

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
Asociația Pentru
Apărarea Victimei
Apoio a Vitima



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

Parteneri:

Associação Portuguesa de Apoio à Vítima (APAV) | Portugalia

Parteneri:

Ministério da Administração Interna (MAI) | Portugalia

Procuradoria-Geral da República (PGR) | Portugalia

PT Portugal | Portugalia

Weisser Ring | Germania

Centrul de Acțiune pentru Egalitate și Drepturile Omului (ACTEDO) | România

ISBN: 978-989-53116-1-3

Descriere CIP:

Titlu:

Manual de formare:

Asistență specializată pentru victimele criminalității informatice

Autor:

2021 © APAV – Associação Portuguesa de Apoio à Vítima

Adresă:

APAV – Associação Portuguesa de Apoio à Vítima

Rua José Estêvão, 135 A

1150-201 Lisabona

Portugalia

Tel.: +351 213 587 900

Email: apav.sede@apav.pt

Website: www.apav.pt

Facebook: www.facebook.com/APAV.Portugal

Introducere	5
a. Prezentarea Formării	7
a.1. Obiectivele Formării	7
a.2. Structura și programul	7
a.3. Durata	9
a.4. Formatori	9
a.5. Evaluarea și certificarea formării	9
b. Organizarea Formării	11
b.1. Resurse	11
b.2. Notițe pentru Formator	12
Anexe	15
PARTEA 1 – SĂ ÎNȚELEGEM CRIMINALITATEA INFORMATICĂ	37
MODULUL 1 – ÎNȚELEGEREA FENOMENELOR DE CRIMINALITATE INFORMATICĂ	37
Tipuri de criminalitate informatică	37
Concepte și definiții	37
Factori de risc și vulnerabilitățile comportamentale legate de victimizarea informatică	40
MODULUL 2 – CADRUL LEGISLATIV PRIVIND CRIMINALITATEA INFORMATICĂ	45
Criminalitatea informatică în dreptul internațional și în acquis-ul Uniunii Europene	45
Cadrul legislativ privind criminalitatea informatică la nivel național	45
Principalele provocări în cercetare și în aplicarea legii	46
MODULUL 3 – VICTIMIZAREA ȘI IMPACTUL CRIMINALITĂȚII INFORMATICE	49
Prevalența criminalității informatice	49
Impactul asupra victimelor individuale	50
• Consecințe asupra sănătății fizice, psihologice și emoționale	50
• Impactul financiar	51
• Teama de criminalitatea informatică și percepțiile cu privire la securitatea cibernetică	51
PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME	55
MODULUL 4 – ASPECTE FUNDAMENTALE ÎN SPRIJINUL SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII INFORMATICE	55
Structurarea sprijinului specializat victimelor criminalității informatice	55
• Empatie, tehnici de comunicare și sprijin emoțional	55
• Colectarea informațiilor	56
• Evaluarea riscurilor și elaborarea planurilor de securitate	56
• Identificarea nevoilor de sprijin	57
• Intervenția în criză	58
MODULUL 5 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII CIBER-DEPENDENTE	63
Modi operandi și natura infracțiunilor	63
Strategii de prevenire	64
Strategii de intervenție	65
• Strategii de conservare a dovezilor digitale	65
• Cui și cum să raportați/denunțați	66
• Strategii de depășire a victimizării și impactele acesteia	66
MODULUL 6 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE FRAUDELOR ONLINE	71
Tipurile de infracțiuni, Modi operandi și natura infracțiunilor	71
• Înșelăciuni în comerțul electronic (e-commerce)	71
• Fraude bancare	71
• Înșelăciuni în relațiile intime (romance scams)	72
Strategii de prevenire	73
Strategii de intervenție	74
• Strategii de conservare a dovezilor digitale	74
• Cui și cum să raportați/denunțați	74
• Strategii de depășire a victimizării și impactele acesteia	74

MODULUL 7 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE FURTULUI DE IDENTITATE ONLINE	81
Modi operandi și natura infracțiunilor	81
Strategii de prevenire	83
Strategii de intervenție	83
• Strategii de conservare a dovezilor digitale	83
• Cui și cum să raportați/denunțați	83
• Strategii de depășire a victimizării și impactele acesteia	84
MODULUL 8 – SPRIJIN SPECIALIZAT PENTRU COPII ȘI TINERI VICTIME ALE ABUZULUI SEXUAL ONLINE	89
Tipuri, modi operandi și natura infracțiunii	89
• Diseminarea conținutului de abuz sexual asupra copiilor (CSAM)	89
• Conținut cu abuz sexual asupra copiilor generat online	89
• Auto-producere de conținut	90
• Transmiterea în direct a abuzului sexual asupra copiilor	90
• Ademenire (grooming online)	90
• Ademenire pe rețelele sociale și pe jocurile video online	91
Strategii de prevenire	91
Strategii de intervenție	91
• Strategii de conservare a dovezilor digitale	91
• Cui și cum să raportați/denunțați	92
• Strategii de depășire a victimizării și impactele acesteia	92
MODULUL 9 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE CYBERBULLYING-ULUI	99
Modi operandi și natura infracțiunilor	99
Strategii de prevenire	100
Strategii de intervenție	100
• Strategii de conservare a dovezilor digitale	100
• Cui și cum să raportați/denunțați	100
• Strategii de depășire a victimizării și impactele acesteia	101
MODULUL 10 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE ÎNȘELĂCIUNILOR ONLINE ÎN RELAȚIILE INTIME: CYBERSTALKING ȘI PORNOGRAFIA NON-CONSENSUALĂ	107
Tipuri, Modi operandi și natura infracțiunilor	107
• Cyberstalking	107
• Partajarea nonconsensuală a imaginilor	107
Strategii de prevenire	108
Strategii de intervenție	108
• Strategii de păstrare a dovezilor digitale	108
• Cui și cum să raportați/denunțați	109
• Strategii de depășire a victimizării și impactele acesteia	109

INTRODUCERE

DESPRE MANUAL

În prezent, aproximativ 90% dintre cetățenii Uniunii Europene au acces la internet¹, odată cu creșterea utilizării zilnice a internetului de către utilizatori². Într-o lume din ce în ce mai globalizată, în care nu doar frontierele fizice, dar și cele virtuale sunt estompate, riscurile asociate cu utilizarea internetului sunt sporite. Prin urmare, nu este surprinzător faptul că victimizarea prin fraudă sau furt de date constituie al șaselea risc global și, al șaptelea risc cel cu probabil să apară, este victimizarea în urma unei infracțiuni cibernetice.³

Criminalitatea informatică s-a răspândit în toate domeniile criminalității, cu atacuri îndreptate nu numai împotriva oamenilor și a patrimoniului, ci și împotriva statelor, cu impact asupra structurilor critice, a economiei și, în esență, a securității și coeziunii rețelei sociale.

Copiii sunt un grup deosebit de vulnerabil la cibervictimizare, având în vedere limitarea lor naturală a capacităților de reziliență cibernetică și conștientizarea redusă a riscurilor asociate cu utilizarea internetului, precum și faptul că accesul la internet are loc tot mai devreme, din cauza prin acces facil la smartphone-uri și tablete.⁴ În consecință, este important să acordați atenție la conținutul sexual explicit auto-produs, adică creat chiar de copii sau de tineri. Pe de altă parte, infracțiunile legate de conținut cu abuzuri sexuale asupra copiilor și exploatarea minorilor și ademenirea minorilor în vederea săvârșirii actelor sexuale, prin utilizarea internetului, găsesc o mai mare posibilitate de succes în complexitatea internetului.⁵

De asemenea, persoanele cu vârsta de peste 55 de ani au fost, la fel, asociate cu o expunere majoră la riscurile inerente utilizării internetului, fiindu-le mai dificil să fie informați cu privire la aceste riscuri și, în consecință, adoptarea unor măsuri personale de securitate digitală este mai puțin probabilă.⁶

Rezoluția Parlamentului European din 3 octombrie 2017 privind combaterea criminalității informatice (2017/2068 (INI))⁷, exprimă considerații importante cu privire la impactul asupra siguranței persoanelor, integritatea datelor lor cu caracter personal, precum și asupra protecției vieții private și a libertăților fundamentale, datorită creșterii semnificative a atacurilor *ransomware*, *botnets* și a interferențelor neautorizate cu sistemele informatice, subliniind necesitatea armonizării dispozițiilor legale privind criminalitatea informatică și abuzul și exploatarea sexuală asupra copiilor *online* în diferite State Membre. În acest scop, este esențială consolidarea cooperării între *stakeholders* și între state.

La rândul lor, victimele criminalității informatice ar trebui să beneficieze pe deplin de toate drepturile lor,⁸ iar statele membre ar trebui să se concentreze pe prevenire și conștientizare și pe sprijin specializat în caz de victimizare.

Prin urmare, este o nevoie urgentă de a îmbunătăți înțelegerea criminalității informatice, în special în ceea ce privește populația în general, specialiștii și factorii de decizie politică, și de a promova răspunsuri concertate în lupta împotriva criminalității informatice. În acest scop, se subliniază necesitatea de a uni forțele și competențele Statelor, ale industriei, ale organismelor de poliție penală, ale organelor poliției judiciare, ale *mass-media* și ale organizațiilor societății civile pentru a asigura investigații eficiente și pentru a asigura o abordare axată pe drepturile victimelor.

Astfel, cu scopul de a crea instrumente utile de conștientizare și instruire în lupta împotriva criminalității informatice, prin stabilirea procedurilor și instruirea specializată în sprijinirea și capacitatea acestor victime, a fost elaborat în cadrul Proiectului ROAR, **“ROAR - Manual de Formare: Asistență Specializată pentru Victimele Criminalității Informatice (Project ROAR-Training Manual: Specialised Support to Victims of Cybercrime)**, coordonată de APAV (Asociația Portugheză pentru Sprijinire a Victimelor), în parteneriat cu Garda Națională Republicană, Procuratura Generală și Altice

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

² În contextual european, a se vedea *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. A se vedea de asemenea *Barometrul APAV / INTERCAMPUS, Percepția populației privind Securitatea Cibernetică*, Martie 2020, pp. 11-12.

⁷ P8_TA(2017)0366, Rezoluția Parlamentului European, din 3 octombrie 2017, privind lupta împotriva criminalității informatice [2017/2068(INI)].

⁸ Stabilite în Directiva 2012/29/EU.

Portugalia, precum și cu partenerul internațional Weisser Ring (Germania) și Centrul de Acțiune pentru Egalitate și Drepturile Omului – ACTEDO (România). Acest proiect, cofinanțat de Fondul pentru Securitate Internă - Poliția Uniunii Europene, urmărește să sensibilizeze societatea civilă în general și, în special, potențialele victime ale acestui tip de criminalitate, contribuind la creșterea rezilienței cibernetice, la numărul de infracțiuni informatice raportate autorităților și la cererea de servicii specializate de sprijin.

Acest Manual de Formare stabilește o serie de recomandări de formare pentru un public bine definit și esențial în sprijinirea victimelor criminalității informatice – specialiști în sprijinirea victimelor – concentrându-se, de asemenea, pe prevenirea și combaterea fenomenului, oferind exemple și materiale utile, pragmatice și actualizate cu realitatea europeană.

Acest Manual de Formare nu intenționează să se concentreze asupra conținutului pe care îl abordează, ci mai degrabă să stabilească linii directoare pentru organizarea activităților de formare pentru publicul-țintă menționat anterior, vizând, pe lângă propunerea de sugestii procedurale pentru un sprijin mai bun și mai eficient acordat victimelor criminalității informatice, să promoveze o reflecție comună în rândul cursanților cu privire la conceptele-cheie precum „victimele criminalității”, „criminalitatea informatică”, „securitatea cibernetică” sau „reziliența cibernetică”.

Așadar, Cursul “Sprijin Specializat pentru Victimele Criminalității Informatice” este organizat în felul următor.

- a.** Prezentarea formării
- b.** Organizarea formării
- c.** Desfășurarea cursului de formare
- d.** Sesiuni de formare
- e.** Resurse didactice
- f.** Bibliografie
- g.** Legislație

INTRODUCERE

a. Prezentarea Formării

Cursul de Formare "Sprijin Specializat pentru Victimele Criminalității Informatică" își propune să familiarizeze și să instruiască specialiștii în sprijinirea victimelor cu privire la fenomenul criminalității informatice, precum și la realitățile conexe și impactul acestora asupra victimelor, cadrul lor legislativ și aspectele importante în comunicarea și interacțiunea cu victimele acestor infracțiuni.

Se intenționează ca Specialiștii în Sprijinirea Victimelor să înțeleagă particularitățile infracțiunilor care au avut loc în mediul digital și impactul pe care acestea îl generează asupra victimelor, pentru a înțelege mai bine nevoile lor speciale în ceea ce privește informarea și sprijinul, și astfel să aducă îmbunătățiri în modul în care oferă sprijin și comunică cu aceste victime.

Obiectivul acestui Curs de Formare este de asemenea de a promova conștientizarea și capacitatea victimelor criminalității informatice, și anume prin crearea mecanismelor de reziliență cibernetică și promovarea creșterii infracțiunilor raportate și garantarea că sistemului de justiție penală și a serviciilor în sprijinirea victimelor furnizează răspunsuri, adecvate, adaptate și centrate pe victimă și nevoilor sale speciale.

SCOPUL CURSULUI

La sfârșitul Cursului de Formare, cursanții ar trebui să fie capabili să recunoască corect diferitele tipuri și concepte asociate cu criminalitatea informatică, precum și alte aspecte la fel de importante pentru intervenția cu victimele criminalității informatice, și anume: cadrul legislativ privind criminalitatea informatică; factorii de risc și impactul criminalității informatice; aspectele fundamentale ale sprijinului specializat victimelor criminalității informatice; sprijinul specializat pentru victimele a diferitor tipuri de infracțiuni cibernetice, inclusiv modi operandi, strategii specifice de intervenție și prevenire.

STRUCTURA ȘI DISTRIBUȚIA TEMPORALĂ A CURSULUI

	INTRODUCERE ȘI CONTEXT	DURATĂ
	Prezentarea formatorului Prezentarea cursanților Prezentarea obiectivelor și a conținutului intervenției de formare	5 Minute
	PARTEA 1 - SĂ ÎNȚELEM CRIMINALITATEA INFORMATICĂ	
Modulul 1	Înțelegerea fenomenelor de criminalitate informatică Tipuri de criminalitate informatică Concepte și definiții Factori de risc și vulnerabilități comportamentale legate de cibervictimizare	30 Minute
Modulul 2	Cadrul legislativ privind criminalitatea informatică Criminalitatea informatică în dreptul internațional și în <i>acquis-ul</i> Uniunii Europene Cadrul legislativ privind criminalitatea informatică la nivel național Principalele provocări în investigare și în aplicarea legii	45 Minute
Modulul 3	Victimizarea și impactul criminalității informatice Prevalența criminalității informatice Impactul asupra victimelor individuale Consecințele asupra sănătății fizice, psihologice și emoționale Impact financiar Teama de criminalitatea informatică și percepțiile asupra securității cibernetice	20 Minute
	PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME	
Modulul 4	Aspecte fundamentale în sprijinul specializat pentru victimele criminalității informatice Structurarea sprijinului specializat pentru victimele criminalității informatice Empatie, tehnici de comunicare și sprijin emoțional Colectarea de informații Evaluarea riscurilor și elaborarea planurilor de securitate Identificarea necesităților de sprijin Intervenție în criză	80 Minute

INTRODUCERE

a. Prezentarea Formării

Modulul 5 Sprijin specializat pentru victimele infracțiunilor cibernetice

Modi operandi și natura infracțiunilor
Strategii de prevenire
Strategii de intervenție
Strategii pentru păstrarea dovezilor digitale
Cui și cum să raportați / denunțați
Strategii pentru a depăși victimizarea și impactul acesteia

40 Minute

Modulul 6 Sprijin specializat pentru victimele fraudelor online

Tipuri, *modi operandi* și natura infracțiunilor
Înșelăciuni în comerțul electronic (*e-commerce*)
Fraude bancare;
Înșelăciuni în relații intime (*romance scams*)
Strategii de prevenire
Strategii de intervenție
Strategii pentru păstrarea dovezilor digitale
Cui și cum să raportați / denunțați
Strategii pentru a depăși victimizarea și impactul acesteia

40 Minute

Modulul 7 Sprijin specializat pentru victimele furtului de identitate online

Modi operandi și natura infracțiunii
Strategii de prevenire
Strategii de intervenție
Strategii pentru păstrarea dovezilor digitale
Cui și cum să raportați / denunțați
Strategii pentru a depăși victimizarea și impactul acesteia

40 Minute

Modulul 8 Sprijin specializat copiilor și tinerilor victime ale abuzului sexual online

Tipuri, *modi operandi* și natura infracțiunilor
Diseminarea conținutului cu abuz sexual asupra copiilor (CSAM)
Conținut cu abuz sexual asupra copiilor generat online
Auto-producere de conținut
Abuzul sexual asupra copiilor în direct
Ademenire (*grooming online*)
Ademenire pe rețele sociale și în jocurile video online
Strategii de prevenire
Strategii de intervenție
Strategii pentru păstrarea dovezilor digitale
Cui și cum să raportați / denunțați
Strategii pentru a depăși victimizarea și impactul acesteia

40 Minute

Modulul 9 Sprijin specializat pentru victimele de cyber-bullying

Modi operandi și natura infracțiunii
Strategii de prevenire
Strategii de intervenție
Strategii pentru păstrarea dovezilor digitale
Cui și cum să raportați / denunțați
Strategii pentru a depăși victimizarea și impactul acesteia

40 Minute

Modulul 10 Sprijin specializat pentru victimele înșelăciunilor online în relațiile intime: cyberstalking și pornografia non-consensuală

Tipuri, *modi operandi* și natura infracțiunilor
Cyber-stalking
Pornografia non-consensuală
Strategii de prevenire
Strategii de intervenție
Strategii pentru păstrarea dovezilor digitale
Cui și cum să raportați / denunțați
Strategii pentru a depăși victimizarea și impactul acesteia

40 Minute

INTRODUCERE

a. Prezentarea Formării

Fiecare modul este prezentat inițial cu un **scurt cadru teoretic / conceptual** iar ulterior este organizat schematic printr-un **plan de sesiune**, în felul următor:

- Tema
- Destinatari
- Durata sesiunii
- Obiectiv general
- Obiective specifice
- Conținut programatic
- Metodologie
- Resurse pedagogice / didactice
- Evaluare | Exerciții
- Observații

DURATA TOTALĂ A CURSULUI

Durata totală a acestui Curs de Formare este de 7 ore (420 minute).

Cursul trebuie predat o zi.

FORMATORI

Se recomandă ca formatorii să dețină un certificat acreditat de formator (emis sau recunoscut de A.N.C.) și să aibă pregătire în domeniul științelor sociale și umane.

EVALUAREA ȘI CERTIFICAREA FORMĂRII

Evaluarea Formării

Evaluarea rezultatelor formării se efectuează:

- De către formatori prin Raportul de Evaluare a Cursanților (a se vedea modelul în anexă acestui manual);
- De către cursanți, prin Raportul de Evaluare a Formării (a se vedea modelul în anexă acestui manual).

Certificarea cursanților:

- Eliberarea unui Certificat de Participare la Formarea Profesională - document emis de o entitate de formare care certifică că cursantul a urmat un curs de formare (a se vedea modelul certificatului în anexă);
- Evaluarea cursanților se realizează într-un mod continuu și interactiv, concentrându-se pe observarea performanței în exercițiile propuse.

INTRODUCERE

b. Organizarea formării

Acest Manual cuprinde în structura sa: exerciții, materiale pentru prezentare, cum ar fi prezentări *PowerPoint*, materiale pentru distribuire și pentru a susține dinamizarea sesiunilor de formare.

Resurse

Pentru desfășurarea Cursului de Formare, este necesar să se ia în considerare diferitele resurse pe care le vom enumera mai jos.

Resurse spațiale și materiale

Resursele spațiale și materiale joacă un rol esențial în organizarea unui curs de Formare, iar formatorul ar trebui să ia în considerare în prealabil locul unde va fi desfășurat cursul, resursele materiale utilizate și inventarul materialelor. În mod ideal, numărul cursanților per curs ar trebui să fie între 10 și 18.

Prin urmare, vă sugerăm să verificați următorul *checklist*:

CRITERII

CHECKLIST

- Sala de curs are acustică și iluminare adecvate
- Sala de curs se află în stare perfectă de igienă și curățenie.
- Există destule prize
- Condițiile și aspectul meselor și al scaunelor sunt adecvate
- Există un calculator cu software adecvat (*Office PowerPoint*)
- Este data show, coloane și ecran de proiecție
- Există foi albe și pixuri pentru a le distribui cursanților
- Există materiale didactice pentru a fi distribuite cursanților
- Există o tablă albă și markere

Cursanții ar trebui să fie informați cu privire la locurile în care își pot lua masa pe durata cursului și localizarea mijloacelor de transport în comun pe care le pot folosi, cum ar fi stațiile de autobuz, stațiile de metrou și stații de taxi cele mai apropiate.

INTRODUCERE

b. Organizarea formării

SFATURI PENTRU FORMATOR

PREGĂTIREA CURSULUI DE FORMARE

- Citiți, înțelegeți și rețineți conținutul ROAR - Manual de Formare: Sprijin Specializat pentru Victimele criminalității informatice.
- Familiarizați-vă cu resursele disponibile în Manualul menționat, inclusiv materialul vizual propus [prezentări PowerPoint], precum și cu exercițiile și materialele care trebuie distribuite
- Completați și citiți Manualul de Formare consultând conținutul Manualului ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor
- Luați la cunoștință obiectivele și programul cursului de formare
- Pregătiți în număr suficient toate documentele [programe, formulare de înscriere, materiale didactice etc.] pentru a fi distribui cursanților
- Pregătiți foi albe și pixuri suficiente pentru a fi distribuite cursanților
- Verificați fișa de prezență, formularele de Evaluare a Satisfacției de Formare și formularul de Evaluare Individuală a cursanților
- Verificați condițiile sălii, ținând cont de numărul de cursanți care vor participa la cursul de formare
- Verificați condițiile software-ului, data show-ului, difuzoarele și ecranului

LA ÎNCEPUTUL CURSULUI DE FORMARE

- Organizați o primire bună a cursanților
- Accentuați importanța cursului - exprimați importanța acțiunii și a rezultatelor care se așteaptă să fie atinse
- Prezentați obiectivele și programul cursului de formare

ÎN TIMPUL CURSULUI DE FORMARE

- Interacționați și comunicați cu cursanții și promovați un climat de apropiere
- Colectați feedback intermediar cu privire la formare, deoarece puteți mereu să faceți corecții sau să schimbați strategiile de dinamizare
- Validați și accentuați mesajele
- Întrebați dacă sunt nelămuriri

LA FINALUL CURSULUI DE FORMARE

- Completați Raportul de Evaluare al cursanților
- Evaluați reacția cursanților la curs prin distribuirea formularelor de Evaluare a Satisfacției la Formare

Prezentările PowerPoint ar trebui să ghideze și să sprijine dezvoltarea / dinamizarea acestui Curs de Formare, dar nu ar trebui doar citite. Ar trebui adăugate oral Informații suplimentare și / sau complementare pentru a consolida prezentarea conținutului.

În timpul prezentării, trebuie acordată atenție imaginii și să vă asigurați că aceasta este focalizată și centrată și că poate fi văzută de oriunde în sala de curs în care are loc formarea. Luminozitatea imaginii trebuie ajustată astfel încât cursanții să poată citi diapozitivele, fără a le întuneca.

Formatorul ar trebui să fie preocupat de modul în care expune conținutul programului, și prin urmare trebuie să ia în considerare următoarele aspecte:

- Tonul vocii;
- Gesturile;
- Atitudini / pozițiile corpului;
- Expresia feței;
- Citirea numelor participanților;

INTRODUCERE

b. Organizarea formării

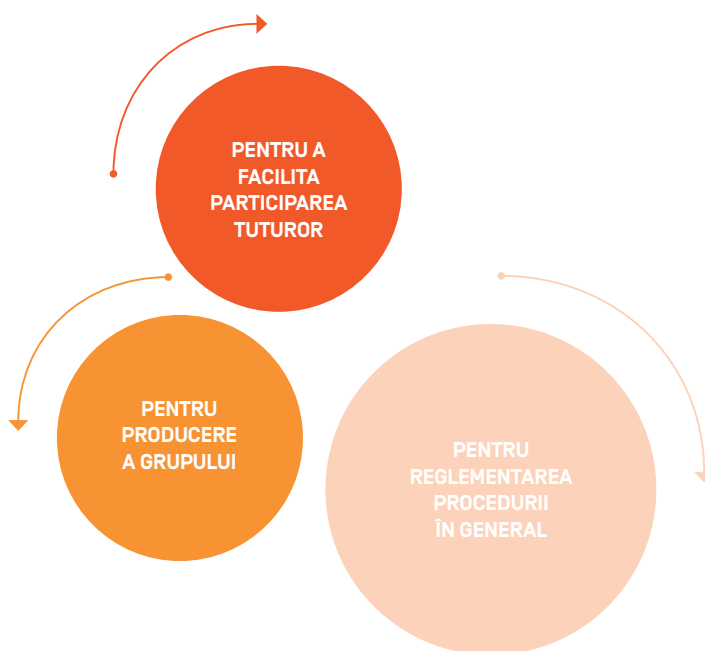
- Imaginile;
- Exemplele;
- Simțul umorului;
- Folosirea analogiilor.

De asemenea, ar trebui să fiți atenți la modul în care promovați participarea grupului și la modul în care utilizați materialele audiovizuale pentru a explica, a arăta și a ilustra.

De asemenea, formatorul trebuie să fie conștient de faptul că întreaga expunere are:



Totodată, formatorul ar trebui să nu uite de faptul că este responsabil:



Pe parcursului formării, formatorul ar trebui să urmărească:

- Să sublinieze ideile principale;
- Să le selecteze și să le pună în valoare;
- Să se asigure că participanții au înțeles materialul parcurs;
- Să își asume diferite funcții: să organizeze, să ghideze, să direcționeze, informeze, interpreteze, reformuleze, animeze, stimuleze, să se refere, modereze și să reconcilieze, ori de câte ori este necesar. Trebuie să facă acest lucru fără ca participanții să simtă acest lucru, ceea ce implică:
 - Să fie capabil și tacticos în relațiile cu oameni, și respectiv cu cursanții prezenți;
 - Abilitatea de a gândi limpede și rapid;
 - Să fie capabil să se exprime cu ușurință;
 - Să rămână imparțial;
 - Să încerce să fie analitic;
 - Să nu se arate influențat;
 - Să prezinte autocontrol;
 - Să fie răbdător.

INTRODUCERE

b. Organizarea formării

Ar trebui să îndeplinească rolul și tehnicile de animator, prin:

- Reformularea opiniilor individuale, care facilitează exprimarea, acordă importanță celor care le emit și încurajează ceilalți participanți să asculte ideile emise, stimulând interacțiunile;
- Sinteză, care are o importanță fundamentală și se desfășoară la toate nivelurile: reformularea și sinteza a unei intervenții mai lungi sau sinteza a două sau mai multe opinii:
 - Sinteza pe propoziție;
 - Rezumat parțial la fiecare punct al planului de sesiune;
 - Sinteza finală.

Formatorul ar trebui să ia în considerare un ansamblu de tehnici:

ÎNTREBAREA DE TEST	Folosită pentru a defini un cuvânt sau un concept pe care participanții îl folosesc cu conotații diferite. De asemenea, este folosită pentru a defini un cuvânt necunoscut pe care un participant l-a folosit.
APEL DIRECT LA PARTICIPARE	Folosit pentru a promova schimbul / participarea unui participant care rămâne tăcut mult timp sau pentru a da cuvântul unui participant care își exprimă interesul de a participa
ÎNTREBAREA ECOU	Întrebare adresată formatorului de către un participant și revenită în aceeași formă, cerându-i să împărtășească propriul răspuns
ÎNTREBAREA PRELUARE	Repetarea întrebării adresate formatorului de către un participant unui alt participant
ÎNTREBAREA OGLINDĂ	Repetarea întrebării adresate formatorului de către un participant, returnând-o grupului
RELANSAREA	Repetarea unei întrebări puse anterior și la care grupul nu răspunsese încă

În plus față de tehnicile anterioare, formatorul poate face cursul de formare mai atractiv și mai plăcut, expunându-și ideile sub formă de întrebări, în loc să facă afirmații directe.

Încheierea sesiunii / modulului și / sau a zilei de formare este un moment extrem de important. O sinteză bună este esențială, prin urmare, formatorul ar trebui:

- Să fie concis;
- Să evidențieze cele mai importante faze și / sau concepte și să menționeze punctele cheie semnificative;
- Să promoveze schimbul de opinii și feedback din partea participanților cu privire la acțiune;
- Să sintetizeze.

ANEXE

- Program
- Cronologie
- Formular de înscriere
- Prezențe și Rezumate
- Înregistrarea evenimentelor și renunțărilor
- Evaluarea satisfacției la formare - cursanți interni
- Evaluarea satisfacției la formare - cursanți externi
- Evaluarea individuală a cursanților
- Tabel final

DATELE	COD REF.	DOMENIUL EDUCAȚIEI ȘI FORMĂRII
INTERVENȚIE FORMATIVĂ	INTERN	INTERPRINDERE
DENUMIRE	Societate	
FORMATORI	Societate	
TIMP	N° DE ORE	7 ore
LOCAȚIE		
CONDIȚII PREALABILE	Colaborați direct sau indirect cu victimele criminalității informatice.	
DESTINATARI	Specialiști în Sprijinirea Victimelor	
MODALITATEA DE FORMARE	Altă formare profesională	MODALITATE DE ORGANIZARE
METODOLOGII	Prezența în persoană	
OBIECTIV GENERAL	Expozitive, interogative și active.	
	La sfârșitul formării, cursanții ar trebui să poată recunoaște corect diferitele tipuri și concepte asociate cu criminalitatea informatică, precum și alte aspecte la fel de importante în intervenția cu victimele infracțiunii cibernetice, și anume: cadrul legislativ privind criminalitatea informatică, factorii de risc și impactul criminalității informatice; aspectele fundamentale în sprijinul specializat pentru victimele criminalității informatice; sprijin specializat pentru victimele diferitor tipuri de criminalitate informatică, și anume <i>modi operandi</i> , strategii de intervenție și strategii de prevenire.	

OBIECTIVE SPECIFICE	La sfârșitul formării, cursanții ar trebui să poată să:
	- Distingă corect, infracțiunile cibernetice și infracțiunile facilitate de internet și TIC; - Recunoască, corect, diferite concepte și definiții asociate cu criminalitatea informatică, și anume tipurile de criminalitate informatică; - Identifice corect factorii de risc privind cibervictimizare, asociați cu caracteristicile sociodemografice; - Precizeze, fără erori, vulnerabilitățile comportamentale legate de cibervictimizare, și anume factorii de risc legați de comportamentele utilizării internetului și TIC; - Recunoască, corect, cadrul legislativ privind criminalitatea informatică, în lumina dreptului internațional și a cadrului juridic național; - Identifice în mod corespunzător cel puțin jumătate din provocările abordate în legătură cu investigarea criminalității informatice și aplicarea legii; - Recunoască corect impactul criminalității informatice în diferite domenii ale vieții a victimelor criminalității informatice; - Identifice în mod corespunzător consecințele criminalității informatice asupra percepțiilor privind securitatea cibernetică și frica cu privire la criminalitatea informatică; - Enumere corect toate aspectele și pașii fundamentali în structurarea sprijinului specializat pentru victimele criminalității informatice; - Distingă corect natura și <i>modi operandi</i> ale diferitelor tipuri de criminalitate informatică; - Enumere corect strategiile de intervenție propuse pentru sprijinul specializat pentru victimele diferitelor tipuri de criminalitate informatică; - Recunoască corect strategiile de prevenire a revictimizării propuse în intervenție cu victimele diferitelor tipuri de criminalitate informatică.

Structura programului	Numărul de ore	Formatori
INTRODUCERE ȘI CONTEXT	5'	
- Prezentarea formatorului - Prezentarea cursanților - Prezentarea obiectivelor și conținutului intervenției de formare		
PARTEA 1 - SĂ ÎNȚELEGEM CRIMINALITATEA INFORMATICĂ		
Modulul 1 - Înțelegerea fenomenelor de criminalitate informatică	30'	
- Tipuri de criminalitate informatică - Concepte și definiții - Factori de risc și vulnerabilități comportamentale legate de cibervictimizare		
Modulul 2 - Cadrul legislativ privind criminalitatea informatică	45'	
- Criminalitatea informatică în dreptul internațional și în <i>acquis</i>-ul Uniunii Europene - Cadrul legislativ privind criminalitatea informatică la nivel național - Principalele provocări în investigare și aplicarea legii		

Modulul 3 - Victimizarea și impactul criminalității informatice 20'

- Prevalența criminalității informatice
- Impactul asupra victimelor individuale
 - Consecinele asupra sănătății fizice, psihologice și emoționale
 - Impact financiar
 - Teama de criminalitatea informatică și percepțiile asupra securității cibernetice

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME**Modulul 4 - Aspecte fundamentale în sprijinul specializat pentru victimele criminalității informatice** 80'

- Structurarea sprijinului specializat victimelor criminalității informatice
 - Empatie, tehnici de comunicare și sprijin emoțional
 - Colectarea informațiilor
 - Evaluarea riscurilor și elaborarea planurilor de securitate
 - Identificarea necesităților de sprijin
 - Intervenție în criză

Modulul 5 - Sprijin Specializat pentru Victimele infracțiunilor cibernetice 40'

- *Modi operandi* și natura infracțiunilor
- Strategii de prevenire
- Strategii de intervenție
 - Strategii pentru păstrarea dovezilor digitale
 - Cui și cum să raportați / denunțați
 - Strategii pentru a depăși victimizarea și impactul acesteia

Modulul 6 - Sprijin specializat pentru victimele fraudelor online 40'

- Tipuri, *modi operandi* și natura infracțiunilor
 - Înșelăciuni în comerțul electronic (*e-commerce*)
 - Fraude bancare
 - Înșelăciuni în relații intime (*romance scams*)
- Strategii de prevenire
- Strategii de intervenție
 - Strategii pentru păstrarea dovezilor digitale
 - Cui și cum să raportați / denunțați
 - Strategii pentru a depăși victimizarea și impactul acesteia

Modulul 7 - Sprijin specializat pentru victimele furtului de identitate online 40'

- *Modi operandi* și natura infracțiunii
- Strategii de prevenire
- Strategii de intervenție
 - Strategii pentru păstrarea dovezilor digitale
 - Cui și cum să raportați / denunțați
 - Strategii pentru a depăși victimizarea și impactul acesteia

Modulul 8 - Sprijin specializat pentru copii și tineri care sunt victime ale abuzurilor sexuale online 40'

- Tipuri, *modi operandi* și natura infracțiunilor
 - Diseminarea conținutului cu abuz sexual asupra copiilor (CSAM)
 - Conținut cu abuz sexual asupra copiilor generat online
 - Auto-Producere de conținut
 - Transmiterea în direct a abuzului sexual asupra copiilor
 - Ademenirea (*grooming online*)
 - Ademenire pe rețelele sociale și în jocurile video online
- Strategii de prevenire
- Strategii de intervenție
 - Strategii pentru păstrarea dovezilor digitale
 - Cui și cum să raportați / denunțați
 - Strategii pentru a depăși victimizarea și impactul acesteia

Modulul 9 - Sprijin specializat pentru victimele de cyber-bullying 40'

- *Modi operandi* și natura infracțiunii
- Strategii de prevenire
- Strategii de intervenție
 - Strategii pentru păstrarea dovezilor digitale
 - Cui și cum să raportați / denunțați
 - Strategii pentru a depăși victimizarea și impactul acesteia

Modulul 10 - sprijin specializat pentru victimele înșelăciunilor online în relațiile intime: cyberstalking și pornografia non-consensuală 40'

- Tipuri, *modi operandi* și natura infracțiunilor
 - Cyber-stalking

- Pornografia non-consensuală
- Strategii de prevenire
- Strategii de intervenție
 - Strategii pentru păstrarea dovezilor digitale
 - Cui și cum să raportați / denunțați
 - Strategii pentru a depăși victimizarea și impactul acesteia

RESURSE DIDACTICE ȘI ECHIPAMENTE

Calculator cu *software Office (PowerPoint)* și *Media Player* (sau un program similar) instalat, proiector | *Datashow*, coloane, televizor sau ecran, scaune, prezentare *PowerPoint*.

BIBLIOGRAFIE DE SUPT

APAV [2020]. Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor. Lisabona: APAV.

EVALUAREA CUNOȘȚINȚELOR

Evaluarea prin creșterea așteptărilor și a nivelului de cunoștințe al cursanților pe această temă.

Evaluare formativă / sumativă efectuată prin exerciții practice și verificare obiectivă.

CERTIFICARE

După finalizarea cu succes a cursului, se va emite un Certificat de Formare Profesională prin intermediul platformei SIGO (Sistemul de Informații și Gestionare a Ofertei Educaționale și de Formare) pe baza următoarelor criterii:

- Participarea la curs este mai mare sau egală cu 80%;
- Realizarea activităților propuse în timpul cursului;

Emiterea certificatelor duplicat are costuri aferente.

ANEXE

CURS: Sprijin specializat pentru victimele criminalității informatice

LOCAȚIE:

DATA DE ÎNCEPERE:

ORAR:

DATA DE ÎNCHEIERE:

LUNA

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 31

DIMINEAȚĂ

SEARĂ

Module

Tematică

Formator

1. Înțelegerea fenomenelor de criminalitate informatică
2. Cadrul legislativ privind criminalitatea informatică
3. Victimizarea și impactul criminalității informatice
4. Aspecte fundamentale în sprijinul specializat pentru victimele criminalității informatice
5. Sprijin specializat pentru victimele infracțiunilor cibernetice
6. Sprijin specializat pentru victimele fraudelor *online*
7. Sprijin specializat pentru victimele furtului de identitate *online*
8. Sprijin specializat pentru copii și tineri victime ale abuzurilor sexuale *online*
9. Sprijin specializat pentru victimele de *cyberbullying*
10. Sprijin specializat pentru victimele violenței online în relațiile interpersonale: *cyber-stalking* și partajare non-consensuală a imaginilor

ANEXE

IDENTIFICAREA CURSANTULUI

Numele complet [*]:

Adresă [*]:

Cod poștal [*]:

Oraș [*]:

—

Naționalitate [*]:

Sex [*]:

Țara de origine [*]:

Data de naștere [*]:

Locul nașterii - județ [*]:

Locul nașterii - Județ [*]:

Telefon Mobil [*]:

E-mail [*]:

Tip de document de identificare [*]:

☐ Permis de Ședere
☐ Identificare națională (carte de cetățean / carte de identitate)

☐ Militar
☐ Pașaport

Cod Numeric Personal [*]:

Valabil până la [*]:

NIF [*]:

COMPETENȚE ACADEMICE

Competențe academice [*]:

Alte competențe:

SITUAȚIA PROFESIONALĂ

Situația privind locul de muncă [*]:

☐ 1. Angajat:
☐ 2. Șomer:
☐ 3. Alta. Vă rugăm să specificați:
☐ 4. În căutarea primului loc de muncă

☐ 1.1. Angajat
☐ 1.2. Liber profesionist
☐ 2.1. Șomer (<12 luni)
☐ 2.2. Șomer de lungă durată (> 12 luni)

DATE PROFESIONALE

Companie [*]:

Domeniu de activitate [*]:

Poziție / Funcție [*]:

DATE DE FACTURARE

Adresă:

NIF:

ACȚIUNE DE FORMARE

Denumirea acțiunii de formare [*]:

Datele [*]:

Locul de desfășurare [*]:

ANEXE

Am luat la cunoștință și accept condițiile de înscriere și participare la această acțiune de formare și condițiile generale referitoare la funcționarea formării stabilite în Regulamentul privind Funcționarea Formării? Dacă da, marcați cu X în casetă.

☐

Conform Regulamentul Național privind Protecția Datelor cu Caracter Personal, datele prezentate aici pot fi diseminate doar în scopul monitorizării și evaluării formării. Pe lângă situațiile menționate, autorizați datele dvs. personale să fie utilizate pentru comunicarea inițiativelor și pentru informare de natură asociativă sau profesională din partea APAV - Asociația Portugheză de Sprijin pentru Victimele? Dacă autorizați, marcați cu X în cutie.

☐

NOTĂ: Criterii de selecție pentru înscrierile primite

1. Ordinea de sosire a cererii, dacă numărul de participanți depășește limita maximă stabilită
2. Limita maximă de cursanți prevăzută de fiecare acțiune de formare
3. Respectarea cerințelor prestabilite pentru fiecare acțiune de formare
4. Respectarea termenului limită pentru depunerea cererilor
5. Completarea formularului de înscriere

Declar, pe propria răspundere, că toate elementele cuprinse în acest formular sunt adevărate.

Data: / /

Semnătura cursantului:

ACTIVITATE DE FORMARE

Responsabil formare:

Data:

Localitate:

ANEXE

DATE PROFESIONALE

DATA	COD REF.	DOMENIUL EDUCAȚIEI ȘI FORMĂRII
DENUMIRE	Sprijin Specializat pentru Victimele Criminalității Informatice	
FORMATORI	ORAR	

Nr.	NUMELE COMPLET	SEMNĂTURĂ		ECHIPA DE COORDONARE A FORMĂRII	
		DIMINEAȚĂ	SEARĂ	ORE ȘI TIP DE ABSENȚĂ	
				JUSTIFICATĂ	NEJUSTIFICATĂ
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

REZUMAT

SEMNATURA FORMATORULUI:

SEMNATURA COORDONĂRII PEDAGOGICE:

ANEXE

ÎNREGISTRAREA EVENIMENTELOR ȘI A RETRAGERILOR

DENUMIREA INTERVENȚIEI
FORMATIVE

Sprijin Specializat pentru Victimele Criminalității Informaticе

DOMENIUL EDUCAȚIEI ȘI
FORMĂRII

COD REF.

FOMRATOR

DATA

ORAR

LOCAȚIE

CURSANT

CONTACTE

Evenimente [marcați cu X]

- ☐ Schimbare programului
- ☐ Schimbarea formatorului
- ☐ Defectarea echipamentului
- ☐ Probleme logistice
- ☐ Retragera cursantului *
- ☐ Probleme inerente cursanților
- ☐ Probleme inerente formatorului
- ☐ Problemele inerente colaboratorilor de sprijin a formării
- ☐ Alte. Care?

* Motivul pentru care cursantul a renunțat [marcați cu X]

- ☐ Motiv de sănătate
- ☐ Motive personale
- ☐ Motive profesionale
- ☐ Probleme cu entitatea de formare
- ☐ Altul. Care?

☐ Nu au existat evenimente și retrageri pentru a fi înregistrate

DESCRIERE

DATA:

SEMNATURA COORDONĂRII PEDAGOGICE:

ANEXE

A SE COMPLETA DE CĂTRE MANAGEMENTUL FORMĂRII

Clasificarea Gravității Evenimentului / Plângerii (marcați cu X)

DE GRAD MINOR

- ☐ Impact scăzut asupra desfășurării formării
- ☐ Prima data

GRAV

- ☐ Impactul asupra desfășurării formării
- ☐ Recurent (a doua oară)
- ☐ Posibilitatea ca mai mult de 2 persoane să fie afectate

FOARTE SERIOS

- ☐ Impact mare asupra desfășurării formării
- ☐ Recurență (mai mult de 2 ori)
- ☐ Număr mare de plângeri aferente
- ☐ Necesită intervenție de coordonare

Soluționarea plângerii

Data soluționării

Descrierea soluției

Data

Semnătura Coordonatorului Executiv

Notificare către părțile interesate

Modalitate de comunicare

Data

EVALUARE A SATISFACȚIEI LA FORMARE - CURSANȚI INTERNI

DATA	COD REF.	DOMENIUL EDUCAȚIEI ȘI FORMĂRII
DENUMIREA CURSULUI / MODULULUI Sprijin Specializat pentru Victimele Criminalității Informaticе		
FORMATORI		
LOCAȚIE		DURATĂ

Opinia dvs. este esențială pentru îmbunătățirea calității formării APAV. Aprecieri sinceritatea dvs. pentru a ne ajuta să ne îmbunătățim. Pentru a face acest lucru, trebuie să procedați la evaluare în conformitate cu următoarea scală:

- 1 = **Rău** (evaluare între 0 și 4 puncte);
 2 = **Insuficient** (evaluare între 5 și 9 valori);
 3 = **Suficient** (evaluare între 10 și 13 valori);
 4 = **Bine** (evaluare între 14 și 17 puncte);
 5 = **Foarte Bine** (evaluare între 18 și 20 de puncte).

1. Organizarea formării

- Durata cursului / modulului
- Condițiile sălii de curs (echipament / confort)
- Coordonarea pedagogică

1	2	3	4	5

2. Formator

- Punctualitate
- Claritatea intervențiilor
- Stăpânirea conținutului (teme)
- Răspuns la întrebări / nelămuriri exprimate
- Metode și tehnici utilizate
- Respectarea programului
- Material de formare (documentație, exerciții)

1	2	3	4	5

3. Conținut

- Relația conținutului în raport cu obiectivele și așteptările dvs.
- Utilitatea conținutului în raport cu rolul pe care îl îndeplinește
- Contribuția conținutului pentru îmbunătățirea profesională / personală
- Așteptarea de a pune în aplicare conținutul în termen de 3 luni

1	2	3	4	5

4. Evaluare globală

- Curs / modul

1	2	3	4	5

OBSERVAȚII ȘI SUGESTII PENTRU ÎMBUNĂȚĂȚIRE

SUGEREĂȚI-NE ALTE CURSURI PE CARE AȚI DORI SĂ LE URMĂRIȚI

Numele Formatorului:

EVALUARE A SATISFACȚIEI LA FORMARE- CURSANȚI EXTERNI

DATA	COD REF.	DOMENIUL EDUCAȚIEI ȘI FORMĂRII
DENUMIREA CURSULUI / MODULULUI Sprijin Specializat pentru Victimele Criminalității Informaticе		
FORMATORI		
LOCAȚIE		DURATĂ

Opinia dvs. este esențială pentru îmbunătățirea calității formării APAV. Aprecieri sinceritatea dvs. pentru a ne ajuta să ne îmbunătățim. Pentru a face acest lucru, trebuie să procedați la evaluare în conformitate cu următoarea scală:

- 1 = **Rău** (evaluare între 0 și 4 puncte);
 2 = **Insuficient** (evaluare între 5 și 9 valori);
 3 = **Suficient** (evaluare între 10 și 13 valori);
 4 = **Bine** (evaluare între 14 și 17 puncte);
 5 = **Foarte Bine** (evaluare între 18 și 20 de puncte).

1. Organizarea formării

- Durata cursului
- Condițiile sălii de curs (echipament / confort)
- Coordonarea pedagogică
- Raport Preț/Calitate

1	2	3	4	5

2. Formator

- Relația conținutului în raport cu obiectivele și așteptările dvs.
- Utilitatea conținutului în raport cu rolul pe care îl îndeplinește
- Contribuția conținutului pentru îmbunătățirea profesională / personală
- Așteptarea de a pune în aplicare conținutul în termen de 3 luni

1	2	3	4	5

3. Conținut

- Relația conținutului în raport cu obiectivele și așteptările dvs.
- Utilitatea conținutului în raport cu rolul pe care îl îndeplinește
- Contribuția conținutului pentru îmbunătățirea profesională / personală
- Așteptarea de a pune în aplicare conținutul în termen de 3 luni

1	2	3	4	5

4. Evaluare globală

- Curs / modul

1	2	3	4	5

OBSERVAȚII ȘI SUGESTII PENTRU ÎMBUNĂȚĂȚIRE

SUGEREAȚI-NE ALTE CURSURI PE CARE AȚI DORI SĂ LE URMĂRIȚI

Numele Formatorului:

ANEXE

DATA	COD REF.	DOMENIUL EDUCAȚIEI ȘI FORMĂRII
DENUMIREA CURSULUI / MODULULUI	Sprijin Specializat pentru Victimele Criminalității Informactice	
FORMATORI		
LOCAȚIE	DURATĂ	

1 = **Rău** (evaluare între 0 și 4 puncte);
2 = **Insuficient** (evaluare între 5 și 9 valori);
3 = **Suficient** (evaluare între 10 și 13 valori);
4 = **Bine** (evaluare între 14 și 17 puncte);
5 = **Foarte Bine** (evaluare între 18 și 20 de puncte).

OBSERVAȚII

Formator

Coordonarea Pedagogică

ANEXE

TABEL FINAL

DATA	COD REF.	DOMENIUL EDUCAȚIEI ȘI FORMĂRII
DENUMIREA CURSULUI / MODULULUI	Sprijin Specializat pentru Victimele Criminalității Informaticе	
FORMATORI		
LOCAȚIE		DURATĂ

Opinia dvs. este esențială pentru îmbunătățirea calității formării APAV. Apreciem sinceritatea dvs. pentru a ne ajuta să ne îmbunătățim. Pentru a face acest lucru, trebuie să procedați la evaluare în conformitate cu următoarea scală:

- 1 = **Rău** (evaluare între 0 și 4 puncte);
- 2 = **Insuficient** (evaluare între 5 și 9 valori);
- 3 = **Suficient** (evaluare între 10 și 13 valori);
- 4 = **Bine** (evaluare între 14 și 17 puncte);
- 5 = **Foarte Bine** (evaluare între 18 și 20 de puncte).

Numele complet al formatorului	Nota finală

OBSERVAȚII

Formator	Coordonarea Pedagogică
----------	------------------------

PARTE
PART
PARTEA

1

**COMPREENDER
O CIBERCRIME**

**UNDERSTANDING
CYBERCRIME**

**SĂ ÎNȚELEGEM
CRIMINALITATEA
INFORMATICĂ**

MOD. 1

PARTEA 1 - SĂ ÎNȚELEGEM CRIMINALITATEA INFORMATICĂ

MODULUL 1 - ÎNȚELEGEREA FENOMENELOR DE CRIMINALITATE INFORMATICĂ

PREZENTAREA ȘI CADRUL MODULULUI

Tipuri de criminalitate informatică

În acest Modul, vom încerca să prezentăm definiții posibile a conceptului de criminalitate informatică. În acest scop, facem referire la diferite tipuri și clasificări, pentru a demonstra complexitatea fenomenului și multitudinea de forme sau de tipuri de acțiuni prevăzute.

Aceste definiții și tipuri sunt consolidate în continuare în capitolul 1 - Partea I a *Manualului ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*, astfel încât în acest manual vom prezenta doar o sinteză a acestui conținut, cu accent pe concepte-cheie.

Formatorul ar trebui să sublinieze că criminalitatea informatică poate fi clasificată în:

- **Infrațiuni cibernetice**⁹ - acestea sunt asociate cu noi forme de criminalitate, a căror apariție depinde de existența și utilizarea tehnologiilor informației și comunicațiilor (TIC), a calculatoarelor și a rețelelor de calculatoare (Leukfeldt, Notté & Malsch, 2020; Maimon & Louderback, 2019). Acestea sunt numite infrațiuni cibernetice *strictu sensu*, deoarece comiterea acestor infrațiuni depinde de un sistem informatic și urmărește să atace disponibilitatea, accesul, integritatea, autenticitatea, confidențialitatea, păstrarea și securitatea informațiilor.
- **Infrațiuni facilitate de Internet și de TIC**¹⁰ - se referă la formele tradiționale de criminalitate în care TIC joacă un rol important în comiterea acestor infrațiuni, inclusiv infrațiunile cu motivație financiară, dar și formele de violență interpersonală și infrațiunile sexuale. Hărțuirea/ urmărirea online (*cyberstalking*) sau fraudele *online* sunt câteva exemple (Leukfeldt et al., 2020).

În acest din urmă caz, diversele forme de criminalitate informatică care sunt facilitate sau activate de internet sau de TIC pot de asemenea la rândul lor să fie împărțite în:

- Infrațiuni cibernetice cu motivație financiară (e.g., *phishing*¹¹ e *romance scams*¹²);
- Infrațiuni cibernetice în relațiile interpersonale (e.g., *cyberstalking*¹³);
- Infrațiuni cibernetice sexuale (e.g., *revenge porn*¹⁴).

Concepte și definiții

Să începem prin a defini **infrațiunile cibernetice** cele mai comune, cunoscute de asemenea și sub denumirea de criminalitate informatică *strictu sensu*, a căror prezentarea conceptului este făcută în acest Modul. Cu toate acestea, în Modulele 5 și cele care urmează a acestui Curs de Formare, este efectuată deconstrucția și înțelegerea aprofundată a multora dintre aceste tipuri de criminalitate informatică și sunt prezentate, de asemenea, propuneri specifice de intervenție și prevenire.

Hacking-ul sau **cracking-ul** sunt în mod normal definite ca **accesul neautorizat la sistemele informatice cu intenție de comitere a unei fapte penale** (Grabosky, 2016 cit în Maimon & Louderback, 2019). Acestea sunt asociate cu *cyber-trespassing* ceea ce implică trecerea neautorizată a barierelor invizibile din mediul virtual (Wall, 2001 cit în Maimon & Louderback, 2019).

Hacking-ul include o serie de comportamente, cum ar fi **reproiectarea sistemelor de hardware sau software**, pentru a modifica funcția sa inițială, precum și participarea la propria subcultură (Bachmann, 2010, Holt, 2007, Steinmetz, 2015 cit în Maimon & Louderback, 2019).

Spamming-ul sau **SPAM-ul**, acronim pentru expresia „trimiterea și publicarea publicității în masă”¹⁵, se referă la

⁹ Tradus din expresia *cyber-dependent crimes*.

¹⁰ Tradus din expresia *cyber-enabled crimes*.

¹¹ Acest fenomen este abordat în Modulul 5 al Cursului de Formare.

¹² Acest fenomen este abordat în Modulul 6 al Cursului de Formare.

¹³ Acest fenomen este abordat în Modulul 10 al Cursului de Formare.

¹⁴ Acest fenomen este abordat în Modulul 10 al Cursului de Formare.

¹⁵ Tradus din expresia *Sending and Posting Advertisement in Mass*.

PARTEA 1 - SĂ ÎNȚELEM CRIMINALITATEA INFORMATICĂ

MODULUL 1 - ÎNȚELEGEREA FENOMENELOR DE CRIMINALITATE INFORMATICĂ

trimiterea de date și distribuirea în masă a e-mailurilor care promovează produse, servicii sau scheme de investiții, care pot fi frauduloase și care pot conține programe *malware* sau alt atașament de fișier executabil (Rathi & Pareek, 2013).

Malware este termenul folosit pentru a se referi la o varietate de *software-uri* ostile sau intruzive (de exemplu, viruși de calculator, *worms*¹⁶, *ransomware*¹⁷, *spyware*¹⁸, *adware*¹⁹, *scareware*²⁰ etc.). Este un **software destinat să se infiltreze în echipamente în mod ilegal** pentru a provoca daune, modificări sau a sustrage informații. *Malware*-ul poate lua, de asemenea, forma unui cod executabil, *scripts*, conținut activ și alt *software* (Aycock, 2006 cit în Reep-van den Bergh & Junger, 2018).

Una dintre schemele adesea folosite este publicarea de conținut cu titluri care stârnesc curiozitate sau necesită o acțiune „urgentă”, precum și invitații pentru a instala jocuri sau sugestii pentru a vizita profiluri noi.

Phishing-ul este trimiterea în masă a mesajelor de e-mail - *spamming* - de obicei cu un link către un site web, pe care destinatarii sunt convinși să-l acceseze, apelând la motive sau acțiuni urgente. De regulă, aceste e-mailuri solicită sau indică importanța destinatarilor de „actualizare”, „validare” sau „confirmare” a informațiilor bancare.

Aceste e-mailuri (și paginile la care fac referire) sunt false și constituie o reproducere asemănătoare a notificării inițiale făcute de entitățile bancare, entitățile emitente de credite sau alte entități care permit efectuarea plăților *online*. În momentul accesării acestor pagini se solicită, de regulă, introducerea informațiilor bancare ale utilizatorului, iar ulterior procesului de introducere a datelor bancare este posibilă captarea și utilizarea abuzivă a acestora.

La rândul său, **atacul de tip DDoS** (Distributed Denial of Service, blocarea distribuită a serviciului) se referă la o încercare intenționată de a supraîncărca un anumit sistem informatic, cu scopul de a împiedica utilizarea acestuia (Overvest & Straathof, 2015).

În ceea ce privește infracțiunile facilitate de internet și de TIC, cele mai comune sunt fraudele *online*, furtul de identitate și infracțiunile legate de abuzul sexual și exploatarea copiilor.

Înșelăciunile online pot lua mai multe forme:

- Înșelăciuni în comerțul electronic (*e-commerce*);
- Fraude bancare;
- Înșelăciuni în relații intime (*romance scams*).

Înșelăciuni în comerțul electronic prezintă diferite grade de complexitate, inclusiv scheme simple în care cumpărătorului i se promite să i se trimită un anumit articol, printr-un transfer bancar prealabil, ajungând să nu primească articolul respectiv.

În cazul **fraudei bancare**, ne putem referi la schemele de *phishing* pentru accesarea informațiilor bancare ale victimei, precum și la fraudele cu cardurile de credit. Acestea se referă la utilizarea cardului de credit al altei persoane pentru uz personal, fără cunoștința titularului cardului și a entității emitente (Patel & Singh, 2013).

În ceea ce privește **înșelăciunile în relațiile intime**, acestea apar atunci când agentul încearcă să stabilească o relație de încredere și intimitate, în special prin intermediul internetului și al TIC, cu o anumită țință, ca un preludeu pentru a obține beneficiu personal, și anume beneficii financiare și patrimoniale.

Furtul de identitate include în mod cumulativ următoarele acte:

¹⁶ *Worms* sunt coduri nocive care se răspândesc printr-o rețea, cu sau fără asistență umană (Kienzle & Elder, 2003).

¹⁷ *Ransomware* este un *malware* în sistem prin descărcare și creează un fișier „exe” pentru executare. Obiectivul poate include extorsiunea victimei, prin criptarea informațiilor sale personale (Kansagra, Kumhar & Jha, 2016).

¹⁸ *Spyware* este un program automat care colectează informații despre utilizator și despre obiceiurile sale de utilizare a internetului și transmite aceste informații unei entități externe fără cunoștința sau consimțământului utilizatorului în cauză.

¹⁹ *Adware* este desemnat ca software care afișează sau descarcă automat materiale publicitare (de obicei nedorite) atunci când utilizatorul este online (Gao, Li, Kong, Bissyandé & Klein, 2019).

²⁰ *Scareware* este o formă de *malware* care induce în eroare utilizatorul făcându-l să creadă că calculatorul este infectat când de fapt în realitate sistemul funcționează (Seifert, Stokes, Lu, Heckerman, Colcarnian, Parthasarathy & Santhanam, 2015).

PARTEA 1 - SĂ ÎNȚELEM CRIMINALITATEA INFORMATICĂ

MODULUL 1 - ÎNȚELEGEREA FENOMENELOR DE CRIMINALITATE INFORMATICĂ

- Obținerea de informații personale și/sau confidentiale despre o altă persoană fără încunoștințarea sa;
- Proprietate asupra datelor sau transferul acestor date cu conștientizarea faptului că acestea vor fi utilizate în scopuri ilicite;
- Utilizarea datelor obținute inițial pentru comiterea infracțiunilor.

În ceea ce privește **infracțiunile legate de abuzul sexual asupra copiilor și exploatarea sexuală a copiilor și a tinerilor pe internet**:

- **Abuzul sexual online** poate fi definit ca un concept cuprinzător, care include **orice formă de abuz sexual asupra copiilor în context online**. Acest concept larg include diferite manifestări de abuz și exploatare, de la abuzul sexual fără să intre în contact, facilitat de TIC și internet, rețele sociale sau alte platforme, cum ar fi hărțuirea și ademenirea (*grooming online*), la partajarea de conținut pe *darkweb* (imagini și/sau audio) al abuzului sexual și exploatarea sexuală asupra copiilor, colectate în prealabil sub formă de fotografie sau înregistrări video.
- În contextul abuzului și exploatarea *online* a copiilor, subliniem **abuzul sexual asupra copiilor în direct**: practicarea actelor sexuale cu copii și transmiterea în direct, în special prin intermediul serviciilor de *live streaming*, fiind astfel posibil să fie vizualizat de alte persoane.
- De asemenea, subliniem **grooming-ul online**, care poate fi definit ca un **proces de manipulare** și o **formă de ademenire**. De obicei, începe cu o abordare non-sexuală, respectiv prin intermediul internetului și al TIC, care includ jocurile *online* și rețele sociale, în scopul de a stabili o relație de încredere cu copilul și pentru a-l convinge să se întâlnească față în față cu cineva, astfel încât copilul să fie abuzat sexual. Stabilirea unei relații de încredere cu copilul, mediată de internet și de TIC, poate viza, de asemenea, **convingerea copilului în ceea ce privește producerea și partajarea conținutului sexual**.
- În urma acestei forme de abuz sexual și exploatare, copilul poate fi supus **amenințărilor și șantajului de diseminare sau partajare a conținutului sexual auto-produs**, în scopul de a obține favoruri sexuale, bani sau alte beneficii. Acest fenomen se numește **șantajare sexuală a copiilor**.

În explorarea conceptelor și fenomenelor de abuz sexual și exploatare *online* a copiilor este, de asemenea, abordată în acest Modul, o problemă terminologică importantă:

- expresiile **material de abuz sexual asupra copiilor** și **materialul de exploatare sexuală a copiilor**²¹ încearcă să înlocuiască, cel puțin în contexte ilegale sau juridice, conceptul de pornografie infantilă (terminologia încă prevăzută în legislația națională și internațională).

În contextul agresiunii *online* în relațiile interpersonale, vom elucida cele mai comune cazuri, respectiv *cyberbullying*, *cyberstalking*, și pornografie non-consensuală.

Cyberbullying-ul rezultă din utilizarea a TIC și a internetului, iar unele dintre comportamentele care operaționalizează această formă de agresiune *online* pot include: diseminarea de informații negative/false cu intenția de a defăima victima (prin recurgerea la apeluri telefonice, mesaje text, mesaje video, e-mail, *chat room*, site-uri web, rețele sociale); urmărirea obsesională a victimei (prin aceleași mijloace) (APAV, 2011; Jahankhani et al., 2014). Putem evidenția, de asemenea, situații de *cyber-bullying* cu caracter sexual, cum ar fi schimbul *online* de zvonuri sau minciuni despre comportamentul sexual al victimei sau schimbul de informații *online* într-un mod non-consensual cu privire la intimitatea victimei.

Cyberbullying diferă de modalitățile cele mai convenționale de *bullying*:

- datorită posibilității de a fi practicat în orice moment al zilei, indiferent de necesitatea contactului direct dintre victimă și agresor;
- datorită potențialului de anonimat care este garantat agresorului;
- datorită potențialului ridicat de "publicitate" și audiența aferentă;
- datorită dificultății de a elimina conținutul creat (Stopbullying. Gov, 2017).

²¹ Tradus din expresiile *child sexual abuse material* (CSAM) și *child sexual exploitation material* (CSEM).

PARTEA 1 - SĂ ÎNȚELEM CRIMINALITATEA INFORMATICĂ

MODULUL 1 - ÎNȚELEGEREA FENOMENELOR DE CRIMINALITATE INFORMATICĂ

Cyberstalking-ul, pe de altă parte, poate fi definit ca o formă de *stalking* care are de asemenea un caracter intruziv, repetitiv și persistent care provoacă teamă victimei și caracterizează această formă de persecuție și hărțuire persistentă, și este practicat prin intermediul internetului și TIC, cu scopul de a amenința și a hărțui victima (Maran & Begotti, 2019).

Practicile de cyberstalking pot include diferite comportamente de urmărire: efectuarea mai multor încercări de contact nedorite de victimă, prin telefon, e-mail și rețele sociale; instalarea programelor *spyware* în calculatorul victimei; accesarea, fără permisiunea victimei, la e-mailul lor și/sau la contul rețelelor sociale pentru a monitoriza informațiile cu caracter personal și viața de zi cu zi a victimei și/sau pentru a acționa în numele acesteia (Martellozzo & Jane, 2017).

De asemenea, în cadrul violenței *online* în contextul relațiilor interpersonale, putem evidenția, pe lângă *cyberbullying* și *cyberstalking*, **pornografia non-consensuală prin imagini și înregistrări video**.

Motivațiile pentru diseminarea acestui conținut pot fi:

- **Șantajarea sau constrângerea sexuală a victimei.**
- **Răzbunare**, adesea denumită ca *revenge porn*, ceea ce implică diseminarea non-consensuală a imaginilor intime ale unui partener, de obicei după sfârșitul relației, ca o formă de răzbunare.

Factori de risc și vulnerabilitățile comportamentale cu privire la cibervictimizare

Factorii de risc se referă la caracteristicile, condițiile sau variabilele asociate cu o anumită persoană care sporesc probabilitatea apariției unor rezultate negative sau nedorite (Reppold et al., 2002 cit în Maia et al., 2016).

Astfel, **factorii de risc asociați cu cibervictimizarea** sunt caracteristici sau condiții care pot spori probabilitatea sau vulnerabilitatea unei anumite persoane în urma criminalității informatice.

În cazul criminalității informatice, caracteristicile individuale nu se pot dovedi la fel de semnificative pentru producerea victimizării, deoarece criminalitatea informatică implică o interacțiune directă minoră (sau chiar inexistentă) între victimă și autorul infracțiunii. De exemplu, în cazul programelor *malware*, este dificil să se determine, în mod concret, cine va fi victima care va fi infectată cu *software*-ul dăunător, deoarece orice calculator poate fi infectat, indiferent de caracteristicile individuale ale actorilor (Ngo & Paternoster, 2011).

Cercetarea nu este deosebit de vastă în acest domeniu, la fel ca în multe altele asociate cu înțelegerea criminalității informatice. Cu toate acestea, sunt evidențiate următoarele:

- **Factorii de risc asociați cu caracteristicile sociodemografice**

În acest Modul vor fi abordați factori precum **sexul, vârsta și nivelul de școlarizare**. *Manualul ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*, în capitolul 3 – Partea I, explorează rezultatele și concluziile unor studii în care factorii de risc aferente victimizării care a rezultat din criminalitate informatică au fost examinați și în care au fost măsurate astfel de variabile, în vederea caracterizării unui profil sociodemografic al victimelor diferitor forme de criminalitate informatică.

- **Factorii de risc asociați cu utilizarea internetului și a TIC**

Câteva concepte cum ar fi educația tehnologică și efectul de dezinhibare, sunt explorate în acest Modul, ca factori care pot spori sau reduce vulnerabilitatea la cibervictimizare:

- **Educația tehnologică** se referă la conștientizarea, cunoștințele și competențele care permit unei anumite persoane să acționeze în mediile digitale și la utilizarea eficientă a internetului, a TIC și a echipamentelor și instrumentelor aferente (Holt & Bossler, 2008).
- **Efectul de dezinhibare** se referă la procesul sau efectul de dezinhibare care rezultă din modul în care distanța

PARTEA 1 - SĂ ÎNȚELEGEM CRIMINALITATEA INFORMATICĂ

MODULUL 1 - ÎNȚELEGEREA FENOMENELOR DE CRIMINALITATE INFORMATICĂ

fizică are loc în interacțiunea sau comunicarea prin TIC, absența contactului direct în procesul de comunicare, anonimatul mai mare și percepția unui control mai mare asupra procesului de interacțiune. Efectul dezinhibării poate contribui la expunerea unor situații și/sau la adoptarea unor comportamente *online* care sporesc vulnerabilitatea la cibervictimizare (Agustina, 2015).

Pe lângă aceste concepte, în acest Modul explorăm și alți factori de risc de cibervictimizare, cum ar fi **nivelurile de utilizare** a internetului și a TIC și **tipul de activități desfășurate** pe Internet sau prin intermediul internetului și a TIC.

După cum s-a menționat în cazul factorilor de risc socio-demografici, *Manualul ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*, în capitolul 3 – Partea I abordează, de asemenea, mai îndeaproape, fiecare dintre acești **factori de risc de cibervictimizare asociați cu comportamentul utilizatorilor de internet și TIC**.

Acestea fiind spuse, pentru o înțelegere mai profundă a conținutului cuprins în acest Modul, vă propunem pe lângă lectura atentă a conceptelor-cheie de mai sus și a materialul audiovizual propus (*PowerPoint*), să consultați *Manualul ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*, respectiv capitolele 1 și 3 – Partea I.

PARTEA 1 - SĂ ÎNȚELEM CRIMINALITATEA INFORMATICĂ

MODULUL 1 - ÎNȚELEGEREA FENOMENELOR DE CRIMINALITATE INFORMATICĂ

PLANUL SESIUNII NR. 1

1. Identificarea acțiunii

Denumire Curs de Formare Sprijin Specializat pentru Victimele Criminalității Informaticice

Module / subiecte Introducere și Context
Înțelegerea fenomenelor criminalității informaticice

Data sesiunii **Orar** **Durata sesiunii** 35 de minute

Formatori

2. Obiective specifice La sfârșitul sesiunii, cursanții ar trebui să poată să:

- Recunoască corect pe ceilalți cursanți și formatorul;
- Recunoască corect obiectivele și conținutul intervenției de formare;
- Distingă corect infracțiunile cibernetice și infracțiunile facilitate de internet și TIC;
- Recunoască corect diferite concepte și definiții aferente criminalității informaticice, și anume tipurile de criminalitate informatică;
- Identifice corect factorii de risc de cibervictimizare, asociați cu caracteristicile sociodemografice;
- Evidențieze, fără erori, vulnerabilitățile comportamentale legate de cibervictimizare.

3. Structura sesiunii

	Conținutul programului	Metodologie	Resurse pedagogice / didactice	Evaluare Exerciții	Timp (minute)
Introducere	Introducere și context: Prezentarea și sondajul așteptărilor Prezentarea formatorului Prezentarea stagiarelor Prezentarea obiectivelor și a conținutului programului al intervenției de formar	Expozitivă și activă	Calculator: Datashow și ecran de proiecție	Observare	5
	Tipuri de criminalitate informatică: • Infracțiuni cibernetice vs infracțiuni facilitate de internet și TIC	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
Dezvoltare	Concepte și definiții: • Hacking, spamming, malware, phishing și DDoS • Fraude online: înșelăciuni în comerțul electronic (e-commerce), fraude bancare și înșelăciuni în relații intime (romance scams) • Furt de identitate online • Abuz și exploatare sexuală asupra copiilor online: abuz sexual asupra copiilor în direct, ademenire (grooming online) și conținut cu abuz sexual asupra copiilor • Cyber-bullying • Cyber-stalking și partajare non-consensuală a imaginilor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	10
	Factori de risc și vulnerabilități comportamentale cu privire la cibervictimizare: • Factorii de risc asociați cu caracteristicile sociodemografice • Factorii de risc asociați cu utilizarea internetului și a TIC	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	10
Concluzie	Rezumat concludent și clarificarea nelămuririlor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5

OBSERVAȚII

Destinatari:

Specialiști în sprijinirea victimelor

Data: / /

Formator:

PARTEA 1 - SĂ ÎNȚELEM CRIMINALITATEA INFORMATICĂ

MODULUL 1 - ÎNȚELEGEREA FENOMENELOR DE CRIMINALITATE INFORMATICĂ

INSTRUCȚIUNI ȘI INFORMAȚII ESENȚIALE PENTRU FORMATOR

CONCORDANȚA CU CONȚINUTUL

Planul Sesiunii *Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*

	PARTE	CAPITOL
Introducere și Context	Nu corespund Folosiți Programul Cursului de Formare (a se vedea anexele)	
Tipuri de criminalitate informatică	Partea I - Înțelegere	Capitolul 1 - 1.2.
Concepte și definiții	Partea I - Înțelegere	Capitolul 1 - 1.3.
Factori de risc și vulnerabilități comportamentale cu privire la cibervictimizare	Partea I - Înțelegere	Capitolul 3 - 3.2.
Rezumat concludent și clarificarea nelămuririlor	Nu corespund	

MOD. 2

PARTEA 1 - SĂ ÎNȚELEGEM CRIMINALITATEA INFORMATICĂ

MODULUL 2 - CADRUL LEGISLATIV PRIVIND CRIMINALITATEA INFORMATICĂ

PREZENTAREA ȘI CADRUL MODULULUI

În acest Modul, formatorul va prezenta, în conformitate cu capitolul 2 - Partea I a *Manual ROAR - înțelegerea și prevenirea criminalității informatice sprijinirea și capacitatea victimelor*, cadrul legislativ privind criminalitatea informatică.

În acest scop și într-un registru considerabil de expozitiv, criminalitatea informatică va fi abordată în **Legislația internațională și acquis-ul Uniunii Europene**, și anume:

- Convenția Consiliului Europei privind criminalitatea informatică, 23 noiembrie 2001²²;
- Convenția privind protecția copiilor împotriva exploatării și abuzurilor sexuale, cunoscută ca Convenția de la Lanzarote²³;
- Strategia de Securitatea Cibernetică a Uniunii Europene²⁴;
- Rezoluția Parlamentului European privind lupta împotriva criminalității informatice din 3 octombrie 2017²⁵.

Acest modul prezintă, pe scurt, câteva directive ale Uniunii Europene:

- Directiva 2011/93 / UE - privind combaterea abuzului sexual și a exploatării sexuale a copiilor și a pornografiei infantile și care înlocuiește Decizia-cadru a Consiliului 2004/68 / JAI²⁶;
- Directiva 2013/40 / UE – Privind atacurile sistemelor informaționale și care înlocuiește Deciziei-Cadru 2005/222 / JAI a Consiliului²⁷;
- Directiva (UE) 2019/713 - Privind combaterea a fraudei și a falsificării mijloacelor de plată, altele decât numerarul și care înlocuiește Deciziei-cadru a Consiliului 2001/413 / JAI²⁸;
- Directiva 2000/31 / CE - Privind comerțul electronic²⁹;
- Regulamentul 679/2016 – Punerea în aplicare a regulamentului general privind protecția datelor cu caracter personal (RGPD)³⁰.

Acest Modul prezintă, de asemenea, câteva dintre demersurile întreprinse la nivel european și internațional, în vederea combaterii criminalității informatice, printre care Asociația INHOPE³¹.

Modulul prezintă în continuare **cadrul legislativ privind criminalitatea informatică la nivel național**.

Cazul României

Sistemul juridic românesc nu dispune de o lege specială privind criminalitatea informatică, aceste infracțiuni fiind sancționate în principal în conformitate cu Noul Cod Penal din România, precum și cu alte legi speciale.

Următoarele infracțiuni informatice sunt reglementate de Noul Cod Penal:

Titlul II (Infracțiuni contra patrimoniului), Cap. IV: Fraude comise prin sisteme informatice și mijloace de plată electronice

- **Art. 249: Frauda informatică**

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:32013JC0001&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 Directiva 2011/93 / UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual și a exploatării sexuale a copiilor și a pornografiei infantile și care înlocuiește Decizia-cadru 2004/68 / JAI a Consiliului, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32011L0093&from=PT>.

²⁷ Directiva 2013/40 / UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și înlocuirea Deciziei-cadru a Consiliului 2005/222 / JAI, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0040&from=DE>.

²⁸ Directiva (UE) 2019/713 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind combaterea fraudei și falsificarea mijloacelor de plată altele decât numerarul și înlocuirea Deciziei-Cadru 2001/413 / JAI a Consiliului, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L0713&from=PT>.

²⁹ Directiva 2000/31 / CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special comerțul electronic, pe piața internă („Directiva privind comerțul electronic”), <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000L0031&from=EN>.

³⁰ Regulamentul 679/2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679-20160504>.

³¹ A se vedea <https://www.inhope.org/EN>.

PARTEA 1 - SĂ ÎNȚELEM CRIMINALITATEA INFORMATICĂ

MODULUL 2 – CADRUL LEGISLATIV PRIVIND CRIMINALITATEA INFORMATICĂ

- **Art. 250: Efectuarea de operațiuni financiare în mod fraudulos**
- **Art. 251: Acceptarea operațiunilor financiare efectuate în mod fraudulos**

Titlul VII (Infrațiuni contra siguranței publice), Cap. VI: Infrațiuni contra siguranței și integrității sistemelor și datelor informatice

- **Art. 360: Accesul ilegal la un sistem informatic**
- **Art. 361: Interceptarea ilegală a unei transmisii de date informatice**
- **Art. 362: Alterarea integrității datelor informatice**
- **Art. 363: Perturbarea funcționării sistemelor informatice**
- **Art. 364: Transferul neautorizat de date informatice**
- **Art. 365: Operațiuni ilegale cu dispozitive sau programe informatice**

Titlul VIII. Infrațiuni care aduc atingere unor relații privind conviețuirea socială, Cap. I: Infrațiuni contra ordinii și liniștii publice

- **Art. 374 Pornografia infantilă:**
 - Producerea, deținerea, procurarea, stocarea, expunerea, promovarea, distribuirea, precum și punerea la dispoziție de materiale pornografice cu minori
 - Îndemnarea sau recrutarea unui minor pentru participarea la un spectacol pornografic, obținerea de foloase de pe urma unui astfel de spectacol în cadrul căruia participă minori sau exploatarea unui minor în orice alt fel pentru realizarea de spectacole pornografice
 - Vizionarea de spectacole pornografice cu minori
 - Pedepsă mai aspră dacă faptele au fost săvârșite printr-un sistem informatic
 - Agravantă dacă faptele au fost săvârșite de un membru de familie, de o persoană în a cărei îngrijire se află minorul sau dacă fapta i-a pus în pericol viața

De asemenea, Legea 217/ 2003 pentru prevenirea și combaterea violenței domestice numește violența cibernetică printre tipurile de **violență domestică**, care este definită ca fiind „hărțuire online, mesaje online instigatoare la ură pe bază de gen, urmărire online, amenințări online, publicarea nonconsensuală de informații și conținut grafic intim, accesul ilegal de interceptare a comunicațiilor și datelor private și orice altă formă de utilizare abuzivă a tehnologiei informației și a comunicațiilor prin intermediul calculatoarelor, telefoanelor mobile inteligente sau altor dispozitive similare care folosesc telecomunicațiile sau se pot conecta la internet și pot transmite și utiliza platformele sociale sau de e-mail, cu scopul de a face de rușine, umili, speria, amenința, reduce la tăcere victima.”

Acest Modul se încheie, în cele din urmă, cu prezentarea și reflecția asupra **principalelor provocări în investigarea criminalității informatice și aplicarea legii**:

- Principalele provocări în investigarea și aplicarea legii, în ceea ce privește criminalitatea informatică, sunt transversale către statele europene, fiind resimțite în special de organele de poliție judiciară și de Ministerul Public:
 - Difuzarea rapidă a conținutului online, anonimatul pe care îl oferă unele platforme și tehnicile de criptare³² face dificilă sau chiar imposibilă urmărirea provenienței conținutului ilegal *online*;
 - Dificultatea armonizării mecanismelor de blocare a conținutului ilegal facilitează reparația aceluiasi conținut în domenii aflate în alte țări;
 - Complexitatea instrumentelor capabile să prelucreze cantități mari de date într-o perioadă scurtă;
 - Termenele strânse pentru păstrarea dovezilor de către furnizorii de servicii de internet - ISP (*Internet Service Providers*);
 - Cooperarea cu țările terțe care găzduiesc conținut ilegal;
 - Dilema dintre confidențialitate și previziune de metode ascunse de investigare.

³² A se vedea, de exemplu, Modulele 8, 9 și 10 ale acestui Curs de Formare, în care este explorată criptarea end-to-end

PARTEA 1 - SĂ ÎNȚELEM CRIMINALITATEA INFORMATICĂ

MODULUL 2 - CADRUL LEGISLATIV PRIVIND CRIMINALITATEA INFORMATICĂ

PLANUL SESIUNII Nr. 2

1. Identificarea acțiunii

Denumire Curs de Formare Sprijin Specializat pentru Victimele Criminalității Informatică

Module / teme Cadrul legislativ al criminalității informatică

Data sesiunii **Orar** **Durata sesiunii** 45 de minute

Formatori

2. Obiective specifice La sfârșitul sesiunii, cursanții ar trebui să poată să:

- Recunoască corect cadrul legislativ al criminalității informatică, în lumina dreptului internațional;
- Recunoască corect cadrul legislativ al criminalității informatică la nivel național;
- Identifice în mod corespunzător cel puțin jumătate din provocările abordate cu privire la investigarea criminalității informatică și aplicarea Legii.

3. Structura sesiunii

	Conținutul programului	Metodologie	Resurse pedagogice / didactice	Evaluare / Exerciții	Timp (minute)
Introducere	Criminalitatea informatică în dreptul internațional și în acquis-ul Uniunii Europene	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
	Criminalitatea informatică în dreptul internațional și în acquis-ul Uniunii Europene: • Convenția Consiliului Europei privind Criminalitatea Informatică • Convenția privind Protecția Copiilor împotriva Exploatării și a Abuzurilor Sexuale • Strategia de Securitate Cibernetică a Uniunii Europene • Rezoluția Parlamentului European privind lupta împotriva criminalității informatică • Directiva 2011/93 / UE - privind combaterea abuzului sexual și a exploatarei sexuale a copiilor și a pornografiei infantile • Directiva 2013/40 / UE - În ceea ce privește atacurile împotriva sistemelor informatice • Directiva (UE) 2019/713 - privind combaterea fraudei și a falsificării mijloacelor de plată altele decât numerarul • Directiva 2000/31 / CE - privind comerțul electronic • Regulamentul 679/2016 - regulamentul general privind protecția datelor cu caracter personal (RGPD)	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	15
	Cadrul legislativ privind criminalitatea informatică la nivel național	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	20
Dezvoltare	Principalele provocări în investigare și aplicarea legii	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	3
	Rezumat concludent și clarificarea nelămuririlor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	2
Concluzie					

OBSERVAȚII

Destinatari:

Specialiști în sprijinirea victimelor

Data: / /

Formator:

PARTEA 1 – SĂ ÎNȚELEM CRIMINALITATEA INFORMATICĂ

MODULUL 2 – CADRUL LEGISLATIV PRIVIND CRIMINALITATEA INFORMATICĂ

INSTRUCȚIUNI ESENȚIALE ȘI INFORMAȚII PENTRU FORMATOR

CONCORDANȚA CU CONȚINUTUL

Planul Sesiunii *Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*

	PARTE	CAPITOL
Criminalitatea informatică în dreptul internațional și în acquis-ul Uniunii Europene	Partea I - Înțelegere	Capitolul 2 - 2.1. și 2.2.
Cadrul legislativ privind criminalitatea informatică la nivel național	Partea I - Înțelegere	Capitolul 2 - 2.3.
Principalele provocări în investigare și în aplicarea legii	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Rezumat concludent și clarificarea nelămuririlor	Nu corespund	

MOD. 3

PARTEA 1 – SĂ ÎNȚELEGEM CRIMINALITATEA INFORMATICĂ

MODULUL 3 – VICTIMIZAREA ȘI IMPACTUL CRIMINALITĂȚII INFORMATICE

PREZENTAREA ȘI CADRUL MODULULUI

Prevalența criminalității informatice

Deși criminalitatea informatică este intens studiată și se bucură de interes crescut, **informațiile despre dimensiunea reală a victimizării în urma diferitelor tipuri de criminalitate informatică sunt încă incipiente**, prin urmare, nu se știe care sunt proporțiile reale ale prevalenței sale în populație (Reep-van den Bergh & Junger, 2018).

În România, conform Eurobarometrului special 464a, cea mai frecventă formă de criminalitate informatică în 2017 a fost software-ul malițios, cu 39% din români afirmând că au descoperit astfel de software-uri pe dispozitivele lor.³³ Românii au mai căzut victime și (în ordinea frecvenței acestora): emailuri și telefoane frauduloase prin care li se solicitau date personale, precum parole, informații bancare etc. (22% dintre respondenți), contul de email sau contul de rețele de socializare compromis (18%);³⁴ furt online de identitate (11%)³⁵ și fraude legate de cardul bancar sau plăți electronice (9%).³⁶

În ceea ce privește pornografia infantilă, 30% dintre români, de departe cea mai mare proporție dintre țările U, afirmă că au descoperit accidental astfel de materiale online.³⁷ Cu toate acestea, în mod îngrijorător, doar 52% dintre toți respondenții au indicat că ar contacta Poliția în această situație³⁸, semnalând o nevoie urgentă de informare a populației și creșterea gradului de conștientizare a nevoii de a raporta astfel de materiale către autorități.

Confirm Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism – DIICOT, cele mai frecvente tipuri de infracțiuni informatice în 2018 au fost:

- **atacuri de tip ransomware**, în special cele care se auto-propagă: **ransomworms**, precum WannaCry, Arena Dharma, care produc daune materiale substanțiale în rândul victimelor sale și care au un puternic impact emoțional negativ. Se așteaptă ca aceste atacuri să devină mai frecvente în viitor, iar stoparea lor este o provocare reală atât pentru sectorul public, cât și pentru cel privat.
- **atacuri de tip man-in-the-browser și man-in-the-middle**, unde un Troian se interpune între două părți, permițând atacatorului să intercepteze comunicarea (date personale, transferuri bancare etc.)
- **programe malware direcționate către bănci**, care implică viruși trimiși prin fișiere executabile cu funcții de backdoor, create prin intermediul platformei Cobalt Strike, care permit atacatorilor să transfere bani în conturi bancare frauduloase.
- **comerțul ilegal prin Darknet** a crescut în 2018, iar faptul că principalele mijloace de plată sunt criptomonedele (în special Bitcoin, Ethereum și Monero) face dificilă identificarea atacatorilor. A existat, de asemenea, o creștere a **criptominării frauduloase**.
- atacurile complexe asupra bancomatelor și sistemelor bancare sunt, de asemenea, în creștere, incluzând, dar fără a se limita la, inserarea profundă (**deep insert skimming**), care presupune copierea datelor pe banda magnetică a cardurilor de credit.
- **materialele de exploatare sexuală a copiilor** (child sexual exploitation material - CSAM) continuă să fie o provocare. Deși aceste materiale sunt în general produse de făptași, există o creștere a materialului auto-generat, care este apoi utilizat pentru constrângerea și șantajarea victimelor. De asemenea, este în creștere și **streaming-ul live** care implică minori.³⁹

Tendințele din România în materie de criminalitate informatică sunt asemănătoare și corespund celor internaționale, conform raportului IOCTA (Internet Organised Crime Threat Assessment) din 2018.⁴⁰

³³ R. Comisia Europeană, *Special Eurobarometer 464a: Europeans' Attitude towards Cybersecurity*, 2017, p. 77.

³⁴ Ibid., p. 74.

³⁵ Ibid., p. 68.

³⁶ Ibid., p. 75.

³⁷ Ibid., p. 71.

³⁸ Ibid., p. 99.

³⁹ DIICOT, *Raport de activitate 2018*, Februarie 2019, pp. 29-30.

⁴⁰ Europol, *IOCTA - Internet Organised Crime Threat Assessment 2018*, available at <https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018> [accessed December 20th, 2019].

PARTEA 1 – SĂ ÎNȚELEM CRIMINALITATEA INFORMATICĂ

MODULUL 3 – VICTIMIZAREA ȘI IMPACTUL CRIMINALITĂȚII INFORMATICE

Pentru mai multe informații, vă rugăm să consultați Capitolul 1 – Partea I din *Manualul ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*, care prezintă studii, sondaje și rapoarte dedicate prevalenței sau incidenței acestor fenomene.

Impact asupra victimelor individuale

În acest punct al Modulului este explorat în special conținutul capitolului 4 – Partea I din *Manualul ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*. Pentru aprofundarea cunoștințelor cu privire la consecințele diferitelor tipuri de criminalitate informatică, acest capitol trebuie consultat.

În orice caz, în Modulele 5-10 ale acestui Curs de Formare, în care sunt elaborate *strategii pentru a depăși victimizarea și impactul acesteia*, consecințele experiențelor de cibervictimizare vor fi iarăși abordate, de data aceasta în funcție de tipul de criminalitate informatică.

După cum se menționează în *Manualul ROAR*, se consideră, în general, că efectele cu care se confruntă victimele criminalității informatice nu diferă, cel puțin în mod semnificativ, de consecințele cu care se confruntă victimele infracțiunilor *tradiționale*.

Trebuie remarcat faptul că impactul criminalității informatice asupra victimei poate varia foarte mult, fiind agravat sau atenuat în funcție de un set de:

- **Variabile individuale**, respectiv caracteristici sociodemografice și abilități și comportamente de utilizare a internetului;
- **Variabilele asociate cu criminalitatea informatică** propriu-zise, cum ar fi tipul de criminalitate informatică, durata cibervictimizării, nivelul de publicitate al cibervictimizării și (eventuala) relație cu autorul criminalității informatice;
- **Variabile asociate cu rețeaua de sprijin** formală și informală.

Consecințe asupra sănătății fizice, psihologice și emoționale

De la început, trebuie remarcat faptul că, în mare parte, consecințele emoționale și psihologice în urma criminalității informatice sunt de obicei subestimate, criminalitatea informatică fiind înțeleasă ca o categorie de infracțiune cu impact redus (Button, Lewis, & Tapley, 2014a cit in Jansen & Leukfeldt, 2018).

Câteva dintre consecințele și reacțiile cel mai frecvent menționate sunt (Leukfeldt et al., 2019; Cross et al., 2016; De Kimpe et al., 2020; Jansen & Leukfeldt, 2018; Cross et al., 2016):

- Pierderea încrederii;
- vinovăție;
- rușine;
- furie și frustrare;
- anxietate și retrăirea incidentelor;
- frică și tristețe;
- frământare interioară;
- sentimente de nesiguranță, neajutorare și dezamăgire;
- scăderea nivelului de încredere în sine și a nivelului de încredere față de ceilalți;
- izolare socială;
- depresie și ideea suicidară;
- scăderea randamentului/productivității;
- simptome fizice, cum ar fi tulburări de somn, oboseală excesivă, probleme cu apetitul, dureri de cap și grețuri.

PARTEA 1 – SĂ ÎNȚELEGEM CRIMINALITATEA INFORMATICĂ

MODULUL 3 – VICTIMIZAREA ȘI IMPACTUL CRIMINALITĂȚII INFORMATICE

Impact financiar

Consecințele financiare ale criminalității informatice pot include (Leukfeldt et al., 2019):

- costurile suportate de victime ca urmare a actului la care au fost supuse, inclusiv costuri suplimentare aferente sănătății, cheltuieli de deplasare, telecomunicațiile și/sau necesitatea înlocuirii echipamentelor;
- pierderea de timp și pierderea orelor de lucru și eventuală pierdere ulterioară a venitului;
- costuri suplimentare legate de necesitatea de a schimba viața de zi cu zi și stilul de viață, inclusiv adoptarea de măsuri de securitate și punerea în aplicare a unor mecanisme de securitate cibernetică mai eficiente, schimbarea locuinței și/sau schimbarea locului de muncă/învățământ, printre altele.

Teama de criminalitatea informatică și percepțiile asupra securității cibernetice

În ceea ce privește impactul criminalității informatice asupra victimelor individuale, *Manualul ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*, explorează de asemenea, teama de criminalitate informatică și riscul perceput de cibervictimizare. Această tematică va fi, de asemenea, abordată în acest Modul. Prin urmare, formatorul ar trebui să consulte capitolul 4 – Partea I din Manual și să țină seamă de următoarele concepte-cheie:

- **Teama de infracțiune** poate fi definită ca o reacție emoțională la infracțiune și/sau la simbolurile aferente acesteia.
- **Riscul perceput** constituie o judecată cognitivă în care oamenii își evaluează propriul risc sau probabilitatea de victimizare, în funcție de experiențele lor personale, contextul/mediul social și circumstanțele, care, la rândul lor, se reflectă în teama de infracțiune (Ferraro, 1995, Rontree, 1998 cit în Yucedal, 2010).

Așadar:

Percepția riscului de cibervictimizare, ca rezultat a proceselor cognitive care includ analiza experiențelor personale de cibervictimizare (în cazul în care acestea există) și a indiciilor de victimizare/infracțiune care provin din stilul de viață *online*, poate duce la **reacții comportamentale orientate spre o protecție mai mare**, care includ punerea în aplicare a măsurilor/mecanismelor de securitate cibernetică și modificarea comportamentelor de utilizare a internetului și a TIC (Yucedal, 2010).

Câteva studii sunt dedicate estimării fricii în raport cu criminalitatea informatică.⁴¹

⁴¹ A se vedea studiul de caz din Special Eurobarometer 423: Cyber security, disponibil accesând: https://www.europeandataportal.eu/data/datasets/s2019_82_2_423_eng?locale=en.

PARTEA 1 – SĂ ÎNȚELEGEM CRIMINALITATEA INFORMATICĂ

MODULUL 3 – VICTIMIZAREA ȘI IMPACTUL CRIMINALITĂȚII INFORMATICE

PLANUL SESIUNII Nr. 3

1. Identificarea acțiunii

Denumire Curs de Formare Sprijin Specializat pentru Victimele Criminalității Informatică

Module / subiecte Victimizarea și impactul criminalității informatice

Data sesiunii **Orar** **Durata sesiunii** 20 de minute

Formatori

2. Obiective specifice

La sfârșitul sesiunii, cursanții ar trebui să poată să:

- Recunoască corect impactul criminalității informatice în diferite domenii ale vieții victimelor criminalității informatice;
- Identifice în mod corespunzător consecințele criminalității informatice asupra percepțiilor privind securitatea cibernetică și teama privind criminalitatea cibernetică.

3. Structura sesiunii

	Conținutul programului	Metodologie	Resurse pedagogice / didactice	Evaluare / Exerciții	Timp (minute)
Introducere	Prevalența criminalității informatice	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
Dezvoltare	Impactul asupra victimelor individuale: • Consecințele asupra sănătății fizice, psihologice și emoționale • Impact financiar • Teama de criminalitatea informatică și percepțiile asupra securității cibernetică	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	13
Concluzie	Rezumat concludent și clarificarea nelămuririlor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	2

OBSERVAȚII

Destinatari:

Specialiști în sprijinirea victimelor

Data: / /

Formator:

PARTEA 1 – SĂ ÎNȚELEM CRIMINALITATEA INFORMATICĂ

MODULUL 3 – VICTIMIZAREA ȘI IMPACTUL CRIMINALITĂȚII INFORMATICE

INSTRUCȚIUNI ESENȚIALE ȘI INFORMAȚII PENTRU FORMATOR

CONCORDANȚA CU CONȚINUTULUI

Planul Sesiunii	<i>Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor</i>	
	PARTE	CAPÍTULO
Prevalența criminalității informatice	Partea I - Înțelegere	Capitolul 1 - 1.3. A se vedea câmpurile PRIM-PLAN STATISTICI PE SCURT
Impactul asupra victimelor individuale	Partea I - Înțelegere	Capitolul 4 - 4.1.
Rezumat concludent și clarificarea nelămuririlor	Nu corespund	

PARTE
PART
PARTEA

2

**APOIO
ESPECIALIZADO
A VÍTIMAS DE
CIBERCRIME**

**SPECIALISED
SUPPORT TO
VICTIMS OF
CYBERCRIME**

**ASISTENȚĂ
SPECIALIZATĂ
PENTRU VICTIME**

MOD. 4

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 4 - ASPECTE FUNDAMENTALE ÎN SPRIJINUL SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII INFORMATICE

PREZENTAREA ȘI CADRUL MODULULUI

Structurarea sprijinului specializat pentru victimele criminalității informatice

Acest Modul propune o primă abordare a acestui Curs de Formare în sprijinirea și asistența victimelor criminalității informatice.

Prin urmare, își propune să prezinte un ansamblu de linii directoare fundamentale și domenii-cheie care trebuie luate în considerare în intervenția cu victimele criminalității informatice, indiferent de tipul (tipurile) de criminalitate informatică la care a fost supusă victima. În următoarele Module, vom încerca, la rândul său, să consolidăm cunoștințele cursanților referitor la strategiile specifice de prevenire și intervenție pentru fiecare tip de criminalitate informatică (de la infracțiunile cibernetice la infracțiuni facilitate de internet și TIC), în vederea depășirea experienței de cibervictimizare și impactul acesteia de către victima căreia i se acordă sprijin.

Așadar, acest Modul va aborda următoarele subiecte:

- Competențe – personale și tehnice – esențiale pentru un profesionist care acordă asistență – Specialist în Sprijinirea Victimelor, și anume empatia și competențe de comunicare;
- Sprijin emoțional;
- Colectare de informații;
- Evaluarea riscului de revictimizare și elaborarea unor planuri de securitate;
- Identificarea necesităților de sprijin;
- Intervenția în criză.

Trebuie menționat, totuși, că, în cadrul acestui Modul, este prezentat un rezumat al conținutului capitolelor 1, 2 și 3 - Partea II a *Manualului ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*. Pentru a consolida cunoștințele cu privire la subiectele tratate, vă recomandăm să citiți cu atenție capitolele menționate.

Empatie, tehnice de comunica și sprijin emoțional

Sprijinul acordat victimelor criminalității informatice necesită un set de competențe cheie și indispensabile din partea specialistul care acordă sprijin:

- **Empatie:** se referă la capacitatea de a se pune în perspectiva victimei infracțiunii, de a fi sensibil la situația cu care se confruntă victima și de a intuit și înțelege sentimentele și semnificațiile pe care le atribuie infracțiunii; este o competență fundamentală pentru stabilirea unei relații de sprijin și încredere.
- **Alte competente personale sunt:**
 - Vocația;
 - Capacitatea de autogestionare emoțională și de a stabili relații interpersonale pozitive;
 - Gestionarea stresului prin o abordare pozitivă și capacitatea de a soluționa într-un mod pașnic problemele interpersonale și/sau interinstituționale;
 - Respectarea demnității umane și toleranță și respectarea diferențelor și diversității culturale.

Referitor la **competențele tehnice**, pe lângă necesitatea unei formări specifice pentru intervenția cu victimele criminalității informatice și educația tehnologică⁴², sunt esențiale **competențele de comunicare** în contactul și sprijinul victimelor criminalității informatice, și anume să asculte, dar și capacitatea de a transmite informații și mesaje clare și inteligibile în cadrul procesului de sprijin (Pessoa et al., 2011).

Comunicarea și empatia sunt fundamentale pe toată perioada de intervenție și sprijinire a victimei criminalității informatice și, în special, în sprijinul emoțional.

Pe scurt, **sprijinul emoțional** care trebuie acordat unei victime a criminalității informatice este bazat pe dimensiunile și atitudinile specialistului în sprijinirea victimei, printre care se află:

⁴² A se vedea deconstrucția conceptului în Modulul 1 al acestui Curs de Formare.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 4 - ASPECTE FUNDAMENTALE ÎN SPRIJINUL SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII INFORMATICE

- **Comunicarea empatică** și ascultarea activă;
- **Limbajul non-verbal**;
- **Luarea în considerare a plângerii și respectarea ritmului** de deschidere a victimei;
- **Promovarea exprimării emoționale a victimei și validarea** experienței de cibervictimizare.

Colectarea de informații

Colectarea informațiilor este un proces central pentru sprijin și intervenție.

La început, primul contact cu victima urmărește acest proces de colectare și adunare de informații, fiind cert faptul că acestea sunt etape circulare și constante care îmbunătățesc în mod regulat orice proces de sprijin și intervenție cu victima.

Pe scurt, procesul de colectare a informațiilor, urmărește să răspundă la 3 domenii:

1. Experiența personală și de pre-victimizare;
2. Experiența de cibervictimizare;
3. Experiența post-victimizare.

Colectarea informațiilor de la victima criminalității informatice va permite:

- Obținerea de informații referitoare la situația criminalității informatice cu care se confruntă;
- Evaluarea impactului și a consecințelor;
- Evaluarea riscului și stabilirea măsurilor de securitate;
- Identificarea nevoilor victimei;
- Punerea în practică a resurselor și serviciilor cele mai adecvate pentru a răspunde acestor nevoi.

Evaluarea riscului și elaborarea planurilor de securitate

Evaluarea gradului de risc urmărește să estimeze **probabilitatea producerii a noi situații de cibervictimizare împotriva victimei**.

Procesul de evaluare rezultă din:

- **Informații împărtășite de victimă** cu privire la experiența de cibervictimizare;
- Utilizarea acestor informații pentru a **identifica (în mod mai mult sau mai puțin structurat) factorii de risc de revictimizare** prezenți în fiecare situație (și merită o atenție deosebită, în ceea ce privește intervenția și planificarea comportamentelor de protecție personală *online* și a măsurilor de securitate cibernetică, în vederea prevenirii revictimizării);
- **Experiența și raționamentul specialistul** în sprijinirea victimei.

În general, putem spune că evaluarea riscului de revictimizare ar trebui să se concentreze pe **3 domenii de risc**:

1. Caracteristicile ale victimei;
2. Caracteristicile, particularitățile și dinamica criminalității informatice;
3. Caracteristicile autorului criminalității informatice.

În acest Modul, vom explora câteva **variabile și factori de risc asociați cu fiecare dintre domeniile de risc** menționați mai sus și care pot fi luați în considerare de către specialistul care acordă sprijin victimelor în procesul de intervenție cu aceștia. *Manualul ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*, în Capitolul 3 - Partea I și Capitolul 3 - Partea II, expune în mod detaliat factorii de risc care pot fi luați în considerare.

Acest Modul vizează, de asemenea, creșterea gradului de conștientizare în rândul specialiștilor / cursanților referitor la nevoia de mecanisme și strategii de evaluare a riscurilor victimei, care să fie întotdeauna însoțite de elaborarea unor **planuri de securitate**:

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 4 - ASPECTE FUNDAMENTALE ÎN SPRIJINUL SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII INFORMATICE

- Strategii de prevenire a revictimizării, convenite și definite între victima și specialistul în sprijinirea victimei, care includ măsuri și comportamente de protecție împotriva noilor situații de criminalitate, precum și strategii și instrucțiuni practice pentru a face față și a acționa, în fața unei eventuale reproducerii a cibervictimizării.

Identificarea nevoilor de sprijin

În urma colectării de informații de la victimă și luând în considerare rezultatele evaluării a riscului de revictimizare, este important ca specialistul să identifice necesitățile de sprijin ale **victimei criminalității informatice**.

În general, se poate afirma că nevoile victimelor criminalității informatice sunt similare cu nevoile victimelor altor forme mai tradiționale de criminalitate (Leukfeldt et al., 2020).

Astfel, pot fi identificate (Cross et al., 2016; Leukfeldt et al., 2020):

- **Nevoi emoționale și psihologice**, cu accent pe recunoaștere în calitate de victimă a infracțiunii, pentru valorificarea și validarea experienței de cibervictimizare, pentru accesul la sprijin și pentru recuperarea/repararea consecințelor a infracțiunii de care a fost victimă;
- **Nevoile de informare și nevoile legate de procedurile penale**, în special în ceea ce privește serviciile de sprijinire existente, drepturile, plângerea și stadiul procedurii penale.
- **Nevoile practice și financiare**, cum ar fi eliminarea conținutului online, cooperarea cu entități și compensația financiară.

În capitolul 4 - Partea I a *Manualului ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor* sunt puse la dispoziție informații detaliate pentru o înțelegere mai bună a nevoilor identificate în rândul (și de) victimelor criminalității informatice.

În cazul concret al **nevoilor legate de drepturi și de procedura penală**, este esențial să se asigure că, în orice etapă a procedurii penale, victima are acces la informații cu privire la drepturile sale, astfel încât să poată beneficia de ele:

- Specialistul în sprijinirea victimei trebuie să fie familiarizat cu cadrul legislativ privind criminalitatea informatică, abordat în Modulul 2 al acestui Curs de Formare;
- Specialistul în sprijinirea victimei ar trebui să cunoască, de asemenea, etapele procedurii penale și drepturile victimelor infracțiunilor, prevăzute legal, pentru a le ajuta să le înțeleagă și să le exercite, printre care:
 - Dreptul la informare;
 - Dreptul de a primi dovada plângerii;
 - Dreptul la traducere;
 - Dreptul de a accesa serviciile de sprijinire a victimelor;
 - Dreptul de a fi ascultat;
 - Drepturi în cazul neacuzării a inculpatului;
 - Dreptul la servicii de mediere;
 - Dreptul la informare sau la protecția legală;
 - Dreptul la compensație pentru participarea la proces și rambursarea cheltuielilor;
 - Dreptul la restituirea bunurilor;
 - Dreptul la despăgubire;
 - Dreptul la protecție;
 - Drepturile victimelor cu nevoi speciale de protecție;
 - Dreptul de a fi uitat⁴³.

Aceste drepturi sunt prezentate mai detaliat în *Manual ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*, capitolul 3 - Partea II. A se vedea și textul integral al Directivei 2012/29 / UE⁴⁴.

De asemenea, în capitolul 3 - Partea II din același Manual, sunt propuse anumite strategii care pot contribui la identificarea nevoilor de sprijin în desfășurarea și pe parcursul procesului de intervenție.

⁴³ Acest drept, spre deosebire de precedentele, nu face parte din Directiva 2012/29 / UE. Acesta este conținut în articolul 17 din Regulamentul general pentru protecția datelor cu caracter personal.

⁴⁴ Disponibil în <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012L0029>.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 4 - ASPECTE FUNDAMENTALE ÎN SPRIJINUL SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII INFORMATICE

În urma identificării nevoilor de sprijin, informare și protecție, poate fi necesară **orientarea (internă sau externă)** victimei criminalității informatice către servicii / răspunsuri de specialitate, respectiv la nivel legal, psihologic și social sau de altă natură.

În acest Modul, este, de asemenea, identificat și definit fenomenul de **victimizare secundară**: a doua formă de victimizare, în urma răspunsului inadecvat furnizat de sistemele și structurile și de discrepanța acestora în raport cu interesele, nevoile și drepturile victimelor.

Intervenția în criză

Experiența de cibervictimizare poate constitui un eveniment care generează o **situație de criză** pentru victimă, fiind observabilă, de exemplu, prin reacții psihologice intense a victimei.

Intervenția în criză (sau primul ajutor psihologic) este o **intervenție intensivă, concentrată și limitată în timp**, orientată spre soluționarea problemelor actuale cu scopul de a răspunde la obiective specifice. Este o intervenție de sprijin inițial, de asistență practică, neinvazivă, în situații de criză sau de urgență.

Acest Modul explorează obiectivele și etapele intervenției în criză, iar această intervenție poate fi rezumată în aspecte cheie, cum ar fi:

- Evaluarea securității victimei și a resurselor (personale și sociale) pentru a răspunde în mod adecvat unei situații;
- Operaționalizarea intervenției vizând recuperarea și reorganizarea victimei.

În *Manualul ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*, capitolul 3 - Partea II, etapele de intervenție în criză sunt acoperite în detaliu.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 4 - ASPECTE FUNDAMENTALE ÎN SPRIJINUL SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII INFORMATICE

PLANUL SESIUNII Nr. 4

1. Identificarea acțiunii

Denumire Curs de Formare Sprijin Specializat pentru victimele criminalității informatice

Module / subiecte Aspecte fundamentale în sprijinul specializat pentru victimele criminalității informatice

Data sesiunii **Orar** **Durata sesiunii** 80 de minute

Formatori

2. Obiective specifice

La sfârșitul sesiunii, cursanții ar trebui să poată să:

- Enumere corect toate aspectele și pașii fundamentali în structurarea sprijinului specializat pentru victimele criminalității informatice, care ar trebui să includă:
 - Empatie și tehnici de comunicare;
 - Sprijin emoțional;
 - Colectarea de informații;
 - Evaluarea riscului și dezvoltarea planurilor de securitate;
 - Identificarea nevoilor de sprijin;
 - Intervenție în criză.

3. Structura sesiunii

	Conținutul programului	Metodologie	Resurse pedagogice / didactice	Evaluare / Exerciții	Timp (minute)
Introducere	Structurarea sprijinului specializat pentru victimele criminalității informatice	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
	Structurarea sprijinului specializat pentru victimele criminalității informatice: • Empatie, tehnici de comunicare și sprijin emoțional • Colectarea de informații • Evaluarea riscurilor și elaborarea planurilor de securitate • Identificarea nevoilor de sprijin • Intervenție în criză	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	60
Dezvoltare	Exercițiul nr. 1	Activă	Tablă / <i>flipchart</i> , marker și regulile exercițiului nr. 1	Observare	10
	Rezumat concludent și clarificarea nelămuririlor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
Concluzie					

OBSERVAȚII

Destinatari:

Specialiști în sprijinirea victimelor

Data: / /

Formator:

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 4 - ASPECTE FUNDAMENTALE ÎN SPRIJINUL SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII INFORMATICE

INSTRUCȚIUNI ESENȚIALE ȘI INFORMAȚII PENTRU FORMATOR

CONCORDANȚA CU CONȚINUTULUI

Planul Sesiunii

Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor

	PARTE	CAPITOL
Structurarea sprijinului specializat pentru victimele criminalității informatice		
Empatie, tehnici de comunicare și sprijin emoțional	Partea II - Continuați	Capitolul 1 - 1.1. și 1.2. Capitolul 2 - 2.1. și 2.2.
Colectare de informații	Partea II - Continuați	Capitolul 2 - 2.3.
Evaluarea riscurilor și elaborarea planurilor de securitate	Partea I - Înțelegere	Capitolul 3 - 3.2.
Identificarea nevoilor de sprijin	Partea II - Continuați	Capitolul 3 - 3.2.
	Partea I - Înțelegere	Capitolul 4 - 4.2.
Intervenție în criză	Partea II - Continuați	Capitolul 3 - 3.3.
Exercițiul nr. 1	Nu corespund	
	A se vedea regulile exercițiului nr. 1	
Rezumat concludent și clarificarea nelămuririlor	Nu corespund	

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 4 - ASPECTE FUNDAMENTALE ÎN SPRIJINUL SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII INFORMATICE

REGULILE EXERCIȚIULUI Nr. 1

Modul / temă	Aspecte fundamentale în sprijinul specializat pentru victimele criminalității informatice	REF.	DOMENIU EDUCAȚIEI ȘI FORMĂRII
Obiective	Acest exercițiu are drept scop consolidarea aspectelor fundamentale care trebuie luate în considerare în sprijinul specializat pentru victimele criminalității informatice, urmărind, în special, să promoveze reflecția cursanților în raport cu un ansamblu de practici și atitudini ale specialiștilor în sprijinirea victimelor care ar putea beneficia sau afecta intervenția și sprijinul acordat unei victime.		
Executare	Pe baza Tabelului 3 [disponibil la punctul 2.1. din capitolul 2 - Partea II a <i>Manualui ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor</i>, formatorul ar trebui să scrie pe tablă / flipchart care se află în sala de formare un set de atitudini și practici care pot avea loc în contextul contactului cu victimele criminalității informatice. Aceste practici și atitudini pot fi sau nu pozitive pentru succesul intervenției care urmează să fie desfășurată. Cu toate că pot fi selectate alte practici enumerate în tabel, propunem următoarele pentru a fi discutate în grup: a) <i>Minimizarea problemei sau impactului experienței de cibervictimizare raportată de victimă.</i> b) <i>Oferirea de soluții la problema prezentată de victimă sau la nevoile identificate.</i> c) <i>Promisiunea față de victimă cu privire la soluționarea problemei prezentate sau răspunsul la nevoile identificate.</i> d) <i>Încurajarea victimei să împărtășească experiența sa de cibervictimizare, precum și gândurile, sentimentele și reacțiile sale.</i> e) <i>Împărtășirea cu victima experiențele personale sau situații asemănătoare în ceea ce privește cibervictimizarea.</i> După ce a fost pusă la dispoziție pe tablă / flipchart, formatorul ar trebui să întrebe grupul, referitor la fiecare afirmație, în ce măsură fiecare dintre atitudini / practici poate fi sau nu adecvată, promovând reflecția cursanților. Din dezbateră promovată cu privire la fiecare afirmație, ar trebui să rezulte următoarea soluție: a) Practica / atitudine necorespunzătoare. Este importantă recunoașterea și validarea victimei și experiența sa ca formă de criminalitate și victimizare. Ca atare, este important să îi explicăm victimei că, în contextul sprijinirii, raportul și experiența sa contează și că specialistul crede ceea ce i se spune. Este important să explicați că există alte persoane care se confruntă cu situații asemănătoare cu a sa, schimbând noțiunea de „caz unic” și să încadrați orice reacții, emoții, sentimente și gânduri în cadrul experienței de cibervictimizare trăită. b) Practica / atitudine necorespunzătoare. Respectarea deciziilor și autonomiei victimei este esențială. Deși explorarea posibilelor soluții poate fi realizată în comun între victimă și specialist, acesta nu ar trebui să înlocuiască victima în procesul de luare a deciziilor sau să ofere soluții victimei, fără a o implica în procesul decizional. În schimb, el ar trebui să prezinte și să exploreze avantajele și dezavantajele fiecărei decizii, astfel încât victima să poată lua decizii în cunoștință de cauză. c) Practica / atitudine necorespunzătoare. Furnizarea victimei cu un fals sentiment de siguranță și / sau promovarea așteptărilor nerealiste cu privire la rolul și / sau soluționarea situației și / sau nevoilor poate fi contraproductiv și poate duce la o rupere a relației de încredere dintre victima și specialistul și / sau frustrarea victimei cu privire la eșecul / nemulțumirea unor astfel de nevoi. d) Practica / atitudine adecvată. Cu toate acestea, este important să ne asigurăm că sunt respectate momentele și dorințele victimei, fără a forța schimbul de informații în momentele în care victima nu este pregătită sau în condiții de a face acest lucru. e) Practică / atitudine necorespunzătoare. Schimbul de informații din partea specialistului / de experiențe personale, ca mijloc de abordare a victimei, poate fi contraproductiv și poate duce la ruperea relației profesionale care se intenționează între victimă și specialist. Deconstrucția convingerilor asupra vulnerabilității unice ar trebui, în schimb, să se realizeze prin prezentarea informațiilor factuale, cum ar fi prevalența asociată cu criminalitatea informatică la care a fost supusă victima sau numărul de victime cărora li se acordă sprijin care au fost obiect unor situații de victimizare asemănătoare.		
Notițe	A se vedea capitolul 2 [punctul 2.1.] Din partea II a <i>manualului ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor</i>		

MOD. 5

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 5 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII CIBER-DEPENDENTE

PREZENTAREA ȘI CADRUL MODULULUI

Conceptele centrale aferente infracțiunilor cibernetice sunt explorate în Modulul 1 al acestui Curs de Formare. Cu toate acestea, acest Modul, în continuarea Modulului anterior în care au fost abordate orientările centrale și aspectele cheie în intervenția cu victimele criminalității informatice, are ca scop aprofundarea cunoștințelor cursanților cu privire la intervenția concretă care urmează să fie efectuată în cazul infracțiunilor cibernetice. În acest scop, vor fi explorate strategiile de intervenție și prevenire a revictimizării, precum și *modi operandi* și natura infracțiunilor în cauză.

Modi operandi și natura infracțiunii

Infracțiunile cibernetice pot fi definite ca orice infracțiune **care poate fi comisă doar prin intermediul calculatoarelor, rețelelor de calculatoare sau altor forme de TIC**. După cum s-a menționat deja, acestea sunt infracțiuni care în absența internetului nu ar putea fi săvârșite.

Astfel, acestea includ activități precum crearea și diseminarea de **malware** și **hacking** pentru a fura date personale sau industriale confidențiale și / sau **atacuri DDoS** pentru a provoca daune financiare și / sau reputaționale.

Victimele acestui tip de infracțiuni pot fi distincte:

- persoane juridice (cum ar fi companii și organizații);
- persoane fizice (adică orice cetățean).

În comiterea acestui tip de infracțiune, sunt folosite mai multe tipuri de atacuri, dintre care vom sublinia **ransomware**, **furtul de informații confidențiale** (*Data compromise*) și **atacuri DDoS**.

Ransomware-ul este un tip de software dăunător sau malware, conceput pentru a **interzice accesul la un sistem sau la datele calculatorului până la plata unei răscumpărări**. *Ransomware*, este răspândit de obicei prin e-mailuri de *phishing* sau când accesați un *website* infectat.

Forma cea mai răspândită de comitere de atacuri *ransomware* continuă să aibă loc prin intermediul **Inginerii Sociale** și prin **trimiterea de e-mailuri de phishing**, adesea deja direcționată către acea persoană sau companie (*spear phishing*), ca modalitate de a accesa calculatorul / rețeaua de calculatoare / a acelei entități și, astfel, de a efectua criptarea datelor.

Un alt vector de atac folosit este **exploatarea vulnerabilităților în protocoalele de acces la distanță ale calculatoarelor**: în aceste cazuri, atacatorul încearcă să exploateze vulnerabilitățile a *softwarului* propriu zis pentru a avea astfel acces la distanță la calculator.

Ransomware-ul și tipurile de atacuri pe care le vom analiza constituie infracțiuni, prevederile și sancționarea acestora pot fi găsite în Noul Cod Penal, în Cap. VI: Infracțiuni contra siguranței și integrității sistemelor și datelor informatice.

Furtul de informații personale online este, de asemenea, un alt tip de criminalitate informatică comun. Se referă în special la obținerea ilegală de informații financiare, și anume date ale cardului de credit, datele bancare sau portofele de criptomonede. Accesul la aceste informații au o mare valoare, deoarece permite vânzarea acestor informații sau utilizarea acestora pentru a fura bunurile victimelor.

Pe lângă informațiile bancare, există și alte tipuri de informații personale despre victimele cu valoare ridicată. În acest context, accesul la informațiile personale ale victimelor permite atacatorului să creeze *e-mailuri de phishing* care vizează în mod specific aceste victime (*spear phishing*). Avantajul acestui atac este faptul că este mai precis și, prin urmare, mai credibil pentru victimă, întrucât *e-mailurile* conțin date cu caracter personal ale victimei. Câteva exemple de infracțiuni care folosesc acest *modus operandi* sunt **frauda online** și **accesul ilegal**.

Furtul de informații personale online poate fi caracterizat de **trei etape**:

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 5 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII CIBER-DEPENDENTE

- 1) **Investigare:** Infractorul informatic caută vulnerabilitățile țintei; aceste vulnerabilități pot fi chiar persoanele propriu zise (fizice), infrastructurile de rețea sau dispozitivele electronice;
- 2) **Atac:** Odată identificate punctele slabe, infractorul informatic începe atacul:
 - împotriva dispozitivelor electronice personale, pentru exploatarea vulnerabilităților lor în scopul de a obține acces la ele.
 - prin inginerie socială, în care oamenii sunt vulnerabilitatea propriu-zisă, fiind înșelați de atacatori și făcuți să dezvăluie informații care vor permite accesul la dispozitivele electronice sau la rețea.
- 3) **Filtrarea datelor:** După obținerea accesului la dispozitivele electronice, infractorul informatic poate căuta datele relevante pe care dorește să le sustragă. Dacă aceleași dispozitive sunt conectate la o rețea, infractorul informatic poate să se infiltreze în rețea și să atace alte dispozitive.

Atacurile DDoS (Distributed Denial of Service, blocarea distribuită a serviciului) sunt concepute pentru a degrada serviciile *online*, cum ar fi **website-uri, e-mailuri și servicii DNS** (Domain Name System). Pentru a atinge aceste obiective, infractorul informatic poate folosi mai multe **forme de atac**:

- Utilizarea mai multor calculatoare pentru a direcționa un volum mare de trafic către serviciile *online*, pentru a le face indisponibile temporar;
- Redirecționarea serviciilor *online* ale unei companii (de exemplu, website-uri), în încercarea de a redirecționa utilizatorii către un alt site decât cel al companii respective.

Datorită caracteristicilor sale, acest tip de practică penală afectează în special persoanele juridice, iar persoanele fizice ajung să fie victime indirecte, deoarece accesul la anumite servicii este imposibil din cauza atacului.

Atacurile de tip DDoS sunt, de asemenea, reglementate și sancționate conform Art. 363 din Noul Cod Penal, Perturbarea funcționării sistemelor informatice.

Strategii de prevenire

În ceea ce privește **atacurile ransomware și furtul de informații confidențiale**, se aplică următoarele strategii de prevenire:

- Activarea filtrării de *spam* puternice pentru a împiedica intrarea *e-mailurilor de phishing* în cutiile poștale de email. De asemenea, se recomandă utilizarea mecanismelor de autentificare prin e-mail cu *Sender Policy Framework (SPF)*, raportarea și conformitatea autentificării mesajelor de domeniu (DMARC) și *Domain Keys Identified Mail (DKIM)*, pentru a împiedica falsificarea e-mailurilor;
- Utilizarea mecanismelor de analiză a fișierelor executabile ale e-mailurilor trimise sau primite, împiedicând utilizatorii să le primească;
- Configurarea *firewall*-ului pentru a bloca accesul la IP-uri (*Internet Protocol*) despre care se știe deja că sunt o amenințare;
- Configurarea antivirusului și a programelor de anti-*malware* pe toate calculatoarele și configurarea acestora în vederea efectuării de scanări periodice;
- Implementarea acțiunilor de formare și conștientizare a riscurilor online, în special în rândul angajaților și directorilor companiei, deoarece aceștia pot fi victime ale acestui tip de atacuri;
- Aplicarea „Principiului Privilegiilor Minime” în companii / organizații: niciunui utilizator nu i se va acorda acces administrativ mai mare decât cel strict necesar pentru exercitarea activității sale.

În ceea ce privește **atacurile de tip DDoS** (Distributed Denial of Service, blocarea distribuită a serviciului), întrucât acestea survin în special în cadrul serviciilor *online* furnizate de persoane juridice, cele din urmă trebuie să se asigure că serviciile lor *online* continue să fie active, chiar și în fața unui atac. În acest scop, pot fi implementate următoarele mecanisme de prevenire:

- Definirea în prealabil care este nivelul de serviciu adecvat care trebuie menținut în mod permanent pentru utilizatori;
- Definirea funcționalităților serviciului *online* la care entitatea / persoana juridică poate renunța în cazul unui atac;

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 5 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII CIBER-DEPENDENTE

- Identificarea împreună cu echipa de IT (*Information Technology*) a entității / persoanei juridice sau cu Webhost-ul contractat pentru găzduirea serviciilor *online*, ce măsuri sunt puse în aplicare pentru protejarea împotriva atacurilor cibernetice și anume:
 - Care este rezistența la un atac de negare de serviciu;
 - Care sunt costurile (în cazul în care acestea există) de a suferi acest tip de atac;
 - Care este limita de trafic începând de la care Webhost-ul este obligat / trebuie să notifice entitatea / persoana juridică precum că serverele sale trebuie închise;
 - Ce măsuri prevăzute de Webhost și de echipa IT sunt declanșate automat, atunci când există acest tip de atacuri.
- Protejarea domeniilor entității / persoanei juridice, folosind blocarea registrului de domeniu⁴⁵ și confirmarea faptului că detaliile registrului de domeniu sunt corecte;
- Să verifice care sunt punctele de contact responsabile pentru partajarea informațiilor între entitatea / persoana juridică și Webhost-ul și dacă aceasta este o rețea de contact 24/7, adică dacă aceste puncte de contact sunt disponibile în fiecare zi a săptămânii și în orice moment din zi;
- Stabilirea unei rețele de contacte în afara rețelei, în cazul în care celelalte linii de contact eșuează;
- Implementarea mecanismelor de monitorizare, în timp real, a atacurilor de refuz de serviciu;
- Separarea diverselor servicii esențiale (ex.: e-mail) de alte servicii care pot fi mai ușor atacate (ex.: servicii de *webhosting*);
- Punerea la dispoziție unei versiuni alternative a *website-ului* cu informații esențiale care poate fi accesată.

Strategii de intervenție

Strategii pentru păstrarea dovezilor digitale

Cu privire la acest tip de criminalitate informatică, pe lângă măsurile care pot fi luate pentru păstrarea probelor, este esențial să se adopte strategii de atenuare a unui atac și să se raporteze entităților care pot oferi asistență tehnică și cu competențe de cercetare penală.

În ceea ce privește atacurile **ransomware** sau orice alt atac care are drept scop interferența sau sabotarea sistemului informatic, trebuie să se adopte următoarele măsuri:

- Să se pună imediat toate sistemele *offline*;
- Să se asigure că *backups* (copiile de siguranță) nu conțin *malware*;
- Să se contacteze imediat Centrul Național de Răspuns la Incidente de Securitate Cibernetică CERT-RO la 1911⁴⁶ să sprijine și să raporteze atacul informatic către autorități - Poliție;
- Dacă este posibil și după caz, să colectați și să asigurați o parte din datele care nu au fost infectate de virus;
- Dacă este posibil, modificați parolele rețelei și a tuturor conturilor *online* după atac. După eliminarea virusului, modificați din nou datele de acces a tuturor conturilor;
- Ștergeți datele de înregistrare și fișierele care împiedică încărcarea virusului;

Multe dintre aceste măsuri sunt aplicabile și situațiilor / atacurilor care au implicat **furtul de informații confidențiale online**; în cazul unui atac *malware* pe dispozitive sau rețea, toate dispozitivele trebuie puse *offline*, urmate de schimbarea tuturor datelor de acces (numele de utilizator și parola). De asemenea, ar trebui să se identifice sursa scurgerii de informații și să corecteze vulnerabilitățile. În cele din urmă, atacul informatic trebuie raportat autorităților competente.

În ceea ce privește atacurile de refuz de serviciu, pot fi luate următoarele măsuri:

- Transferul de servicii online către un serviciu *Cloud* cu capacitate mare de trafic și cu capacitatea de a găzdui un *website* nedinamic;
- Angajarea unei companii / serviciu care oferă mecanisme de combatere a atacurilor de refuz de serviciu sau pentru a trece la soluții interne - INHOUSE - prin intermediul tehnicienilor specializați responsabili pentru punerea în aplicare a acestor măsuri;

⁴⁶ A se vedea <https://cert.ro/>.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 5 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII CIBER-DEPENDENTE

- Dezactivarea serviciilor care permit ca acest atac de refuz de serviciu să fie eficient (ex.: având o versiune a websiteului pregătită pentru lansare).

Cui și cum să raportați / denunțați

Pentru plângere în urma acestui tip de atacuri, ar trebui să fie contactate autoritățile responsabile pentru cercetare penală în această materie, care, la fel ca alte cazuri de criminalitate informatică, este, în cazul României, Poliția Română.

Strategii pentru a depăși victimizarea și impactul acesteia

Înțelegerea dinamicii, impactului și consecințelor în urma experiențelor de cibervictimizare este foarte importantă pentru ca specialistul în sprijinirea victimei să poată ajuta victima să depășească experiența infracțională.

În acest context, pe lângă conținutul pedagogic propus în Modulul 3, este important să citiți capitolele 3 și 4 - Partea I a *Manualul ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*.

După cum s-a menționat deja în Modulul 3, studiile existente cu privire la impactul și consecințele cibervictimizării sunt limitate și se consideră că consecințele suferite de victimele criminalității informatice nu se disting de consecințele resimțite de victimele altor crime.

Pe lângă consecințele asupra sănătății victimelor individuale, asupra impactului financiar și asupra fricii de criminalitate informatică, în cazul specific al infracțiunilor cibernetice, nu ne putem uita doar la consecințele propriu-zise, ci și la scopul în care infractorul informatic a utilizat datele victimei, la care a avut acces nelegitim.

În ceea ce privește strategiile pentru a ajuta victima în depășirea situației criminalității informatice, acest Modul va explora aspectele cheie deja abordate în Modulul anterior referitor la intervenția și sprijinul victimelor criminalității informatice. De asemenea, se recomandă, pentru o abordare aprofundată a acestei teme, să consultați capitolul 2 - Partea II *Manualul ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*.

Printre obiectivele unui astfel de sprijin și intervenție se remarcă următoarele:

- Luare în considerare a plângerii / cererea de sprijin și validarea experienței;
- Furnizarea de informații cu referire la criminalitate și prevalența acesteia.
- Prevenirea noilor infracțiuni, inclusiv prin dezvoltarea împreună cu victima, a planurilor de securitate.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 5 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII CIBER-DEPENDENTE

PLANUL SESIUNII Nr. 5

1. Identificarea acțiunii

Denumire Curs de Formare Sprijin Specializat pentru victimele criminalității informatice

Module / teme Sprijin Specializat pentru victimele infracțiunilor informatice

Data sesiunii **Orar** **Durata sesiunii** 40 de minute

Formatori

2. Obiective specifice

La sfârșitul sesiunii, cursanții ar trebui să poată să:

- Distingă corect natura și modi operandi ale infracțiunilor informatice;
- Enumere strategiile de intervenție propuse în sprijinul specializat pentru victimele infracțiunilor informatice;
- Recunoască corect strategiile de prevenire a victimizării propuse pentru intervenția cu victimele infracțiunilor informatice.

3. Structura sesiunii

	Conținutul programului	Metodologie	Resurse pedagogice / didactice	Evaluare Exerciții	Timp (minute)
Introducere	Exercițiul nr. 2	Activă	Regulile exercițiului nr. 2, fișa exercițiului nr. 2 și pixuri	Observare	5
	Modi operandi și natura infracțiunilor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
Dezvoltare	Strategii de prevenire	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
	Strategii de intervenție: • Strategii pentru păstrarea dovezilor digitale • Cui și cum să raportați / denunțați • Strategii pentru a depăși victimizarea și impactul acesteia	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	20
Concluzie	Rezumat concludent și clarificarea nelămuririlor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5

OBSERVAȚII

Destinatari:

Specialiști în sprijinirea victimelor

Data: / /

Formator:

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 5 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII CIBER-DEPENDENTE

INSTRUCȚIUNI ȘI INFORMAȚII ESENȚIALE PENTRU FORMATOR

CONCORDANȚA CU CONȚINUTUL

Planul Sesiunii	<i>Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor</i>	
	PARTE	CAPITOL
Exercițiul 2	Nu corespund	
	A se vedea Regulile Exercițiului nr. 2	
Modi operandi și natura infracțiunilor	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii de prevenire	Nu se potrivesc	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii de intervenție		
Strategii pentru păstrarea dovezilor digitale	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Cui și cum să raportați / denunțați	Nu se potrivesc	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii pentru a depăși victimizarea și impactul acesteia	Partea II - Continuați	Capitolul 2 - 2.1.
	A se vedea Prezentarea și Cadrul Modulului	
Rezumat concludent și clarificarea nelămuririlor	Nu corespund	

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 5 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII CIBER-DEPENDENTE

REGULILE EXERCIȚIULUI nr. 2

Modul / temă	Sprijin specializat pentru victimele infracțiunilor cibernetice	COD REF.	DOMENIUL EDUCAȚIEI ȘI FORMĂRII
Obiective	Acest exercițiu își propune, printr-o activitate scurtă și atractivă, să reamintim câteva concepte cheie cuprinse în Modulul 1 (legate de fenomenele și atacurile cibernetice aferente infracțiunilor cibernetice) și să facă o introducere la Modulul 5 în care va fi detaliată sprijinirea victimelor infracțiunilor informatice.		
Executare	Formatorul ar trebui să distribuie Fișa de Exerciții cursanților, explicând că fiecare definiție / expresie totală / parțială prezentată în coloana A, trebuie să corespundă unui fenomen / concept enumerat în coloana B. Ar mai trebui să menționeze cursanților că dispun de 60 de secunde pentru a face asocierea dintre definiții / Coloana A și fenomene / Coloana B. Apoi, formatorul ar trebui să corecteze împreună / grup mare, și să clarifice nelămuririle, în cazul în care acestea există. Fenomenele / conceptele (Coloana B) și definițiile / frazele (Coloana A) sunt după cum urmează: <i>Hacking</i>: Implică acces neautorizat la sistemele informatice. <i>Spamming</i>: Se referă la trimiterea și publicarea publicității în masă. <i>Malware</i>: Este un software ostil sau invaziv. Infracțiuni Cibernetice: se referă la criminalitatea informatică propriu-zisă. <i>Phishing</i>: Este folosit pentru accesul nelegitim la informații confidențiale. Atac DDoS (blocarea distribuită a serviciului): Este legat de supraîncărcarea unui sistem.		
Notițe	Consultați Prezentarea și Cadrul Modulului		

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 5 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE CRIMINALITĂȚII CIBER-DEPENDENTE

FIȘA EXERCITIULUI NR. 2

Asociați, cu fiecare dintre definițiile prezentate în coloana A, fenomenul corespunzător prezentat în coloana B.

COLOANA A

Este un software ostil sau intruziv

Se referă la criminalitatea informatică propriu-zisă.

Implică acces neautorizat la sistemele informatice

Este legat de supraîncărcarea unui sistem

Este utilizat pentru accesul nelegitim la informații confidentiale

Se referă la trimiterea și publicarea de publicitate în masă

COLOANA B

Hacking

Spamming

Malware

Infrațiuni Cibernetice

Phishing

Atac de refuz de serviciu

MOD. 6

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 6 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FRAUDELOR ONLINE

PREZENTAREA ȘI CADRUL MODULULUI

În România, putem distinge două tipuri de înșelăciuni: infracțiunea de *înșelăciune* „tradițională”, prevăzută și sancționată conform articolului 244 din Noul Cod Penal, și infracțiunea de *fraudă informatică*, prevăzută și sancționată conform articolului 249 din Noul Cod Penal:

- **Înșelăciune** – definită în Art. 244 din Noul Cod Penal ca fiind „Inducerea în eroare a unei persoane prin prezentarea ca adevărată a unei fapte mincinoase sau ca mincinoasă a unei fapte adevărate, în scopul de a obține pentru sine sau pentru altul un folos patrimonial injust și dacă s-a pricinuit o pagubă”.
- **Frauda informatică** – definită în Art. 249 din Noul Cod Penal ca fiind „Introducerea, modificarea sau ștergerea de date informatice, restricționarea accesului la aceste date ori împiedicarea în orice mod a funcționării unui sistem informatic, în scopul de a obține un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane”.

Acest Modul va explora tipurile de fraude *online* care sunt cele mai semnificative din punct de vedere statistic și cele care cauzează cel mai mare prejudiciu material asupra victimelor, și anume:

- Înșelăciuni în comerțul electronic (*e-commerce*);
- Fraude bancare;
- Înșelăciuni în relații intime (*romance scams*).

În orice caz, aceste fenomene sunt explorate în capitolul 1 - Partea I a *Manualului ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*.

Tipuri, modi operandi și natura infracțiunii

Înșelăciuni în comerțul electronic [*e-commerce*]

Înșelăciunile în comerțul electronic prezintă diferite grade de complexitate:

- de la scheme mai simple, în care cumpărătorul i se promite trimiterea unui anumit articol prin poștă, în urma unui transfer bancar, care nu ajunge să fie primit;
- până la scheme mai elaborate, care pot implica falsificarea documentelor, cum ar fi dovezile de transfer bancar, exploatarea vulnerabilităților în *website*-uri de cumpărături *online* care stochează datele bancare ale utilizatorilor (carduri de credit sau de debit), care sunt accesate și folosite de infractorul informatic pentru a fi vândute pe *darkweb* sau pentru a efectua tranzacții bancare fără cunoștința victimei în cauză (*card not present fraud*).

De asemenea, la nivelul comerțului electronic, pot exista și **înșelăciuni la licitațiile pe internet**, și anume atunci când articolele cumpărate sunt produse false sau obținute prin mijloace ilicite sau când vânzătorul promovează sau pune la dispoziție articole inexistente spre vânzare (Jahankhani și colab., 2014).

Frauda bancară

Frauda bancară se concentrează în principal pe atacurile de **phishing** care pot viza victimele individuale, dar și entități juridice (precum companii și organizații). Modul în care funcționează *phishing-ul* a fost deja acoperit:

- ca regulă generală, prin primirea de *e-mailuri* sau SMS-uri, victima este condusă să dea clic pe un link pe care consideră că aparține entității bancare căreia este titular și este condusă pe un website conceput să arate ca cel al entității bancare la care este titular. Proiectarea acestui *website* se realizează folosind o tehnică numită *pharming*, un termen atribuit atacului care se bazează pe tehnica *DNS cache poisoning* (otrăvire a cache-ului DNS), care constă în coruperea Sistemului de Nume de Domeniu - DNS (Domain Name System) pe o rețea de calculatoare, prin care Localizatorul Uniform de Resurse - URL (*Uniform Resource Locator*) al unui *website* se direcționează către un server diferit de cel original.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 6 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FRAUDELOR ONLINE

Înșelăciune cu cardul de credit se referă la utilizarea cardului de credit al altei persoane pentru uz personal, fără cunoștința titularului cardului și a entității emitente (Patel & Singh, 2013). Există mai multe infracțiuni cibernetice care pot fi folosite pentru a obține acces la astfel de carduri și detalii despre acestea, cum ar fi *phishing*-ul, *spamming*-ul sau *hacking*-ul (Jahankhani și colab., 2014).

De asemenea, este de remarcat **skimming fraud**, care constă în copierea benzii magnetice a unui card de plată, fără cunoștința sau consimțământul titularului cardului, atunci când se folosește cardul la un bancomat sau la un punct de vânzare.

Recent, au început să se înregistreze și alte tipuri de atacuri asupra sistemelor informatice, și anume asupra bancomatelor, într-un proces numit **jackpotting**, care urmărește emiterea de bani în bancomate, prin comanda infractorului. Atacul asupra bancomatelor poate avea loc prin introducerea de *malware* în sistemul informatic al echipamentului / bancomat sau prin conexiunea *hardware*, numită „*Black-Box*”.

Înșelăciuni în relații intime [romance scams]

Înșelăciunile în relațiile intime se întâmplă atunci când agentul încearcă să stabilească o relație de încredere și intimitate, și anume prin internet și TIC, cu o anumită țintă, ca prelude pentru a obține un beneficiu personal, respectiv beneficii financiare și materiale. Acțiunile frauduloase pot implica accesul la banii victimei, conturi bancare, carduri de credit, pașapoarte, conturi de *e-mail* sau numere de identificare naționale sau obligarea victimei să comită infracțiuni în numele agentului.

În acest Modul, vom explora *modi operandi* ale acestor trei tipuri de fraude, precum și strategiile de prevenire și intervenție pe care cursantul, în calitate de Specialist în Sprijinirea Victimei ar trebui să le ia în considerare atunci când oferă sprijin victimelor ale fraudelor *online*.

În ceea ce privește **fraudele din comerțul electronic**, în special fraudele cele mai comune - care nu sunt asociate cu exfiltrarea utilizatorilor -, putem spune că majoritatea au loc pe platformele de vânzare *online*, unde persoanele individuale pot să cumpere și să vândă bunuri.

Când autorul faptei se prezintă în calitate de vânzător:

- Publică reclame false prin intermediul platformelor de vânzare-cumpărare cu privire la diverse articole – locuințe de închiriat, animale de companie, mașini la mâna a doua, bărci, biciclete etc.
- Anunțul poate include poze și alte detalii - de obicei copiate dintr-un alt anunț publicat de către un vânzător autentic - și poate indica, de asemenea, vânzarea articolului respectiv la un preț mai mic;
- Atunci când victima se arată interesată de un articol, autorul poate pretinde, de exemplu, că se află în deplasare sau că s-a mutat într-o altă localitate, și prin urmare o companie de transport va livra marfa, după primirea plății. În urma efectuarea plății, victima poate primi o chitanță falsă prin e-mail, chiar dacă nu va primi articolul achiziționat și nici nu va putea contacta vânzătorul;
- În cazul imobilelor, autorul va juca rolul de proprietar al unui imobil de cumpărare sau închiriere. Atunci când victima își manifestă interesul față de imobil, autorul va aduce diferite pretexte pentru a nu arăta proprietatea în persoană cumpărătorului interesat, susținând, de exemplu, că se află în afara țării / în alt oraș. Dacă victima își menține interesul de achiziționare a imobilului sau să îl închirieze, i se va solicita plata unei sume în avans.

Când autorul faptei se prezintă în calitate de cumpărător:

- Vânzătorul publică un anunț pe o platformă pentru cumpărarea și vânzarea unor articole și primește un *e-mail* sau un mesaj de la o persoană potențial interesată să cumpere articolul, aparent din altă țară (ținând cont de greșelile de ortografie și gramaticale pe care textul le conține);
- Partea interesată solicită datele bancare ale vânzătorului (numărul de identificare bancară - IBAN - sau datele privind plățile prin Paypal®), pentru a efectua plata și informează că îl va contacta o companie de transport pentru colectarea articolului;
- Ca urmare, cumpărătorul îl contactează din nou pe vânzător, informându-l că nu poate efectua plata către

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 6 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FRAUDELOR ONLINE

transportator și că, prin urmare, a transferat valoarea articolului plus costul cheltuielilor privind transportul în contul vânzătorului;

- Cumpărătorul îi cere vânzătorului să efectueze plata către transportator, prin servicii de transfer de bani, și astfel îi furnizează datele necesare (numele și adresa așa-zisei companii de transport). În mod normal, pentru a crește credibilitatea schemei, cumpărătorul atașează la acest *e-mail* o dovadă (falsă) a așa-zisului transfer efectuat vânzătorului.

În **frauda bancară**, cel mai utilizat *modus operandi* este trimiterea de *e-mailuri* de *phishing*. A se vedea exemplul folosit în suportul vizual al acestui Modul (*PowerPoint*):

- Exemplul *e-mailului* tipic de *phishing* are drept scop să copieze imaginea și *lettering* unei notificări efectuate de o entitate bancară;
- De regulă, acest tip de *e-mail* invită destinatarul să descarce un fișier sau să facă clic pe un link care îl redirecționează către un *website* unde trebuie să-și introducă datele personale;
- Aceste *website-uri* sunt concepute cu scopul de a fi foarte asemănătoare cu *website-urile* autentice ale entităților bancare (a se vedea metoda explicată în Modulul 5).

Referitor la **înșelăciunile în relațiile amoroase**, putem identifica următoarele *modi operandi*:

- Crearea unui profil fals pe rețelele sociale, pe aplicații de întâlniri sau alte platforme de *chat* și interacțiune socială;
- Stabilirea contactului cu ținte aparent mai vulnerabile, și anume persoane cu profiluri publice (setări de confidențialitate);
- Crearea unei legături emoționale cu ținta identificată anterior, colectând cât mai multe informații despre aceasta;
- Dezvoltarea unei narațiuni cu scopul de a extorca bunurile personale / financiare ale țintei.

Strategii de prevenire

În acest punct al Modulului, formatorul ar trebui să transmită cursanților următoarele strategii pe care aceștia, în calitate de Specialiști în Sprijinirea Victimei, le pot folosi în intervenție cu victima căreia i se acordă sprijin pentru a **preveni fraudele în comerțul electronic sau fraudele bancare**:

- Nu cumpărați bunuri prin intermediul rețelelor Wi-Fi neprotejate (Wi-Fi public sau rețele unde nu este necesară o parolă).
- Selectați platforme și *website-uri* de cumpărături *online* cunoscute și de încredere care oferă metode de plată sigure.
- Verificați și recunoașteți *website-uri* sigure:
 - Website-ul ar trebui să aibă un simbol cu un lacăt în stânga, chiar înainte de adresa *website-ului*;
 - Adresa URL a website-ului trebuie să conțină certificatul - „https://”; care conține „s” de la „securizat” adăugată la „http”, adresa URL a website-urilor trebuie verificată întotdeauna, și anume atunci când adresele sunt partajate prin mesaj sau *e-mail*;
- Nu furnizați informații personale sau date personale solicitate prin *e-mailuri*, mesaje, apeluri, *website-uri* nesolicitate;
- Să verificați numelui expeditorului de *e-mail* – erori de dactilografiere sau alte erori înseamnă că expeditorul de *e-mail* nu este / reprezintă cine pretinde că este.

Pentru prevenirea **înșelăciunilor în relațiile amoroase**, formatorul ar trebui să transmită cursanților următoarele strategii pe care aceștia, în calitate de Specialiști în Sprijinirea Victimelor, le pot folosi în intervenție cu victima căreia i se acordă sprijin:

- Verificați fotografia de profil (de exemplu, prin motorul de căutare de imagini *Tin Eye* sau *Google Chrome*, făcând clic pe butonul din partea dreaptă a mouse-ului și alegând opțiunea „căutare imagine pe Google”);
- Efectuați o căutare pe Google®, copind paragrafe ale mesajelor primite prin *chat* sau *e-mail*, pentru a înțelege dacă este o abordare / comunicare deja cunoscută și raportată de alte persoane;
- Verificați dacă există erori de ortografie care indică faptul că limba în care persoana comunică nu limba sa maternă;
- Verificați dacă agentul solicită de mai multe ori ca comunicarea să fie purtată prin intermediul platformelor de chat precum Facebook®, WhatsApp®, Kik®, SMS, Messenger® sau Skype®.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 6 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FRAUDELOR ONLINE

Strategii de intervenție

Strategii pentru păstrarea dovezilor digitale

În contextul acestui Modul, formatorul ar trebui să prezinte cursanților strategiile care pot fi explicate victimelor în procesul de sprijinire, cu privire la păstrarea dovezilor. Apoi, câteva dintre aceste strategii sunt identificate în funcție de tipul de fraudă *online*.

Cum să conservăm dovezile în caz de fraude în **comerțul electronic și fraude bancare**:

- În cazul transferurilor patrimoniale, țineți evidența acestor transferuri și contactați entitatea bancară;
- Să depuneți plângere penală la autoritățile competente;
- Solicitați sprijin din partea structurilor de sprijinire a victimelor pentru a face față suferinței emoționale cauzate de situația de victimizare și pentru a asigura monitorizarea pe întregul parcurs a procedurii penale.

Pe lângă strategiile menționate mai sus, în cazul unei înșelăciuni într-o relație amoroasă, ar trebui să se:

- Păstreze toată evidența comunicării purtate cu autorul infracțiunii;
- Raporteze profilul autorului infracțiunii pe *website*, rețeaua socială sau platforma de întâlniri *online*.

Este important ca Specialistul în Sprijinirea Victimei să fie disponibil pentru a asista și / sau a monitoriza victima în procedura de operaționalizare a strategiilor menționate mai sus.

Cui și cum să raportați / denunțați

Atât **înșelăciunile**, cât și **fraudele informatice** trebuie raportate Poliției sau organelor de urmărire penală (Parchet).

Strategii pentru a depăși victimizarea și impactul acesteia

Nesiguranța ce decurge din pierderea stabilității financiare are un impact negativ asupra victimelor fraudelor *online*.

Pe lângă **prejudiciul financiar**, victima fraudei poate manifesta un set divers de **simptome și consecințe** care rezultă din experiența victimizării, care sunt comune tuturor victimelor infracțiunilor, inclusiv:

- **Flashback-url**: gânduri constante despre ceea ce s-a întâmplat;
- **Anxietate**, care poate fi asociată și cu dificultăți de concentrare;
- **Dificultăți legate somn și coșmaruri**;
- **Sentiment de vinovăție**, care poate fi, de asemenea, consolidat de posibile reacțiile ale persoanelor mai apropiate, după dezvăluirea experienței de cibervictimizare;
- **Furie**, uneori asociată cu gânduri de răzbunare;
- **Frică** să fie iarăși victimă unei infracțiuni;
- **Modificări de dispoziție**;
- **Tulburări fizice** cum ar fi, de exemplu, tulburări de alimentație, dureri în piept, amețeli, dureri de cap, dureri de spate și gât, probleme digestive sau transpirații.

În ceea ce privește liniile directe pentru a asista victimele în depășirea situației criminalității informatice, acest Modul va explora aspectele cheie deja acoperite în Modulul 4 în legătură cu intervenția și sprijinirea victimelor criminalității informatice. De asemenea, este recomandat, pentru o abordare aprofundată a acestei teme, să consultați Capitolul 2 - *Manualului ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*.

Fără a aduce atingere liniilor directe fundamentale pentru intervenție abordate în Modulul 4, sunt considerate deosebit de importante în cazul sprijinirii victimelor fraudelor *online*, **strategiile de sprijin emoțional**, prezentate mai jos:

- Ascultarea empatică, demonstrând faptul că ascultați în mod activ și înțelegeți ceea ce vi se spune și valorizați

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 6 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FRAUDELOR ONLINE

reacțiile, emoțiile / sentimentele, comportamentele, gândurile și semnificațiile atribuite de victimă experienței sale de cibervictimizare de fraudă *online*;

- Demonstrați că credeți ceea ce povestește victima despre ceea ce i s-a întâmplat, fără să judecați sau fără a exprima judecăți de valoare;
- Standardizați reacțiile prezentate, prin încadrarea / contextualizarea reacțiilor victimei în contextul emoțional al situației trăite;
- Puneți la dispoziție serviciile oferite, explicând modul în care acestea pot ajuta victima.

Ar trebui, de asemenea, să fie evidențiate **alte strategii de sprijin** în acest punct al Modulului:

- Informați, într-un mod simplu, succint și clar, și transmiteți informații esențiale victimei despre ceea ce s-a întâmplat și pașii următori ce trebuie urmați, utilizând un limbaj adaptat la caracteristicile victimei;
- Nu promovați așteptări nerealiste cu privire la rolul Specialistului în Sprijinirea Victimei și / sau cu privire la soluționarea situației;
- Nu luați decizii în locul victimei și respectați alegerile acesteia;
- Informați despre posibilitatea revictimizării, prin abordarea unor posibile scenarii cu care victima s-ar mai putea confrunta;
- Elaborați un plan de redresare economică împreună cu victima, cu scopul de a oferi strategii victimei pentru a restabili controlul asupra vieții sale;
- Prevenirea noilor infracțiuni, prin conștientizarea importanței adoptării strategiilor de prevenire deja descrise în acest Modul.

Cazul specific al victimelor înșelăciunilor în relații intime (*romance scams*)

În acest punct al Modulului, formatorul ar trebui să abordeze și cazul specific de intervenție cu victimele înșelăciunilor în relații intime. Pornind de la exercițiul nr. 3 (a se vedea Planul Sesiunii), sunt detaliate reacțiile și consecințele emoționale și psihologice a acestei forme de victimizare, și anume:

- Vinovăție intensă;
- Sentiment de nedreptate și neîncredere generalizată față de alte persoane;
- Rușine că au fost înșelați;
- Reticența în a denunța infracțiunea către autoritățile de poliție, mai ales dacă au descoperit că făptuitorul este cineva apropiat și în care au avut încredere, precum un membru al familiei sau un prieten;
- Izolare socială.

În plus față de strategiile mai sus menționate, formatorul ar trebui să abordeze și următoarele strategii:

- Recomandați reluarea progresivă a activităților, inclusiv a obiceiurilor de utilizare a internetului și a TIC;
- Încurajați consolidarea implicării în activități apreciate anterior, și anume activități *offline*;
- Mobilizați sprijinul social și, dacă victima dorește acest lucru și cu acordul său, să implice familia și / sau prietenii în procesul de recuperare, solicitându-le ajutorul pentru a preveni evitarea și izolarea, de exemplu;
- Evitați supraprotejarea de către familie și prieteni (fără a neglija siguranța victimei).

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 6 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FRAUDELOR *ONLINE*

PLANUL SESIUNII Nr. 6

1. Identificarea acțiunii

Denumire	Curs de Formare Sprijin Specializat pentru Victimele criminalității informatice		
Module / teme	Sprijin specializat pentru victimele fraudelor online		
Data sesiunii	Orar	Durata sesiunii	40 de minute
Formatori			

2. Objetivos Especificos

La sfârșitul sesiunii, cursanții ar trebui să poată să:

- Distingă corect natura și *modi operandi* ale fraudelor *online*, inclusiv înșelăciunile în comerțul electronic, fraudele bancare și înșelăciunile în relații intime;
- Enumere corect strategiile de intervenție propuse în sprijin specializat pentru victimele fraudelor *online*;
- Recunoască corect strategiile de prevenire a revictimizării propuse în intervenția cu victimele fraudelor *online*.

3. Structura sesiunii

	Conținutul programului	Metodologie	Resurse pedagogice / didactice	Evaluare Exerciții	Timp (minute)
Introducere	Tipuri de înșelăciuni <i>online</i> : • Înșelăciuni în comerțul electronic • Fraude bancare • Înșelăciuni în relații intime	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	2
	<i>Modi operandi</i> și natura infracțiunilor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	10
Dezvoltare	Strategii de prevenire	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
	Strategii de intervenție: • Strategii pentru păstrarea dovezilor digitale • Cui și cum să raportați / denunțați • Strategii pentru a depăși victimizarea și impactul acesteia	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	15
Concluzie	Exercițiul nr. 3	Activă	Regulile exercițiului nr.3 și EXERCIȚIUL nr.3	Observare	5
	Rezumat concludent și clarificarea nelămuririlor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	3

OBSERVAȚII

Destinatari:

Specialiști în sprijinirea victimelor

Data: / /

Formator:

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 6 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE FRAUDELOR ONLINE

INSTRUCȚIUNI ȘI INFORMAȚII ESENȚIALE PENTRU FORMATOR

CONCORDANȚA CU CONȚINUTUL

Planul Sesiunii *Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*

	PARTE	CAPITOL
Tipuri de fraude online	Partea I - Înțelegere	Capitolul 1 - 1.3.
	A se vedea Prezentarea și Cadrul Modulului	
Modi operandi și natura infracțiunilor	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii de prevenire	Nu se potrivesc	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii de intervenție		
Strategii pentru păstrarea dovezilor digitale	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Cui și cum să raportați / denunțați	Nu corespund	
	A se vedea Prezentarea și cadrul modulului	
Strategii pentru a depăși victimizarea și impactul acesteia	Partea II - Continuați	Capitolul 2 - 2.1.
	A se vedea Prezentarea și Cadrul Modulului	
Exercițiul nr. 3	Nu corespund	
	A se vedea Regulile Exercițiului nr. 3	
Rezumat concludent și clarificarea nelămuririlor	Nu corespund	

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 6 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FRAUDELOR ONLINE

REGULILE EXERCITIULUI Nr. 3

Modul / temă	Modulul 6 - Sprijin specializat pentru victimele înșelăciunilor online	COD REF.	DOMENIUL EDUCAȚIEI ȘI FORMĂRII
Obiective	Acest exercițiu își propune să consolideze informațiile și conținutul acoperit în acest Modul, în special în ceea ce privește natura infracțiunilor de fraudă online și strategiile de prevenire a revictimizării și a intervenției.		
Executare	Formatorul ar trebui să citească EXERCITIUL Nr. 3 (sau să ceară unuia dintre cursanții prezenți să îl citească cu voce tare). Vă propunem distribuirea acestui Caz cursanților sau proiecția Cazului pe tablă, pentru lectură. După lectură, formatorul trebuie să prezinte grupului următoarele întrebări: 1. Ce fel de înșelăciune este identificabilă în acest caz? 2. Care sunt consecințele victimizării evidențiate de victima acestui caz? 3. Ce ar trebui să ia în considerare Specialistul în Sprijinirea Victimei în intervenția / sprijinul acordat victimei? În timpul dezbaterii grupului, formatorul trebuie să țină cont de următoarele orientări cu privire la întrebările de mai sus: 1. Raportarea Lucindei se încadrează într-o situație de înșelăciune în relațiile intime. 2. În situația raportată de Rodica, sentimentele de vinovăție, rușinea, neîncrederea față de intențiile altora și izolarea / evitarea interacțiunilor / relațiilor sociale sunt evidente, în conformitate cu consecințele și reacțiile manifestate de victimele ale <i>romance scams</i>. Rezistența la plângere este, de asemenea, evidentă, datorită existenței unei relații strânse (de prietenie) cu autorul faptei. 3. Trebuie evidențiate unele aspecte cheie ale intervenției: ascultarea empatică, demonstrați că credeți în situația raportată; Încadrarea reacțiilor în contextul situației trăite de victimă; recomandați reluarea activităților și implicarea în activități apreciate (și anume <i>offline</i>); mobilizați persoanele din rețeaua semnificativă (dacă victima arată dorința de a ai implica); prevenirea noilor infracțiuni, prin transmiterea măsurilor de securitate / securitate cibernetică; prezentați avantajele și dezavantajele legate de plângere. A se vedea informațiile disponibile în Prezentarea și Cadrul Modulului.		
Notițe	Consultați Prezentarea și Cadrul Modulului		

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 6 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FRAUDELOR ONLINE

EXERCITIUL Nr. 3

Rodica, în vârstă de 55 de ani, văduvă, mamă a trei copii, toți persoane majore. Cel mai tânăr are 23 de ani și a plecat de acasă anul trecut. În prima ședință de sprijin, a spus următoarele:

„Știu că a fost vina mea, a fost doar vina mea, nu mai am vârstă pentru așa ceva ... Dar mă simt atât de singură de când fiul meu cel mic a plecat de acasă ... Și această prietenă de a mea sau, drept vorbind, am crezut că este prietena mea, Florina ... a venit la mine cu această poveste că sunt încă tânără, că aș putea să-mi găsesc pe cineva care să-mi țină companie, că ea avea o colegă de serviciu care și-a găsit un iubit pe Facebook. Ei bine, nu intenționat - m-am gândit, eu proasta! - câteva zile mai târziu am o cerere de prietenie pe Facebook de la un domn pe nume Marius, foarte prezentabil. Avea vârsta de 60 de ani, a divorțat cu mult timp înainte, cu copiii deja mari. A început să vorbească cu mine și m-a tratat atât de bine ... Nu mi s-a acordat atâta atenție de atât de mult timp ... Am simțit că aș avea din nou 20 de ani! Mi-a spus că locuiește în Statele Unite, dar că se gândește să se întoarcă în România. Am crezut tot ceea ce mi-a spus, m-am și uitat la bilete de avion ca să merg la el ... În fine ... La scurt timp după aceea a început să spună că unul dintre copiii lui este foarte bolnav și că trebuie să trimită bani fiului. Numai că el nu reușea să facă transferuri din Statele Unite în România - mi-a explicat de ce, dar sincer, nici măcar nu mi-a păsă de explicație, pentru că voiam doar să-l pot ajuta, tocmai într-o situație atât de tulburătoare precum boala unui fiu ... - și mi-a cerut să fac aceste transferuri. Și le-am făcut, le-am tot făcut ... Am transferat peste 5.000 de euro ... Și acum aflu că toate acestea au fost parte din planul Florinei ... Nu a existat niciodată niciun Marius ... [plângând ...] Cum am putut fi atât de proastă?! Ce rușine ... A fost doar vina mea că am vrut să am pe cineva ... Sunt foarte bine singură, nu vreau prieteni, sau altceva! Uitați-vă, vreau doar să-mi recuperez banii, dar nu vreau să fac plângere. Nu o pot face, nu vreau să i se întâmple nimic rău, are copii mici, știți ... ”

MOD. 7

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 7 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FURTULUI DE IDENTITATE *ONLINE*

PREZENTAREA ȘI CADRUL MODULULUI

Furtul de identitate include obținerea neautorizată de date personale și / sau secrete ale victimei, deținerea datelor sau transferul acestora în cunoștință de cauză că vor fi utilizate în scopuri infracționale.

Aceste acte corespund **furtului de identitate *online*** atunci când datele personale și / sau confidențiale ale victimei sunt obținute prin intermediul internetului și / sau când datele obținute, prin orice mijloace, sunt transferate prin intermediul internetului și / sau utilizate pentru a comite o infracțiune.

Dacă infracțiunea are loc doar într-una dintre fazele descrise, comportamentul corespunzător - obținerea, proprietatea sau utilizarea acesteia - trebuie practicat prin intermediul internetului, pentru a se potrivi conceptului.

Putem identifica **trei faze distincte**:

1. Faza de obținere a datelor cu caracter personal [prin internet];
2. Faza de proprietate asupra datelor sau transferul de date [prin internet], știind că acestea vor fi folosite pentru comiterea unei infracțiuni;
3. Faza de utilizare a datelor pentru a comite infracțiuni [prin internet].

Pot fi identificate **3 tipuri de furturi de identitate**:

- Infracțiuni care nu au legătură directă cu victima, ci au fost comise în numele său;
- Infracțiunile care are ca obiectiv îmbogățirea autorului infracțiunii sau a terților și cauzarea daunelor directe victimei;
- Infracțiuni care urmăresc defăimarea victimei.

În acest Modul, vom aborda *modii operandi* ale furtului de identitate *online*, precum și strategiile de prevenire și intervenție pe care formatorul, în calitate de Specialist în Sprijinirea Victimei, ar trebui să le ia în considerare atunci când acordă sprijin victimelor acestui tip de criminalitate informatică.

Modi operandi și natura infracțiunii

Furtul de identitate nu este, în sine, o infracțiune, care intenționează doar să descrie un fenomen de obținere neautorizată a datelor cu caracter personal, în vederea comiterii unei activități infracționale. Prin urmare, atunci când vorbim de furtul de identitate, putem vorbi despre o multitudine de infracțiuni prevăzute și pedepsite în Noul Cod Penal din România.

Acest Modul ale Cursului face parte dintr-un exercițiu (a se vedea Planul Sesiunii) pentru a exemplifica diferitele infracțiuni prevăzute legal care pot fi încadrate într-o situație de furt de identitate *online*, cum ar fi: infracțiunea de fals în documente (art. 256, alin. 1, lit. a) din CP); infracțiune de acces ilegal (art. 6, alin. 1 din Legea Criminalității Informatic); infracțiunea de fraudă informatică (art. 221, alin. 1 din CP).

În ceea ce privește *modi operandi* ale infracțiunilor de furt de identitate, putem identifica două metode:

- **Cele mai puțin tehnologice**, folosind așa-numita Inginerie Socială pentru a obține informații personale de la victime;
- **Cele mai tehnologice**, în care interacțiunea cu victima nu este un element fundamental pentru comiterea acestei infracțiuni.

În ceea ce privește **metodele de Inginerie Socială** ca modalitate de comitere a furtului de identitate, pot fi identificate următoarele:

- Exploatarea factorului uman, ca element de vulnerabilitate pentru securitatea cibernetică;
- Actul de manipulare psihologică care tinde să conducă pe cineva să dezvolte o acțiune specifică sau să dezvăluie informații confidențiale;

Metodele mai puțin tehnologice pot fi mai ușor de utilizat decât metodele mai tehnologice (cum ar fi *malware*-ul sau *hacking*-ul), în special pentru infractorii cibernetici care au competențe tehnice reduse pentru a utiliza anumite instrumente și / sau nu au resursele necesare pentru a le obține pe *darkweb*.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 7 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FURTULUI DE IDENTITATE ONLINE

Exemple:

- *Vishing* (obținerea de date prin contactarea telefonică - infractorii cibernetici apelează din ce în ce mai mult, la *native speakers*);
- *Romance scams*;
- *Sextortion*;
- Ademenirea a minorilor *online*;
- Scotocirea în gunoi;
- Interceptarea e-mailului;
- Furtul documentelor care conțin informații personale sau financiare privind victima;
- Folosirea identității unei persoane care poate solicita acest tip de date / informații;
- Obținerea de informații de la persoane apropiate victimei;
- Contactarea victimei cu pretenții false pentru a obține informații confidențiale;
- Cumpărarea acestor informații;
- Observarea victimei în timp ce folosește informații pe care infractorul vrea să le obțină;
- Furt de *hardware* sau telefon mobil care conține informații personale sau secrete ale victimei.

În ceea ce privește **metodele cele mai tehnologice** de obținere a datelor cu caracter personal, subliniem următoarele:

1. Furt de identitate prin *Phishing*:

- Trimiterea de e-mailuri în masă cu un atașament care duce către o pagină *web*;
- Victima furnizează autorului infracțiunii, informații personale / parole / coduri de acces; prin accesul la pagina *web* menționată,
- Autorul infracțiunii accesează pagina autentică a instituției bancare, introduce datele victimei și retrage bani din cont;
- Spălare de bani: procesul prin care autorul sau autorii unor activități infracționale acoperă proveniența bunurilor și a veniturilor (avantajelor) obținute ilegal, și transformă lichiditatea care provine din acele activități în capital reutilizabil legal, prin omiterea provenienței sau a proprietarului propriu-zis al fondurilor

2. Furt de identitate prin utilizarea de *Malware*:

- *Malware, software* care poate fi răspândit în diverse feluri, în vederea infiltrării ilegale în echipamentele, calculatoarele și rețelele, cu scopul de a fura informații, de a modifica informațiile sau de a provoca daune:
 - Prin intermediul unui link sau fișier primit prin e-mail;
 - Prin descărcarea de filme sau jocuri;
 - Prin accesarea unor *website*-uri compromițătoare;
 - Odată cu instalarea de aplicații compromițătoare, etc.

Un exemplu de **furt de identitate care îmbină Ingineria Socială și metodele tehnologice** este ***Spear Phishing***: crearea de e-mailuri de *phishing* folosind tehnici de Inginerie Socială pentru a personaliza mesaje și website-uri în funcție de destinatar, și prin urmare crește credibilitatea Informațiilor și induce victima în eroare să acceseze informații confidențiale.

În cele mai comune situații de furt de identitate *online*, putem identifica:

1. *Phishing*-ul pentru obținerea accesului la contul de *e-mail*:

- Odată ce datele personale și confidențiale ale victimei au fost obținute, infractorul informatic poate avea acces la contul de *e-mail* al victimei, folosind oricare dintre metodele sofisticate menționate mai sus cu obiectivul de a lua la cunoștință conținutul de *e-mail*, de a stabili contactul cu banca victimei - de obicei cu managerul de cont - pentru a efectua tranzacții bancare sau pentru a folosi acel cont de *e-mail* pentru a da credibilitate e-mailurilor pe care intenționează să le trimită și care vă vor fi în mod normal cereri de ajutor financiar.

2. *Phishing* pentru obținerea accesului la contul bancar:

- Trimiterea în masă de emailuri (*spamming*);
- Mesajele conțin un link către o pagină falsă a entității bancare;

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 7 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FURTULUI DE IDENTITATE *ONLINE*

- Pe pagina falsă, vi se cere să completați / să trimiteți date confidențiale.

3. Defăimare pe rețelele sociale:

- Există situații de furt de identitate care au drept scop defăimarea victimei pe o rețea socială, care au loc de obicei în cadrul relațiilor de prietenie sau relațiilor amoroase:
 - Crearea unui profil fals;
 - Utilizarea profilului real al victimei, folosind datele de acces a acesteia:
 - Victima propriu-zisă furnizează date infractorului;
 - Infractorul obține aceste date prin alte mijloace.

Strategii de prevenire

În acest punct al Modulului, formatorul ar trebui să transmită cursanților următoarele strategii pentru **a preveni furtul de identitate online**, pe care aceștia, în calitate de Specialiști în Sprijinirea Victimelor, le pot folosi în intervenție cu victima căreia i se acordă sprijin:

- Configurați antivirusul și programele de anti-*malware* pe dispozitive și configurați programele pentru a efectua scanări periodice;
- Activați filtrele de *spam*;
- Protejați dispozitivele, folosind metode de autentificare care folosesc date biometrice sau, ca alternativă, coduri de blocare și instalarea *software*-ului antivirus pe dispozitive;
- Verificați și recunoașteți website-urile sigure (a se vedea informațiile din Modulul 6 despre această temă);
- Nu furnizați informații personale sau date personale solicitate prin *e-mailuri*, mesaje, apeluri, website-uri nesolicitate;
- Verificați numelui expeditorului de *e-mail* – erori de dactilografiere sau alte erori înseamnă că expeditorul de *e-mail* nu este / reprezintă cine pretinde că este.
- Verificați dacă există erori de ortografie care indică faptul că limba în care persoana comunică nu limba sa maternă.

Strategii de intervenție

Strategii pentru păstrarea dovezilor digitale

În contextul acestui Modul, formatorul ar trebui să prezinte cursanților strategiile care pot fi explicate victimelor în procesul de sprijinire, pentru păstrarea dovezilor. Întrucât furtul de identitate poate viza o multitudine de scopuri infracționale, mai jos sunt prezentate câteva strategii generale:

- Conservați dovezile de pe rețelele sociale, prin copierea adresei URL a conținutului ilegal și capturile de ecran ale conținutului respectiv (a se vedea Modulul 10, pentru informații suplimentare cu privire la copierea adresei URL);
- În cazul transferurilor patrimoniale, țineți evidența acestor transferuri și contactați entitatea bancară;
- Depuneți plângere penală la autoritățile competente;
- Solicitați asistență structurilor de sprijinire a victimelor pentru a face față suferinței emoționale cauzate de situația de victimizare și pentru a asigura monitorizarea pe întregul parcurs a procedurii penale.

Este important ca Specialistul în Sprijinirea Victimei să fie disponibil pentru a asista și / sau a monitoriza victima în procedura de operaționalizare a strategiilor menționate mai sus.

Cui și cum să raportați

Furtul de identitate nu este o infracțiune propriu-zisă. Cu toate acestea, poate fi un mijloc pentru comiterea unei multitudini de infracțiuni prevăzute și pedepsite de Noul Cod Penal din România. Portughez. Raportați orice suspiciune privind o infracțiune care implică furtul de identitate Poliției sau Parchetului.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 7 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FURTULUI DE IDENTITATE ONLINE

Strategii pentru a depăși victimizarea și impactul acesteia

Furtul de identitate implică, pentru victimă, o tulburare gravă și o mulțime de timp petrecut pentru a repara consecințele infracțiunii. Pe lângă **pierderea de timp**, o consecință frecvent menționată de victime, **impactul emoțional** în urma furtului de identitate este descris ca fiind similar cu reacțiile victimelor infracțiunilor violente. Multe victime consideră că le este încălcată intimitatea, se simt dezorientate, neajutorate, temându-se că infracțiunea se va repeta și sunt suspicioase cu privire la intențiile oamenilor din jur. Dacă furtul de identitate al victimei are ca scop defăimarea pe rețelele sociale, impactul, pe care **promovarea / audiența** îl adaugă la infracțiunea comisă, agravează simptomele de disconfort emoțional și psihologic.

Fără a aduce atingere liniilor directoare fundamentale pentru intervenție abordate în Modulul 4 a acestui Curs de Formare, sunt considerate deosebit de importante în cazul sprijinul victimelor furtului de identitate *online*, **strategiile de sprijin**, prezentate mai jos:

- Oferiți suport emoțional victimei, prin a asculta, a valida experiența și prin a standardiza / încadra reacțiile;
- Explicați victimei că există alte persoane care se confruntă cu situații similare cu ale victimei, schimbând noțiunea de „caz unic”;
- Informați, într-un mod simplu, succint și clar, și transmiteți informații esențiale victimei despre ceea ce s-a întâmplat și pașii următori ce trebuie urmați, utilizând un limbaj adaptat la caracteristicile victimei;
- Explicați diferitele tipuri de sprijin acordate de care poate beneficia, transmițând astfel mesajul că victima nu este singură pe parcursul întregului proces;
- Nu promovați așteptări nerealiste cu privire la rolul specialistului în Sprijinirea Victimei și / sau cu privire la soluționarea situației;
- Explicați victimei că, datorită naturii însăși a situațiilor de furt de identitate, poate surveni comiterea altor infracțiuni împotriva sa, consolidând disponibilitatea de a-i acorda sprijin;
- Prevenirea noilor infracțiuni, prin conștientizarea importanței adoptării strategiilor de prevenire deja descrise în acest Modul.

Ori de câte ori este posibil, prezentarea acestor strategii (precum și a următoarelor) trebuie să fie însoțită de exemple concrete de operaționalizare, cu scopul de a familiariza cursanții cu limbajul și forma de comunicare care urmează să fie puse în aplicare în contactul cu victima pe întregul parcurs de sprijinire / asistență. Astfel de exemple sunt disponibile în materialul vizual (*PowerPoint*).

Victimele furtului de identitate pot fi **reticente în a denunța infracțiunile de care au fost țintă către autoritățile de poliție**, mai ales dacă au descoperit că autorul infracțiunii este o persoană apropiată și de încredere, cum ar fi un membru al familiei sau un prieten. În aceste situații, pe lângă strategiile de mai sus, este important ca Specialistul în Sprijinirea Victimei să:

- Accentueze curajul de a căuta sprijin și de a împărtăși experiență personală de cibervictimizare;
- Asiste victima în procesul decizional privind plângerea (fără a lua decizii în numele victimei și / sau fără să influențeze procesul), expunând avantajele și dezavantajele fiecărei opțiuni, în vederea luării unor decizii în cunoștință de cauză;
- Transmite informațiile esențiale victimei privind drepturile sale după depunerea plângerii, reiterând faptul că sprijinul este independent de plângere.

Uneori, victimele furtului de identitate *online* se simt **nedreptățite**, cu nevoia de a-și demonstra nevinovăția sau **dezamăgite / frustrate** de rezultatul procedurii penale. Specialistul în Sprijinirea Victimei ar trebui să fie conștient de existența acestor tipuri de gânduri și să acționeze asupra lor:

- Să accentueze faptul că crede în raportul victimei;
- Să valideze experiența și să recunoască efectele cauzate de situația de victimizare la cele mai diverse niveluri (psihologic și emoțional, social și în alte domenii afectate);
- Să evalueze încercările anterioare de protecție / soluționare;
- Să prevină vinovăția;
- Să propună împărtășirea sentimentelor și fricilor cu cei în care are încredere, să le recomande acestora din urmă să se arate disponibili pentru a asculta, fără a pune presiune pe schimbul de sentimente;
- Să explice că recuperarea în urma victimizării este independentă de rezultatul procedurii penale;
- Să pună la dispoziție sprijin psihologic.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 7 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FURTULUI DE IDENTITATE *ONLINE*

PLANUL SESIUNII Nr. 7

1. Identificarea acțiunii

Denumire Curs de Formare Sprijin Specializat pentru Victimele Criminalității Informaticе

Module / teme Sprijin Specializat pentru Victimele Furtului de Identitate *online*

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

Formatori

2. Obiective specifice La sfârșitul sesiunii, cursanții ar trebui să poată să:

- Distingă corect natura și modi operandi ale furtului de identitate online;
- Enumere corect strategiile de intervenție propuse în sprijinul specializat pentru victimele furtului de identitate online;
- Recunoască corect strategiile de prevenire a revictimizării propuse pentru intervenția cu victimele furtului de identitate *online*.

3. Structura sesiunii

	Conținutul programului	Metodologie	Resurse pedagogice / didactice	Evaluare Exerciții	Timp (minute)
Introducere	Exercițiul nr. 4	Activă	Regulile Exercițiului nr.4 și EXERCIȚIULnr.4	Observare	5
	<i>Modi operandi</i> și natura infracțiunii	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	10
Dezvoltare	Strategii de prevenire	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
	Strategii de intervenție: • Strategii pentru păstrarea dovezilor digitale • Cui și cum să raportați / denunțați • Strategii pentru a depăși victimizarea și impactul acesteia	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	15
Concluzie	Rezumat concludent și clarificarea nelămuririlor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5

OBSERVAȚII

Destinatari:

Specialiști în sprijinirea victimelor

Data: / /

Formator:

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 7 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE FURTULUI DE IDENTITATE *ONLINE*

INSTRUCȚIUNI ESENȚIALE ȘI INFORMAȚII PENTRU FORMATOR

CONCORDANȚA CU CONȚINUTUL

Planul Sesiunii *Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*

	PARTE	CAPITOL
Exercițiul nr. 4	Nu corespund	
	Vezi Regulile Exercițiului nr. 4	
<i>Modi operandi</i> și natura infracțiunii	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii de prevenire	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii de intervenție		
Strategii pentru păstrarea dovezilor digitale	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Cui și cum să raportați / denunțați	Nu se corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii pentru a depăși victimizarea și impactul acesteia	Partea II - Continuați	Capitolul 2 - 2.1.
	A se vedea Prezentarea și Cadrul Modulului	
Rezumat concludent și clarificarea nelămuririlor	Nu corespund	

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 7 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FURTULUI DE IDENTITATE *ONLINE*

REGULILE EXERCITIULUI nr. 4

Modul / temă	Sprijin Specializat pentru victimele furtului de identitate <i>online</i>	COD REF.	DOMENIUL EDUCAȚIEI ȘI FORMĂRII
Obiective	Acest exercițiu își propune conștientizarea cu privire la particularitățile situațiilor de furt de identitate <i>online</i> și natura acestui fenomen, și să atragă atenția în special referitor infracțiunilor care pot fi comise în cadrul acestuia.		
Executare	Formatorul ar trebui să citească Exercițiul nr. 4 (sau să solicite unuia dintre cursanții prezenți să îl citească cu voce tare). Vă propunem distribuirea acestui Caz cursanților sau proiecția sa pe tablă, pentru lectură. După lectură, formatorul ar trebui să întrebe grupul referitor la infracțiunile prezente în acest Caz. În timpul dezbaterii grupului, formatorul ar trebui să facă referire la <i>cadrul legislativ privind criminalitatea informatică la nivel național</i> (a se vedea Modulul 2) și să demonstreze clar că, în acest Caz, există mai multe infracțiuni identificabile: • Conduita creării unui e-mail fals corespunde infracțiunii de uz de fals (Art. 323 din Codul Penal); • Conduita de acces la contul de e-mail al soției lui Mihai corespunde infracțiunii de Acces ilegal la un sistem informatic (Art. 360, Codul Penal); • Încercările de obținere de credit în numele lui Mihai, corespund infracțiunii de fraudă informatică (Art. 249, Codul Penal).		
Notițe	Consultați Prezentarea și Cadrul Modulului		

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 7 - SPRIJIN SPECIALIZAT PENTRU VICTIMELE FURTULUI DE IDENTITATE *ONLINE*

EXERCIȚIUL Nr. 4

Mesajele au fost trimise către mai multe adrese de *e-mail* care păreau a fi de la serviciul *webmail* utilizat și care au solicitat actualizarea parolei.

Soția lui Mihai a introdus datele și, astfel, infractorul a avut acces la contul său de e-mail, luând la cunoștință nenumărate date personale, precum și cele referitoare la familie. Ulterior, Mihai a fost contactat de două societăți emitente de credit care doreau să confirme că cererile pentru obținerea creditului în numele său erau legitime. Mihai, care nu a accesat niciodată un credit, a explicat că nu a solicitat credit la niciuna dintre societăți. A fost uimit de cantitatea de date cu caracter personal pe care infractorul le știa. Cererile au fost respinse. O lună mai târziu, Mihai s-a dus la bancă, cu intenția de a lua un împrumut pentru a achiziționa o locuință nouă. Împrumutul a fost respins datorită numeroaselor cereri pentru obținere de credit depuse în numele său în ultimele luni.

MOD. 8

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 8 - SPRIJIN SPECIALIZAT PENTRU COPII ȘI TINERI VICTIME ALE ABUZULUI SEXUAL *ONLINE*

PREZENTAREA ȘI CADRUL MODULULUI

În acest Modul, vor fi examinate diferite moduri de exprimare a abuzului sexual asupra copiilor și tinerilor *online*.

Abuzul sexual *online* este un concept cuprinzător și acoperă **orice formă de abuz sexual asupra copiilor în contextul *online***. Prin urmare, acest concept include diferite manifestări de abuz și exploatare, de la abuzuri sexuale fără contact, facilitate de TIC și de Internet, de rețelele sociale sau alte platforme, cum ar fi hărțuirea și ademenirea (*grooming online*), până la partajarea de conținut pe *darkweb* (imagini și / sau audio) de abuz sexual și exploatare a copiilor, colectate prealabil în fotografie sau video.

Se va pune un accent deosebit pe înțelegerea fenomenelor de **ademenire** (*grooming online*) și **diseminarea a conținutului de abuz sexual asupra copiilor *online***.

Cantitatea de material de abuz și exploatare sexuală a copiilor (CSAM) care urmează să fie diseminate *online* continuă să crească, o tendință confirmată de autoritățile de aplicare a legii și de organizațiile neguvernamentale care își desfășoară activitatea în domeniul analizei și raportării conținutului de abuz sexual *online*. Diseminarea acestui conținut are un impact grav asupra victimelor, care sunt supuse unor procese de revictimizare, de fiecare dată când fotografiile sau înregistrările video sunt vizualizate și / sau partajate.

Modul de diseminare a acestui material se efectuează în continuare prin intermediul rețelelor / *peer-to-peer* (P2P) și accesul anonim, cum ar fi browserele de acces la *Darknet* (de exemplu, Tor).

În paralel, a existat o creștere constantă a distribuției CSAM prin intermediul rețelelor sociale. Dificultatea de a conserva dovezile pe unele dintre aceste rețele fac investigarea autorităților să fie extrem de dificilă. Există cazuri în care astfel de conținut / materiale sunt partajate de copiii înșiși și ulterior partajate cu colegii care, la rândul lor, distribuie altor colegi până când, în cele din urmă, acest conținut / materiale ajung pe platformele de distribuție CSAM. În multe cazuri, infractorii care distribuie CSAM *online* sunt implicați și în situații de abuz sexual asupra copiilor. Nivelul ridicat al cererii pentru acest tip de material perpetuează abuzul și victimizarea continuă a copiilor.

Din punct de vedere legal în România, CSAM constituie infracțiunea de pornografie infantilă.

La nivel internațional, se pledează pentru renunțarea la conceptul de „pornografie infantilă”, dat fiind că (adică persoanele adulte implicate, în mod consensual, în comportament erotic în imagini, înregistrările video și / sau scriere, destinate să provoace excitare sexuală) nu reflectă ceea ce stă la baza situațiilor de abuz sexual asupra copiilor. Din acest motiv, se susține că, atunci când facem referire la materialul „pornografie infantilă”, se să se folosească terminologia „Conținut de abuzul sexual asupra copiilor”.

Pe lângă aceste fenomene, ademenirea *online* merită, totodată o atenție specială. În acest scop, vom aborda *modi operandi* care stau la baza ademenirii *online* pe rețelele sociale și jocurile *online*, ținând cont de faptul că aceste platforme ocupă o mare parte din timpul de utilizare a internetului și TIC de către copii și tineri.

În orice caz, pe lângă lectura conținutului acestui Modul, propunem formatorului să consulte Capitolul 1 - Partea I a Manualului ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor.

Tipuri, *modi operandi* și natura infracțiunilor

Diseminarea conținutului de abuz sexual asupra copiilor [CSAM]

Conținut cu abuz sexual asupra copiilor generat online

În prezent, există două moduri care au fost evidențiate, ca mijloace de diseminare a conținutului de abuz sexual asupra copiilor *online*:

- Conținut auto-produs / auto-generat de minori;
- Căutarea a sesiunilor de *live-streaming* de abuzuri sexuale asupra copiilor.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 8 - SPRIJIN SPECIALIZAT PENTRU COPII ȘI TINERI VICTIME ALE ABUZULUI SEXUAL ONLINE

Auto-producere de conținut

Accesul crescând a copiilor și a tinerilor, la vârste tot mai fragede, la smartphone-uri și alte dispozitive, împreună cu percepția redusă a riscului cu privire la partajarea de conținut intim, au legătură cu apariția unor situații de auto-producere de conținut intim.

Trebuie să se facă o distincție între **conținutul intim care este (auto) produs voluntar** de către copil sau tânăr și **conținutul intim (auto) produs sub constrângere sau șantajare de către o altă persoană**:

- Referitor la prima categorie, există un număr din ce în ce mai mare de copii și tineri care publică fotografii sau înregistrările video, prin intermediul rețelelor sociale sau al platformelor de *chat*, cu alți colegi și prieteni, și prin urmare, devin mai vulnerabili la situațiile de abuz și exploatare sexuală *online*, cum ar fi ademenirea *online* (*grooming online*) săvârșită de persoane adulte care pretind a fi colegi.
- La acest nivel, putem menționa, ca exemplu, *sextingul*, ca formă de auto-producere a conținutului - text, imagini și / sau înregistrările video - de natură sexuală și partajarea acestui conținut, de obicei în mod consensual și între colegi.
- Deși această producere și partajare este voluntară, poate duce la situații ulterioare de șantajare, ademenire și alte forme de abuz sexual *online*.
- La fel, conținutul auto-produs poate fi, în primă instanță, distribuit colegilor, dar în cele din urmă poate ajunge pe rețelele de abuz sexual *online*. Astfel de cazuri pot ulterior expune copiii și tinerii la situații de constrângere sau șantajare de către terți care, prin amenințare și / sau șantaj, încearcă să constrângă copiii la (auto) producerea conținutului sexual suplimentar.

Transmiterea în direct ale Abuzurilor sexuale asupra copiilor

Odată cu îmbunătățirea infrastructurilor și viteza conexiunii la internet, s-a înregistrat o creștere a cererii de **sesiuni de live-streaming de abuz sexual asupra copiilor**: vizionarea conținutului de abuz sexual asupra copiilor în direct.

Aceste situații sunt frecvente în țările care sunt deja cunoscute ca locuri de destinație a turismului sexual pentru abuzul minorilor. Aceste transmisii de *streaming* sunt plătite și sunt adesea promovate pe website-uri pornografice pentru adulți. Odată ce se află de existența acestui serviciu / transmisie de *streaming*, utilizatorii sunt direcționați către platforme criptate care permit conferințe video. Adesea, atacatorilor care beneficiază de aceste servicii / transmisii de *streaming* li se oferă posibilitatea de a oferi instrucțiuni cu privire la modul în care doresc să se practice abuzuri sexuale asupra copiilor, în timp real. Utilizatorii care caută acest tip de conținut pot, de asemenea, să se deplaseze în țări în care au loc sesiuni de *live streaming* pentru practicarea abuzului sexual, de data aceasta față în față.

Ademenire [*grooming online*]

Grooming-ul online poate fi definit ca un **proces de manipulare** și o **formă de ademenire** a copiilor și a tinerilor. De obicei, începe cu o abordare non-sexuală, respectiv prin intermediul internetului și al TIC, care includ jocurile *online* și rețele sociale, în scopul de a stabili o relație de încredere cu copilul și pentru a-l convinge să se întâlnească față în față cu cineva, astfel încât copilul să fie abuzat sexual. Stabilirea unei relații de încredere cu copilul, mediată de internet și de TIC, poate viza, de asemenea, **convingerea copilului în ceea ce privește producerea și partajarea conținutului sexual**.

Grooming-ul *online* permite autorilor să selecteze tipul de victimă pe care doresc să o manipuleze și să o ademenească și au opțiunea de a alege în mod specific vârsta și / sau aspectul fizic al victimei. În plus, grooming-ul *online* permite ademenirea în simultan a unui număr mare de victime, printre alte avantaje pentru autorul procesului de manipulare și ademenire *online*, cum ar fi posibilitatea „dispariției”, prin schimbarea identității sale, în cazul în care victima refuză sau ignoră avansurile, reapărând cu o altă identitate, pentru a aborda aceeași victimă, de data aceasta, știind mai multe despre limitele și preferințele sale.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 8 - SPRIJIN SPECIALIZAT PENTRU COPII ȘI TINERI VICTIME ALE ABUZULUI SEXUAL ONLINE

Ademenirea pe rețelele sociale și pe jocurile video online

Abordarea mijloacelor de ademenire a copiilor și a tinerilor *online* începe cu prezentarea informațiilor despre utilizarea sporită a platformelor de jocuri online (A se vedea *PowerPoint*).

Agresorii profită de anonimatul oferit de platformele de jocuri video *online* și de conștientizarea redusă în rândul copiilor și a tinerilor (utilizatorii acestor platforme) cu privire la riscurile *online* pentru comiterea proceselor de ademenire și manipulare.

În acest scop, agresorii folosesc platforme de jocuri *online* pentru a dobândi încrederea acestor copii și tineri și, ulterior, pentru a convinge victimele să folosească alte platforme de comunicare *online* - Facebook® Messenger, Instagram®, WhatsApp®, Viber®, Telegram®, Snapchat®, etc. - să mențină comunicarea și relația cu acești copii și tineri și, în acest fel, să-i ademenească în scopuri sexuale.

Apariția cazurilor de ademenire *online* în acest context a motivat platformele de jocuri *online* să creeze măsuri de prevenire a ademenirii *online*, inclusiv prin crearea de politici de securitate și ghiduri specifice pentru copii și familii.

Strategii de prevenire

Pentru a **preveni situațiile de abuz sexual online**, în acest punct al Modulului, formatorul ar trebui să transmită cursanților următoarele strategii pe care aceștia, în calitate de Specialiști în Sprijinirea Victimelor, le pot folosi în intervenția cu copilul / tânărul care este victimă și cu familia sa:

- Creșterea gradului de conștientizare a importanței educației copilului sau tânărului pentru utilizarea sigură și conștientă a internetului și a TIC și identificarea situațiilor și contextelor de risc *online*;
- Creșterea gradului de conștientizare a definiției unor reguli clare pentru utilizarea internetului și a TIC: de exemplu, plasarea jocurilor video / calculatoarelor într-un spațiu comun a casei și / sau permiterea utilizării dispozitivelor mobile / electronice numai în zonele comune ale casei;
- Accentuarea importanței monitorizării sau supravegherii comportamentului *online* al copilului sau tânărului aflat în întreținere: și anume, dacă primește apeluri de la numere necunoscute, dacă petrece mult timp *online* și până foarte târziu, o izolare bruscă de familie și prieteni, precum și tipul de cereri de prietenie primite și originea acestora;
- Configurarea, împreună cu copiii și tinerii în întreținere, a setărilor de confidențialitate ale rețelelor sociale și ale paginilor / profilurilor, eliminând informațiile personale sau de altă natură care pot identifica adresa de domiciliu, școala, numărul de telefon mobil etc;

Familia joacă un rol foarte important în ceea ce privește protecția copiilor și a tinerilor împotriva riscurile utilizării internetului și a TIC. Puteți găsi informații despre importanța familiei în prevenirea criminalității informatice împotriva copiilor și tinerilor în capitolul 4 - Partea II a *Manualului ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*. De asemenea, este importantă implicarea familiei în sprijinul și intervenția cu copiii și tinerii care sunt victime ale criminalității informatice, inclusiv în educația copilului sau tânărului victimă pentru utilizarea conștientă și sigură a internetului și a TIC. A se vedea Capitolul 2 - Partea II a *Manualului ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*.

Strategii de intervenție

Strategii pentru păstrarea dovezilor digitale

De asemenea, în acest Modul, pe lângă abordarea dinamicilor și a *modi operandi* a diferitelor forme de abuz sexual asupra copiilor și tinerilor *online* și prezentarea măsurilor de prevenire a victimizării mai sus menționate, formatorul ar trebui să prezinte cursanților strategiile care pot fi explicate copilului și tânărului victimă (și familiilor acestora) în procesul de sprijinire, pentru păstrarea probelor. Să analizăm unele dintre aceste strategii:

- Încetarea la orice formă de comunicare cu agresorul;
- Să nu blocheze sau să dezactiveze rețeaua socială / platforma de comunicare pe care agresorul a folosit-o

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 8 - SPRIJIN SPECIALIZAT PENTRU COPII ȘI TINERI VICTIME ALE ABUZULUI SEXUAL ONLINE

pentru a comunica cu victima; această indicație este mai importantă pentru platformele de comunicare care folosesc criptarea de la capăt la capăt⁴⁷ - cum ar fi WhatsApp® sau Viber®, printre altele -, ceea ce înseamnă că nu este posibil accesarea la copiii conversațiilor, odată ce au fost șterse de utilizatori;

- Să păstreze toată evidența a comunicării cu agresorul (de exemplu, luând capturi de ecran), inclusiv imaginile și / sau înregistrările video trimise și primite;
- Să salveze toate informațiile care permit identificarea agresorului, cum ar fi: numele de utilizator, adresa URL a profilului rețelei sociale (a se vedea strategiile de intervenție propuse în Modulul 10), ID Skype®, detaliile transferului bancar (dacă s-a cerut o sumă în numerar);
- Să nu cedeze cerințelor / șantajul agresorului;
- Depunerea unei plângeri penale la autoritățile competente;
- Să solicite sprijin din partea structurilor de sprijinire a victimelor pentru a face față suferinței emoționale cauzate de situația de victimizare și pentru a asigura monitorizarea pe întregul parcurs a procedurii penale.

Cui și cum să raportați

În ceea ce privește **vizualizarea conținutului de abuz sexual asupra copiilor online**, oricine se confruntă cu acest tip de conținut / material, ar trebui să raporteze autorităților naționale sau autorităților competente din țara lor (Poliției sau Parchetului) și / sau platformelor concepute pentru a denunța conținutul ilegal *online*, așa cum este cazul entităților / *hotlines* care aparțin la INHOPE⁴⁸ - în cazul României este vorba de esc_ABUZ al organizației Salvați Copiii⁴⁹. Aceste entități nu numai că transmit cazurile raportate autorităților naționale competente pentru investigații ulterioare, dar și dispun de unele instrumente care permit eliminarea rapidă a acestui conținut și păstrarea a dovezilor.

Suspiciunile privind **ademenirea copiilor sau constrângerea sexuală online** ar trebui raportate autorităților sau structurilor de sprijinire a victimelor specializate. De asemenea, este extrem de important raportarea acestor cazuri, de îndată ce se ia la cunoștință astfel de cazuri, având în vedere, ca de obicei, pot exista și alți copii / tineri aflați în pericol care să fie obiect unor situații de abuz și exploatare sexuală de către același agresor.

Toate aceste acțiuni constituie infracțiuni sexuale comise împotriva minorilor și trebuie raportate la Poliție sau Parchet.

Strategii pentru a depăși victimizarea și impactul acesteia

În Capitolul 2 menționat mai sus - Partea II a *Manualului ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*, sunt detaliate câteva particularități aferente intervenției cu copii și tinerii care sunt victimele criminalității informatice, și anume:

- Îndeplinirea caracteristicilor și **stadiilor de dezvoltare** ale copilului sau tânărului;
- Luarea în considerare, ori de câte ori este posibil, **implicarea familiei**;
- Concentrarea asupra **educației** pentru utilizarea sigură și conștientă a TIC și a internetului, ca un comportament de **protecție împotriva revictimizării**.

Prin urmare, formatorul ar trebui să distribuie cursanților tabelele în anexă. *Etapele-cheie în procesul de dezvoltare a copilului / tânărului și Abordarea și comunicarea cu copiii și tinerii de diferite grupe de vârstă* (A se vedea Planul Sesiunii).

Acest Modul va aborda cu precizie acele particularități care ar trebui să ghideze intervenția oricărui Specialist în Sprijinirea Victimei, și să exploreze **achiziții (achizițiile de dezvoltare) așteptate pentru fiecare grupă de vârstă** a copilului/tânărului și, în consecință, modul în care ar trebui să se desfășoare comunicarea și intervenția cu copilul / tânărul victimă. De asemenea, abordează efectele cibervictimizării copiilor / tinerilor asupra familiei.

⁴⁷ Este un mecanism de siguranță care protejează datele în timpul unui schimb de mesaje, astfel încât conținutul să poată fi accesat doar de ambele părți ale comunicării, adică de către expeditor și destinatar.

⁴⁸ INHOPE este o rețea internațională care agregă mai multe entități / hotlines care, în diferite țări, efectuează servicii de raportare a conținutului ilegal online. A se vedea <https://www.inhope.org/EN>.

⁴⁹ Informații la <https://oradenet.ro/esc-abuz>.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 8 - SPRIJIN SPECIALIZAT PENTRU COPII ȘI TINERI VICTIME ALE ABUZULUI SEXUAL ONLINE

În plus, ia în considerare, de asemenea, **impactul și consecințele experienței de cibervictimizare** sexuală asupra copilului sau tânărului, în conformitate cu capitolul 4 - Partea I *Manualului ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor* și Modulul 3 al acestui Curs de Formare. De asemenea, ia în considerare sinteza consecințelor experienței de cibervictimizare sexuală prezentată în tabelul următor:

Consecințe asupra sănătății emoționale și psihologice

- Șoc, mai ales atunci când violența sexuală este săvârșită de cineva pe care copilul / tânărul îl cunoaște sau are încredere;
- Furie în raport cu autorul infracțiunii și în raport cu ea însăși, pentru că nu a putut evita situația de victimizare;
- Vinovăție și rușine;
- Anxietate, inclusiv gânduri și amintiri frecvente despre cele întâmplate;
- Diferite temeri, inclusiv că situația de violență se va repeta, de a fi singur, de faptul că nimeni nu crede în relatarea sa, de consecințele pentru autorul infracțiunii (mai ales dacă victima îl cunoaște);
- Scăderea stimei de sine (nu se mai place);
- Tristețe profundă.

Consecințe asupra sănătății fizice

- Leziuni și răni legate de violența sau forța fizică folosită;
- Leziuni și răni legate direct de violența sexuală, cum ar fi leziuni ale organelor sexuale, durere, sângerare, scurgere;
- Probleme legate de sănătatea sexuală și reproductivă, cum ar fi infecțiile cu transmitere sexuală;
- Sarcini nedorite;
- Scăderea apetitului;
- Insomnie și coșmaruri în timpul nopții (asociate cu gânduri constante despre ceea ce s-a întâmplat) sau somn în exces.

Modificări ale comportamentului

- Mai multă agresivitate față de alți oameni și de sine (inclusiv auto-mutilarea);
- Comportamente regresive (de exemplu, dormit cu lumina aprinsă, pipi în pat iarăși);
- Izolarea socială față de colegi, prieteni și familie;
- Interesul scăzut față de școală și scăderea performanței școlare;
- Lipsa de interes față de activitățile apreciate anterior;
- Modificări ale comportamentului sexual.

Astfel, fără a aduce atingere liniilor directe fundamentale pentru intervenție abordate în Modulul 4 al acestui Curs de Formare, sunt considerate deosebit de importante, în cazul sprijinul copiilor / tinerilor victime ale abuzurilor sexuale *online* și familiilor acestora (sau tutori legali sau alți furnizori de asistență) care monitorizează copilul / tânărul), **strategiile de sprijin** prezentate mai jos:

- Informați, într-un mod simplu, succint și clar, și transmiteți informațiilor esențiale tutorei legal, furnizorului de asistență sau altei persoane adulte sau tânărului însuși, în cazul în care vine singur, cu privire la:
 - **Obligația de a sesiza autoritățile competente:** Conform art. 267, CP (Omisiunea sesizării), există obligația funcționarului public de a raporta infracțiuni către autoritățile judiciare. („Funcționarul public care, luând cunoștință de săvârșirea unei fapte prevăzute de legea penală în legătură cu serviciul în cadrul căruia își îndeplinește sarcinile, omite sesizarea de îndată a organelor de urmărire penală se pedepsește cu închisoare de la 3 luni la 3 ani sau cu amendă.”)
- Contactul rapid cu poliția sau autoritățile judiciare permite investigarea să se desfășoare mai rapid, victima să fie audiată într-o perioadă mai scurtă de timp și să se păstreze dovezile fizice și / sau mărturiile acesteia.
- Importanța examinării copilului sau a tânărului într-un consult medical, în special în cazul unor situații de abuz sexual *online* care au ca rezultat victimizarea sexuală a copilului sau a tânărului în contextul față în față (*offline*) (a se vedea tabelul de mai sus și consecințele asupra sănătății fizice).
- Copilul sau tânărul ar trebui, de asemenea, să fie informat că specialistul / tutorele legal / furnizorul de asistență va trebui să contacteze alte entități (și anume autoritățile de poliție sau judiciare), pentru a-l ajuta mai bine.
- Explicați copilului / tânărului victimă și familiei / tutorele legal pașii ulterioarii plângerii și funcționarea procedurii penale.
- Oferiți sprijin pe tot parcursul procesului, inclusiv psihologic, atât copilului / tânărului victimă, cât și membrilor familiei / tutorilor legali / furnizorilor de asistență.
- Accentuați strategiile de prevenire abordate anterior.

În plus față de considerentele și strategiile centrale de mai sus, atunci când interacționează / comunică cu copilul sau tânărul victimă de abuz sexual *online*, specialistul în sprijinirea victimelor ar trebui să consolideze aspectele

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 8 – SPRIJIN SPECIALIZAT PENTRU COPII ȘI TINERI VICTIME ALE ABUZULUI SEXUAL *ONLINE*

și strategiile deja acoperite în Modulele anterioare ale Cursului. A se vedea, de asemenea, capitolul 2 - Partea II a *Manualului ROAR - Partea II a Manualului ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*.

În cazul copiilor și tinerilor, dintre toate strategiile, subliniem importanța de a transmite, în cel mai clar mod posibil, că:

- Nimic din ceea ce se întâmplă nu este vina victimei;
- Nimic din ceea ce victima ar fi spus sau făcut nu justifică faptul că a fost forțată, înșelată sau convinsă să se implice sexual cu o altă persoană;
- Nimeni nu are dreptul să oblige victima să întrețină relații sexuale împotriva voinței sale (nici măcar cei apropiați nu au acest drept);
- Autorul infracțiunii este singurul responsabil pentru ceea ce i s-a întâmplat.

De asemenea, atunci când interacționează / comunică cu membrii familiei / tutorii legali / furnizorii de asistență, specialistul în sprijinirea victimei ar trebui să:

- Sublinieze faptul că divulgarea cibervictimizării de către copil / tânăr trebuie încurajată, creditată și validată de persoane semnificative / adulți de încredere;
- Accentueze, împreună cu membrii familiei / tutorii legali / furnizorii de asistență, că este esențial ca aceștia să rămână disponibili pentru a sprijini copilul / tânărul victimă și să-l asculte, fără să aibă loc acțiuni de hiperprotecție sau presiune cu scopul ca victima să împărtășească gândurile / emoțiile și / sau amintirile cu privire la întâmplarea de cibervictimizare;
- Să crească gradul de conștientizare privind necesitatea de a nu împărtăși cu copilul / tânărul victimă promisiuni nerealiste sau rezultate magice, având în vedere ceea ce se poate întâmpla, atât în procesul de recuperare psihologică și emoțională, cât și în procedura penală.

În cazul specialiștilor care au monitorizat copilul / tânărul victimă, specialistul ar trebui:

- Să informeze cu privire la necesitatea de a respecta procedurile interne stabilite, asigurarea confidențialității copilului / tânărului și să se limiteze la aspectele esențiale în schimbul de informații intra și interinstituționale referitoare la situația de victimizare.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 8 - SPRIJIN SPECIALIZAT PENTRU COPII ȘI TINERI VICTIME ALE ABUZULUI SEXUAL ONLINE

PLANUL SESIUNII Nr. 8

1. Identificarea acțiunii

Denumire Curs de Formare Sprijin Specializat pentru Victimele Criminalității Informaticе

Module / teme Sprijin Specializat copiilor și tinerilor victime ale abuzurilor sexuale online

Data sesiunii **Orar** **Durata sesiunii** 40 de minute

Formatori

2. Obiective specifice

La sfârșitul sesiunii, cursanții ar trebui să poată:

- Distinge corect natura și *modi operandi* ale diferitelor forme ale abuzurilor sexuale asupra copiilor care sunt abordate online, și anume diseminarea conținutului al abuzului sexual asupra copiilor și *grooming online*;
- Enumere corect strategiile de intervenție propuse în sprijinul specializat pentru copii și tineri care sunt victime ale abuzurilor sexuale online;
- Recunoaște corect strategiile de prevenire a victimizării propuse pentru intervenție cu copiii și tinerii care sunt victime ale abuzurilor sexuale online.

3. Structura sesiunii

	Conținutul programului	Metodologie	Resurse pedagogice / didactice	Evaluare Exerciții	Temp (minute)
Introducere	• Tipuri de abuz sexual asupra copiilor online: • Diseminarea conținutului de abuz sexual asupra copiilor: conținut cu abuz sexual asupra copiilor generat online; auto-producere de conținut; transmiterea în direct a abuzurilor sexuale asupra copiilor • Ademenire (<i>grooming online</i>): Ademenire pe rețelele sociale și jocurile video online	Expozitivă și activă	Computer: <i>Datashow</i> și ecran de proiecție	Observare	10
	<i>Modi operandi</i> și natura infracțiunilor	Expozitivă și activă	Computer: <i>Datashow</i> și ecran de proiecție	Observare	5
Dezvoltare	Strategii de prevenire	Expozitivă și activă	Computer: <i>Datashow</i> și ecran de proiecție	Observare	5
	Strategii de intervenție: • Strategii pentru păstrarea dovezilor digitale • Cui și cum să raportați / denunțați • Strategii pentru a depăși victimizarea și impactul acesteia	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție; Tabelele - Anexă ⁵⁰	Observare	15
Concluzie	Rezumat concludent și clarificarea nelămuririlor	Expozitivă și activă	Computer: <i>Datashow</i> și ecran de proiecție	Observare	5

OBSERVAȚII

Destinatari:

Specialiști în sprijinirea victimelor

Data: / /

Formator:

⁵⁰ Tabelele - Anexă Etapele cheie în procesul de dezvoltare a copilului / tânărului și Abordarea și comunicarea cu copiii și tinerii de diferite grupe de vârstă, din Manual ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor, disponibile în paginile următoare.

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 8 – SPRIJIN SPECIALIZAT PENTRU COPII ȘI TINERI VICTIME ALE ABUZULUI SEXUAL *ONLINE*

INSTRUCȚIUNI ESENȚIALE ȘI INFORMAȚII PENTRU FORMATOR

CONCORDANȚA CU CONȚINUTUL

Planul Sesiunii *Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*

	PARTE	CAPITOL
Tipuri de abuz sexual asupra copiilor online	Partea I - Înțelegere	Capitolul 1 - 1.3.
	A se vedea Prezentarea și Cadrul Modulului	
Modi operandi și natura infracțiunilor	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii de prevenire	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii de intervenție		
Strategii pentru păstrarea dovezilor digitale	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Cui și cum să raportați / denunțați	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii pentru a depăși victimizarea și impactul acesteia	Partea II - Continuați	Capitolul 2 - 2.1. și 2.4.
	A se vedea Prezentarea și Cadrul Modulului	
Rezumat concludent și clarificarea nelămuririlor	Nu corespund	

PARTEA 2 - ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 8 - SPRIJIN SPECIALIZAT PENTRU COPII ȘI TINERI VICTIME ALE ABUZULUI SEXUAL ONLINE

Tabel - Anexă: Etapele cheie în procesul de dezvoltare a copilului / tânărului

	dezvoltarea fizică	dezvoltarea emoțională și cognitivă [inclusiv limbajul]	dezvoltarea socială și morală
3-6 ani	- Poate desena și realiza alte lucrări manuale - Poate scrie propriul său nume - Corpul se dezvoltă, asumându-și formele corpului adult - Dexteritatea și capacitatea de coordonare cresc	- Își amintește de experiențele de familie - Are un anumit vocabular - Poate adapta vorbirea în funcție de caracteristicile interlocutorului (cum ar fi vârsta, sexul și statutul social)	- Poate interpreta, prezice și influența reacțiile altor persoane - Stabilește primele prietenii - Apar emoțiile conștiente de sine (cum ar fi rușinea și vinovăția) - Are un control relativ asupra emoțiilor sale
6-12 ani	- Crește progresiv în greutate și înălțime - Scrierea de mână devine mai mică și mai lizibilă - Desenele sunt mai structurate - Sunt frecvente jocurile și glumele care implică alergare, confuzie și competiție - Se dezvoltă capacitatea de reacție rapidă în termeni de dexteritate motorie - Se pot observa indicatori pubescenti, în special în cazul fetelor	- Gândurile și atenția sunt mai concentrate - Raționament inductiv - Poate stabili relația dintre experiențe și evenimente specifice - Îmbunătățirea vocabularului	- Devine mai independent și mai responsabil - Distinge între a avea succes și a nu avea succes - Este conștient de eforturile sale vs întâmplare / noroc în obținerea unui rezultat dat - Se poate pune în locul celui alt (empatie)
12-18 ani	- Pubertate - Menstruație și creșterea țesutului adipos în cazul fetelor - Vocea devine mai gravă și există o creștere a masei musculare în cazul băieților - Un interes sporit privind sexualitatea	- Poate discuta eficient - Este mai conștient de sine și mai concentrat - Dezvoltarea raționamentului ipotetic-deductiv - Este capabil de ajustări subtile în vorbire - Poate planifica și lua decizii	- Creșterea conflictelor cu părinții / familia - Apropierea de grupul de colegi și apariția situațiilor de presiune a colegilor - Căutarea a propriei identități - Dezvoltarea relațiilor intime

Tabel - Anexă: Abordarea și comunicarea cu copiii și tinerii de diferite grupe de vârstă

	1-6 ani	6-12 ani	12-18 ani
Prezentare	Se adresează, în special, copilului. Este încă prea mic pentru a putea înțelege informațiile furnizate.	Copilul arată un interes sporit față de informațiile furnizate și o capacitate mai mare de a le înțelege.	Înțelege informațiile furnizate, dar poate fi reticent cu privire la participarea a unui program de intervenție sau la un proces de sprijin a victimelor.
Descriere a evenimentului	Se exprimă în mod preferențial prin desene sau jocuri, neglijând expresia verbală.	Prezintă mai multe detalii decât copiii mai mici. Copiii mai mari preferă să se exprime verbal, refuzând uneori utilizarea desenelor și jocurilor.	Descrierea evenimentului este detaliată. Pot fi observate sentimente de auto-culpabilitate.
Psiho-educație	Se adresează în special familiei / părinților. Cu toate acestea, copilul va asimila informații simple, cum ar fi recunoașterea situației, astfel încât să poată simula o modalitate de a face față acesteia.	Se adresează copilului, și integrează familia / părinții în procesul de psihoeducare.	Adresat / prin copil.

MOD. 9

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 9 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE CYBERBULLYING-ULUI

PREZENTAREA ȘI CADRUL MODULULUI

Acest Modul vizează înțelegerea fenomenului de *cyberbullying*, precum și intervenția cu victimele respective, în vederea depășirii impactului cibervictimizării și prevenirea victimizării.

Pe lângă lectura conținutului acestui Modul, propunem, de asemenea formatorului consultarea *Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor* așa cum am propus și pentru celelalte module ale acestui Curs.

Modi operandi și natura infracțiunii

Cyberbullying reprezintă o extindere a bullying-ului, a hărțuirii și intimidării. Dacă bullyingul implică agresiune „față în față”, în cea ce privește *cyberbullyingul* agresiunea și vătămarea se desfășoară *online*, prin internet și TIC.

Cyberbullyingul se manifestă prin schimbul de texte agresive sau umilitoare, fotografii și / sau înregistrările video către o altă persoană, punând în joc identitatea persoanei și afectându-i stima de sine. Faptul că *cyberbullyingul* se practică prin intermediul internetului - pe rețelele sociale și / sau prin aplicații de mesagerie precum WhatsApp® - permite agresorului să nu trebuiască să se confrunte direct cu victima, simțindu-se mai puțin inhibat atunci când atacă, cu mai puțină teamă de a fi pedepsit și, prin urmare, mai puternic.

Cyber-bullying-ul poate fi practicat:

- unu la unu (numai între victimă și agresor);
- unul la mai mulți (de exemplu, un atacator postează ceva *online* care mulți oameni pot vizualiza);
- de la mulți la mulți (când mulți agresori postează ceva ce mulți oameni vor putea vizualiza).

Cyberbullyingul permite ca agresorii să acționeze anonim, folosind adesea identități false (care le permit să se disocieze de moralitatea acțiunilor lor) și scheme de gândire care justifică comportamentul lor, cum ar fi:

- Ascunderea sau reducerea la minim a propriului rol, „deplasând” sau diluând responsabilitatea;
- Distorsionarea sau devalorizarea impactului comportamentului;
- Învinuirea și dezumanizarea victimei.

Formele obișnuite de violență privind *cyberbullyingul* sunt:

- *Flaming* - discuții *online*, folosind e-mailuri care conțin limbaj vulgar și furios;
- *Harasement* - trimiterea în mod repetat de mesaje inadecvate, ostile și jignitoare;
- *Impersonation* - asumându-și identitatea altcuiva și trimiterea / publicarea materialului sau a conținutului care urmărește să afecteze reputația sau prietenii;
- *Outing* – Punerea la dispoziție informațiilor personale, jenante sau imagini, ale altei persoane *online*, fără consimțământul acesteia;
- *Trickery* - a face pe cineva să dezvăluie informații personale / confidențiale sau jenante și apoi să le distribuie *online*;
- *Exclusion* – excluderea a unei persoane, într-un mod intenționat și crud, dintr-un grup *online*;
- *Cyberstalking* - hărțuirea repetată și intensă, care include amenințări sau generează frică semnificativă;
- *Happy slapping* - agresiuni “face to face” care sunt comise de o persoană (sau de mai multe) împotriva victimei, agresiunea fizică fiind înregistrată de terți care ulterior diseminează episodul pe rețelele sociale.

Există, de asemenea, practici de *cyberbullying* cu o componentă sexuală, cu scopul de a ataca demnitatea victimei și sfera vieții private, cum ar fi:

- Distribuirea *online* a zvonurilor sau minciunilor privind comportamentul sexual al victimei;
- Utilizarea unui limbaj sexual ofensator sau discriminatoriu *online* împotriva victimei;
- Furtul identității a victimei și distribuirea ulterioară a conținutului sexual care implică victima sau hărțuirea sexuală a altor persoane;

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 9 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE CYBERBULLYING-ULUI

- Recurgerea la amenințări și intimidare din cauza identității de gen sau a orientării sexuale a victimei;
- Practica *body shaming-ului* – adăugare de comentarii disprețuitoare cu privire la aspectul fizic al victimei

Strategii de prevenire

Pentru a **preveni situațiile de cyberbullying**, în acest punct al Modulului, formatorul ar trebui să transmită cursanților următoarele strategii pe care aceștia, în calitate de specialiști în sprijinirea victimelor, le pot folosi în intervenția cu victima:

- Încetarea la orice formă de comunicare cu agresorul;
- Nu blocați sau să dezactivați rețeaua socială / platforma de comunicare pe care agresorul a folosit-o pentru a comunica cu victima; deoarece platformele WhatsApp® sau Viber® folosesc criptarea de la capăt la cap (a se vedea Modulul 8);
- Nu furnizați informații personale sau date personale solicitate prin e-mail, mesaje, apeluri, *website*-uri nesolicitate;
- Configurați setările de confidențialitate ale rețelelor sociale și ale paginilor / profilurilor, eliminând informațiile personale sau de altă natură care pot identifica adresa de domiciliu, școala, numărul de telefon mobil etc.;
- Activarea filtrelor de *spam* și de hărțuire;
- Înregistrați contactele importante pe telefonul dvs. mobil, astfel încât să puteți cere ajutor cu ușurință în caz că aveți nevoie;
- De asemenea, puteți înregistra contactele a resurselor de sprijin și a serviciilor comunitare, care pot fi importante în depășirea / recuperarea situației de victimizare;
- Căutați drumuri alternative către locurile care le frecvențați de obicei;
- Împărtășiți persoanele de încredere situația și rutina obișnuită;
- Încearcă-ți să fiți în compania oamenilor în care aveți încredere și evitați să mergeți singur;
- În cazul în care vă confrunțați față în față cu agresorul *online*, ar trebui să reacționați fără violență și cu seninătate, căutând ajutor cât mai curând posibil sau persoanelor apropiate;
- În situații de pericol, ar trebui să căutați un loc sigur sau unde se află mai multe persoane. Pot fi, de asemenea, activate contacte de urgență.

Strategii de intervenție

Strategii pentru păstrarea dovezilor digitale

În contextul acestui Modul, pe lângă abordarea dinamicilor și a *modi operandi* în situații de *cyberbullying* și prezentarea măsurilor de prevenire a revictimizării mai sus menționată, formatorul ar trebui să prezinte cursanților strategiile care pot fi explicate victimei în procesul de sprijinire, pentru păstrarea probelor. Să analizăm unele dintre aceste strategii:

- După ce comunicarea cu agresorul a încetat, rețeaua socială / platforma de comunicare pe care agresorul a folosit-o pentru a comunica cu victima nu ar trebui blocată sau dezactivată;
- Păstrați toată evidența a comunicării cu agresorul (de exemplu, luând capturi de ecran), inclusiv imaginile și / sau înregistrările video trimise și primite;
- Salvați toate informațiile care permit identificarea agresorului, cum ar fi: numele de utilizator, adresa URL a profilului rețelei sociale (a se vedea strategiile de intervenție în Modulul 10), ID-ul Skype® etc. ;
- Depunerea unei plângeri penale la autoritățile competente;
- Solicitați sprijin din partea structurilor de sprijinire a victimelor pentru a face față suferinței emoționale cauzate de situația de victimizare și pentru a asigura monitorizarea pe tot parcursul procedurii penale.

Cui și cum să raportați / denunțați

Cyberbullying-ul, în funcție de natura faptelor comise, poate fi încadrat ca infracțiunea de hărțuire (Art. 208, CP), amenințare (Art. 206, CP), șantaj (Art. 207, CP), violarea vieții private (Art. 226, CP) sau altele.

În cazul minorilor sub 14 ani, legea română (Art. 113, Cod Penal) aplică o prezumție absolută de lipsă de discernământ,

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 9 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE CYBERBULLYING-ULUI

ceea ce înseamnă că măsuri educative pot fi aplicate pentru minorii sub 14 ani care comit infracțiuni. Pentru minorii cu vârste între 14 și 16 ani există o prezumție relativă a lipsei de discernământ, ce poate fi răsturnată prin probe în sensul prezenței discernământului la respectiva persoană, și, peste minorii peste 16 ani, o prezumție relativă a discernământului. Pe lângă sancțiunile penale sau măsurile educative dispuse de instanță, există și posibilitatea aplicării măsurilor disciplinare de către școlile care au cunoștință de situații de *cyberbullying*.

În orice caz, situațiile de *cyberbullying* trebuie raportate entităților competente pentru a le sancționa, și anume:

- Școala (dirigintele clasei, directorul școlii, și, dacă intervenția acestor agenții eșuează, raportați situația la Inspectoratele Școlare Județene/ ale Mun. București);
- Organele de Poliție pentru situații care constituie infracțiuni și aduc un pericol siguranței persoanei/ copilului;
- la Telefonul Copilului: 116111
- la HELPLINE cu număr unic la nivel național destinat victimelor violenței domestice: 0800500333.

Strategii pentru a depăși victimizarea și impactul acesteia

În urma aspectelor cheie privind intervenția cu victimele criminalității informatice abordate în Modulul 4 și **strategiile de prevenire și intervenție** deja subliniate, specialistul în sprijinirea victimelor trebuie să ofere victimei un set de orientări practice, ținând cont și de asistența deja explorată în Modulul 8 (în ceea ce privește, în mod specific, **comunicarea cu copii / tineri** de diferite grupe de vârstă).

Specialistul ar trebui să ia în considerare, totodată **impactul experienței de cibervictimizare** și consecințele resimțite de victimă în structurarea asistenței și sprijinului acordat victimei de *cyberbullying*. A se vedea modulul 3 al acestui Curs de Formare, precum și capitolul 4 - Partea I a *Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*.

Pe lângă reacțiile și consecințele abordate în acele resurse, în cazul specific al *bullying*-ului împotriva copiilor și tinerilor, fie că este vorba de *cyberbullying* sau *bullying* convențional, există și alte consecințe care trebuie evidențiate și care pot fi resimțite de victimele ținte ale intervenției:

- Să-le fie frică să meargă la școală și să facă totul pentru a nu merge (de exemplu, prefăcându-se bolnave);
- Scăderea performanței școlare;
- Îndepărtare / izolare față de prieteni și alte persoane cu care le plăcea să conviețuiască;
- Pierderea interesului pentru activitățile apreciate anterior;
- Simptome fizice și probleme de sănătate: dificultăți de adormire; coșmaruri frecvente; dureri de stomac, greață sau amețeli (de exemplu, atunci când cred că trebuie să meargă la școală sau când intră în incinta școlii); dureri de cap; transpirație, bătăi rapide ale inimii (de exemplu, atunci când cred că trebuie să meargă la școală sau când intră în incinta școlii).

În acest fel, formatorul poate stabili următoarele **strategii de sprijin**:

- Standardizarea reacțiilor prezentate;
- Furnizarea de informații cu privire la prevalența infracțiunilor în rândul persoanelor din grupul de vârstă al victimei, pentru a schimba ideea de „vulnerabilitate unică” și eventualele sentimente de singurătate și de neînțelegere care decurg din aceasta;
- Accentuarea faptului că victima nu este de vină pentru ceea ce i se întâmplă și că vina și responsabilitatea sunt exclusiv ale agresorului;
- Încurajarea implicării în activități apreciate anterior, și anume activități *offline*;
- Dacă este dorința victimei și cu acordul acesteia, specialistul poate implica membrii familiei și / sau prietenii în procesul de recuperare;
- Oferiți sprijin pe tot parcursul procesului, inclusiv psihologic;
- Consolidarea strategiilor de prevenire abordate anterior.

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 9 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE CYBERBULLYING-ULUI

PLANUL SESIUNII N° 9

1. Identificarea acțiunii

Denumire	Curs de Formare Sprijin Specializat pentru Victimele Criminalității Informaticе		
Module / teme	Sprijin specializat pentru victimele furtului de <i>cyberbullying</i>		
Data sesiunii	Orar	Durata sesiunii	40 de minute
Formatori			

2. Obiective specifice

La sfârșitul sesiunii, cursanții ar trebui să poată:

- Distinge corect natura și modi operandi al cyberbullying-ului;
- Enumere corect strategiile de intervenție propuse pentru sprijin specializat pentru victimele de cyberbullying;
- Recunoască corect strategiile de prevenire a revictimizării propuse în intervenția cu victimele de cyberbullying.

3. Structura sesiunii

	Conținutul programului	Metodologie	Resurse pedagogice / didactice	Evaluare Exerciții	Timp (minute)
Introducere	<i>Modi operandi</i> și natura infracțiunii	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
	Strategii de prevenire	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
Desenvoltamento	Strategii de intervenție: • Strategii pentru păstrarea dovezilor digitale • Cui și cum să raportați / denunțați • Strategii pentru a depăși victimizarea și impactul acesteia	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	15
	Exercițiul nr. 5	Activă	Regulile exercițiului nr.5	Observare	10
Conclusão	Rezumat concludent și clarificarea nelămuririlor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5

OBSERVAȚII

Destinatari:

Specialiști în sprijinirea victimelor

Data: / /

Formator:

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 9 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE CYBERBULLYING-ULUI

INSTRUCȚIUNI ESENȚIALE ȘI INFORMAȚII PENTRU FORMATOR

CONCORDANȚA CU CONȚINUTUL

Planul Sesiunii *Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*

	PARTE	CAPITOL
<i>Modi operandi</i> și natura infracțiunii	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii de prevenire	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii de intervenție		
Strategii pentru păstrarea dovezilor digitale	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Cui și cum să raportați / denunțați	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii pentru a depăși victimizarea și impactul acesteia	Partea II - Continuați	Capitolul 2 - 2.1.
	A se vedea Prezentarea și Cadrul Modulului	
Exercițiul nr. 5	Nu corespund	
	Vezi Regulile Exercițiului nr. 5	
Rezumat concludent și clarificare a nelămuririlor	Nu corespund	

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 9 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE CYBERBULLYING-ULUI

REGULILE EXERCITIULUI nr. 5

Modul / temă	Sprijin specializat pentru victimele cyberbullying-ului	COD REF.	DOMENIUL EDUCAȚIEI ȘI FORMĂRII
Obiective	Acest exercițiu are drept scop consolidarea informațiilor și a conținutului programului al acestui Modul, abordând natura situațiilor de cyberbullying, precum și strategiile de intervenție care ar trebui introduse de specialistul în sprijinirea victimelor de cyberbullying.		
Executare	Formatorul ar trebui să distribuie EXERCITIUL nr. 5, pentru lectură individuală a cursanților. După lectură, formatorul ar trebui să întrebe grupul despre formele de agresiune / violență prezente în Cazul respectiv. În timpul dezbaterii grupului, formatorul ar trebui să evidențieze sau să accentueze, în funcție de opiniile și schimbul de idei a cursanților, agresiunile identificabile în dinamica <i>cyberbullying</i>-ului prezente în Caz: excludere, schimb de zvonuri și agresiune verbală. În acest caz specific, este important ca formatorul să sublinieze, de asemenea, posibilitatea ca situația de <i>cyberbullying</i> să aibă loc în simultan cu <i>bullying-ul</i> convențional, în raport cu victima (Bogdan), deoarece victima și agresorul prezintă o relație strânsă (adică sunt colegi de clasă). Ar trebui luată în considerare în intervenția și în stabilirea strategiilor de prevenire a revictimizării, posibilitatea ca situațiile de agresiune online să fie însoțite de violență <i>offline</i> (adică "face to face") În urma reflecției de grup cu privire la dinamica <i>bullying</i>-ului și a <i>cyberbullying</i> prezente, formatorul ar trebui să solicite participarea a doi dintre cursanți, pentru simularea unei sesiuni de sprijin / asistență: • unul dintre cursanți trebuie să joace rolul lui Bogdan (victima în acest exercițiu), folosind textul Cazului pentru a explica, în cuvintele sale, situația de violență trăită; • celălalt cursant trebuie să joace rolul specialistul în sprijinirea victimei. În această simulare, este important ca formatorul să fie atent la cursantul care joacă rolul de specialist. Ar trebui să fie evidențiate strategiile de sprijin cuprinse în domeniul <i>Strategiilor de Intervenție pentru Prezentarea și Cadrul Modulului</i>. Ar trebui, de asemenea, să fie explorate <i>Strategiile de Prevenire</i> a revictimizării, abordate și în Prezentarea și Cadrul acestui Modul. De asemenea, formatorul ar putea promova participarea celorlalți cursanți, și în special cerând sugestii de strategii care ar putea fi luate în considerare și alte aspecte relevante în simularea sesiunii de sprijinire / asistență, și anume: • furnizarea de sprijin emoțional; • colectarea de informații; • evaluarea riscurilor și stabilirea măsurilor de securitate; • identificarea nevoilor de sprijin. Se vizează, în acest caz, integrarea obiectivelor acestui Modul cu conținutul programului deja acoperit în Modulul 4, respectiv aspectele centrale în sprijinul specializat victimelor de <i>cyberbullying</i>.		
Notițe	Consultați Prezentarea și Cadrul Modulului		

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 9 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE CYBERBULLYING-ULUI

EXERCITIUL nr. 5

Bogdan are 12 ani. Activitatea sa preferată, în ultimele 5 luni, a fost să joace un joc *online*. Acest joc se juca în grup și Bogdan făcea parte din grupul creat de Paul, cel mai bun prieten al său din copilărie. În acest grup, făceau parte și alți colegi de clasă, cu care Bogdan și Paul se jucau. În ultima perioadă, Paul a avut note foarte rele și părinții lui l-au comparat cu Bogdan, spunând: "Ar trebui să fii ca Bogdan. El este un student pe măsură!". Paul s-a supărat foarte tare și a devenit gelos pe Bogdan. Incapabil să facă față emoțiilor, le-a descărcat pe Bogdan: l-a exclus din grupul de joc și l-a insultat agresiv: „Nu ești bun de nimic! Nu știi să joci, doar ne faci pe noi toți să rămânem în urmă! Ești o piedică pentru noi! Du-te, și învață, tocilarule!”

În plus, Paul a răspândit pe chatul de grup zvonul că Bogdan a fost „să se plângă” părinților lui Paul, spunând că Paul lipsește la ore ca să se joace.

Colegii s-au alăturat lui Paul, deoarece le este întrucâtva teamă de el. Paul este cu doi ani mai mare decât ceilalți colegi și este mai înalt și mai puternic.

MOD. 10

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 10 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE ÎNŞELĂCIUNILOR ONLINE ÎN RELAȚIILE INTIME: CYBERSTALKING ȘI PORNOGRAFIA NON-CONSENSUALĂ

Una din trei persoane întreține relații *online*⁵¹. În acest context, una din zece persoane a raportat că a distribuit deja fotografii intime ale lor.

În plus, se estimează că 55% dintre persoanele care întrețin relații *online*, au fost deja victime unor tipuri de infracțiuni⁵².

Acest Modul prezintă în mod special două fenomene de cibervictimizare asociate cu riscurile prezenței *online* și a utilizării TIC și a internetului pentru stabilirea unor relații interpersonale mai intime: *cyberstalking*-ul și pornografia non-consensuală.

Tipuri, modi operandi și natura infracțiunii

Cyberstalking

Cyberstalking-ul poate fi definit ca utilizarea TIC cu scopul de a amenința sau de a hărțui victima. La fel ca *stalking*-ul, *cyberstalking*-ul este un tip de violență care se distinge prin caracterul său intruziv și repetitiv în sfera vieții private a victimei, și îi provoacă astfel frică și nesiguranță. În consecință, victimele se confruntă cu o stare continuă de anxietate care le afectează calitatea vieții, și le forțează, în cele din urmă, să-și schimbe activitățile zilnice.

Faptul că această persecuție are loc online permite agresorului să aibă la dispoziție mai multe mijloace pentru a menține activitatea infracțională, precum și pentru a ataca un număr mai mare de victime. Agresorii pot fi persoane pe care victima îi cunoaște, precum și persoane apropiate / intime, sau prieteni sau (foști) iubiți, dar și persoane pe care victima nu le cunoaște.

Cele mai comune forme de *cyber-stalking* sunt:

- Hărțuirea victimei;
- Furt de identitate;
- Amenințări;
- Contacte sexuale nedorite - de exemplu, trimiterea, fără consimțământ, de *dick pics* (se referă la imagini ale organelor genitale masculine trimise / primite prin dispozitive electronice) de către agresor ca o modalitate de a hărțui victima;
- Apeluri insistente din partea atacatorului nedorite de victimă.

Pornografia non-consensuală

În contextul relațiilor intime, poate avea loc partajarea *online* a mesajelor sexuale, înregistrările video sau imaginilor, practici denumite **sexting** (rezultă din combinația cuvintelor „sex” (sex) și „texting” (trimitere de mesaje) și care presupune schimbul de mesaje erotice, cu sau fără poze, prin telefonul mobil, *chat*-uri sau rețele sociale.

Practica *sextingului* de comun acord, în contextul unei relații intime, poate fi sănătoasă. Cu toate acestea, poate crește și vulnerabilitatea la a persoanelor implicate.

Pornografia non-consensuală prin imagini și înregistrările video poate fi definită ca diseminarea unei imagini intime, fără consimțământul persoanei care vede imaginea sa fiind distribuită, atunci când se aștepta ca această imagine să fie păstrată confidențială. O imagine intimă este aceea în care o persoană este goală sau își expune sânii, organele genitale sau zona anală sau este implicată în activitate sexuală. Poate fi orice înregistrare vizuală, inclusiv o fotografie, film sau înregistrare video.

Motivațiile pentru difuzarea acestor imagini și înregistrările video pot fi:

- **Șantajarea (*sextorsion*) sau constrângerea victimei:** autorul infracțiunii, după ce a primit, în mod consensual, înregistrări video sau fotografii de natură sexuală din partea victimei, amenință dezvăluirea lor în cazul în care victima nu furnizează un nou conținut auto-produs de natură sexuală sau nu acceptă o întâlnire față în față;

⁵¹ A se vedea <https://www.kaspersky.com/blog/online-dating-report/>.

⁵² Idem.

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 10 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE ÎNȘELĂCIUNILOR ONLINE ÎN RELAȚIILE INTIME: CYBERSTALKING ȘI PORNOGRAFIA NON-CONSENSUALĂ

- **Răzbunare/ Pornografie non-consensuală:** această practică este, de asemenea, denumită de regulă **revenge porn**, și se referă la divulgarea non-consensuală a imaginilor intime de către un partener în raport cu celălalt, de obicei la sfârșitul unei relații. Este un fenomen obișnuit în situațiile de violență în relațiile intime, inclusiv violența domestică, în care, la sfârșitul relației, sunt difuzate imaginile și / sau înregistrările video (sau difuzarea lor este amenințată) ale fostului partener / în rândul familiei și prietenilor, rețelele sociale sau chiar pe *website*-uri pornografice, ca formă de represalii în urma încheierii relației.

Strategii de prevenire

Pentru a preveni **situațiile de cyber-stalking și de partajare non-consensuală a imaginilor**, în acest punct al Modulului, formatorul ar trebui să transmită cursanților următoarele strategii pe care ei, în calitate de specialiști în sprijinirea victimelor, le pot folosi în intervenția cu copilul / tânărului victimă și familia acestuia:

- Încetarea la orice formă de comunicare cu agresorul;
- Nu blocați sau să dezactivați rețeaua de socială / platforma de comunicare pe care agresorul a folosit-o pentru a comunica cu victima; deoarece platformele WhatsApp® sau Viber® folosesc criptarea de la capăt la cap (a se vedea Modulul 8);
- Nu furnizați informații personale sau date personale solicitate prin e-mail, mesaje, apeluri, *website*-uri nesolicitate;
- Configurați setările de confidențialitate și siguranță ale profilurilor/ conturilor ale rețelelor sociale și alte platforme, eliminând informațiile personale sau de altă natură care pot identifica adresa de domiciliu, școala, numărul de telefon mobil etc.;
- Activarea filtrelor de *spam* și de hărțuire;
- Creșterea gradului de conștientizare a riscurilor inerente utilizării internetului și a TIC în relații și explicarea modului de funcționare a platformelor de comunicare și a modului în care acestea pot fi folosite în siguranță. Este important abordarea problemelor legate de „safe sexting” în rândul tinerilor adulți și adulților, și anume prin utilizarea platformelor care folosesc criptarea “end-to-end” și care au opțiunea de a nu permite să rămână în memorie imaginile sau înregistrările video în telefonului destinatarului;
- Editați imaginile / înregistrările video, în special de natură intimă, înainte de a le partaja / disemina, pentru a proteja identitatea, eliminând elemente de identificare personală, cum ar fi fața, semnele și / sau tatuajele, precum și georeferențierea imaginii ;
- Configurați setările de confidențialitate și securitate ale profilurilor/ conturilor pe rețelele sociale și alte platforme.

Strategii de intervenție

Strategii pentru păstrarea dovezilor digitale

În plus contextul acestui Modul, formatorul trebuie să prezinte cursanților strategiile care pot fi explicate victimei în procesul de sprijinire, pentru păstrarea dovezilor. Această secțiune a Modulului explorează, de asemenea, unele dintre dificultățile asociate cu păstrarea dovezilor și care decurg din caracteristicile platformelor utilizate pentru comunicare (criptare end-to-end).

Să analizăm unele dintre aceste strategii:

Situațiile de *cyber-stalking* și diseminare / partajare non-consensuală a imaginilor apar în mod obișnuit pe rețelele sociale sau pe platformele de chat *online*, unde pot fi găsite multe dovezi de comitere a infracțiunii.

- Cea mai eficientă metodă pentru protejarea dovezilor pe rețelele sociale este de a face **capturi de ecran** ale conținutului pe care doriți să îl raportați. Cu toate acestea, este esențial ca, în aceste capturi de ecran, **URL**-ul (Localizator Uniform de Resurse) al conținutului respectiv să fie vizibil.
- Prin adresa URL, chiar dacă conținutul nu mai este disponibil pe platformă, autoritățile pot cere companiilor să le furnizeze informații cu privire la persoana care a publicat conținutul.

Aceste strategii de conservare a dovezilor sunt prezentate prin exemple concrete în cadrul rețelelor sociale:

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 10 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE ÎNŞELĂCIUNILOR ONLINE ÎN RELAȚIILE INTIME: CYBERSTALKING ȘI PORNOGRAFIA NON-CONSENSUALĂ

- Puteți **identifica o adresă URL specifică a unei postări sau unui comentariu** pe Facebook®:
 - Faceți clic pe ora sau data la care a fost făcută publicarea sau a fost adăugat comentariul;
 - Când faceți clic pe ora sau data, se generează o nouă fereastră în browserul de internet. În acea fereastră, este vizibil URL-ul corespunzător publicării sau comentariului. Această adresă URL trebuie copiată / salvată și raportată autorităților.

Problema cu platformele de chat care utilizează criptarea end-to-end (E2E encryption)

Criptarea end-to-end se referă la faptul că numai destinatarul și expeditorul pot vedea mesajul necriptat, ceea ce înseamnă că, dacă conținutul conversației este șters, autoritățile nu au nicio modalitate de a solicita registrul conversațiilor entităților care furnizează serviciul respectiv. Aceste platforme de comunicare - cum ar fi WhatsApp® - se dovedesc a fi avantajoase pentru eventualii autori ai acestor tipuri de infracțiuni cibernetice.

În aceste cazuri, este deosebit de importantă necesitatea de a face **capturi de ecran**, ca formă de conservare a probelor.

De asemenea, este important să se definească **mecanismele de stocare automată (backups)** în setările aplicației, pentru a avea acces la informații, chiar dacă acestea sunt eliminate de oricare dintre părțile interesate.

Cui și cum să raportați / denunțați

Tipurile de violență descrise - *cyberstalking* și pornografia non-consensuală - pot constitui mai multe infracțiuni, și anume **violarea vieții private** (art. 226, CP), **fals informatic** (Art. 325, CP), **hărțuire** (art. 208, CP) și **șantaj** (Art. 207, CP).

De asemenea, în contextul relațiilor intime în situații de **violență domestică**, a fost introdusă o nouă formă de violență domestică în Legea 217/ 2003 pentru prevenirea violenței domestice și anume **violența cibernetică**, definită ca: „hărțuire online, mesaje online instigatoare la ură pe bază de gen, urmărire online, amenințări online, publicarea nonconsensuală de informații și conținut grafic intim, accesul ilegal de interceptare a comunicațiilor și datelor private și orice altă formă de utilizare abuzivă a tehnologiei informației și a comunicațiilor prin intermediul calculatoarelor, telefoanelor mobile inteligente sau altor dispozitive similare care folosesc telecomunicațiile sau se pot conecta la internet și pot transmite și utiliza platformele sociale sau de e-mail, cu scopul de a face de rușine, umili, speria, amenința, reduce la tăcere victima”. De reținut că Legea 217/ 2003 reglementează **ordinul de protecție**, astfel că acesta poate fi solicitat inclusiv pentru situații de violență cibernetică.

Toate aceste infracțiuni pot fi raportate Poliției și Parchetului.

Strategii pentru a depăși victimizarea și impactul acesteia

În urma aspectelor cheie privind intervenția cu victimele criminalității informatice lucrate în Modulul 4 și strategiile de prevenire și intervenție deja subliniate, specialistul în sprijinirea victimelor trebuie să ofere victimei un set de orientări practice.

Specialistul ar trebui să ia în considerare, totodată **impactul experienței de cibervictimizare** și consecințele resimțite de victimă în structurarea asistenței și sprijinului acordat victimei de *cyberbullying*. A se vedea Modulul 3 al acestui Curs de Formare, precum și capitolul 4 - Partea I a *Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*.

Prin cazurile prezente în exercițiul propus (a se vedea Planul Sesiunii), formatorul va avea ocazia să abordeze dinamica fiecărei forme de cibervictimizare, precum și consecințele și strategiile cheie care ar trebui folosite în procesul de intervenție.

În situația de **cyberstalking**, formatorul ar trebui să prezinte cursanților un set de strategii pe care să le poată folosi în cadrul sprijinului și intervenției acordate victimei. Acum să analizăm, strategiile de securitate:

- Evitați contactarea și / sau confruntarea cu autorul comportamentelor de *cyber-stalking*;
- Nu răspundeți la nici o încercare de contact din partea autorului actelor de *cyber-stalking* și păstrați copii ale

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 10 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE ÎNȘELĂCIUNILOR ONLINE ÎN RELĂȚIILE INTIME: CYBERSTALKING ȘI PORNOGRAFIA NON-CONSENSUALĂ

acelor încercări de contact / mesaje;

- Păstrați toate scrisorile, e-mailurile, SMS-urile, biletele, cadourile și / sau alte materiale pe care vi le-a trimis persoana care v-a hărțuit;
- Informați persoanele apropiate - familia și prietenii, colegii de la locul de muncă / de la sala de sport / de școală, vecinii - despre situația de cibervictimizare, astfel încât în niciun caz să nu poată aceștia furniza informații autorului comportamentelor de hărțuire;
- Alegeți drumuri alternative la cele pe care le folosiți de obicei pentru a vă deplasa;
- Rugați pe cineva de încredere să vă însoțească la mașină sau chiar la transportul pe care îl utilizați în mod normal;
- Când călătoriți cu mașina, țineți ușile încuiate în timpul călătoriei; asigurați o distanță sigură față de vehiculul din față, în cazul în care trebuie să schimbați drumul / banda de circulație;
- Rețineți orice incidente suspecte, creând un registru detaliat al comportamentelor de care sunteți victimă;
- În situații de pericol, trebuie să căutați un loc sigur sau unde se află mai multe persoane. De asemenea, puteți activa contactele de urgență.

Să analizăm și alte strategii de sprijin:

- Explicați și Accentuați faptul că nu este vina victimei, ci autorului comportamentelor;
- Transmiteți ideea că victima are dreptul să spună nu;
- Transmiteți ideea că agresorul poate folosi strategii de manipulare / șantaj: cu scopul de a face victima să se simtă vinovată, și de a o convinge să facă ceva ce agresorul își dorește;
- Explicați victimei cum să procedeze pentru a proteja dovezile digitale (a se vedea informațiile de mai sus);
- Furnizați strategii de siguranță și contacte de urgență;
- Indicați victimei cui și cum să raporteze / denunțe;
- Furnizați strategii de prevenire și intervenție pentru a preveni noi infracțiuni (a se vedea informațiile de mai sus);
- Accentuați reluarea activităților.

În ceea ce privește **pornografia non-consensuală**, formatorul ar trebui să prezinte cursanților un set de strategii pe care să le poată folosi în cadrul sprijinului și intervenției cu victima:

- Validați și recunoașteți experiența lor de cibervictimizare și încadrați reacțiile victimei în cadrul unei experiențe de viață anormale;
- Reduceți vinovăția;
- Asigurați-vă că victima înțelege că nu ar trebui să cedeze niciodată șantajului de către agresor - cedarea nu va opri comportamentul agresorului;
- Furnizați, într-un mod simplu, concis și clar, strategiile de prevenire și intervenție prezentate anterior;
- Oferiți sprijin, inclusiv sprijin psihologic;
- Luați în considerare posibilitatea de colaborare cu serviciul psihiatric, în cazul în care există ideea suicidară.

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 10 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE ÎNŞELĂCIUNILOR ONLINE ÎN RELAȚIILE INTIME: CYBERSTALKING ȘI PORNOGRAFIA NON-CONSENSUALĂ

PLANUL SESIUNII Nr. 10

1. Identificarea acțiunii

Denumire	Curs de Formare Sprijin Specializat pentru Victimele Criminalității Informaticе		
Module / teme	Sprijin Specializat pentru victimele violenței online în relațiile interpersonale: <i>cyber-stalking</i> și partajare non-consensuală a imaginilor		
Data sesiunii	Orar	Durata sesiunii	40 de minute
Formatori			

2. Obiective specifice

La sfârșitul sesiunii, cursanții ar trebui să poată să:

- Distinge corect natura și *modi operandi* ale violenței online în relațiile interpersonale, și anume *cyber-stalking*-ul și pornografia non-consensuală;
- Enumere corect strategiile de intervenție propuse în sprijinul specializat pentru victimele de *cyber-stalking*-ului și victimelor partajării non-consensuale a imaginilor;
- Recunoască corect strategiile de prevenire a revictimizării propuse în intervenția cu victimele *cyber-stalking*-ului și victimele partajării non-consensuale a imaginilor.

3. Structura sesiunii

	Conținutul programului	Metodologie	Resurse pedagogice / didactice	Evaluare / Exerciții	Timp (minute)
Introducere	Tipuri: • <i>Cyber-stalking</i> • Pornografia non-consensuală	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
	<i>Modi operandi</i> și natura infracțiunilor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
Dezvoltare	Strategii de prevenire	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5
	Strategii de intervenție: • Strategii pentru păstrarea dovezilor digitale • Cui și cum să raportați / denunțați • Strategii pentru a depăși victimizarea și impactul acesteia	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	10
	Exercițiul nr. 6	Activă	Regulile Exercițiului nr. 6 și Cazul A și Cazul B Exercițiul nr. 6	Observare	10
Concluzie	Rezumat concludent și clarificarea nelămuririlor	Expozitivă și activă	Calculator: <i>Datashow</i> și ecran de proiecție	Observare	5

OBSERVAȚII

Destinatari:

Specialiști în sprijinirea victimelor

Data: / /

Formator:

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 10 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE ÎNȘELĂCIUNILOR ONLINE ÎN RELAȚIILE INTIME: CYBERSTALKING ȘI PORNOGRAFIA NON-CONSENSUALĂ

INSTRUCȚIUNI ESENȚIALE ȘI INFORMAȚII PENTRU FORMATOR

CONCORDANȚA CU CONȚINUTUL

Planul Sesiunii *Manual ROAR – de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitatea victimelor*

	PARTE	CAPITOL
<i>Modi operandi</i> și natura infracțiunii	Partea I - Înțelegere	Capitolul 1 -1.3.
	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii de prevenire	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii de intervenție		
Strategii pentru păstrarea dovezilor digitale	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Cui și cum să raportați / denunțați	Nu corespund	
	A se vedea Prezentarea și Cadrul Modulului	
Strategii pentru a depăși victimizarea și impactul acesteia	Partea II - Continuați	Capitolul 2 - 2.1.
	A se vedea Prezentarea și Cadrul Modulului	
Exercițiul nr. 6	Nu corespund	
	A se vedea Regulile Exercițiului nr. 6	
Rezumat concludent și clarificarea nelămuririlor	Nu corespund	

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 10 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE ÎNŞELĂCIUNILOR ONLINE ÎN RELAȚIILE INTIME: CYBERSTALKING ȘI PORNOGRAFIA NON-CONSENSUALĂ

REGULILE EXERCITIULUI Nr. 6

Modul / temă	Sprijin specializat pentru victimele violenței online în relațiile interpersonale: cyber-stalking și partajare non-consensuală a imaginilor	COD REF.	DOMENIUL EDUCAȚIEI ȘI FORMĂRII
Obiective	Acest exercițiu are drept scop consolidarea informațiilor și a conținutului programului al acestui Modul, abordând natura situațiilor de <i>cyberbullying</i> și de pornografie nonconsensuală, precum și strategiile de intervenție care ar trebui introduse de specialistul în sprijinirea victimelor.		
Executare	Formatorul ar trebui să împartă grupul de cursanți în 2 până la 4 grupuri mici. Prima jumătate a grupului creat trebuie să primească Cazul A al Exercițiului nr. 6, iar cealaltă jumătate a grupului creat trebuie să primească Cazul B al Exercițiului nr. 6. Cazul A descrie o situație de <i>cyberstalking</i> și Cazul B o situație de pornografie non-consensuală [<i>revenge porn</i>]. Formatorul ar trebui să ceară fiecăruia dintre grupurile mici create să citească cu atenție cazul respectiv și să definească, ca grup, măsurile și strategiile care trebuie puse în aplicare în sprijinul fiecărei victime. Apoi, ar trebui să solicite grupului (grupurilor) cărora li s-a atribuit Cazul A să împărtășească sugestiile lor de strategie. În dezbateră Cazului, ar trebui să evidențieze strategiile de intervenție rezumate în Prezentarea și Cadrul Modulului. Ar trebui să repetați procedura pentru dezbateră Cazului B.		
Notițe	Consultați Prezentarea și Cadrul Modulului		

PARTEA 2 – ASISTENȚĂ SPECIALIZATĂ PENTRU VICTIME

MODULUL 10 – SPRIJIN SPECIALIZAT PENTRU VICTIMELE ÎNȘELĂCIUNILOR ONLINE ÎN RELAȚIILE INTIME: CYBERSTALKING ȘI PORNOGRAFIA NON-CONSENSUALĂ

CAZUL A – EXERCIȚIUL Nr. 6

Raluca, 22 de ani, studentă la universitate.

Unul dintre marile hobby-uri ale Ralucăi este fotografia. Raluca a petrecut ore întregi făcând poze cu peisajele care i-au plăcut. De asemenea, a petrecut mult timp editându-și pozele.

Una dintre cele mai mari plăceri ale Ralucăi a fost să vadă succesul muncii sale, prin *like*-urile urmăritorilor săi, în fotografiile sale publicate pe Instagram®. Din acest motiv, contul său de Instagram® era „deschis” și accepta toate cererile de urmărire.

În ultimele 5 luni, Raluca a fost victimă a *cyber-stalking*-ului pe rețelele sociale.

Agresorul, Eugen, a abordat-o inițial printr-o simplă cerere de urmărire, urmată de o invitație la cină. Raluca a refuzat, susținând că nu este interesată de relații amoroase. Eugen a pus la îndoială acest refuz și a întrebat-o pe Raluca de ce îl trata cu dispreț, de ce îl respingea. Raluca a răspuns politicos, susținând că nu-l cunoaște și că, prin urmare, nu poate accepta. Profilul lui Eugen nu avea poze care să-l poată identifica.

Eugen i-a spus că, deși ea nu-l cunoaște, el o cunoaște bine. Apoi a început să creeze profiluri false, folosind datele personale ale Ralucăi (de ex. adresa, data nașterii, adresa părinților, numele fratelui) sau care reflectă amenințări (de exemplu: „Te prind și nici nu știi ce îți fac”). O să te omor, e ceea ce meriți. “;

Au fost create sute de profile false. Pe lângă depunerea unei plângeri, Raluca a fost forțată să-și șteargă profilul de Instagram®, să își schimbe locuința și facultatea. Pe lângă faptul că trăiește permanent cu frică și nesiguranță, dorișta sa de a fotografia a încetat să mai existe.

La prima ședință de asistență, Raluca raportează următoarele:

„Motivul pentru care vin aici este să mă asigur că fac lucrurile corect. Vreau doar să mă asigur că fac ceea ce trebuie. Nu înțeleg ce am făcut. Ar fi trebuit să spun da? Am fost nepoliticoasă? ”

CAZUL B – EXERCIȚIUL nr. 6

Maria, în vârstă de 43 de ani, împărtășește următoarele la prima ședință de asistență:

„Am fost într-o relație de aproximativ 8 ani. Am locuit împreună. Nu a fost agresiv cu mine, ne înțelegeam bine. Pur și simplu a încetat să-mi mai placă de el. Nu mă mai simțeam împlinită și nici fericită în acea relație. Am terminat relația acum aproximativ 6 luni.

De atunci, a început să mă amenințe că o să trimită poze de ale mele, pe care i le-am trimis odată. Sunt fotografii intime, în care îmi expun corpul.

La început, a fost doar o încercare ca noi să fim din nou împreună. Am înțeles, pentru că știu că era disperat ... Am fost o persoană foarte importantă pentru el. Pe lângă asta, el este o persoană care are puțini prieteni. Pe lângă faptul că am fost soția lui, am fost prietena lui de nădejde la fiecare oră.

Dar, după o lună, amenințările au început să fie mai frecvente, erau tot mai multe și au devenit amenințări zilnice. De o săptămână, el mă amenință că va trimite fotografiile tuturor prietenilor, familiei și oamenilor de locul meu de muncă.

Nu am cedat. Nu mai este aceeași persoană, m-a dezgustat! Astăzi m-am trezit și mi-a trimis de dimineață un *printscreen* al unui e-mail pe care l-a trimis: șefului meu, tuturor colegiilor mei (suntem 24, nu-i lipsea 1!), părinților mei, fraților mei și mătușilor și unchilor. Cum o să reușesc să ies din nou din casă? Cum? Nu pot merge la serviciu! Nu mă pot uita la fețele colegilor mei! Niciodată nu mă va lua cineva în serios (plânsul convulsiv). Ar fi trebuit să cedez, ar fi trebuit să cedez... Sau nu ar fi trebuit să mă despart niciodată de el, de ce m-am despărțit de el? Nu mai vreau să trăiesc ... (plâns convulsiv). ”



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



Disclaimer:

O conteúdo deste manual representa a opinião do autor apenas e é da sua exclusiva responsabilidade. A Comissão Europeia não assume qualquer responsabilidade pela utilização que possa ser feita a partir das informações contidas neste manual.

Disclaimer:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Disclaimer:

Conținutul acestei publicații reprezintă doar opiniile autorului și este responsabilitatea sa exclusivă. Comisia Europeană nu își asumă nicio responsabilitate pentru utilizarea informațiilor pe care le conține.