *e-mails*, mensagens, chamadas, *websites* não solicitados;
- Configurar as definições de privacidade de redes sociais e páginas/perfis, eliminando informação pessoal ou outra que possa identificar a morada de casa, escola, número de telemóvel, etc.;
- Ativação de filtros de *spam* e de assédio;
- Gravar contactos telefónicos importantes no telemóvel, para poder pedir ajuda facilmente, caso precise;
- Podem também registar-se contactos dos recursos de apoio e serviços da comunidade que podem ser importantes na superação/recuperação da situação de vitimação;
- Procurar caminhos alternativos para os locais que costuma frequentar;
- Partilhar com pessoas adultas de confiança a situação e as rotinas habituais;
- Procurar andar na companhia de pessoas em quem confie e evitar andar sozinho/a;
- No caso de se ser confrontado cara-a-cara com o/a agressor(a) *online*, deverá reagir-se sem violência e com serenidade, procurando ajuda o mais rápido possível ou pessoas que estejam próximas;
- Em situação de perigo, deve ser procurado um local seguro ou onde estejam mais pessoas. Também podem ser acionados os contactos de emergência.

Estratégias de intervenção

Estratégias para preservação de prova digital

Ainda neste Módulo, para além da abordagem às dinâmicas e *modi operandi* em situações de ciber-*bullying* e da apresentação de medidas de prevenção da revitimação supra, o/a formador(a) deve apresentar junto dos/as formandos/as estratégias que podem ser explicadas à vítima em processo de apoio, para a preservação da prova. Vejamos algumas delas:

- Depois de cessadas as comunicações com agressor(a), não deve ser bloqueada ou desativada a rede social/plataforma de comunicação que o/a agressor(a) utilizou para comunicar com a vítima;
- Guardar todos os registos da comunicação com o/a agressor(a) (por exemplo, tirando capturas de ecrã), incluindo de imagens e/ou vídeos enviados e recebidos;
- Guardar todas as informações que permitam identificar o/a agressor(a), como: nome do/a utilizador(a), URL do perfil da sua rede social (Veja-se estratégias de intervenção no Módulo 10), ID do Skype®, etc.;
- Apresentar queixa-crime junto das autoridades competentes;
- Solicitar apoio junto de estruturas de apoio à vítima, para lidar com o sofrimento emocional causado pela situação de vitimação e garantir acompanhamento ao longo do processo-crime.

A quem e como reportar/denunciar

O ciber-*bullying*, quando praticado por menores de 12 anos, devido à inimputabilidade em razão da idade, pode levar a que sejam decretadas **medidas de Promoção e Proteção**, de acordo com a Lei de Proteção de Crianças e Jovens em Perigo - Lei n.º 147/99, de 01 de Setembro. Podem ainda ser aplicadas medidas disciplinares pelas Escolas que tenham conhecimento de situações de ciber-*bullying*.

Entre os 12 e os 16 anos de idade, as práticas de ciber-*bullying* podem ser punidas pela **Lei Tutelar Educativa**, quando as condutas constituam crime:

- A prática, por menor com idade compreendida entre os 12 e os 16 anos, de facto qualificado pela lei como crime dá lugar à aplicação de medida tutelar educativa, em conformidade com as disposições da presente lei.

Segundo o disposto no artigo 19.º do Código Penal, depois dos 16 anos de idade, todo o tipo de violência praticada que constitua crime é punida de acordo com a Legislação Penal.

Em todo o caso, as situações de ciber-*bullying* devem ser reportadas junto das entidades com competência para as punir, a saber:

- Escola (diretor(a) de turma, direção da escola, direção do agrupamento de escolas e, caso a resposta destes órgãos falhe, comunicar a situação à Direção de Serviço de Segurança Escolar);
- Órgãos de Polícia Criminal (através dos/as agentes ou guardas responsáveis pelo Programa Escola Segura);
- Comissão de Proteção de Crianças e Jovens;
- Ministério Público.

Estratégias para superar a vitimação e seus impactos

Na sequência dos aspetos-chave para a intervenção com vítimas de cibercrime trabalhadas no Módulo 4 e das **estratégias de prevenção e intervenção** já delineadas, cumpre ao/à profissional de apoio (TAV) facultar à vítima um conjunto de orientações práticas, considerando também os cuidados já abordados no Módulo 8 (no que respeita, concretamente, à **comunicação com crianças/jovens** de diferentes faixas etárias).

O/a profissional de apoio, na estruturação do atendimento e apoio à vítima de ciber-*bullying*, deve também ter em consideração o **impacto da experiência de cibervitimação** e as consequências sentidas pela vítima. Veja-se o Módulo 3 deste Curso de Formação, bem como o capítulo 4 - Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*.

Para além das reações e consequências abordadas nesses recursos, no caso específico do *bullying* contra crianças e jovens, seja ele ciber-*bullying* ou *bullying* convencional, há outras consequências a destacar e que podem ser experienciadas pelas vítimas alvo da intervenção:

- Ficar com medo de ir para a escola e fazer tudo para não ir (por exemplo, fingir estar doente);
- Quebra no rendimento escolar;
- Afastamento/isolamento face a amigos/as e outras pessoas com quem gostavam de conviver;
- Perda de interesse relativamente a atividades previamente apreciadas;
- Sintomas físicos e problemas de saúde: dificuldade em adormecer; pesadelos frequentes; dores de barriga, enjoos ou tonturas (por exemplo, quando pensam que têm de ir para a escola ou quando entram na escola); dores de cabeça; suores, batimento cardíaco acelerado (por exemplo, quando pensam que têm de ir para a escola ou quando entram na escola).

Desta forma, o/a formador(a) poderá estacar as seguintes **estratégias de apoio**:

- Normalizar as reações apresentadas;
- Fornecer informações sobre a prevalência do crime entre pessoas da faixa etária da vítima, no sentido de romper com a ideia de "vulnerabilidade única" e com eventuais sentimentos de solidão e incompreensão daí decorrentes;
- Deixar muito clara a ideia de que a vítima não tem culpa do que lhe está a acontecer e de que a culpa e responsabilidade são exclusivamente do/a agressor(a);
- Incentivar o reforço do envolvimento em atividades anteriormente apreciadas, nomeadamente atividades *offline*;
- Caso seja vontade da vítima e com a sua autorização, envolver familiares e/ou amigos/as no processo de recuperação;
- Disponibilizar apoio ao longo do processo, inclusivamente psicológico;
- Reforçar as estratégias de prevenção abordadas anteriormente.

Apoio Especializado a Vítimas de Cibercrime

PARTE II - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME

Módulo 9 – Apoio especializado a vítimas de ciber-bullying

Módulo 9 – Apoio especializado a vítimas de ciber-bullying

a. Modi operandi e natureza do crime

O ciber-*bullying* constitui uma extensão do *bullying,* mas a agressão e a ofensa são realizadas *online*, através da internet e das TIC.

O ciber-*bullying* manifesta-se através da partilha de textos, fotos e/ou vídeos agressivos ou humilhantes para com outra pessoa, colocando a sua identidade em causa e afetando a sua autoestima. O facto de o ciber-*bullying* ser praticado através da internet - nas redes sociais e/ou através de aplicações de mensagens como o WhastApp® - possibilita que o/a agressor(a) não tenha de confrontar diretamente a vítima, sentindo-se menos inibido no momento de agredir, com menos medo de vir a ser punido/a e, por isso, mais poderoso/a.

Módulo 9 – Apoio especializado a vítimas de ciber-bullying

a. Modi operandi e natureza do crime

O ciber-*bullying* pode ser praticado:
- de um para um (apenas entre vítima e agressor(a));
- de um para muitos (por exemplo, um(a) agressor(a) publica algo *online* que muitas pessoas podem ver);
- de muitos para muitos (quando muitos/as agressores/as partilham algo que muitas pessoas vão poder ver).

O ciber-*bullying* possibilita que os/as agressores/as atuem de forma anónima, muitas vezes recorrendo a identidades falsas (que lhes permitem dissociar-se da moralidade dos seus atos) e a esquemas de pensamento que justificam as suas condutas, como:
- Obscurecer ou minimizar o seu próprio papel, deslocando ou diluindo a sua responsabilidade;
- Distorcer ou desvalorizar o impacto do comportamento;
- Culpar e desumanizar a vítima.

Módulo 9 – Apoio especializado a vítimas de ciber-bullying

a. Modi operandi e natureza do crime

As **situações mais comuns** de violência no ciber-*bullying* são:

- *Flaming* – discussões *online*, utilizando mensagens eletrónicas com linguagem vulgar e enraivecida;
- *Harassement* – enviar repetidamente mensagens inadequadas, hostis e insultuosas;
- *Impersonation* – fazer passar-se por outra pessoa e enviar/publicar material ou conteúdo que visa prejudicar a sua reputação ou amizades;
- *Outing* – partilhar informação pessoal, embaraçosa ou imagens *online* de outra pessoa, sem o seu consentimento;
- *Trickery* – levar alguém a revelar informação pessoal/confidencial ou embaraçosa e, posteriormente, partilhá-la *online*;
- *Exclusion* – excluir alguém, intencionalmente e de forma cruel, de um grupo *online*;
- *Cyberstalking* – assédio repetido, intenso, que inclui ameaças ou gera um medo significativo;
- *Happy slapping* – agressões cara-a-cara que são cometidas por uma pessoa ou por várias contra a vítima, estando a agressão física a ser gravada por terceiros que, mais tarde, partilham o episódio nas redes sociais.

Módulo 9 – Apoio especializado a vítimas de ciber-bullying

a. Modi operandi e natureza do crime

Há também práticas de ciber-*bullying* com componente sexual, com o objetivo de atacar a dignidade e a esfera da vida privada da vítima, tais como:

- Partilha *online* de boatos ou mentiras sobre o comportamento sexual da vítima;
- Uso de linguagem sexual ofensiva ou discriminatória *online* contra a *vítima*;
- Furto de identidade da vítima e subsequente partilha de conteúdo sexual envolvendo a vítima ou assediando sexualmente outras pessoas;
- Recurso a ameaças e intimidação por causa pela identidade de género ou orientação sexual da vítima;
- Prática de *body shamming* - partilha de comentários depreciativos relativos ao aspeto físico da vítima.

Módulo 9 – Apoio especializado a vítimas de ciber-bullying

b. Estratégias de prevenção

Para **prevenir situações de ciber-*bullying***, o TAV deve transmitir à vítima:

- Parar toda a comunicação com o/a agressor(a);
- Não bloquear ou desativar a rede social/plataforma de comunicação que o/a agressor(a) utilizou para comunicar com a vítima, uma vez que plataformas como WhatsApp® ou Viber® usam encriptação ponto a ponto (Veja-se Módulo 8);
- Não fornecer informação pessoal ou dados pessoais pedidos através de *e-mails*, mensagens, chamadas, *websites* não solicitados;
- Configurar as definições de privacidade de redes sociais e páginas/perfis, eliminando qualquer tipo de informação pessoal ou outra que possa identificar a morada de casa, escola, número de telemóvel, etc.;
- Ativação de filtros de *spam* e de assédio;

Módulo 9 – Apoio especializado a vítimas de ciber-bullying

b. Estratégias de prevenção

Para **prevenir situações de ciber-*bullying***, o TAV deve transmitir à vítima:

- Gravar contactos telefónicos importantes no telemóvel, para poder pedir ajuda facilmente, caso precise;
- Podem também registar-se contactos dos recursos de apoio e serviços da comunidade que podem ser importantes na superação/recuperação da situação de vitimação;
- Procurar caminhos alternativos para os locais que costuma frequentar;
- Partilhar com pessoas adultas de confiança a situação e as rotinas habituais;
- Procurar andar na companhia de pessoas em quem confie e evitar andar sozinho/a;
- No caso de se ser confrontado cara-a-cara com o/a agressor(a) *online*, deverá reagir-se sem violência e com serenidade, procurando ajuda o mais rápido possível ou pessoas que estejam próximas;
- Em situação de perigo, deve ser procurado um local seguro ou onde estejam mais pessoas. Também pode ser acionados os contactos de emergência.

Módulo 9 – Apoio especializado a vítimas de ciber-bullying

c. Estratégias de intervenção

i. Preservação da prova digital

- Depois de cessadas as comunicações com agressor(a), não deve ser bloqueada ou desativada a rede social/plataforma de comunicação que o/a agressor(a) utilizou para comunicar com a vítima;
- Guardar todos os registos da comunicação com o/a agressor(a) (por exemplo, tirando capturas de ecrã), incluindo de imagens e/ou vídeos enviados e recebidos;
- Guardar todas as informações que permitam identificar o/a agressor(a), como: nome do/a utilizador(a), URL do perfil da sua rede social (ver estratégias de intervenção no módulo 10), ID do Skype®, etc.;
- Apresentar queixa-crime junto das autoridades competentes;
- Solicitar apoio junto de estruturas de apoio à vítima, para lidar com o sofrimento emocional causado pela situação de vitimação e garantir acompanhamento ao longo do processo-crime.

Módulo 9 – Apoio especializado a vítimas de ciber-bullying

c. Estratégias de intervenção

ii. A quem e como reportar/denunciar

O ciber-*bullying*, quando praticado por menores de 12 anos, devido à inimputabilidade em razão da idade, pode levar a que sejam decretadas **medidas de Promoção e Proteção**, de acordo com a **Lei de Proteção de Crianças e Jovens em Perigo** - Lei n.º 147/99, de 01 de Setembro.

Podem ainda ser aplicadas medidas disciplinares pelas Escolas que tenham conhecimento de situações de ciber-*bullying*.

Entre os 12 e os 16 anos de idade, as práticas de ciber-*bullying* podem ser punidas pela **Lei Tutelar Educativa (LTE)**, quando as condutas constituam crime:

"A prática, por menor com idade compreendida entre os 12 e os 16 anos, de facto qualificado pela lei como crime dá lugar à aplicação de medida tutelar educativa, em conformidade com as disposições da presente lei."

Módulo 9 – Apoio especializado a vítimas de ciber-bullying

c. Estratégias de intervenção

ii. A quem e como reportar/denunciar

Artigo 19.º do Código Penal - **A partir dos 16 anos de idade**, todo o tipo de violência praticada que constitua crime é punida de acordo com a Legislação Penal.

Em todo o caso, as situações de ciber-*bullying* devem ser reportadas junto das entidades com competência para as punir, a saber:

- Escola (diretor(a) de turma, direção da escola, direção do agrupamento de escolas e, caso a resposta destes órgãos falhe, comunicar a situação à Direção de Serviço de Segurança Escolar);
- Órgãos de Polícia Criminal (através dos/as agentes ou guardas responsáveis pelo programa Escola Segura);
- Comissão de Proteção de Crianças e Jovens;
- Ministério Público

Módulo 9 – Apoio especializado a vítimas de ciber-bullying

c. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação

Estratégias de apoio:

- Normalizar as reações apresentadas;
- Fornecer informações sobre a prevalência do crime entre pessoas da faixa etária da vítima, no sentido de romper com a ideia de "vulnerabilidade única" e com eventuais sentimentos de solidão e incompreensão daí decorrentes;
- Deixar muito clara a ideia de que a vítima não tem culpa do que lhe está a acontecer e de que a culpa e responsabilidade é exclusivamente do/a agressor(a);
- Incentivar o reforço do envolvimento em atividades anteriormente apreciadas, nomeadamente as atividades *offline*.
- Caso seja vontade da vítima e com a sua autorização, envolver familiares e/ou amigos/as no processo de recuperação.
- Disponibilizar apoio ao longo do processo, inclusivamente psicológico.
- Reforçar as estratégias de prevenção abordadas anteriormente.

Situações Mais Comuns de *Cyberbullying*

"Cyber-bullying Facts – Top 10 Forms of Cyber Bullying" (2016)

https://www.youtube.com/watch?time_continue=186&v=0Xo8N9qlItk&feature=emb_logo

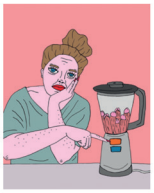
Situações Mais Comuns de *Cyberbullying*
Exercício

Fonte: NY Times

Fonte: Psychology Today

Situações Mais Comuns de *Cyberbullying*
Exercício

Fonte: Vice



Fonte: Bricks Magazine

PLANO DE SESSÃO Nº 9

1. Identificação da Ação

Designação	Curso de Formação Apoio Especializado a Vítimas de Cibercrime		
Módulos/ temas	Apoio especializado a vítimas de furto de ciber-*bullying*		
Data da Sessão	**Horário**	**Duração da Sessão**	40 minutos
Formadores/as			

2. Objetivos Específicos

No final da sessão, os/as formandos/as deverão ser capazes de:

- Distinguir, corretamente, a natureza e *modi operandi* do ciber-*bullying*;
- Enumerar, de forma correta, estratégias de intervenção propostas para o apoio especializado a vítimas de ciber-*bullying*;
- Reconhecer, de forma correta, estratégias de prevenção da revitimação propostas para a intervenção junto de vítimas de ciber-*bullying*.

3. Estrutura da Sessão

	Conteúdos Programáticos	Metodologia	Recursos Pedagógicos/ Didáticos	Avaliação | Exercícios	Tempo (minutos)
Introdução	*Modi operandi* e natureza dos crimes	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
Desenvolvimento	Estratégias de prevenção	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
	Estratégias de intervenção: • Estratégias para preservação de prova digital • A quem e como reportar/denunciar • Estratégias para superar a vitimação e seus impactos	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	15
	Exercício n.º 5	Ativa	Regras do Exercício n.º 5 e Caso do Exercício n.º 5	Observação	10
Conclusão	Síntese conclusiva e esclarecimento de questões	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5

OBSERVAÇÕES

Destionatários/as:
Técnicos/as de Apoio à Vítima (TAV)

Data: / / **Formador(a):**

INSTRUÇÕES E INFORMAÇÕES ESSENCIAIS PARA O/A FORMADOR(A)

CORRESPONDÊNCIA DE CONTEÚDOS

Plano de Sessão	*Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*	
	PARTE	CAPÍTULO
Modi operandi e natureza do crime	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Estratégias de prevenção	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Estratégias de intervenção		
Estratégias para preservação de prova digital	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
A quem e como reportar/denunciar	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Estratégias para superar a vitimação e seus impactos	Parte II - Proceder Ver Apresentação e Enquadramento do Módulo	Capítulo 2 – 2.1.
Exercício n.º 5	Sem correspondência Ver Regras do Exercício n.º 5	
Síntese conclusiva e esclarecimento de questões	Sem correspondência	

REGRAS DO EXERCÍCIO N.º 5

Módulo/Tema	Apoio especializado a vítimas de ciber-*bullying*	CÓD. REF.	ÁREA DE EDUCAÇÃO E FORMAÇÃO

Objetivos

Este exercício tem como objetivo consolidar a informação e conteúdo programático deste Módulo, abordando a natureza das situações de ciber-*bullying*, bem como as estratégias de intervenção que devem ser acionadas pelo/a TAV no apoio a vítimas de ciber-*bullying*.

Execução

O/A formador[a] deve distribuir o Caso do Exercício n.º 5, para leitura individual dos/as formandos/as.

Depois da leitura, o/a formador[a] deverá questionar o grupo sobre as formas de agressão/violência presentes no Caso.

No decurso da participação do grupo, deve o/a formador[a] salientar ou reforçar, em função das opiniões e partilhas dos/as formandos/as, as agressões identificáveis na dinâmica de ciber-*bullying* presente no Caso: exclusão, partilha de boatos e agressão verbal. Neste caso em concreto, importa que o/a formador[a] saliente também o potencial de a situação de ciber-*bullying* coocorrer com situações de *bullying* convencional, relativamente à vítima [João], na medida em que vítima e agressor/a apresentam uma relação de proximidade [i.e., são colegas de turma]. A possibilidade de as situações de agressão online serem acompanhadas por violência *offline* [ou seja, cara-a-cara] deve ser considerada na intervenção e na definição de estratégias de prevenção da revitimação.

Na sequência da reflexão em grupo realizada relativamente às dinâmicas de *bullying* e ciber-*bullying* presentes, o/a formador[a] deverá solicitar a participação de dois/duas dos/as formandos/as, para a simulação de uma sessão de apoio/atendimento:

- um dos/as formandos/as deverá desempenhar o papel de João [vítima do Caso deste Exercício], recorrendo ao texto do Caso para explicar, pelas suas palavras, a situação de violência vivida;
- o/a outro/a formando/a deverá desempenhar o papel da profissional de apoio/TAV.

Nesta simulação, importa sobretudo que o/a formador[a] esteja atento/a ao/à formando/a que desempenha o papel de TAV. Devem ser destacadas as estratégias de apoio contidas no campo *Estratégias de Intervenção* da Apresentação e Enquadramento do Módulo. Devem também ser exploradas as *Estratégias de Prevenção* da revitimação abordadas também na Apresentação e Enquadramento deste Módulo.

O/a formador[a] poderá também promover a participação dos/as demais formandos/as, nomeadamente solicitando sugestões de estratégias a considerar e outros aspetos relevantes a contemplar na simulação da sessão de apoio/atendimento, nomeadamente:

- a prestação de apoio emocional;
- a recolha de informação;
- a avaliação do risco e definição de medidas de segurança;
- a identificação de necessidades de apoio.

Pretende-se, neste caso, articular os objetivos deste Módulo com o conteúdo programático já abordado no Módulo 4, nomeadamente com os aspetos centrais no apoio especializado a vítimas de cibercrime.

Notas

Consultar Apresentação e Enquadramento do Módulo

CASO DO EXERCÍCIO N.º 5

João tem 12 anos. A sua atividade preferida, nos últimos 5 meses, foi jogar um jogo *online*. Este jogo era jogado em grupo e João pertencia ao grupo criado por Rui, o seu melhor amigo de infância. Neste grupo, estavam também outros/as colegas de turma, com quem João e Rui jogavam. No último período, Rui teve muito más notas e os pais compararam-no ao João, dizendo: "Devias era ser como o João. Ele é que é um aluno como deve ser!". Rui ficou com muita raiva e inveja de João. Não conseguindo lidar com as suas emoções, descarregou-as no João: excluí-o do grupo de jogo e insultou-o agressivamente: "Não prestas para nada! Não sabes jogar, só nos atrasas a todos! És uma pedra nos nossos sapatos! Vai mas é estudar, seu marrão caixa de óculos!"

Para além disto, Rui espalhou no chat do grupo o boato de que o João tinha ido "fazer queixinhas" aos pais de Rui, dizendo que o Rui faltava às aulas para ficar a jogar.

Os/As colegas ficaram do lado de Rui, visto terem algum receio dele. Rui é dois anos mais velho que os/as restantes colegas e é mais alto e forte.

MOD. 10

MOD. 10

Uma em cada três pessoas mantém relacionamentos *online*[44]. Neste contexto, uma em dez pessoas refere já ter partilhado fotos íntimas suas.

Para além disso, crê-se que 55% das pessoas que mantêm relacionamentos *online*, já foi vítima de algum tipo de crime[45].

Este Módulo apresenta precisamente dois fenómenos de cibervitimação associados aos riscos da presença *online* e da utilização das TIC e da internet para o estabelecimento de relacionamentos interpessoais de maior intimidade: o ciber-*stalking* e a partilha não-consensual de imagens.

Tipos, *modi operandi* e natureza do crime

Ciber-stalking

O ciber-*stalking* pode ser definido como o uso das TIC para ameaçar ou assediar a vítima. Tal como o *stalking*, o ciber-*stalking* é um tipo de violência caracterizado pelo seu carácter intrusivo e repetitivo na esfera da vida privada da vítima, causando-lhe medo e insegurança. Consequentemente, as vítimas experienciam um estado contínuo de ansiedade que afeta a sua qualidade de vida, forçando-as, no limite, a mudar as suas rotinas diárias.

O facto de esta perseguição acontecer online permite ao/à agressor(a) ter à sua disposição vários meios para manter a atividade criminosa, bem como atacar um número superior de vítimas. Os/As agressores/as podem ser alguém que a vítima conhece, bem como pessoas mais próximas/íntimas, como amigos/as ou (ex-)companheiros/as, mas também pessoas que a vítima não conhece.

As formas mais comuns de ciber-*stalking* são:

- Assédio da vítima;
- Furto de identidade;
- Ameaças;
- Contactos de natureza sexual indesejados – por exemplo, envio, sem consentimento, de *dick pics* (diz respeito a imagens de órgãos genitais masculinos enviadas/recebidas através de dispositivos eletrónicos) por parte do/a agressor(a), como forma de incomodar a vítima;
- Contactos insistentes e indesejados.

Partilha não-consensual de imagens

No contexto das relações de intimidade, pode haver lugar à partilha *online* de mensagens de cariz sexual, vídeos ou imagens, comportamento designado por ***sexting*** (resulta da combinação das palavras '*sex*' (sexo) e '*texting*' (envio de SMS)) e que pressupõe a troca de mensagens eróticas, com ou sem fotos, via telemóvel, chats ou redes sociais.

A prática de *sexting* de forma consensual, no âmbito de um relacionamento íntimo, pode ser saudável. Poderá também, no entanto, aumentar a vulnerabilidade das pessoas envolvidas à **partilha não-consensual de imagens**.

A partilha não-consensual de imagens e vídeos pode ser definida pela divulgação de imagem íntima, sem consentimento da pessoa que vê a sua imagem ser partilhada, quando a mesma esperava que esta imagem fosse mantida em sigilo. Uma imagem íntima é aquela em que uma pessoa está nua, ou expondo os seus seios, órgãos genitais ou região anal, ou está envolvida em atividade sexual. Pode ser qualquer gravação visual, incluindo uma fotografia, filme ou gravação de vídeo.

As motivações para a divulgação destas imagens e vídeos podem ser:

- **Extorsão ou coação da vítima**: o/a autor(a) do crime, depois de receber, de forma consensual, vídeos ou

[44] Veja-se https://www.kaspersky.com/blog/online-dating-report/.

[45] *Idem.*

fotografias de cariz sexual da vítima, ameaça a divulgação das mesmas, caso a vítima não forneça novos conteúdos autoproduzidos de natureza sexual ou não aceda a um encontro pessoal;

- **Vingança**: esta prática também é comumente designada como ***revenge porn***, dizendo respeito à divulgação não-consensual de imagens íntimas por parte de um(a) companheiro/a relativamente ao/à outro/a, habitualmente no término de uma relação. É um fenómeno comum em situações de violência nas relações íntimas, incluindo violência doméstica, em que, aquando do final da relação, são divulgadas imagens e/ou vídeos (ou é ameaçada a sua divulgação) do/a respetivo/a ex-companheiro/a junto de familiares e amigos/as, redes sociais ou mesmo *websites* pornográficos, como forma de retaliação pelo facto de ter terminado o relacionamento.

Estratégias de prevenção

Para **prevenir situações de ciber-*stalking* e de partilha não-consensual de imagens**, neste ponto do Módulo, o/a formador(a) deve transmitir aos/às formandos/as as seguintes estratégias que estes/as, enquanto profissionais de apoio (TAV), poderão utilizar na intervenção com a criança/jovem vítima e a sua família:

- Parar toda a comunicação com o/a agressor(a);
- Não bloquear ou desativar a rede social/plataforma de comunicação que o/a agressor(a) utilizou para comunicar com a vítima, uma vez que plataformas como WhatsApp® ou Viber® usam encriptação ponta a ponta (Veja-se Módulo 8);
- Não fornecer informação pessoal ou dados pessoais requeridos através de *e-mails*, mensagens, chamadas, *websites* não solicitados;
- Configurar as definições de privacidade e segurança dos perfis/contas em redes sociais e outras plataformas, eliminando informação pessoal ou outra que possa identificar a morada de casa, escola/trabalho, número de telemóvel, etc.;
- Ativação de filtros de *spam* e de assédio;
- Sensibilizar para os riscos inerentes à utilização da internet e das TIC nos relacionamentos e explicar o funcionamento das plataformas de comunicação e o modo como podem ser utilizadas de forma segura. Com jovens adultos e pessoas adultas, é importante abordar questões relacionadas com o "*safe sexting*", nomeadamente através do uso de plataformas que utilizam encriptação ponta a ponta e que têm a opção de não permitir que as imagens ou vídeos fiquem gravadas no telemóvel do/a destinatário/a;
- Editar as imagens/vídeos, nomeadamente de natureza íntima, antes da sua partilha/divulgação, de forma a proteger a identidade, removendo elementos de identificação pessoal, como o rosto, sinais e/ou tatuagens, bem como a georreferenciação da imagem;
- Configurar as definições de privacidade e segurança dos perfis/contas em redes sociais e outras plataformas.

Estratégias de intervenção

Estrategias para preservação de prova digital

Ainda neste Módulo, o/a formador(a) deve apresentar junto dos/as formandos/as estratégias que podem ser explicadas à vítima em processo de apoio, para a preservação da prova. Esta secção do Módulo explora também algumas das dificuldades associadas à preservação de prova e que advêm das características das próprias plataformas utilizadas para comunicar (encriptação ponta a ponta).

Vejamos algumas delas.

As situações de ciber-*stalking* e de divulgação/partilha não-consensual de imagens ocorrem comumente nas redes sociais ou em plataformas de conversação *online*, residindo aí muitas das provas da prática de crime.

- O método mais eficaz para salvaguarda de provas nas redes socias são as **capturas de ecrã** do conteúdo que se pretende denunciar. Contudo, é essencial que, nessas capturas de ecrã, esteja visível o **URL** (Localizador Uniforme de Recursos) dos respetivos conteúdos.
- Através do URL, mesmo que o conteúdo já não esteja disponível na plataforma, as autoridades podem solicitar às empresas que lhes forneçam informação relativas a quem publicou o conteúdo.

Estas estratégias de preservação de prova são apresentadas através de exemplos concretos das redes sociais:

- É possível **identificar um URL específico de um *post* ou comentário** no Facebook®:
  - Clicar no horário ou data em que foi realizada a publicação ou em que o comentário foi publicado;
  - Ao clicar no horário ou data, é gerada uma nova janela no navegador da internet. Na referida janela, é visível o URL que corresponde ao da publicação ou comentário. Este URL deve ser copiado/guardado e partilhado com as autoridades.

O problema das plataformas de conversação que usam encriptação de Ponta a Ponta (E2E *encryption*)

A **encriptação de ponta a ponta** prende-se com o facto de apenas recetor(a) e emissor(a) conseguirem ver a mensagem desencriptada, o que significa que, caso o conteúdo da conversação seja apagado, as autoridades não têm forma de pedir o registo das conversações às entidades que disponibilizam o serviço. Estas plataformas de comunicação - como WhatsApp® - acabam por ser vantajosas para eventuais autores/as deste tipo de cibercrimes.

Nestes casos, a necessidade de realizar **capturas de ecrã**, como salvaguarda de prova, é particularmente importante.

É também importante definir mecanismos de **armazenamento automático *(backups)*** nas definições da aplicação, de forma a ter acesso à informação, mesmo que seja eliminada por algum dos intervenientes.

A quem e como reportar/denunciar

Os tipos de violência descritos – ciber-*stalking* e partilha não-consensual de imagens - podem constituir a prática de vários crimes, nomeadamente **devassa da vida privada** (arts. 192º e 197º do CP) e **gravação e fotografias ilícitas** (art. 199º do CP).

Também no contexto de relações íntimas no crime de **violência doméstica**, foi introduzida a alínea b) do n.º 2 do art. 152.º do CP pela Lei n.º 44/2018, que visou precisamente dar proteção particular aos dados pessoais (designadamente imagem ou som, o que inclui vídeos, filmes e fotos) sobre a intimidade (nomeadamente a sexualidade) e a reserva da vida privada de qualquer vítima (dados privados que são sensíveis), quando são difundidos (divulgados/espalhados) através da internet ou de outros meios de difusão pública generalizada (como, por exemplo, através das redes sociais), sem o consentimento da vítima.

Esta qualificação especial/agravação do crime de violência doméstica visa o combate ao ciber-*stalking* em contexto de violência doméstica, entendido como as condutas que consistem em "enviar correios eletrónicos, mensagens de texto e mensagens instantâneas ofensivas ou ameaçadoras, publicar comentários ofensivos sobre a vítima na internet, partilhar fotografias ou vídeos íntimos da mesma através da internet" e que são vividas como "mais intrusivas para as vítimas" e "provocam mais efeitos psicológicos adversos".

Estas condutas podem ser denunciadas junto de qualquer órgão de polícia criminal ou Ministério Público.

Estratégias para superar a vitimação e seus impactos

Na sequência dos aspetos-chave para a intervenção com vítimas de cibercrime trabalhadas no Módulo 4 e das estratégias de prevenção e intervenção já delineadas, cumpre ao/à profissional de apoio (TAV) facultar à vítima um conjunto de orientações práticas.

O/a profissional de apoio, na estruturação do atendimento e apoio à vítima, deve também ter em consideração o **impacto da experiência de cibervitimação** e as consequências sentidas pela vítima. Veja-se o Módulo 3 deste Curso de Formação, bem como o capítulo 4 - Parte I do *Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*.

Através de Casos presentes no Exercício proposto (Ver Plano de Sessão), o/a formador(a) terá oportunidade para

explorar as dinâmicas de cada forma de cibervitimação, bem como as consequências e as estratégias-chave que deverão ser utilizadas no processo de intervenção.

No caso do **ciber-*stalking***, o/a formador(a) deve apresentar junto dos/as formandos/as um conjunto de estratégias que poderão utilizar no âmbito do apoio e intervenção com a vítima. Ora vejamos, as estratégias de segurança:

- Evitar contactar e/ou confrontar o/a autor(a) dos comportamentos de ciber-*stalking*;
- Não responder a qualquer tentativa de contacto efetuada pelo/a autor(a) das condutas de ciber-*stalking* e guardar cópias dessas tentativas de contacto/mensagens;
- Guardar todas as cartas, *e-mails*, SMS, bilhetes, presentes e/ou outros materiais que a pessoa que o/a tem assediado lhe tenha enviado;
- Informar pessoas próximas – familiares e amigos/as, colegas de trabalho/ginásio/escola, vizinhos – da situação de cibervitimação, para que em nenhuma circunstância forneçam informações ao/à autor(a) dos comportamentos de assédio;
- Optar por caminhos alternativos aos que usualmente utiliza para se deslocar;
- Pedir a alguém de confiança que o/a acompanhe ao carro ou até ao transporte que normalmente utiliza;
- Quando se deslocar de carro, manter as portas trancadas durante o percurso; garantir uma distância de segurança em relação ao veículo da frente, caso tenha necessidade de mudar de caminho/faixa de rodagem;
- Anotar quaisquer incidentes suspeitos, criando um registo detalhado dos comportamentos de que tem sido alvo;
- Em situação de perigo, deve ser procurado um local seguro ou onde estejam mais pessoas. Também pode ser acionados os contactos de emergência.

Vejamos também outras estratégias de apoio:

- Explicar e reforçar que a culpa não é da vítima, mas do/a autor(a) dos comportamentos;
- Transmitir a ideia de que a vítima tem o direito de dizer que *não*;
- Transmitir a ideia de que o/a agressor(a) pode fazer uso de estratégias manipulatórias/chantagem: fazer com que a vítima se sinta culpada, com o intuito de a levar a fazer algo que este deseja;
- Explicar à vítima como proceder no sentido de salvaguardar a prova digital (veja-se informação supra);
- Facultar estratégias de segurança e contactos de emergência;
- Indicar à vítima a quem e como reportar/denunciar;
- Facultar estratégias de prevenção e intervenção para evitar novos crimes (veja-se informação supra);
- Reforçar a retoma de atividades.

No caso da **partilha não-consensual de imagens**, o/a formador(a) deve apresentar junto dos/as formandos/as um conjunto de estratégias que poderão utilizar no âmbito do apoio e intervenção com a vítima:

- Validar e reconhecer a sua experiência enquanto cibervitimação e enquadrar as reações da vítima no âmbito de uma experiência de vida anormal;
- Reduzir a culpabilização;
- Certificar-se que a vítima compreendeu que nunca deverá ceder a chantagens por parte do/a agressor(a) – a cedência não cessará o comportamento do/a agressor(a);
- Facultar, de forma simples, concisa e clara, as estratégias de prevenção e intervenção anteriormente delineadas;
- Disponibilizar apoio, nomeadamente o apoio psicológico;
- Equacionar a possibilidade de articulação com serviço de psiquiatria, caso exista ideação suicida.

Apoio Especializado a Vítimas de Cibercrime

PARTE II - APOIO ESPECIALIZADO A VÍTIMAS DE CIBERCRIME

Módulo 10 - Apoio especializado a vítimas de violência online nas relações interpessoais: ciber-stalking e partilha não-consensual de imagens

a. *Modi operandi* e natureza do crime

Ciber-*stalking*

O ciber-*stalking* pode ser definido como o uso das TIC para ameaçar ou assediar a vítima. Tal como o *stalking* (perseguição), o ciber-*stalking* é um tipo de violência caracterizado pelo seu carácter intrusivo e repetitivo na esfera da vida privada da vítima, causando-lhe medo e insegurança. Consequentemente, as vítimas experienciam um estado contínuo de ansiedade que afeta a sua qualidade de vida, forçando-as, no limite, a mudar as suas rotinas diárias.

O facto de esta perseguição acontecer *online* permite ao/à agressor(a) ter à sua disposição vários meios para manter a atividade criminosa, bem como atacar um número superior de vítimas.

Os/As agressores/as podem ser alguém que a vítima conhece, bem como pessoas mais próximas/íntimas, como amigos/as ou ex-companheiros(as), mas também pessoas que a vítima não conhece.

a. *Modi operandi* e natureza do crime

Ciber-*stalking*

As formas mais comuns são:

- Assédio da vítima;
- Furto de identidade;
- Ameaças;
- Contactos de natureza sexual indesejados – por exemplo, envio, sem consentimento, de *dick pics* (diz respeito a imagens de órgãos genitais masculinos enviadas/recebidas através de dispositivos eletrónicos) por parte do/a agressor/a, como forma de incomodar a vítima;
- Contactos insistentes e indesejados.

a. *Modi operandi* e natureza do crime

Partilha não-consensual de imagens

A divulgação não consensual de imagens e vídeos pode ser definida pela partilha de imagem íntima, sem consentimento da pessoa que vê a sua imagem ser partilhada, quando a mesma esperava que esta imagem fosse mantida em sigilo.

Uma imagem íntima é aquela em que uma pessoa está nua, ou expondo seus seios, órgãos genitais ou região anal, ou está envolvida em atividade sexual. Pode ser qualquer gravação visual, incluindo uma fotografia, filme ou gravação de vídeo.

a. *Modi operandi* e natureza do crime

Partilha não-consensual de imagens

A prática de *Sexting*, como já abordado no Módulo 6 na parte referente às burlas nos relacionamentos íntimos, particularmente quanto aos ***Riscos dos Relacionamentos Online***, pode aumentar a vulnerabilidade das pessoas envolvidas à partilha não-consensual de imagens.

Várias são as **motivações** que podem estar na base da divulgação das imagens:

- Extorsão ou coação da vítima
- Vingança

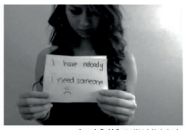
Divulgação Não Consensual de Imagens e Vídeos

Os contextos onde estas imagens podem vir a ser partilhadas ou obtidas sem o consentimento das vítimas podem ser vários, nesse sentido vamos detalhar três destes contextos, a saber:

- *Sextortion*
- *Non consensual image sharing ("Revenge Porn")*
- *Grooming*

Sextortion

Uma das piores consequências do *Sexting* é a ***Sextortion***, uma forma de coação em que o/a autor/a do crime depois de receber de forma consensual vídeos ou fotografias de cariz sexual da vítima, ameaça a divulgação das mesmas caso a vítima não forneça mais fotos ou vídeos, dinheiro, ou não aceda a que se encontre pessoalmente com o agressor/a.



Amanda Todd, Fonte: Watch Nederland

É exemplo de uma destas situação o trágico suicídio de Amanda Todd em 2012, quando tinha 15 anos de idade, motivado pelo facto de estar a ser vítima de coação por parte de uma pessoa que conhecera num chat na internet, que após Amanda ter partilhado foto em topless, foi coagida por esta pessoa a partilhar mais conteúdo seu de cariz sexual, sob ameaça de divulgação da sua foto aos seus familiares e amigos.

Revenge Porn

Outro fenómeno associado aos relacionamentos *Online* é a divulgação não consensual de imagens íntimas por parte de um/a companheiro/a relativamente ao outro/a no termino de uma relação (muito vezes designado, embora indevidamente, por culpabilizador da vítima, como **Revenge Porn**).

É um fenómeno comum em relacionamentos onde existe violência doméstica, onde aquando do final da relação são divulgadas imagens do respetivo ex-companheiro/a junto de familiares e amigos, redes sociais ou mesmo sites pornográficos, como forma de retaliação pelo facto do/a companheiro/a ter terminado o relacionamento.

b. Estratégias de prevenção

- Parar toda a comunicação com o/a agressor(a);
- Não bloquear ou desativar a rede social/plataforma de comunicação que o/a agressor(a) utilizou para comunicar com a vítima, uma vez que plataformas como WhatsApp® ou Viber® usam encriptação ponto a ponto (Veja-se Módulo 8);
- Não fornecer informação pessoal ou dados pessoais pedidos através de *e-mails*, mensagens, chamadas, *websites* não solicitados;
- Configurar as definições de privacidade e segurança dos perfis/contas em redes sociais e outras plataformas, eliminando qualquer tipo de informação pessoal ou outra que possa identificar a morada de casa, escola/trabalho, número de telemóvel, etc.;
- Ativação de filtros de *spam* e de assédio;

b. Estratégias de prevenção

- Sensibilizar para os riscos inerentes à utilização da internet e das TIC nos relacionamentos e explicar o funcionamento das plataformas de comunicação e o modo como podem ser utilizadas de forma segura. Com jovens adultos e pessoas adultas, é importante abordar questões relacionadas com o "*safe sexting*", nomeadamente através do uso de plataformas que utilizam encriptação ponto a ponto e que têm a opção de não permitir que as imagens ou vídeos fiquem gravadas no telemóvel do/a destinatário/a;
- Editar as imagens/vídeos, nomeadamente de natureza íntima, antes da sua partilha/divulgação, de forma a proteger a identidade, removendo elementos de identificação pessoal, como o rosto, sinais e/ou tatuagens, bem como a georreferenciação da imagem;
- Configurar as definições de privacidade e segurança dos perfis/contas em redes sociais e outras plataformas.

c. Estratégias de intervenção

i. Preservação da prova digital

Salvaguarda de Prova nas Redes Sociais

Muitas das situações de Cibercrime ocorrem através das redes sociais, sejam situações de *Cyberbullying*, furto de identidade, burlas, sendo necessário às vítimas ou às estruturas de apoio à vítima saber salvaguardar a prova da existência destas situações de crime nessas redes socais.

O método mais eficaz para salvaguarda de provas nas redes socias são as **capturas de ecrã** do conteúdo que se pretende denunciar, mas muitas vezes, só isso não é suficiente, sendo por isso necessário e essencial que nessas capturas de ecrã esteja visível o URL (Localizador Uniforme de Recursos) dos respetivos conteúdos, bem como a data e hora da captura.

Através do URL mesmo que o conteúdo já não esteja disponível na plataforma, as autoridades podem solicitar às empresas que lhes forneçam informação relativas a quem publicou o conteúdo.

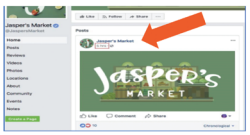
c. Estratégias de intervenção

Salvaguarda de Prova nas Redes Sociais

Exemplo do Facebook

Por exemplo, um perfil de Facebook® pode conter conteúdo que viola os padrões de comunidade, mas pode o mesmo referir-se a um determinado *post* em vez de ser todo o perfil. Assim sendo, de modo a salvaguardar a prova e as autoridades conseguirem investigar é possível identificar um URL específico do *post* em concreto, seguindo as seguintes instruções:

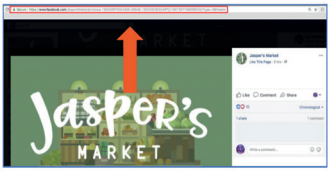
1. Clique no horário ou data em que foi feita a publicação:



c. Estratégias de intervenção

Salvaguarda de Prova nas Redes Sociais

Exemplo do Facebook

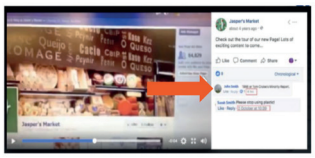


2. Ao clicar no horário ou data da publicação esta irá gerar uma nova janela no seu navegador da internet. Deve copiar o URL desta nova janela pois o mesmo corresponde ao da publicação. É este URL que deve ser partilhado com as autoridades.

c. Estratégias de intervenção

Salvaguarda de Prova nas Redes Sociais

Salvaguarda de Comentários nas Redes Sociais



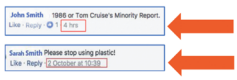
Como já foi referido é de extrema importância reportar o URL específico do conteúdo que se pretende denunciar. Para denunciar um comentário a uma publicação devo seguir os seguintes passos:

c. Estratégias de intervenção

Salvaguarda de Prova nas Redes Sociais

Salvaguarda de Comentários nas Redes Sociais

1. Clique no horário ou na data em que o comentário foi publicado.



2. Ao fazê-lo irá gerar uma nova janela. Deverá copiar o URL da nova janela e guardá-lo como prova.

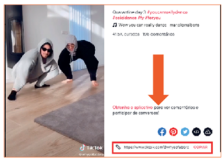
c. Estratégias de intervenção

Salvaguarda de Prova nas Redes Sociais

Salvaguarda nas Redes Sociais

Os procedimentos para a rede Social Facebook podem ser aplicados a outras redes sociais, como por exemplo o Instagram.

Na rede Social TikTok o processo também é muito fácil uma vez que para cada vídeo que é partilhado é disponibilizado o respetivo URL do conteúdo.



O Problema das Plataformas de Conversação que usam Encriptação de Ponta a Ponta
(E2E *encrytpion*)

Muitos/as criminosos/as tentam aliciar as vítimas a comunicar em plataformas que usem tecnologias de encriptação que impeçam as próprias empresas que disponibilizam o serviço de chat a ter acesso às mesmas.

A encriptação de ponta a ponta prende-se com o facto de apenas recetor e emissor conseguirem ver a mensagem desencriptada o que significa que se o conteúdo for apagado as autoridades não têm forma de pedir a estas entidades que disponibilizam o serviço, os registos das conversas.

Fonte: FAVPNG


Fonte: WIRE


Fonte: Signal

O Problema das Plataformas de Conversação que usam Encriptação de Ponta a Ponta
(E2E *encrytpion*)

Nestes casos a necessidade de retirar capturas de ecrã como salvaguarda de prova ganha aqui muito maior importância, uma vez que em muitos casos é a única forma de provar a existência de crime se as conversas forem apagadas.

É também importante definir mecanismos de armazenamento automático (*backups*) nas definições da aplicação de forma a ter acesso à informação mesmo que esta seja apagada por algum/a dos/as intervenientes.

Fonte: FAVPNG


Fonte: WIRE


Fonte: Signal

Atividade – Debate

"How Encryption Works - and How It Can Be Bypassed" (2016)

https://www.youtube.com/watch?v=TImdsUglGv4

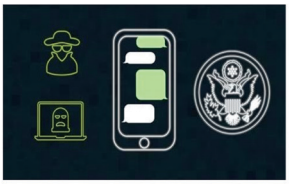


Tabela de Prova:

Ferramenta para ajudar as vítimas na organização da recolha de prova

Data	O que aconteceu	Provas de que aconteceu	Quem suspeito que tenha sido o/a autor/a	Prova de que foi o/a autor/a	Provas que ainda preciso e quem as pode ter
Jan 1-2 2020	Às 16h00 encontrei fotos íntimas minhas que foram divulgadas em website – url: https://....	Guardei estas páginas com as minhas imagens íntimas como PDF no meu computador	Ex-namorado(a)	O ex-namorado(a) tirou essas fotos. O ex-namorado(a) já me tinha ameaçada com exposição das fotos. Por exemplo, [insira detalhes] Recebi mensagem de texto às 16:00 indica: "vais-te arrepender." Captura de ecrã dessa mensagem guardada em computador.	Temos amigo em comum (referir nome do amigo) que recebeu mensagem de ex-namorado(a) onde este dizia que iria publicar fotos intimas minhas, estou à espera que me envie essas mensagens

Desafios à Investigação:

- Provar que o/a acusado/a é realmente a pessoa que postou as fotos, e não um terceiro com quem as fotos foram compartilhadas;
- As vítimas frequentemente não se apercebem que as fotos foram compartilhadas fora do relacionamento;
- O uso de smartphones leva a que fotos e vídeos sejam captadas com desconhecimento da vítima, com maior facilidade;
- Dificuldade em convencer vítima, amigos e familiares a salvaguardar as imagens e vídeos como prova em vez de as apagar.

b. Estratégias de intervenção

ii. A quem e como reportar/denunciar

Os tipos de violência descritos – ciber-*stalking* e a partilha não-consensual de imagens - podem constituir a prática de vários crimes, nomeadamente **devassa da vida privada** (arts. 192º e 197º do CP); **gravação e fotografias ilícitas** (art. 199º do CP).

Também no contexto de relações íntimas no crime de **violência doméstica** , foi introduzida a alínea b) do n.º 2 do art. 152.º do CP pela Lei n.º 44/2018, que visou precisamente dar proteção particular aos dados pessoais (designadamente imagem ou som, o que inclui vídeos, filmes e fotos) sobre a intimidade (nomeadamente a sexualidade) e a reserva da vida privada de qualquer vítima (dados privados que são sensíveis), quando são difundidos (divulgados/espalhados) através da internet ou de outros meios de difusão pública generalizada (como, por exemplo, através das redes sociais), sem o consentimento da vítima.

Estas condutas podem ser denunciadas junto de qualquer órgão de polícia criminal ou Ministério Público.

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

A divulgação não consensual de imagens e vídeos íntimos tem fortes impactos na vitimação:

- Números significativos de vítimas experimentam "Rutura social" – a situação de vitimação tem um impacto tão forte que altera drasticamente todos os aspetos das suas vidas.
- As ameaças são percebidas como reais e levando a que as vítimas façam tudo o que lhes está a ser pedido.
- Intenso isolamento de amigos, familiares, mundo *online* e da sociedade em geral.
- As vítimas reportam um abuso constante e contínuo por parte dos/as agressores/as.
- Este tipo de situação tem potencial de ter impacto negativo não apenas na vida das vítimas , mas também de pessoas próximas como familiares e amigos.

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

Estratégias a utilizar pelo/a TAV no âmbito de **partilha não-consensual de imagens:**

- Validar e reconhecer a sua experiência enquanto cibervitimação e enquadrar as reações da vítima no âmbito de uma experiência de vida anormal;
- Reduzir a culpabilização;
- Certificar-se que a vítima compreendeu que nunca deverá ceder a chantagens por parte do/a agressor(a) – a cedência não cessará o comportamento do/a agressor(a);
- Facultar, de forma simples, concisa e clara, as estratégias de prevenção e intervenção anteriormente delineadas;
- Disponibilizar apoio, nomeadamente o apoio psicológico;
- Equacionar a possibilidade de articulação com serviço de psiquiatria, caso exista ideação suicida.

Módulo 10 - Apoio especializado a vítimas de violência online nas relações interpessoais: ciber-stalking e partilha não-consensual de imagens

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

Estratégias a utilizar pelo/a TAV no âmbito de **ciber-stalking:**

- Explicar e reforçar que a culpa não é da vítima, mas do/a autor(a) dos comportamentos;
- Transmitir a ideia de que a vítima tem o direito de dizer que *não*;
- Transmitir a ideia de que o/a agressor(a) está a usar uma estratégia manipulatória: fazer com que a vítima se sinta culpada, com o intuito de a levar a fazer algo que este deseja;
- Explicar à vítima como proceder no sentido de salvaguardar a prova digital (já abordadas);
- Facultar estratégias de segurança e contactos de emergência;
- Indicar à vítima a quem e como reportar;
- Facultar estratégias de prevenção e intervenção para evitar novos crimes (já abordadas);

Módulo 10 - Apoio especializado a vítimas de violência online nas relações interpessoais: ciber-stalking e partilha não-consensual de imagens

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

Estratégias de **segurança** a transmitir à vítima de **ciber-stalking:**

- Evitar contatar e/ou confrontar o/a autor/a dos comportamentos de ciber-*stalking*;
- Não responder a qualquer tentativa de contacto efetuada pelo/a autor(a) das condutas de ciber-*stalking* e guardar cópias dessas tentativas de contacto/mensagens;
- Guardar todas as cartas, *e-mails*, SMS, bilhetes, presentes e/ou outros materiais que a pessoa que o/a tem assediado lhe tenha enviado;
- Informar pessoas próximas – familiares e amigos/as, colegas de trabalho/ginásio/escola, vizinhos – da situação de cibervitimação, para que em nenhuma circunstância forneçam informações ao/à autor/a dos comportamentos de assédio;

Módulo 10 - Apoio especializado a vítimas de violência online nas relações interpessoais: ciber-stalking e partilha não-consensual de imagens

b. Estratégias de intervenção

iii. Orientações práticas para superar a vitimação e seus impactos

Estratégias de **segurança** a transmitir à vítima de **ciber-stalking:**

- Optar por caminhos alternativos aos que usualmente utiliza para se deslocar;
- Pedir a alguém de confiança que o/a acompanhe ao carro ou até ao transporte que normalmente utiliza;
- Quando se deslocar de carro, manter as portas trancadas durante o percurso; manter uma distância de segurança em relação ao veículo da frente, caso tenha necessidade de mudar de caminho/faixa de rodagem;
- Anotar quaisquer incidentes suspeitos, criando um registo detalhado de todos os comportamentos de que tem sido alvo;
- Em situação de perigo, deve ser procurado um local seguro ou onde estejam mais pessoas. Também pode ser acionados os contactos de emergência.

obrigad@

PLANO DE SESSÃO Nº 10

1. Identificação da Ação

Designação Curso de Formação Apoio Especializado a Vítimas de Cibercrime

Módulos/ temas Apoio especializado a vítimas de violência *online* nas relações interpessoais: ciber-*stalking* e partilha não-consensual de imagens

Data da Sessão **Horário** **Duração da Sessão** 40 minutos

Formadores/as

2. Objetivos Específicos

No final da sessão, os/as formandos/as deverão ser capazes de:

- Distinguir, corretamente, a natureza e *modi operandi* da violência *online* nas relações interpessoais, nomeadamente do ciber-*stalking* e da patilha não consensual de imagens;
- Enumerar, de forma correta, estratégias de intervenção propostas para o apoio especializado a vítimas de ciber-*stalking* e vítimas de patilha não-consensual de imagens;
- Reconhecer, de forma correta, estratégias de prevenção da revitimação propostas para a intervenção junto de vítimas de ciber-*stalking* e vítimas de patilha não-consensual de imagens.

3. Estrutura da Sessão

	Conteúdos Programáticos	Metodologia	Recursos Pedagógicos/ Didáticos	Avaliação | Exercícios	Tempo (minutos)
Introdução	Tipos: • Ciber-*stalking* • Partilha não-consensual de imagens	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
Desenvolvimento	*Modi operandi* e natureza dos crimes	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
	Estratégias de prevenção	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5
	Estratégias de intervenção: • Estratégias para preservação de prova digital • A quem e como reportar/denunciar • Estratégias para superar a vitimação e seus impactos	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	10
	Exercício n.º 6	Ativa	Regras do Exercício n.º 6 e Caso A e Caso B do Exercício n.º 6	Observação	10
Conclusão	Síntese conclusiva e esclarecimento de questões	Expositiva e ativa	Computador: *Datashow* e tela para projeção	Observação	5

OBSERVAÇÕES

Destionatários/as:
Técnicos/as de Apoio à Vítima (TAV)

Data: / / **Formador(a):**

INSTRUÇÕES E INFORMAÇÕES ESSENCIAIS PARA O/A FORMADOR(A)

CORRESPONDÊNCIA DE CONTEÚDOS

Plano de Sessão	*Manual ROAR – da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas*	
	PARTE	CAPÍTULO
Tipos, *modi operandi* e natureza do crime	Parte I - Compreender	Capítulo 1 – 1.3.
	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Estratégias de prevenção	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Estratégias de intervenção		
Estratégias para preservação de prova digital	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
A quem e como reportar/denunciar	Sem correspondência Ver Apresentação e Enquadramento do Módulo	
Estratégias para superar a vitimação e seus impactos	Parte II - Proceder	Capítulo 2 – 2.1.
	Ver Apresentação e Enquadramento do Módulo	
Exercício n.º 6	Sem correspondência Ver Regras do Exercício n.º 6	
Síntese conclusiva e esclarecimento de questões	Sem correspondência	

REGRAS DO EXERCÍCIO N.º 6

Módulo/Tema	Apoio especializado a vítimas de violência *online* nas relações interpessoais: ciber-*stalking* e partilha não-consensual de imagens	**CÓD. REF.**	**ÁREA DE EDUCAÇÃO E FORMAÇÃO**

Objetivos

Este exercício tem como objetivo consolidar a informação e conteúdo programático deste Módulo, abordando a natureza das situações de ciber-*stalking* e de partilha não-consensual de imagens, bem como as estratégias de intervenção que devem ser acionadas pelo/a TAV no apoio a vítimas.

Execução

O/A formador[a] deve dividir o grupo de formandos/as em 2 a 4 pequenos grupos. A metade dos grupos criados deve ser entregue Caso A do Exercício n.º 6 e à restante metade dos grupos criados deverá ser entregue o Caso B do Exercício n.º 6.

O caso A retrata uma situação de ciber-*stalking* e o Caso B uma situação de partilha não-consensual de imagens [*revenge porn*].

O/A formador[a] deve pedir a cada um dos pequenos grupos criados para ler atentamente o respetivo Caso atribuído e definir, em grupo, as medidas e estratégias a implementar no apoio a cada vítima.

Em seguida, deve pedir que o[s] grupo[s] a quem tenha sido atribuído o Caso A partilhem as suas sugestões de estratégias. Deve salientar, na discussão do Caso, as estratégias de intervenção sumariadas na Apresentação e Enquadramento do Módulo.

Deverá repetir o procedimento para a discussão do Caso B.

Notas

Consultar Apresentação e Enquadramento do Módulo

CASO A DO EXERCÍCIO N.º 6

Matilde, 22 anos, estudante universitária.

Um dos grandes *hobbies* de Matilde é a fotografia. Matilde passava horas a tirar fotografias a paisagens de que gostava. Passava também muito tempo a editar as suas fotografias.

Um dos maiores gostos de Matilde, era ver o sucesso do seu trabalho, através dos *likes* dos/as seus/as seguidores/as nas suas fotografias publicadas no Instagram®. Por isso, a sua conta de Instagram® era "aberta" e aceitava todos os pedidos para ser seguida.

De há 5 meses para cá, Matilde tem sido vítima de ciber-*stalking* nas redes socias.

O agressor, Carlos, abordou-a inicialmente através de um simples pedido para segui-la, seguido de um convite para jantar. Matilde recusou, alegando que não estava interessada em relacionamentos amorosos. Carlos questionou esta recusa e perguntou a Matilde porque é que ela o desprezava, porque é que o rejeitava. Matilde respondeu educadamente, alegando que não o conhecia e que, por isso, não poderia aceitar. O perfil de Carlos não tinha fotos que o pudessem identificar.

Carlos contou-lhe que, muito embora ela não o conhecesse, ele conhecia-a bem. De seguida, começou a criar perfis falsos, recorrendo a dados pessoais de Matilde (ex.: morada, data de nascimento, morada dos pais, nome do irmão) ou refletindo ameaças (ex.: "Eu apanho-te e nem sabes o que faço."; "Vou-te matar que é o que mereces."; "Ninguém me rejeita.").

Foram centenas os perfis falsos criados. Para além de apresentar queixa, Matilde viu-se obrigada a apagar o seu perfil de Instagram®, a mudar de casa e de faculdade. Além de viver com medo e insegurança contínuos, o seu desejo de fotografar deixou completamente de existir.

No primeiro atendimento, Matilde relata o seguinte:

"O motivo pelo qual eu aqui venho é ter a certeza que estou a fazer as coisas certas. Eu só quero ter a certeza que estou a tomar as atitudes certas. Eu não percebo o que é que eu fiz. Será que eu devia ter dito que sim? Será que fui rude?"

CASO B DO EXERCÍCIO N.º 6

Maria, de 43 anos, partilha o seguinte no primeiro atendimento:

"Estive numa relação durante cerca de 8 anos. Vivíamos juntos. Ele não era agressivo comigo nem nada, dávamo-nos bem. Simplesmente deixei de gostar dele. Já não me sentia preenchida, nem feliz naquela relação. Acabei tudo há cerca de 6 meses.

Desde então, que ele começou a ameaçar que enviava umas fotos minhas, que uma vez, estupidamente, lhe enviei. São fotos íntimas, em que exponho o meu corpo.

Ao início, era só um pedido para que voltássemos a estar juntos. Eu até compreendi, porque sei que estava desesperado...Eu fui muito importante para ele. Ainda para mais, ele é uma pessoa que tem poucos amigos. Além de ser sua mulher, eu era a grande amiga dele para todas as horas.

Mas, passado um mês, as ameaças começaram a ser mais frequentes, foram crescendo e passaram a ser diárias. Desde há uma semana, que ele ameaça que envia as minhas fotos a todos os meus amigos, família e às pessoas do meu trabalho.

Eu não cedi. Ele já não é a mesma pessoa, metia-me nojo! Hoje acordei e ele enviou-me logo de manhã um *print screen* de um *e-mail* que enviou para:

o meu chefe, todos os meus colegas de trabalho (somos 24, ele não falhou 1!), os meus pais, os meus irmãos e as minhas tias. Como é que eu vou voltar a sair de casa? Como? Eu não posso ir trabalhar! Eu não consigo olhar para a cara dos meus colegas! Nunca mais ninguém me vai levar a sério (choro compulsivo). Eu devia ter cedido, eu devia ter cedido...Ou nunca devia ter acabado com ele, porque é que eu acabei com ele? Eu não quero viver mais... (choro compulsivo)."

ROAR
empowering
victims of
cybercrime

APAV
associação portuguesa de
Apoio à Vítima

This Manual was funded by the
European Union's Internal
Security Fund – Police

MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA

WEISSER RING
Wir helfen Kriminalitätsopfern.

ACTEDO

altice