

PROTEUS
- GHIDUL
BUNELOR
PRACTICI
- FURTUL DE
IDENTITATE
PE INTERNET

PROTEUS



Co-funded by the Prevention of and
Fight against Crime Programme
of the European Union

APAV[®]
asociația protejtecna de
Apoyo à Vítima

[illegible]

ISBN	Depozit Legal
978-972-8852-72-6	

Telefon	Fax
+351 21 358 79 00	+351 21 887 63 51

Titlu
Proteus - Ghidul Bunelor Practici - Furtul de
Identitate pe Internet

E-Mail	Website
apav.sede@apav.pt	www.apav.pt

Autor
2015 © APAV
Associação Portuguesa de Apoio à Vítima

APAV
Rua José Estevão, 135 - A
1150-201 Lisboa
Portugal

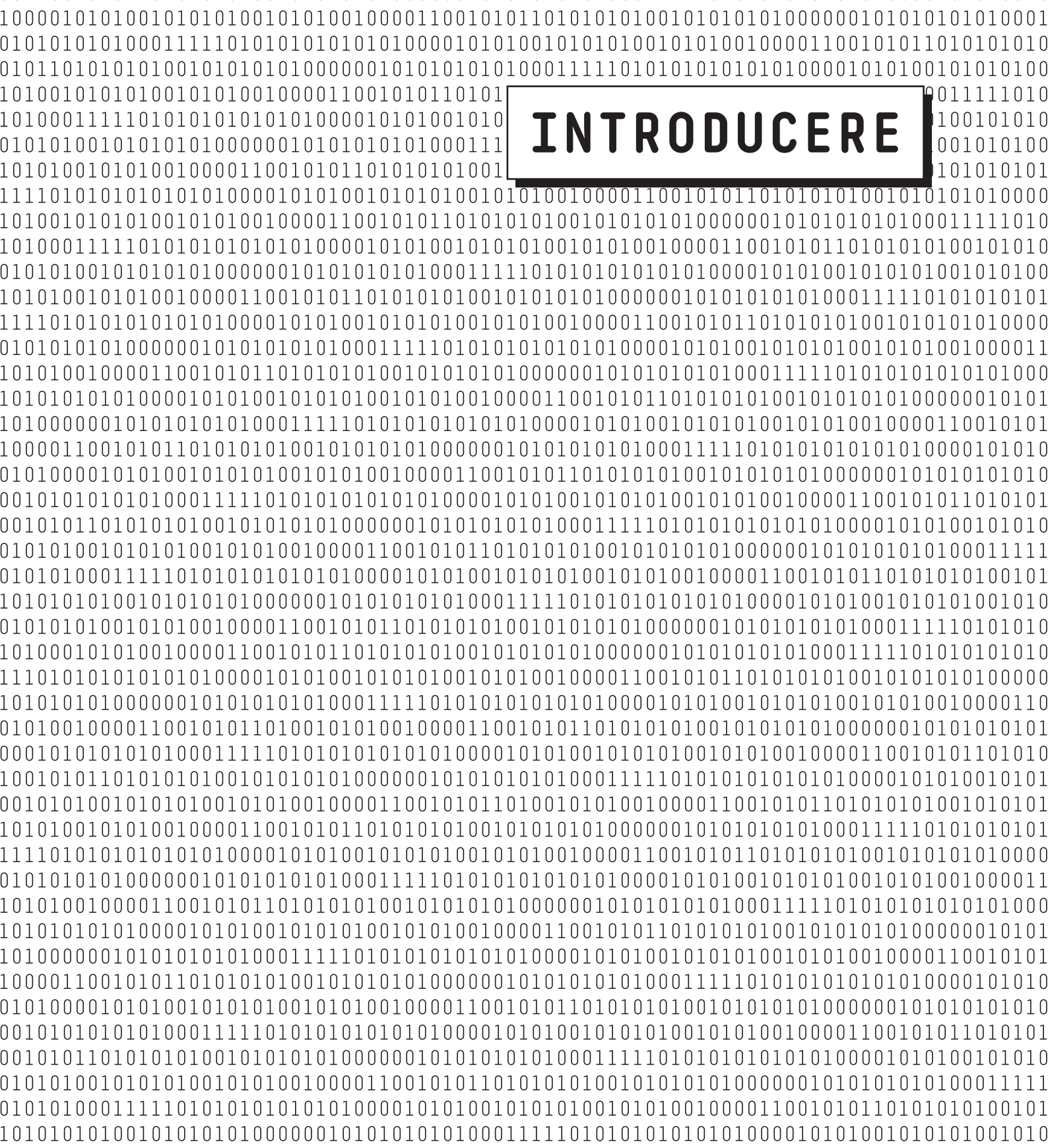
|||||

CONTENTS

|||||

INTRODUCERE	5	c.IMPACTUL EMOȚIONAL	34
		d.IMPACTUL ASUPRA RUTINEI ZILNICE	35
1.STUDII DE CAZ	9	3.4.2. În societate	36
< Cazul 1 >	11	3.5. Dificultăți de investigare	36
< Cazul 2 >	11		
< Cazul 3 >	12	4.CADRUL LEGISLATIV	39
< Cazul 4 >	12	4.1. Cadrul internațional	41
< Cazul 5 >	12	4.2. Legea romana	42
< Cazul 6 >	13		
< Cazul 7 >	13	5. LEGISLAȚIA NAȚIONALĂ APLICATĂ STUDIILOR DE CAZ	45
< Cazul 8 >	13	< Cazul 1 >	47
< Cazul 9 >	14	< Cazul 2 >	47
< Cazul 10 >	14	< Cazul 3 >	47
		< Cazul 4 >	47
2.FURTUL DE IDENTITATE - ÎNSCENAREA	15	< Cazul 5 >	48
2.1. Infracțiunea cibernetică	17	< Cazul 6 >	48
2.1.1. Globalizare	17	< Cazul 7 >	48
2.1.2. Infracțiunile cibernetică – Definiții	17	< Cazul 8 >	48
2.2. Furtul identității	19	< Cazul 9 >	48
2.2.1. Dificultăți legate de terminologie	19	< Cazul 10 >	48
2.2.2. Încercarea de definire	20		
2.3. <i>Modi operandi</i>	21	6. PREVENIRE	51
		6.1. Măsurile de prevenire	53
3.FURTUL IDENTITĂȚII - REALITATEA PRACTICĂ	27	6.2. Semne ale infectării cu malware	59
3.1. Cele mai uzuale situații de furt de identitate prin intermediul internetului	29	6.3. Cum putem identifica semnele furtului identității	59
3.2. Infractorul și victima	30		
3.3. Factori de risc	32	7.ASISTENȚĂ PENTRU VICTIME	61
3.4. Impactul furtului identității	33	7.1. Infectarea cu malware	63
3.4.1. Impactul asupra victimei	33	7.2. Furtul identității	63
a.IMPACTUL FINANCIAR	33		
b.IMPACTUL JURIDIC	34	ANEXE	67
		Glosar	69

|||||



INTRODUCERE

[illegible]

INTRODUCERE

Conform unui studiu realizat în 2013 pe un eșantion de 13.022 de persoane adulte din 24 de țări, cu vârste cuprinse între 18 și 64 ani, se estimează că 378 milioane de persoane pe an, un milion de persoane pe zi și 12 persoane pe secundă cad victime ale infracțiunilor în mediu cibernetic.

Procentul populației online care cade victimă înșelăciunilor legate de identitate înfăptuite prin intermediul internetului și al accesului neautorizat la e-mail variază între 1% și 17% în 21 de țări ale lumii, în timp ce, în aceste țări, doar între 1 și 5% sunt victime ale furturilor sau jafurilor obișnuite.

Toate aceste victime se regăsesc într-o situație de o deosebită vulnerabilitate și nu sunt suficient de protejate față de infracțiunile cibernetice. Fiind de dată recentă, infracțiunea cibernetică este încă subestimată și puțin înțeleasă de populație, în general, iar efectele sale sunt de asemenea subestimate atât în ceea ce privește definirea fenomenului cât și implementarea de către autoritățile competente a măsurilor de contracarare.

Cazurile de furt de identitate în mediul online pot fi foarte complexe, de aceea victimele au nevoie de ajutor personalizat pentru a-și recăpăta echilibrul. Deseori, poate fi nevoie de ajutor pentru operarea mijloacelor electronice de combatere a infracțiunilor electronice, pe care victimele nu le stăpânesc.

Impactul infracțiunilor electronice și în special al furtului de identitate realizat prin intermediul internetului este pe zi ce trece tot mai mare, ca și numărul victimelor care raportează astfel de infracțiuni poliției sau care solicită ajutor, ceea ce face necesară îmbunătățirea reacției și a suportului în acest sens.

În acest context, s-a simțit nevoia alcătuirii acestui ghid, care prin faptul că se concentrează pe problema legată de furtul de identitate pe internet, are menirea de a pregăti personalul implicat în serviciile de asistență a victimelor acestor infracțiuni, precum și alți specialiști care trebuie să înțeleagă acest fenomen și să informeze și să acorde victimelor asistență pentru a întreprinde cele mai bune măsuri de combatere a infracțiunilor cibernetice.

1.

STUDII
DE CAZ

[illegible]

1. STUDII DE CAZ

< Cazul 1 >

Josué, angajat al unei bănci, cunoștea codurile de acces ale serviciului de homebanking al lui Joaquim și le-a vândut unei organizații infracționale, care a accesat contul și a transferat 6000 de euro într-un cont necunoscut.

< Cazul 2 >

Joana se consideră o persoană avizată în ceea ce privește chestiunile legate de securitatea cibernetică și și-a luat totdeauna măsuri de precauție pentru protecția computerului.

Într-o zi, impresionată de ceea ce tocmai citise într-un ziar despre infracțiunile cibernetice în creștere în Portugalia, Joana a decis să facă cercetări pentru a vedea care este cel mai bun antivirus disponibil. Pentru a face acest lucru, a folosit un motor popular de căutare și a găsit, printre altele, o pagină dubioasă care propunea transferul unui antivirus puternic, pe care Joana a hotărât să nu-l accepte, deoarece fusese avertizată să nu accepte decât transferuri de informații din surse fiabile.

În seara aceea, Joana a efectuat o serie de plăți folosind interfața online a băncii proprii.

O săptămână mai târziu, Joana și-a consultat contul din bancă și a constatat dispariția unei sume considerabile de bani.

Poate fi suficientă deschiderea unei pagini web pentru ca un malware să fie instalat pe computer. În acest caz, un program keylogging a fost instalat pe computerul Joanei. Acest program a permis infractorului să captureze toate datele pe care Joana le-a introdus cu ajutorul tastaturii, inclusiv codurile de homebanking.

1. STUDII DE CAZ

< Cazul 3 >

Jandira și copiii ei utilizează internetul pentru căutări online și pentru a trimite e-mailuri.

Cu toate acestea, în ultima lună, computerul Jandirei a devenit atât de lent, încât și ea și copiii au încetat să-l mai folosească. Luna trecută, Jandira a primit un e-mail semnat ReidosHackers, care pretindea că deține controlul asupra computerului său și a cerut suma de 600€ pentru a-I reda libertatea de a-și utiliza propriul computer.

< Cazul 4 >

Josefinei îi place să corespundeze pe e-mail cu prietenii și membrii familiei, unii emigrați în Franța.

Într-o zi, în timp ce verifica dacă a primit răspuns la ultimul e-mail trimis vărului ei Jean-Pierre, s-a pomenit cu un e-mail de la bancă, prin care i se cerea să acceseze un link și să confirme informațiile de identificare prin completarea unui formular.

Josefina a căutat documentele de la bancă și a făcut imediat ceea ce i s-a cerut.

O lună mai târziu, Josefina a fost contactată de managerul de cont care, intrigat de faptul că o mare parte din economiile din cont fusese transferată către un cont necunoscut, se hotărâse să clarifice această îndoială printr-o discuție cu clienta sa.

< Cazul 5 >

José a primit un e-mail, care făcea parte dintr-o schemă de spamming, aparent transmis de serviciul său de webmail, prin care i se cerea să-și actualizeze parola.

Ulterior a fost întrebat de unii colegi și prieteni despre unele e-mailuri pe care le tot primiseră de pe adresa lui de e-mail, prin care le cerea ajutor financiar. Niciunul dintre prietenii săi nu a răspuns la aceste e-mailuri.

1. STUDII DE CAZ

< Cazul 6 >

Joel și Jessica se întâlneau deja de cinci luni, când Jessica a rupt relația.

Joel, furios, a jurat că se va răzbuna, însă Jessica l-a ignorat. Într-o zi, ajungând la școală de dimineață, a observat că toți colegii ei o priveau, șușotind între ei și râzând. A intrat în clasă și și-a întrebat colega, pe Jurema, dacă știa motivul, iar aceasta i-a spus că exista un profil pe Facebook, pe numele Jessicai și cu poza ei la profil, în care pretindea că este dispusă să acorde favoruri sexuale în schimbul unor sume modice de bani.

< Cazul 7 >

Joana, care cunoștea numele complet și adresa Julianei, a creat un cont de e-mail pe numele acesteia din urmă și s-a înscris pe un site de licitații online cu numele și adresa Julianei folosindu-se de e-mailul pe numele ei.

Ulterior, Joana a postat anunțuri pentru vânzarea unor tablete. João, interesat să cumpere, a plătit o tabletă dar nu a primit-o niciodată.

Juliana a fost citată peste un timp, pentru a fi chestionată ca pârâtă într-un caz de escrocherie pe computer.

< Cazul 8 >

Julieta a primit un telefon de la cineva care pretindea a fi de la "Novo Banco" și avea nevoie de confirmarea unor date personale. Julieta a accesat, ușurată că nu rămăsese legată de "Banco Mau". Două luni mai târziu, a primit o factură pentru o serie de cumpărături online care fuseseră făcute cu informațiile de pe cardul ei de credit.

1. STUDII DE CAZ

< Cazul 9 >

O serie de mesaje care păreau a fi transmise de serviciul webmail și prin care se cerea actualizarea unei parole de cont au fost transmise la mai multe adrese de e-mail. Soția lui Julio a introdus datele proprii și astfel infractorul a primit acces la inbox, aflând în felul acesta multe informații personale despre ea și familia ei. Júlio a fost apoi contactat de două companii de credit care doreau să le confirme legitimitatea cererilor de creditare care se făcuseră în numele lui. Júlio, care nu recursese niciodată la vreun credit, a explicat faptul că nu făcuse nicio cerere de împrumut. A fost în același timp uimit de volumul de date personale pe care persoana care voise să-l escrocheze le știa despre el. Cererile de împrumut au fost anulate.

O lună mai târziu, Julio însuși s-a adresat băncii cu intenția de a contracta un împrumut pentru achiziționarea unei case noi. Cererea sa a fost refuzată datorită numărului mare de cereri de împrumut care fuseseră făcute în numele lui, în ultimele luni.

< Cazul 10 >

Jair a fost o victimă a abuzurilor de la intrarea sa la liceu. într-o zi, Jair a venit acasă și a intrat pe contul său de Facebook. Inima aproape că a încetat să-i bată atunci când a constatat că fuseseră postate, prin contul său, niște poze care îl înfățișau pe el, în lenjerie intimă.

L-a cuprins disperarea atunci când și-a dat seama că singura persoană care cunoștea numele de utilizator și parola sa de Facebook era Jaime, singurul său prieten.

2.

FURTUL DE IDENTITATE - INSCENAREA

[illegible]

2. FURTUL DE IDENTITATE - ÎNSCENAREA

2.1. Infracțiunea cibernetică

2.1.1. Globalizare

În anul 2011, cel puțin 2,3 miliarde de persoane, adică peste un sfert din populația lumii, aveau acces la Internet. Conform estimărilor, până în 2020, vor exista șase dispozitive conectate pe persoană. De aceea infracționalitatea se va “hrăni”, din ce în ce mai mult, din Internet.

Tehnologia Informațiilor și Comunicării (TIC) constituie un nou mijloc de a comite infracțiuni. Conectarea globală la internet și utilizarea acestor tehnologii va contribui, de asemenea, la apariția unor noi tipuri de infracțiuni.

În mod similar, TIC facilitează internaționalizarea infracționalității. Cu alte cuvinte, autorul poate comite o infracțiune în Brazilia care să afecteze o victimă din Portugalia, fără niciun fel de dificultate, ceea ce se întâmplă deseori în cazurile de “phishing” ca cel descris în studiul de caz nr. 4 din acest ghid.

Astfel, infracțiunile cibernetice au crescut ca număr, fiind comise fie de organizații infracționale, fie de infractori individuali care caută noi oportunități de a obține profit și alte avantaje, sau de a face rău cuiva apropiat, respectiv prin intermediul rețelelor sociale.

2.1.2. Infracțiunile cibernetice – Definiții

Nu există un consens în privința unei definiții universale a infracțiunii cibernetice. Dreptul național și internațional nu au stabilit o definiție universală și nu există un set de principii consolidate pe acest subiect.

Definițiile infracțiunii cibernetice, conform Oficiului Națiunilor Unite privind Drogurile și Criminalitatea (*United Nations Office on Drugs and Crime*) vor depinde de utilizarea care se va da acestui termen.

Același Departament, confruntat cu instrumentele naționale și internaționale care nu au reușit să dea o definiție în sine a infracțiunii cibernetice, încearcă să descrie conținutul termenului, prin enumerarea acțiunilor sau comportamentelor incluse în acesta.

Sunt enumerate, nu într-un mod exhaustiv, paisprezece comportamente care pot constitui infracțiuni cibernetice, acestea fiind împărțite în trei categorii:

2. FURTUL DE IDENTITATE - ÎNSCENAREA

Acte împotriva confidențialității, integrității și disponibilității datelor și sistemelor	Acte comise prin mijloace informatice în vederea obținerii unor avantaje personale sau beneficii financiare	Acte cu conținut infracțional comise prin mijloace informatice
> Acces ilegal la sistemul computerizat; > Accesul, interceptarea sau achiziția ilegală a datelor informatice; > Interferența ilegală cu date sau sisteme computerizate; > Producerea, distribuirea sau posesia de unelte în vederea utilizării ilegale a computerului; > Încălcarea mijloacelor de protecție sau caracterul privat al mijloacelor de date.	> Frauda sau falsul informatic; > Infracțiuni legate de identitate care sunt comise prin mijloace informatice; > Infracțiuni legate de drepturi de autor și mărci înregistrate comise prin mijloace informatice; > Trimiterea sau controlul trimiterii spam-urilor; > Acte comise prin mijloace informatice care produc daune personale; > Acostarea și atragerea copiilor prin mijloace informatice.	> Incitarea la ură prin mijloace informatice; > Producerea, distribuirea sau deținerea prin mijloace informatice de material pornografic cu copii; > Comiterea prin mijloace informatice a unor acte de sprijinire a terorismului.

În comunicarea transmisă Parlamentului European, Consiliului și Comitetului Regional - *Towards a General Policy on the Fight Against Infracțiunea cibernetică [Către o politică generală privind lupta împotriva infracțiunii cibernetică]* – Comisia Europeană definește infracțiunea cibernetică astfel: «infracțiunile comise prin folosirea rețelilor electronice de comunicare și a sistemelor informatice sau împotriva acestor rețele și sisteme».

Pare că împărțirea conceptului de infracțiune cibernetică într-un concept larg și un concept restrâns asigură o definire mai completă și mai clară. Conceptul mai larg cuprinde toate actele infracționale care ar putea fi comise prin mijloace electronice, chiar dacă acestea sunt simple

2. FURTUL DE IDENTITATE – ÎNSCENAREA

instrumente de realizare și nu integrează tipologia legală. În conceptul restrâns sunt incluse doar acele infracțiuni în care apare componenta digitală ca element al tipului de infracțiune sau chiar ca obiect al acesteia.

2.2. Furtul identității

2.2.1. Dificultăți legate de terminologie

Există multe controverse în jurul termenului de “identitate” și de aceea se impune să spunem clar de la început că, în contextul ghidului de față, termenul se va referi la toate datele personale ale unei persoane care, atunci când sunt folosite de alte persoane, le permite acestora din urmă să acționeze în calitatea victimei cu scopul comiterii de infracțiuni.

Expresia “furt de identitate”, deși a fost aleasă pentru a fi folosită în acest manual, nu definește în mod corect fenomenul la care intenționează să facă referire.

De fapt, niciunul dintre termenii care sunt în mod uzual folosiți în acest context – “furt de identitate”, “jefuirea identității” și “fraudarea identității” – prin influența termenilor din limba engleză – nu se caracterizează prin corectitudine terminologică.

Într-adevăr, cazurile pe care le vom vedea vor presupune faptul că infractorul are nevoie să obțină datele personale sau anumite parole sau coduri personale ale victimelor și să le folosească pentru a comite infracțiuni.

Nu se poate vorbi de furt sau jaf, deoarece sustragerea bunurilor mobile la care face referire Codul Penal (din CP) în art. 203^o și 210^o nu include obținerea datelor sau a parolelor.

De asemenea nu ar trebui să vorbim de fraudă, deoarece acest termen nu are niciun înțeles juridic în cadrul legislativ din Portugalia.

În ceea ce privește limba engleză, termenii “*furtul identității*” și “*fraudarea identității*” par a fi folosiți, în majoritatea cazurilor, cu același înțeles, și anume “*furtul identității*”, mai des folosit în Statele Unite ale Americii, în timp ce “*fraudarea identității*” are o mai mare răspândire în Regatul Unit al Marii Britanii. În Regatul Unit, totuși, s-a făcut efortul de a delimita înțelesurile celor doi termeni.

2. FURTUL DE IDENTITATE - ÎNSCENAREA

Opțiunea oferită de ghidul de față este aceea de a adopta termenul de “furtul identității” pentru a descrie fenomenul avut în vedere, ținând cont de faptul că, în opinia noastră, posibilitatea de a utiliza termenul «fraudarea identității» va fi exclusă, datorită lipsei sale de conținut juridic, precum și a termenului de “jefuirea identității”, având în vedere că nu există violență sau constrângere asociate componentei comportamentale a fenomenului care constituie obiectul atenției noastre.

Astfel, “furtul identității” deși nu constituie o descriere exactă, pare a fi termenul care prezintă cel mai mare grad de corespondență cu aceste comportamente care se intenționează a fi definite și studiate.

2.2.2. Încercarea de definire

Ca și în cazul infracțiunilor cibernetice, nu există o definiție uniformă pentru furtul identității. Vom încerca să definim care sunt actele pe care le găsim ca fiind incluse în acest fenomen, în înțelesul acestui manual.

Să începem prin a enunța în mod clar faptul că furtul identității nu este o infracțiune în Portugalia, ci un fenomen căruia i se aplică o serie de prevederi legale de ordin penal.

Conform Comisiei Federale ale Statelor Unite ale Americii (*USA Federal Trade Commission*) «furtul identității se produce atunci când o persoană folosește informațiile personale ale altei persoane fără a avea permisiunea acesteia din urmă, în scopul comiterii de fraude sau alte infracțiuni».

Conform Grupului pentru prevenția fraudelor (*Fraud Prevention Expert Group*) al Comisiei Europene, esența fenomenului, pentru a prelua din definițiile date pentru *furtul identității* și *fraudarea identității*, este însușirea și utilizarea identității personale a unei persoane în scopul desfășurării de activități ilegale.

Conform Diviziei de infracțiuni economice a Consiliului European, termenul “furtul identității” descrie acțiunile prin care infractorul obține și utilizează prin înșelăciune identitatea altor persoane. Aceste acțiuni pot fi realizate fără folosirea mijloacelor tehnice, dar se pot face și prin intermediul tehnologiei computerizate.

Unele definiții, care diferă de la o țară la alta, se axează mai mult pe acțiunea de obținere a datelor, în timp ce altele presupun existența scopului de a obține aceste date în vederea comiterii unor acte ilegale.

2. FURTUL DE IDENTITATE – ÎNSCENAREA

Elementul comun al tuturor acestor definiții care ne sunt propuse este acele comportamente descrise se referă la una sau mai multe din cele trei etape – etapa obținerii informației personale, etapa de posesie sau transfer de date (știind că acestea vor fi utilizate pentru comiterea unei infracțiuni) și, în cele din urmă, etapa utilizării datelor pentru a comite infracțiunile respective.

Pentru a formula cea mai largă definiție posibilă, se poate spune că furtul identității include obținerea neaprobată a datelor personale și/sau secrete ale victimei, deținerea sau transmiterea lor cunoscând faptul că aceste date urmează a fi folosite în scopuri infracționale și folosirea acestora pentru comiterea unor infracțiuni.

Deoarece acest manual se referă la furtul identității pe Internet, actele vor fi acoperite prin definiția fenomenului, fie că datele personale ale victimei sunt obținute prin intermediul Internetului (cum se întâmplă în cazurile 2 și 4), fie că sunt obținute prin alte mijloace dar sunt transmise prin intermediul Internetului sau utilizate pentru a comite infracțiuni pe Internet (ca în cazurile 1, 8 și 10). În cazul în care infracțiunea se coroborează doar în una dintre aceste etape, comportamentul care îi corespunde – obținerea, deținerea sau utilizarea – trebuie să se petreacă prin intermediul Internetului pentru a se încadra în conceptul avut în vedere în acest document.

Așa cum am menționat, odată ce au fost obținute datele victimei, infractorul poate utiliza aceste date pentru a comite infracțiuni. Aceste infracțiuni pot fi de trei tipuri: infracțiuni care nu sunt legate direct de victimă dar sunt realizate pe numele acesteia, (cazurile 5 și 7), infracțiuni care au drept scop îmbogățirea infractorului sau a unei terțe persoane și care produc daune directe victimelor (cazurile 1, 2, 4, 8 și 9) și infracțiuni care au drept scop defăimarea victimei (cazurile 6 și 10).

2.3. *Modi operandi*

Datele victimei pot fi obținute printr-o largă gamă de mijloace, care tind să devină din ce în ce mai numeroase și mai diversificate. În acest context, inovațiile care au drept scop <inducerea în eroare> atât a mecanismelor de detectare ale utilizatorilor cât și autoritățile sunt permanente. Din acest motiv, abordarea fiecărui mijloc în parte va trebui să fie una generică, pentru a nu fi depășită în scurt timp.

Există metode tradiționale de a obține informațiile personale ale cuiva, cum ar fi căutatul prin gunoiul persoanei, interceptarea corespondenței, furtul documentelor de identitate sau a altor

2. FURTUL DE IDENTITATE - ÎNSCENAREA

documente sau rapoarte/extrase care conțin datele personale sau informațiile financiare ale victimei, infractorul poate pretinde că este un proprietarul unui imobil, un potențial angajator sau orice altă persoană care ar putea să solicite acest gen de informații, poate să încerce să obțină informațiile respective de la persoane apropiate victimelor, poate contacta victima sau băncile cu pretenții false de a obține informații privilegiate (cazul 8), poate cumpăra aceste informații sau chiar spiona victima atunci când folosește informațiile respective (imaginați-vă cazul unui coleg de serviciu al victimei, care observă victima atunci când introduce datele de acces ale propriului cont bancar, pe care apoi le utilizează pentru a retrage bani din cont).

Toate aceste mijloace pot fi incluse în furtul identității pe internet conform definiției de mai sus, odată ce informația obținută prin mijloace ne-informatică poate fi utilizată pentru a comite orice infracțiune prin intermediul internetului.

O altă metodă de a obține datele victimei, fizică fără a fi una tradițională, este aceea a furtului de *hardware*, de exemplu telefonul mobil care conține informații secrete sau personale.

După ce am văzut care sunt principalele metode tradiționale de a comite un furt de identitate legat de internet, vom vedea, în cele ce urmează, care sunt metodele prin care se utilizează aceste noi tehnologii, mai concret internetul.

“Scrisorile nigeriene” așa cum au fost denumite de toată lumea, au apărut inițial chiar sub forma unor scrisori, transmisiuni telex sau fax, iar acum sunt transmise sub forma unor mesaje de e-mail; acestea constituie o metodă de comitere a unui furt de identitate care utilizează atât mijloacele tradiționale de obținere a datelor cât și accesul la internet.

Mesajele pe e-mail vin, în general, scrise într-o limbă engleză săracă și incorectă și se adresa în mod obișnuit unor persoane care dețineau funcții importante în domeniul afacerilor, administrația publică, politică sau alte sectoare cu influență sporită în societate, însă în prezent sunt transmise tuturor. Expeditorul se identifică drept un membru al personalului guvernamental sau al unei companii de stat dintr-un stat african, sau chiar o rudă a unei astfel de persoane.

La început, Nigeria era principala țară de proveniență. Ulterior, expedierea s-a extins și la unele țări din apropierea Nigeriei, iar în ultima vreme acest timp de corespondență vine și din Africa de Sud.

Mesajul constă în propunerea unei afaceri. Expeditorul pretinde că deține o sumă mare de bani

2. FURTUL DE IDENTITATE - ÎNSCENAREA

obținută în virtutea statutului său privilegiat, legat de administrația țării sale.

Prin faptul că spune că nu poate fi asociat public cu această avere având în vedere proveniența acesteia, infractorul justifică necesitatea de a transfera averea în străinătate. Infractorul cere victimei să primească acești bani în contul său personal, pentru un comision de 20% și uneori chiar de 35% din valoarea totală. În acest scop, expeditorul cere datele de cont ale victimei și datele companiei sau organizației din care face parte.

De obicei, aceste elemente nu sunt solicitate din prima scrisoare sau primul e-mail, ci în următoarele, după ce destinatarul a răspuns, acceptând în felul acesta dialogul.

Disponând de datele persoanelor fizice, ale persoanelor juridice și cele legate de conturile bancare, fraudatorii pot comite infracțiuni la scară mondială.

Anunțurile de locuri de muncă din ziare, de pe Internet etc., pot fi false și pot avea doar scopul de a atrage atenția victimelor pentru a obține date care să ajute la comiterea furturilor de identitate. Acestea sunt așa numitele înșelătorii de recrutare, care utilizează și mijloacele tradiționale de obținere a datelor și Internetul.

Este important să menționăm cererile de ajutor trimise pe e-mail sau pe Facebook. "Phishing-ul" realizat pentru a obține acces la contul de e-mail al unei persoane reprezintă o modalitate de a da credibilitate acestor cereri de ajutor – priviți, pentru exemplificare, cazul 5. În același scop, cineva accesează contul de Facebook al unei victime a furtului de identitate. Cererile de ajutor pot fi postate publicate în profilul victimei sau trimis prin intermediul unor mesaje private.

Facebook poate fi utilizat și pentru a obține date privind noi victime ale furtului identității. Prin instalarea de malware pe computere, infractorii publică link-uri pe wall-ul victimei, care redirectionează noua victimă către pagini care îi cer informații personale. Un exemplu ilustrativ pentru astfel de situații este publicarea unui fil video pe pagina unei persoane, iar pentru ca prietenii victimei să poată da like aceștia sunt obligați să introducă o serie de date personale pe o pagină care este controlată de infractor.

Motoarele de căutare, precum Google, care permit căutare pe milioane de pagini în doar câteva secunde, pot fi de asemenea folosite în scopuri ilicite.

2. FURTUL DE IDENTITATE – ÎNSCENAREA

“*Google hacking*” este un termen utilizat pentru a descrie căutările complexe prin intermediul acestor motoare de căutare, cu scopul de a găsi ținte neprotejate și date sensibile pe website-uri. Baza de date *Google Hacking Database* facilitează acest demers. Aceasta este o bază de date care cuprinde căutările prin care sunt identificate datele sensibile. Identifică rapoartele de date (*advisories*) și vulnerabilitățile server-ului, mesajele de eroare care conțin prea multe informații, fișiere care conțin parole, directoare sensibile, pagini care conțin portaluri sau rețele *log-on* sau date vulnerabile precum ecranele de log pentru firewall (*firewall logs*) și în ciuda faptului că *Google* blochează unele dintre cele mai bine cunoscute căutări de hacking pe *Google*, nimic nu poate opri un hacker să spioneze un site și să lanseze căutările de *Google Hacking Database* direct pe conținutul acestuia.

Deseori, muncitorii și angajații întreprinderilor (sau cineva care se pretinde a fi astfel) având acces în companiile în care lucrează la informații secrete de identificare ale managementului sau ale membrilor administrației, ale altor angajați sau clienți ai companiilor, obțin datele acestor entități cu intenția de a comite infracțiuni, deseori intenționând să vândă aceste informații, de cele mai multe ori unor organizații criminale – vezi cazul 1.

Una dintre metodele cele mai obișnuite de a obține date personale pentru a comite furtul identității și care a primit multă atenție din partea autorităților și a presei este așa numitul “*phishing*”.

Această metodă constă în trimiterea unui număr mare de mesaje de e-mail (*spamming*), care conțin un link către o pagină WWW. Această pagină este de obicei o reproducere aproximativă a unei pagini aparținând unei bănci sau unei instituții de credit, de exemplu, și conține elemente de identificare ale entității autentice. Cu toate acestea, este o pagină falsă. Atunci când victima folosește *link-ul* respectiv pentru a intra pe pagina falsă, i se va cere să se identifice prin introducerea unor coduri confidențiale, care conțin contul bancar sau cardul de credit. Aceste date vor permite creatorului paginii să acceseze contul bancar al victimei și să transfere banii existenți către un alt cont sau să utilizeze cardul de credit în avantajul propriu. Studiul de caz 4 reprezintă un exemplu clasic de manifestare a acestui fenomen.

În cazul *phishing-ului*, pot fi identificate patru etape: etapa inițială constă în trimiterea masivă de mesaje e-mail care conțin un link către o pagină web; în a doua etapă, victima trimite propriile informații/parole/coduri de acces autorului infracțiunii – acest moment va consta, în majoritatea cazurilor, în introducerea datelor personale ale victimei pe site-ul fals; în a treia etapă, infractorul intră pe pagina reală a băncii, introduce datele victimei și retrage bani din cont; iar

2. FURTUL DE IDENTITATE – ÎNSCENAREA

a patra etapă constă în spălarea banilor (proces prin care autorii unor activități infracționale ascund originea bunurilor sau a veniturilor obținute pe căi ilegale, transformând lichiditățile provenite din aceste activități în capital care poate fi utilizat legal, fie prin ascunderea originii sau a identității deținătorului adevărat al fondurilor).

În ceea ce privește noile metode de a obține datele private în vederea comiterii unei infracțiuni de furt de identitate, este nevoie să acordăm atenție fenomenului de *pharming*, care este o «tehnică ce folosește metode de diseminare de malware în format *worm* – sub denumirea de worms. Aceasta constă în răspândirea prin *spam* – deci prin e-mail – a fișierelor ascuse, care tot într-un mod ascuns se auto-instalează pe computerul sau sistemele computerizate ale victimelor. Odată instalate, aceste fișiere schimbă – fără cunoștința proprietatului computerului – fișierele de sistem, inclusiv fișierele care conțin bine-cunoscutul «Favorites» și înregistrarea cookies-urilor. Ca urmare a acestei modificări, atunci când proprietarul computerului accesează site-ul obișnuit al băncii, sistemul, modificat în acest mod ingenios, îl redirecționează către un alt website, construit și disponibil online folosind metode identice procedurii numit *phishing*».

O altă tehnică importantă și care trebuie menționată în acest context este cea denumită *sniffing*. Computerele aflate în rețea folosesc aceleași canale de comunicare. Prin canalele comune, computerele pot primi informații transmise către alte computere. Procedul de a capta informația transmisă altor computere se numește *sniffing*.

În fine, să ne referim la *hacking* și *cracking*, ambele fiind accesări ilegale ale sistemelor informatice și, prin urmare, mijloace de a obține informații personale. În acest context, ambii termeni se referă la actul de violare a codurilor de securitate, sau de a obține în mod ilegal coduri de licență ale programelor pentru a obține acces la computerele altor persoane, fără autorizare. Studul de caz nr. 3 descrie o situație în care hacker-ul accesează computerul victimei, preia controlul acestuia și îl face neutilizabil, pentru a cere o recompensă, sau, altfel spus, o sumă de bani ca să rezolve problema pe care a generat-o. Nu avem, în acest caz, de-a face cu un furt al identității prin intermediul internetului, decât dacă hacker-ul a obținut datele Jandiei prin accesarea computerului acesteia.

Procedul denumit *data mining* constă în analizarea datelor, în încercarea de a crea tipare și de a stabili relații între acestea. Această tehnică este utilizată în multe zone de căutare. Există programe computerizate, așa-numitele *data miners*, care colectează, fără permisiune, informațiile disponibile pe internet sau pe computerul victimei, le analizează și creează tipare. Acest lucru

2. FURTUL DE IDENTITATE – ÎNSCENAREA

permite, de exemplu, companiilor, să realizeze proiecții cu privire la comportamentul consumatorilor iar în privința furtului identității face imposibilă organizarea datelor de identitate ale victimei, ca să poată fi folosite de infractor.

În cele din urmă să ne referim la *keylogging*, care constă în utilizarea unui program de calculator – keylogger – care, odată instalat, poate înregistra tot ce se introduce cu ajutorul keyboard-ului. Această metodă îi păcălește până și pe cei mai atenți utilizatori de Internet, cum este Joana, personajul principal din studiul de caz nr. 2.

3.

FURTUL IDENTITĂȚII - REALITATEA PRACTICĂ

[illegible]

3. FURTUL IDENTITĂȚII - REALITATEA PRACTICĂ

3.1. Cele mai uzuale situații de furt de identitate prin intermediul internetului

Realitățile cele mai importante tratate în acest ghid, selectate pentru că sunt cele mai răspândite, sunt cele denumite *phishing*, prin care se obține atât accesul la contul de e-mail al altei persoane (vezi cazul 5) sau la contul bancar (vezi cazul 4) cât și defăimarea persoanei prin intermediul rețelelor sociale (vezi cazurile 6 și 10).

Să analizăm mai întâi *phishing-ul* prin care se obține acces la contul de e-mail. Odată obținute datele personale și sensibile ale victimei, printr-una dintre metodele cele mai sofisticate menționate în capitolul anterior, infractorul poate obține acces la contul de e-mail al victimei și poate vedea conținutul mesajelor, pentru a stabili contactul cu Banca victimei, de obicei cu managerul de cont al victimei, sau poate utiliza acel cont de e-mail pentru a da credibilitate mesajelor pe care intenționează să le trimită și care vor fi, normal, solicitări de ajutor financiar.

Astfel, cele două obiective principale ale *phishing-ului* în vederea accesării unui cont de e-mail sunt: obținerea datelor personale și sensibile ale victimei (prin consultarea conținutului mesajelor și contactarea Băncii) pentru comiterea unei fraude bancare, fie, pur și simplu, pentru a înșela prietenii sau cunoștințele victimei furtului identității, pentru ca aceștia să efectueze transferuri de bani în favoarea infractorului. Observăm, prin urmare, faptul că *phishing-ul* pentru obținerea accesului la contul de e-mail al victimei deseori poate avea ca ultim scop accesul la contul bancar și realizarea unei fraude bancare.

Phishing-ul «tipic» realizat în vederea accesului la contul bancar al victimei, așa cum a fost descris mai sus, este deja, din nefericire, foarte obișnuit în țara noastră.

Într-un alt context, apare furtul identității realizat în vederea defăimării pe rețelele sociale. Acest tip de situație apare frecvent în contextul relațiilor personale, fie prietenie sau o relație de dragoste, cu precădere în rândul tinerilor.

Putem lua în considerare existența a două posibilități pentru furtul identității în vederea defăimării pe o rețea socială: crearea unei pagini sau a unui profil fals cu datele victimei și în numele acesteia și prin fotografii sau fraze care jignitoare (vezi cazul 6) și utilizarea profilului real al victimei pentru a răspândi fapte, judecăți și imagini la fel de jignitoare (vezi cazul 10).

3. FURTUL IDENTITĂȚII - REALITATEA PRACTICĂ

În aceste cazuri, însăși victima este cea care, în contextul unor relații personale apropiate, furnizează datele infractorului, dându-i astfel acces la profilul personal de pe rețeaua de socializare sau la fapte și imagini utilizate pentru a umili victima.

3.2. Infractorul și victima

Este necesar, în acest context, să facem diferența dintre profilul infractorului în cazul furtului identității unde motivația este obținerea unui profit și furtul identității pentru defăimarea pe rețelele sociale.

În încercarea de a construi profilul autorului furtului identității în primul tip de cazuri, este important să facem distincția între autorul care cunoaște victima, fiind un prieten, un membru al familiei sau deoarece are cu victima o relație legitimă și prin urmare, are o mai mare ușurință în a avea acces la informațiile personale ale acesteia și o alege tocmai datorită acestui motiv, pe de o parte, și autorul necunoscut care alege victimele la întâmplare. În ultimele cazuri, este greu de identificat infractorul, deoarece pe lângă faptul că deseori infracțiunile sunt comise de la un alt capăt al globului față de locul în care se află victima, infractorul utilizează totdeauna identitatea victimei, motiv pentru care datele lui personale nu sunt dezvăluite. Din acest motiv nu există mulți infractori cunoscuți ai acestor infracțiuni, de aceea caracteristicile lor rămân necunoscute.

La început, tendința a fost aceea de a ne imagina infractorul cibernetic ca fiind bărbat, student, specialist informatician, cu un IQ peste medie, introvertit și cu aptitudini limitate de interacțiune socială, motivat de provocarea de a învinge mașina și de dorința de a-și demonstra superioritatea intelectuală față de societate.

Cu toate acestea, realitatea a evoluat. Azi, autorul furtului identității prin intermediul Internetului poate fi oricine iar motivația este de a obține datele personale ale victimei și, prin aceasta, de a câștiga un profit și de a avea un beneficiu.

Având în vedere varietatea și numărul mare de mijloace disponibile pentru obținerea datelor potențialelor victime, care ar putea necesita cunoștințe specializate sau doar căutatul prin gu-
noaie, infractorul care comite furtul identității poate fi o persoană care dispune de cunoștințe extinse sau dimpotrivă, cu foarte puține cunoștințe, poate proveni din orice categorie socială și poate avea cele mai diferite caracteristici personale.

3. FURTUL IDENTITĂȚII - REALITATEA PRACTICĂ

Faptul că există mai multe pagini pe WWW care te învață cum să comiți o infracțiune pe computer face ca aceste scheme precum cele despre care am vorbit să fie din ce în ce mai accesibile unor persoane obișnuite care au nevoie de bani.

Totuși, un tip de autor care merită scos în evidență în acest domeniu este *insider-ul*. Vorbim de un angajat cu înaltă calificare, care se bucură de încrederea angajatorului și se folosește de acest avantaj și de cunoștințele pe care le deține despre companie și despre funcționarea și slăbiciunile sistemului computerizat, pentru a obține, a vinde și a utiliza informații privilegiate în scopul săvârșirii de infracțiuni.

Cei mai periculoși infractori în acest tip de infracțiune sunt organizațiile criminale care controlează procesul integral al furtului identității, de la obținerea datelor până la spălarea capitalului.

În ceea ce privește victima, trebuie să fim atenți, pentru că poate fi oricine. Factorul cel mai decisiv în alegerea unei victime de către infractor va fi ușurința cu care va putea obține datele personale. Acest lucru nu înseamnă neapărat că infractorul este cineva apropiat victimei și care are acces la e-mail-ul, la documentele sau computer-ul acesteia, cum ar putea fi un membru al familiei, un prieten sau o altă persoană cu o relație legitimă, deși poate fi, în multe cazuri.

Totuși, în Regatul Unit al Marii Britanii, statisticile arată că cea mai obișnuită țintă a acestor infractori sunt bărbați, cu vârsta cuprinsă între 40 și 50 ani și care au o slujbă. Astfel, infractorii încearcă să fure identitatea persoanelor cu bani fie pentru că vor să fure banii, fie ca să dea credibilitate acțiunilor lor, acelea de a încerca să obțină un credit.

În Statele Unite ale Americii, există o mai mare incidență a actelor de furt al identității în rândul gospodăriilor cu un venit anual care depășește 75,000 dolari și în rândul populației cu vârste cuprinse între 16 și 34 ani.

Deseori, victimele sunt companii, bănci, asigurători sau instituții financiare care preferă să nu raporteze incidentele și să-și rezolve problemele intern, asumându-și pierderile, de teamă ca situația creată să nu conducă la o discreditație a instituției.

În contextul rețelilor sociale, furtul identității se realizează prin intermediul unor persoane care au relații apropiate cu victima și care, dintr-un motiv oarecare, decid să-i facă rău victimei, de exemplu prin crearea unui profil fals defăimător sau prin denigrare pe profilul real al victimei. Acest lucru se va întâmpla deseori în contextul relațiilor dintre foști parteneri care caută să se răzbune.

3. FURTUL IDENTITĂȚII - REALITATEA PRACTICĂ

3.3. Factori de risc

Deoarece victima poate fi oricine, este foarte important să recunoaștem circumstanțele care fac ca utilizatorii de Internet să fie mai vulnerabili și care conduc la creșterea riscului de a deveni o victimă.

Informațiile personale obișnuite ale persoanelor fizice sunt din ce în ce mai accesibile publicului, mai cu seamă prin rețelele sociale și acesta este un aspect de care profită infractorii cibernetici.

Există anumite comportamente ale persoanelor care folosesc rețelele sociale care măresc riscul unui furt al identității, și anume:

- › Neactivarea setărilor de confidențialitate sau păstrarea unui profil foarte accesibil;
- › Împărtășirea multor informații;
- › Acceptarea cererilor de prietenie de la persoane necunoscute;
- › Publicarea de fotografii intime pe rețelele sociale.

Faptul de a lucra mai multe ore online crește de asemenea riscul de a deveni o victimă a infracțiunilor cibernetice, mai ales dacă persoana lucrează de acasă și folosește computerul personal, deoarece, spre deosebire de companii unde angajații lucrează pe computere protejate de tehnicieni angajați, persoanele care lucrează pe cont propriu au computere mai puțin protejate.

Există numeroase comportamente care măresc riscul de a deveni o victimă a infracțiunilor cibernetice, anume:

- › Computerul nu are un program antivirus sau un program antispyware instalat;
- › Click-uri pe link-uri necunoscute;
- › Vizionarea unor fișiere cu conținut destinat adulților;
- › Răspunsuri la mesaje pe rețele sociale, la mesaje de e-mail sau încercări de comunicare pe orice alte căi transmise de persoane necunoscute;
- › Păstrarea în portofel al parolelor sau codurilor PIN sau păstrarea lor în fișiere neprotejate;
- › Comunicarea, chiar și unor persoane de încredere, a parolelor sau codurilor PIN;
- › Utilizarea unor informații ușor accesibile la crearea parolelor, cum ar fi data nașterii, numele mamei sau a animalului de companie;
- › Păstrarea unor documente importante în locuri nesigure;
- › Aruncarea documentelor fără a le distruge mai întâi;

3. FURTUL IDENTITĂȚII - REALITATEA PRACTICĂ

- › Trimiterea de informații confidențiale pe e-mail;
- › Ne-actualizarea antivirus-ului sau a altor programe de protecție instalate pe calculator;
- › Utilizarea conexiunii Wi-Fi.

3.4. Impactul furtului identității

3.4.1. Impactul asupra victimei

Deși oricine poate deveni victimă, există anumite grupuri, cu precădere cele cu venituri mici, minoritățile și persoanele în vârstă, în cazul cărora impactul emoțional, fizic și financiar va fi mai mare, deoarece datorită resurselor economice diminuate, barierelor de limbaj sau problemelor de sănătate, de exemplu, aceste persoane pot avea mai multe dificultăți în raportarea infracțiunii, completarea formularelor, citirea anumitor documente și contactarea și comunicarea cu serviciile destinate sprijinirii victimelor și cu autoritățile. De asemenea, aceste persoane pot întâmpina dificultăți mai mari în ceea ce privește recuperarea în urma pierderilor financiare și a impactului emoțional.

a. IMPACTUL FINANCIAR

Impactul economic poate fi de două feluri: pierderea economică directă, care se referă la suma de bani obținută de infractor prin utilizarea identității victimei, inclusiv valoarea bunurilor sau serviciilor sau valoarea monetară obținută și pierderea economică indirectă, care include toate cheltuielile efectuate de victimă ca urmare a furtului identității (cheltuieli de judecată, telefoane, servicii poștale etc.). Aproximativ 62% din victimele furtului identității pretind că au suferit cel puțin una dintre aceste pierderi economice, conform unui studiu referitor la anii 2006 și 2007.

Costul financiar total al victimelor legat de furtul identității s-a situat la aproximativ 17,3 miliarde de dolari în perioada 2006 și 2007 în SUA și 388 miliarde de dolari în 24 de țări, în anul 2011.

În cazul fraudei bancare sau a cardurilor de credit, băncile deseori preferă să returneze banii victimelor deoarece, de obicei, aceste sume nu sunt foarte importante pentru

3. FURTUL IDENTITĂȚII - REALITATEA PRACTICĂ

aceste instituții și dezvăluirea incidentului ar dăuna reputației instituției. Însă aceste instituții pot avea obligația de a despăgubi victimele.

În Portugalia, jurisprudența Curții de Apel a decis aplicabilitatea art. 796º Codul Civil (CC) – răspunderea față de risc în cadrul contractual – deoarece băncile poartă răspunderea legată de riscurile de defecțiuni ale sistemului sau atacuri cibernetice, atunci când nu pot dovedi că a fost vina victimei și a DL nr. 317/2009 care prevede de asemenea faptul că sarcina probei revine Băncii care trebuie să demonstreze vina victimei pentru a nu plăti despăgubiri. Așadar, instituția bancară are obligația de a demonstra că a fost vina victimei pentru a nu fi obligată să despăgubească victima pentru daunele suferite.

Victima își poate pierde casa și toate economiile. Victima țintită a unei scheme de înșelătorie prin folosirea conturilor de credit poate să aibă probleme în obținerea unui credit nou sau în constituirea unei ipoteci.

b. IMPACTUL JURIDIC

Victima ar putea fi acuzată și urmărită penal pentru infracțiuni pe care nu le-a comis (vezi cazul 7) și poate deveni pârât într-un proces de răspundere civilă, pentru daune pe care nu le-a provocat, sau într-un proces de răspundere contractuală, pentru obligații pe care nu și le-a asumat.

c. IMPACTUL EMOȚIONAL

Deși efectele psihologice pot fi diferite de la o persoană la alta, în funcție de caracteristicile victimei, există o serie de simptome obișnuite printre care se numără: teama, anxietatea, furia sau o lipsă de încredere permanentă și prelungită față de orice și oricine, o stare pe care multe victime o descriu ca «paranoia». Impactul emoțional al furtului identității este descris ca fiind similar cu reacția victimelor unor infracțiuni săvârșite cu violență. Multe persoane își simt intimitatea violată, se simt neputincioase, neajutorate și se tem că infracțiunea se poate repeta.

Nesiguranța generată de pierderea stabilității financiare are un impact foarte puternic

3. FURTUL IDENTITĂȚII - REALITATEA PRACTICĂ

asupra acestor victime. Ca și nevoia de a-și demonstra nevinovăția, ca în studiul de caz 7.

Multe victime se învinovătesc pentru ceea ce s-a întâmplat, se întreabă oare în cine mai pot avea încredere și dacă se va face vreodată dreptate.

Victimele furtului de identitate pe Internet și ale infracțiunilor cibernetice în general pot simți să sunt tratate ca victime “de mâna a doua”, meritând mai puțin sprijin decât celelalte victime, deoarece aceste infracțiuni sunt încă sub-evaluate din punct de vedere social și există puține servicii care ajută aceste victime să-și recapete echilibrul. Aceste victime trebuie de asemenea să știe cum să trăiască cu dezamăgirea faptului că – așa cum se întâmplă în multe cazuri – este imposibil de identificat “hoțul” de identitate. Importanța acestui fapt nu trebuie subestimată, deoarece de fiecare dată când victima se confruntă cu noi datorii sau consecințe ale infracțiunii, este ca și cum ar deveni din nou victimă (re-victimizare).

Efectele infracțiunii sunt diferite atunci când infractorul este o persoană apropiată victimei. În aceste situații victimele pot simți presiunea de a-și asuma responsabilitatea pentru infracțiunea respectivă, pentru a proteja infractorul de consecințe. Victimele ar putea fi reticente în a raporta infracțiunea autorităților polițienești, în cazul în care descoperă că infractorul este cineva apropiat în care au avut încredere, cum ar fi o rudă sau un prieten. De asemenea, este posibil să se simtă rușinați pentru că au fost păcăliți.

d. IMPACTUL ASUPRA RUTINEI ZILNICE

Furtul identității implică o neplăcere serioasă și o mare pierdere de timp atunci când victima intenționează să repare consecințele acestuia. În SUA, conform estimărilor, timpul pe care îl petrec victimele pentru a repara daunele cauzate de infracțiune este de 97 ore, cheltuind, to în medie, 1884 dolari (date furnizate de organizația americană *Identity Theft Resource Center*). În Regatul Unit, victima petrece între 3 și 48 ore pentru a-și “spăla reputația”.

40% dintre victime au declarat că pierderea acestui timp a fost cea mai rea consecință a acestei infracțiuni.

3. FURTUL IDENTITĂȚII - REALITATEA PRACTICĂ

3.4.2. În societate

În Regatul Unit al Marii Britanii, costul pe care economia țării îl plătește ca urmare a infracțiunii furtului identității a fost estimat la 1,3 miliarde de lire pe an. În Australia, pierderile anuale variază între 1 miliard de dolari și peste 3 miliarde de dolari. În Statele Unite, în cursul anului 2005, s-a estimat că pierderile au fost de 5,5 miliarde de dolari. În districtul Lisabona, daunele cauzate de *phishing* în anul 2011 au depășit 2 milioane Euro.

Furtul identității are un cost din ce în ce mai mare pentru instituții precum Băncile, companiile de asigurări și companiile furnizoare de bunuri și servicii. Aceste instituții pot fi obligate să suporte pierderea economică a victimei, cu excepția cazului în care pot demonstra că totul s-a petrecut din neglijența acesteia. Acest impact asupra instituțiilor nu trebuie neglijat deoarece, chiar și dacă nu ar mai exista alt motiv, acesta se va reflecta în cele din urmă asupra costurilor pe care consumatorul va trebui să le suporte pentru a beneficia de serviciile companiilor respective.

Chiar și identitatea unei companii poate fi utilizată fără permisiunea acesteia, iar în acest caz pierderile indirecte vor fi legate de căutările în rândul angajaților, miza pe prevenire și obținerea asigurării.

De asemenea, nu ar trebui subestimată discreditația care poate afecta aceste companii, datorită impactului asupra sistemului economic.

Statele și Guvernele lor pot suferi pierderi directe, atunci când furtul identității se petrece în legătură cu entitățile publice, dar pierderile suferite sunt mai ales indirecte, deoarece trebuie să se axeze pe prevenire, instruire și obținerea resurselor și mijloacelor de care au nevoie poliția și autoritățile judiciare.

3.5. Dificultăți de investigare

Furtul identității pe Internet și infracțiunea cibernetică în general pun probleme serioase atât poliției cât și autorităților judiciare în ceea ce privește investigația. Caracteristicile infracțiunii în sine, precum și alți factori legați de aceasta, fac identificarea autorului actelor și definirea circumstanțelor infracțiunii foarte greu și uneori chiar imposibil de realizat.

3. FURTUL IDENTITĂȚII - REALITATEA PRACTICĂ

Furtul identității are o dimensiune internațională, trans-frontalieră, ca și infracțiunea cibernetică în general și Internetul. Dacă infractorul și victima nu se află în aceeași țară, investigația va fi împiedicată deoarece, pe lângă faptul că ar trebui urmărită o pistă cibernetică, potențial la nivel internațional, este nevoie și de cooperarea poliției și a autorităților judiciare din țările implicate. Principiul suveranității nu permite unei țări să efectueze investigații pe teritoriul altei țări fără permisiunea autorităților locale. Cooperarea dintre autoritățile din diferite țări presupune formalități și timp, care subminează investigațiile.

Se poate spune că infracțiunea cibernetică este atemporală, deoarece între actul inițial al autorului și producerea rezultatului poate exista o perioadă de timp nedefinită, care de asemenea nu facilitează investigarea.

Multe dintre procesele pe care infracțiunea cibernetică le presupune pot fi automatizate (atenție la *spamming*) și programate să se repete, astfel conferind infracțiunii un caracter de permanență.

Infractorii folosesc tehnologii care le permit să rămână aninimi, cum ar fi *spoofing* sau alte programe de anonimat sau încriptare.

Gradul mare de tehnicitate pe care îl presupune investigarea în cazul unei infracțiuni cibernetice necesită implicarea unor entități diverse, care dispun de experiența specifică, precum și utilizarea multor resurse interne, atât de ordin logistic cât și umane, resurse care sunt limitate.

Pe lângă aceste caracteristici specifice, există alți factori care nu favorizează investigarea unei infracțiuni cibernetice în general.

Conform estimărilor, 80% din victimele infracțiunii cibernetice nu raportează autorităților. Acest fapt decurge din lipsa conștientizării statutului de victimă și din lipsa informării cu privire la modalitățile de raportare, dar și din neîncrederea în eficiența investigațiilor poliției sau credința că aceste infracțiuni nu pot fi pedepsite. Un alt motiv pentru care victimele nu raportează este rușinea de a fi fost înșelate.

Companiile, băncile, companiile de asigurări și instituțiile financiare aleg să rezolve problema intern, prin absorbirea pierderilor și neformularea unei plângeri către autorități, de teamă că odată adus la cunoștința publicului, un atac cibernetic ar putea conduce la discreditare și la pierderea încrederii, atât din partea piețelor cât și din partea clienților.

3. FURTUL IDENTITĂȚII - REALITATEA PRACTICĂ

Numărul victimelor crește pe zi ce trece, odată cu creșterea numărului utilizatorilor de Internet.

Există pagini online care conțin informații despre cum pot fi comise anumite infracțiuni prin intermediul computerului și aceste pagini pot fi accesate foarte simplu prin utilizarea celor mai populare motoare de căutare.

În fiecare zi, infractorii creează noi modalități de a accesa datele personale ale persoanelor și de a comite infracțiuni prin folosirea acestora. Noile tehnici se răspândesc rapid prin intermediul pieței negre online.

Un obstacol uriaș în calea investigării infracțiunilor cibernetice este dificultatea serioasă care există în accesarea probelor electronice. Pentru a localiza sursa comunicării, cu alte cuvinte, adresa IP (sau *Internet Protocol Address*), este necesară accesarea registrului fișierelor istorice arhivate de providerii de servicii de Internet, a căror cooperare este esențială.

Este de asemenea foarte importantă asigurarea viabilității probelor digitale. Astfel, accesul la aceste probe, colectarea, conservarea și analiza lor trebuie să se facă totdeauna prin aplicarea procedurilor specifice și de specialiști. Este necesară colectarea cât mai rapidă a probelor, deoarece acestea pot fi distruse foarte ușor. Pentru ca acest lucru să fie realizabil, este esențială cooperarea cu providerii serviciilor de internet, care au obligația de a reține anumite date pe anumite perioade, limitate, de timp.

4.

CADRUL LEGISLATIV

[illegible]

4. CADRUL LEGISLATIV

Implementarea legislației corespunzătoare joacă un rol esențial în prevenirea și combaterea infracțiunilor de tip cibernetic.

Existența acestui cadru este importantă în contextul unei tendințe de creștere a comportamentului infracțional, ca și aptitudinile și competența de investigare a autorităților polițienești, colectarea și păstrarea probelor electronice, jurisdicția, cooperarea și împărtășirea informațiilor, atât între diferite entități naționale cât și cu cele internaționale și responsabilizarea providerilor de servicii de internet.

Deși la nivel național, statele manifestă tendința de a se concentra mai mult pe creșterea caracterului infracțional al comportamentelor, iar nevoia de a elabora o legislație care să acopere și alte chestiuni începe să fie recunoscută.

4.1. Cadrul internațional

Ultimii ani au scos la iveală o preocupare serioasă la nivel internațional față de combaterea infracțiunilor cibernetice. Se remarcă în acest sens, activitatea Consiliului European, a Uniunii Europene și Națiunilor Unite.

Convenția Consiliului European privind Infracțiunile Cibernetice (ECCC) din 23 noiembrie 2001 este instrumentul internațional cel mai răspândit care se utilizează pentru elaborarea legislațiilor naționale privind infracțiunea cibernetică.

ECCC, confruntată cu informatizarea mondială și riscul noilor tehnologii și a Internetului folosite ca mijloc de înlăptuire a infracțiunilor, își propune să implementeze o politică comună care vizează infracțiunile de acest tip și să protejeze societatea de infracțiunea cibernetică, prin adoptarea unei legislații armonizate și prin promovarea cooperării internaționale. Vom aborda în cele ce urmează o serie de infracțiuni vizate de acest instrument internațional (acces ilegal, interceptare ilegală, interferența datelor, interferența sistemelor, folosirea abuzivă a dispozitivelor, falsificarea prin intermediul computerului, fraudele realizate prin intermediul computerului, infracțiuni legate de pornografia infantilă și de încălcări ale drepturilor de autor și ale drepturilor conexe) precum și aspecte legate de aplicarea acestuia în diferite etape ale furtul identității realizat prin intermediul internetului, așa cum a fost definit în acest document. De asemenea, ECCC stabilește norme de cooperare internațională și procedurale din care se inspiră legislația portugheză.

4. CADRUL LEGISLATIV

În contextul Uniunii Europene, se remarcă decizia cadru 2005/222/JHA care privește atacurile asupra sistemelor informatice și Directiva Parlamentului European și a Consiliului European, care a înlocuit primul act legislativ.

Decizia cadru 2005/222/JHA a avut drept scop îmbunătățirea cooperării dintre autoritățile polițienești și judiciare ale Statelor Membre și armonizarea standardelor privind infracțiunea cibernetică.

Directiva Parlamentului European și a Consiliului European 2013/40/EU a fost adoptată, așa cum am evidențiat, pentru a înlocui decizia cadru și prevede ca obiectiv principal «armonizarea legislației penale ale Statelor Membre în domeniul atacurilor asupra sistemelor informatice prin setabilirea unui set minim de reguli privind definirea infracțiunilor penale și sancțiunile aplicabile și îmbunătățirea cooperării dintre autoritățile competente (...)» Directiva prevede ca infracțiuni accesul ilegal, interferența ilegală cu sistemele, interferența ilegală a datelor și interceptarea ilegală și sancționează și utilizarea dispozitivelor în scopuri infracționale.

4.2. Legea romana

Cadrul este dat de Legea 161/2003 titlul III privind combaterea criminalitatii informatice, Legea 365/2002 privind comertul electronic si Codul Penal si Codul de Procedura Penala.

Articol și denumire	Conduțas
Art. 325 - Falsul informatic	Fapta de a introduce, modifica sau șterge, fără drept, date in-formatice ori de a restricționa, fără drept, accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice.
Art. 362 - Alte-rarea integrității datelor informatice	Fapta de a modifica, șterge sau deteriora date informatice ori de a restricționa accesul la aceste date, fără drept.
Art. 363 - Per-turbarea funcți-onării sistemelor informatice	Fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modifi-carea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la date informatice.

4. CADRUL LEGISLATIV

|||||

4. CADRUL LEGISLATIV

Art. 302 - Violarea secretului corespondenței	1) Deschiderea, sustragerea, distrugerea sau reținerea, fără drept, a unei corespondențe adresate altuia precum și divulgarea fără drept a conținutului unei asemenea corespondențe, chiar atunci când aceasta a fost trimisă deschisă ori a fost deschisă din greșeală. (2) Interceptarea, fără drept, a unei convorbiri sau a unei comunicări efectuate prin telefon sau prin orice mijloc electronic de comunicații. (3) Faptele prevăzute în alin. (1) și alin. (2) au fost săvârșite de un funcționar public care are obligația legală de a respecta secretul profesional și confidențialitatea informațiilor la care are acces. (4) Divulgarea, difuzarea, prezentarea sau transmiterea, către o altă persoană sau către public, fără drept, a conținutului unei convorbiri sau comunicări interceptate, chiar în cazul în care făptuitorul a luat cunoștință de aceasta din greșeală sau din întâmplare. (5) Nu constituie infracțiune fapta săvârșită: a) dacă făptuitorul surprinde săvârșirea unei infracțiuni sau contribuie la dovedirea săvârșirii unei infracțiuni; b) dacă surprinde fapte de interes public, care au semnificație pentru viața comunității și a căror divulgare prezintă avantaje publice mai mari decât prejudiciul produs persoanei vătămate. (6) Acțiunea penală se pune în mișcare la plângerea prealabilă a persoanei vătămate.
Art. 228 - Furtul	(1) Luarea unui bun mobil din posesia sau detenția altuia, fără consimțământul acestuia, în scopul de a și-l însuși pe nedrept. (2) Fapta constituie furt și dacă bunul aparține în întregime sau în parte făptuitorului, dar în momentul săvârșirii acel bun se găsea în posesia sau detenția legitimă a altei persoane. (3) Se consideră bunuri mobile și înscrisurile, energia electrică, precum și orice alt fel de energie care are valoare economică.
Art. 249 - Frauda informatică	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.

5.

LEGISLATIA NATIONALA APLICATA STUDIILOR DE CAZ

[illegible]

5. LEGISLAȚIA NAȚIONALĂ APLICATĂ STUDIILOR DE CAZ

< Cazul 1 >

În cazul lui Josué se aplică prevederile referitoare la infracțiunea de acces ilegal iar pentru actele organizației infracționale se aplică prevederile pentru infracțiunea de fraudă informatică Art. 360, 249 CP

< Cazul 2 >

În cazul Joanei, privitor la utilizarea *keylogging*-ului pentru obținerea datelor de acces ale contului bancar, se aplică infracțiunea de interceptare ilegală dar cu referire la utilizarea datelor obținute pentru a intra pe cont *online* pentru a retrage banii se aplică infracțiunea de acces ilegal precum și cea de înșelăciunea prin intermediul computerului Art. 360, 249 CP

< Cazul 3 >

Cazul 3 nu constituie o situație de furt al identității, decât dacă infractorul a obținut datele Jandirei. Infracțiunile de acces ilegal Art. 360 intervenția asupra datelor Art. 362 intervenția și intervenția în sistem Art. 363 se aplică în această situație așa cum a fost descrisă, precum și cea de amenințare, stabilită de Art. 206

< Cazul 4 >

În acest caz de *phishing* este aplicabil falsul în documente Art. 322 pentru crearea unui cont fals de e-mail, tipul juridic de fals realizat pe computer Art. 325 pentru crearea unei pagini *www* false, infracțiunea de acces ilegal Art. 360 pentru accesarea contului online al Josefinei și înșelăciunea prin intermediul computerului Art. 249 pentru transferul de bani din contul acesteia în alt cont.

5. LEGISLAȚIA NAȚIONALĂ APLICATĂ STUDIILOR DE CAZ

< Cazul 5 >

Spamming-ul se pedepsește pentru infracțiunea de intervenție asupra sistemului Art. 363. Pentru crearea unui cont fals de e-mail se aplică prevederile referitoare la infracțiunea de fals în documente (Art. 322 iar pentru accesarea contului de e-mail se aplică prevederile referitoare la infracțiunea de acces ilegal Art. 360. Avem de-a face, de asemenea, cu tentativa de escrocherie prin intermediul computerului Art 249.

< Cazul 6 >

Faptele incriminate sunt cele ce privesc crearea unui cont fals de Facebook, se aplică prevederile referitoare la infracțiunea de fals informatic Art. 325.

< Cazul 7 >

În cazul Joanei se aplică prevederile referitoare la infracțiunea de fraudă prin intermediul computerului Art. 249

< Cazul 8 >

Julietta a fost victima unei escrocherii realizate prin intermediul computerului Art. 24

< Caso 9 >

Pentru crearea unui cont fals de e-mail se aplică prevederile referitoare la falsul în documente Art. 322 iar pentru accesarea contului de e-mail al soției lui Julio se aplică accesul ilegal Art. 360. Avem de-a face, de asemenea, cu tentativa de fraudă informatica Art. 249.

5. LEGISLAȚIA NAȚIONALĂ APLICATĂ STUDIILOR DE CAZ

< Cazul 10 >

Jaime, în posesia informațiilor necesare de a intra în contul de Facebook al lui Jair, a intrat pe acest cont și a publicat fotografii care fuseseră făcute în viața privată a lui Jair, fără acordul acestuia. Infracțiunile aplicabile în acest caz aici sunt accesul ilegal Art. 360, violarea intimității prin intermediul computerului Art. 226

6.

PREVENIRE

[illegible]

6. PREVENIRE

Conform unui studiu al Comisiei Europene din anul 2012, 70% din populația studiată a auzit deja sau a văzut informații referitoare la o infracțiune cibernetică, 31% din aceștia se consideră destul de bine informați cu privire la riscul de infracțiune cibernetică și 7% se consideră foarte bine informați.

Un alt studiu, axat pe 13.000 de utilizatori de Internet din 24 de țări, a arătat că 90% din această populație șterge e-mailurile suspecte primite de la expeditori necunoscuți, 80% utilizează anti-virus și nu deschid fișiere atașate sau link-uri care apar în e-mailuri sau mesaje de la expeditori necunoscuți.

Totuși, în ceea ce privește rețelele sociale, doar 50% au pretins că utilizează opțiunile de setare a confidențialității oferite pentru a controla informațiile pe care le postează și cine vede informațiile pe care le postează și 35% din populația studiată acceptă cereri de prietenie de la persoane necunoscute.

Studiile privind copiii și adolescenții din țările mai puțin dezvoltate arată că această categorie de vârstă prezintă riscuri mai mari de a deveni victime. Un studiu realizat în rândul unei populații de peste 25.000 de copii la vârsta școlară din 7 țări din America de Sud și Centrală a arătat că din 45% din copiii care aveau acasă conexiune la Internet doar 10% aveau protecție anti-virus sau filtrare web pe computer.

Statele trebuie să folosească resursele de care dispun pentru a educa populația înainte ca cetățenii să devină victime. Instruirea comunităților cu privire la metodele de protejare împotriva furtului identității este cea mai eficace măsură de luptă împotriva acestui fenomen.

6.1. Măsuri de prevenire

Atunci când utilizează rețelele sociale, utilizatorul trebuie:

- › Să fie atent la informațiile publicate pe rețelele sociale: informațiile care îl pot face vulnerabil nu ar trebui să fie postate;
- › Să fie atent la informațiile pe care alții le publică despre persoana sa;
- › Să aleagă cu atenție persoanele cărora le oferă acces la informațiile private;
- › Să fie atenți la persoane necunoscute;
- › Să fie sceptic și să nu creadă în orice aude sau citește online;
- › Să cunoască toate condițiile pe care le acceptă atunci când accesează o rețea socială, care deseori presupun pierderea drepturilor asupra conținutului postat.

6. PREVENIRE

Atunci când utilizează e-mail-ul, utilizatorului trebuie:

- › Să nu uite faptul că e-mailurile scrise într-o portugheză necorespunzătoare, cu greșeli gramaticale și de ortografie, fraze incoerente sau chiar cuvinte combinate în portugheză și braziliană cel mai probabil fac parte dintr-o schemă de *phishing*, chiar dacă provin de la un expeditor cunoscut;
- › Să știe acest lucru este valabil în special pentru e-mailurile care anunță câștigarea unui premiu sau care îl informează pe utilizator că este finalist într-un concurs, sau că are o problemă cu propriul cont de e-mail sau că este nevoie să-și valideze datele bancare sau de sistem;
- › Să nu descarce fișiere atașate, să nu facă «click» pe link-urile afișate și să nu răspundă la e-mailurile venite din partea unor persoane străine sau e-mailuri cu un conținut dubios;
- › Să facă un efort de recunoaștere a adresei de e-mail atunci când primesc e-mailuri de la o bancă sau orice altă instituție cu care lucrează;
- › În cazul în care nu recunoaște adresa de e-mail, utilizatorul va contacta instituția și va verifica dacă într-adevăr e-mailul a fost trimis de acolo;
- › Să treacă mouse-ul peste orice link pentru a-l încărca și a verifica astfel în colțul din stânga jos al browser-ului la ce adresă este redirecționat de link-ul respectiv;
- › În cazul în care domeniul link-ului este extern domeniului entității care se presupune că a trimis e-mailul, utilizatorul se va abține de la accesarea lui;
- › Dacă are dubii, să acceseze site-ul <https://www.virustotal.com/pt/#url> sau prin contact suport al entității care se presupune că a expedit e-mailul sau accesați site-ul www.cert.pt și contactați echipa CERT;
- › În cazul în care primește un e-mail neobișnuit de la o persoană cunoscută, care cere ajutor sau date personale, utilizatorul trebuie să fie suspicios deoarece contul respectiv de e-mail se poate să fi fost compromis;
- › Să evite folosirea contului de e-mail al companiei în scop personal;
- › Să nu folosească e-mailul pentru a transmite informații confidențiale;
- › Să actualizeze constant programul utilizat pentru transmiterea e-mailurilor;
- › Închideți opțiunile care permit deschiderea sau afișarea automată a fișierelor sau programelor atașate mesajelor;
- › Închideți opțiunile de executare *Java programs* sau *JavaScript*.

Pentru a-și proteja computerul și dispozitivele mobile, utilizatorul trebuie:

- › Să evite să creeze situații favorabile furtului de computere, telefoane mobile și tablete,

6. PREVENIRE

lasându-le, de exemplu, în mașină;

- › Să-și protejeze computerul de utilizatori răuvoitori, preîn crearea unei parole pentru logarea în sesiunea de lucru atunci când computerul nu a mai fost utilizat;
- › Atunci când împrumută computerul, să nu uite de datele personale pe care acesta le poate conține, având în vedere faptul că datele păstrate pe hard disk pot fi accesate, chiar dacă sunt păstrate într-un fișier protejat cu o parolă;
- › Atunci când vinde sau aruncă un computer, un telefon mobil sau o tabletă, să șteargă toate informațiile personale pe care acestea le pot conține;
- › Să actualizeze permanent programele antivirus, antispyware, firewall și protecție antispam;
- › Să configureze browser-ul utilizat pentru a preveni stocarea de cookies și pop-ups;
- › Să ridice nivelul de securitate al browser-ului la mediu sau mare;
- › Să fie atent la programele instalate, să verifice proveniența acestora – trebuie să provină de la compania care le-a creat sau de la un website fiabil;
- › Să evite să se logheze pe website-uri care postează informațiile personale pe rețele publice sau rețele deschise Wi-Fi, sau pe computere necunoscute;
- › Să fie în mod special atenți la website-uri unde se furnizează date personale, mai ales site-urile bancare – să evite site-urile cu greșeli evidente de ortografie sau de tipar și fără instrucțiuni de siguranță;
- › Să verifice totdeauna conectarea la un website care trebuie să se facă prin «https» - safe mode – și nu «http» - unsafe mode; mai mult, să verifice dacă apare un icon care reprezintă un dispozitiv de securitate sau o cheie;
- › Să folosească doar website-ul oficial al băncii pe care o folosește;
- › Să citească instrucțiunile de confidențialitate ale site-urilor instituțiilor financiare sau altele care presupun dezvăluirea datelor personale, iar dacă nu le înțelege sau nu le acceptă, să ia în considerare alte instituții;
- › La dispozitivele mobile, protecția ecranului trebuie să fie activată;
- › Să activeze opțiunea de ștergere a datelor de la distanță, dacă sunt informații sensibile stocate pe dispozitiv;
- › Să facă backup la conținutul dispozitivelor în mod periodic și să-l păstreze cu atenție (să salveze copii într-un format încriptat cu o parolă bună).
- › Atunci când instalează aplicații pe dispozitiv, să verifice dacă descărcarea se face de pe o sursă sigură și fiabilă și să aibă grijă la permisiunile cerute – de exemplu, dacă o aplicație care nu ar trebui să ceară acces la e-mail face acest lucru, utilizatorul ar trebui să opteze pentru o altă alternativă.

6. PREVENIRE

Pentru a proteja documentele de identitate și datele personale, utilizatorul trebuie:

- › Să poarte în portofel doar documentele necesare zi de zi;
- › Să țină portofelul într-un loc sigur atunci când este la birou;
- › Să țină documentele într-un loc sigur în casă, de exemplu un seif;
- › Să distrugă documentele fizice sau digitale vechi care pot conține date personale sau alte informații similare, pentru a le face imposibil de utilizat;
- › Atunci când comandă cecuri noi, să ceară ca acestea să fie trimise la poștă și nu acasă;
- › Să aibă puține informații personale tipărite pe cecuri;
- › Să verifice legitimitatea celor care solicită informații personale prin telefon, e-mail sau orice alte mijloace și motivul acestei cereri:
 - » Solicitați apelantului să se identifice și să furnizeze un contact al entității pe care se presupune că o reprezintă și să verifice dacă există posibilitatea să nu furnizeze datele imediat și să revină ulterior pentru a face acest lucru;
 - » Încercați să înțelegeți ceea ce are nevoie să afle persoana care vă contactează: instituția financiară cu care lucrați poate dori să știe numele dinainte de căsătorie al mamei pentru a verifica identitatea atunci sunați pentru a afla informații despre cont; totuși dacă cineva sună sau trimite un e-mail pentru a afla numele mamei dinainte de căsătorie, pretizând că aparține de instituția financiară cu care o persoană lucrează, această persoană, respectiv utilizatorul, trebuie să-și amintească faptul că apelantul nu are nevoie de această informație deoarece această informație se află deja în dosar – scopul unui astfel de apel telefonic sau e-mail va fi pur și simplu de a afla această informație în interesul propriu;
 - » Dacă un străin apelează sau transmite utilizatorului un e-mail prin care acesta din urmă este informat că a câștigat un premiu sau un alt tip de beneficiu și este solicitat să dea informații personale, utilizatorul trebuie să ceară apelantului sau expeditorului să trimită un formular de cerere scrisă; dacă nu face acest lucru, utilizatorul trebuie să stopeze contactul; dacă trimite acest formular, utilizatorul trebuie să citească acest formular cu atenție și să se asigure, atunci când transmite datele personale, că transmite aceste date unei companii sau instituții financiare cunoscute și cu o bună reputație.
- › În cazul în care călătorește, pentru a furniza informații personale cuiva care este de încredere, să se asigure că nu este nimeni în jur care poate auzi;

6. PREVENIRE

- › Să informeze firmele sau instituțiile financiare să nu dezvăluie datele personale;
- › Să păstreze informațiile importante în fișiere sau directoare protejate prin parole;
- › Să încrîpeze datele de importanță critică.

Atunci când folosește un serviciu poștal, utilizatorul trebuie:

- › Să încerce să protejeze inviolabilitatea cutiei poștale prin utilizarea unei încuietori corespunzătoare;
- › Să nu permită corespondenței să se acumuleze în așa fel încât să poată fi sustrasă prin deschiderea de intrare;
- › Când călătorește, să solicite să-i fie reținută corespondența și să fie păstrată la cel mai apropiat oficiu poștal, sau să solicite unei rude, unui prieten sau unui vecin în care are încredere să preia și să păstreze corespondența;
- › Să încerce să controleze sosirea scrisorilor așteptate, care conțin carduri de debit sau de credit, extrase de cont sau facturi;
- › Dacă este posibil, să preia și să trimită personal scrisorile care conțin informații sau documente personale, direct la oficiul poștal;
- › Să împiedice emiterea corespondenței la adresele unde nu mai locuiește și să solicite oficiului poștal redirectionarea acestora la adresa actuală.

Pentru a efectua tranzacții financiare sigure, utilizatorul trebuie:

- › Să efectueze tranzacții financiare sigure, doar prin intermediul unor website-uri sigure cu adrese care încep cu "https:" în plus, să verifice dacă apare un icon care reprezintă un dispozitiv de siguranță sau o cheie;
- › Să verifice dacă folosește website-ul oficial al băncii cu care lucrează;
- › Să nu uite că pentru a efectua operațiuni online băncile nu cer niciodată mai mult decât o mică parte din cifrele (de obicei trei) care apar pe cardul de credit;
- › Să nu uite că băncile nu solicită instalarea de aplicații pe telefonul mobil pentru a mări gradul de securitate al operațiunilor – aceste aplicații sunt de obicei malware;
- › În cazul în care există dubii, să contacteze banca prin telefon;
- › Să actualizeze permanent aplicații precum *Java* și *Flash*;
- › Să protejeze toate conturile de credit cu parole.

6. PREVENIRE

Pentru a folosi Instant Messengers, IRC și Chats online în siguranță, utilizatorul trebuie:

- › Să folosească un nume fals care nu permite identificarea sa;
- › Să folosească facilități care au moderator (se aplică doar pentru chat);
- › Să păstreze secretul informațiilor personale;
- › Să înregistreze sesiunile de chat;
- › Să nu deschidă fișiere de email atașate în conversațiile chat.

Pentru a crea parole sigure, utilizatorul trebuie:

- › Să evite folosirea unor secvențe predictibile atunci când creează o parolă;
- › De asemenea, să evite să creeze parole cu taste care sunt apropiate pe tastatură; pe lângă faptul că sunt cunoscute, aceste parole sunt ușor de identificat la momentul introducerii;
- › Atunci când creează o parolă să nu folosească elemente personale asociate cu persoana sa sau cu persoane cunoscute, cum ar fi data de naștere, părți din nume sau prenume, adresă, codul de identificare al contribuabilului;
- › Să utilizeze parole cu lungimea maximă permisă și să fie atenți să nu alcătuiască cuvinte care există în dicționarul portughez sau în orice altă limbă;
- › Să combine litere, cifre și simboluri care nu sunt consecutive;
- › Să fie creativ (de exemplu să conceapă un enunț cu un anumit înțeles și să folosească prima literă a fiecărui cuvânt în alcătuirea parolei);
- › Să combine litere mari cu litere mici și să înlocuiască literele cu cifre sau simboluri;
- › Să seteze parole diferite pentru fiecare serviciu (dacă este nevoie să le notați undeva, le notați într-un loc sigur și nu într-un fișier pe computer);
- › Schimbați parolele periodic.

NOTĂ: Părinții sau persoanele care au în îngrijire minori ar trebui să monitorizeze activitățile online ale copiilor sau adolescenților, asigurându-se că aceștia folosesc măsurile de precauție menționate.

6. PREVENIRE

6.2. Semne ale infectării cu malware

Probabilitatea de a deveni o victimă a furtului identității crește dacă un computer a fost infectat cu un malware. Astfel, este important să cunoaștem simptomele infectării cu malware:

- › Lentoare;
- › Blocaje frecvente;
- › Apariția de mesaje pop-up, imagini, sunete ciudate sau aplicații instalate fără permisiune;
- › Închiderea spontană a mecanismelor de protecție, precum anti-virusul;
- › Inabilitatea sistemului de a recunoaște vocalele accentuate;
- › Activitate constantă și inexplicabilă cu conectare la internet;
- › Schimbarea paginii de primire sau a motorului favorit de căutare;
- › Redirecționarea permanentă către pagini neobișnuite pe internet;
- › Apariția unor noi preferințe în toolbars din browser;
- › Publicarea de comentarii pe rețelele sociale;
- › Stabilirea de conversații pe Instant Messaging (*Skype, Google Talk, etc.*);
- › Mesaje privind neprimirea unor e-mailuri pe care utilizatorului nu le recunoaște ca fiind transmise de el;
- › Apariția icon-ului de *Java* icon în taskbar, fără ca utilizatorul să ruleze vreo aplicație în baza acestei tehnologii.

6.3. Cum putem identifica semnele furtului identității

Efectele furtului identității pot fi mult mai dăunătoare dacă nu sunt depistate cât mai repede posibil. De aceea, pentru a limita efectele, este important ca utilizatorul să fie vigilent și conștient de semnele care îi spun că este victima unui furt de identitate. Să vedem, aşadar, unele dintre strategiile de depistare a acestui fenomen în timp util.

Pentru a depista furtul identității la timp, utilizatorul trebuie:

- › Să fie atent în permanență pentru a observa orice activitate neobișnuită pe contul de e-mail sau pe profilurile rețelelor sociale;
- › Să țină permanent sub observație toate conturile – conturile bancare, conturile de

6. PREVENIRE

investiții și de carduri de credit:

- › Să verifice dacă primește lunar extrasele de cont în care sunt evidențiate ultimele operațiuni efectuate;
- › Să fie caute cu atenție orice operațiuni pe care nu le-a efectuat personal;
- › Să verifice periodic raportul de credit pentru a vedea dacă există dovezi ale unor activități anormale;
- › Să se aboneze la alertele de activitate pe care le oferă companiile financiare;
- › Să cerceteze orice refuz primit la o cerere de credit – poate fi un semn că s-a produs un furt de identitate și a avut loc o folosire necorespunzătoare a contului;
- › Să contacteze instituția financiară dacă nu primește facturile lunare;
- › Dacă utilizatorul primește informația că facturile îi sunt transmise la o altă adresă, trebuie să informeze reprezentantul instituției de faptul că nu a autorizat vreo schimbare de adresă și că altcineva ar putea folosi contul respectiv; în această situație, este esențial să cereți copii ale facturilor și o listă a operațiunilor realizate de la ultima factură.

7.

ASISTENȚĂ PENTRU VICTIME

[illegible]

7. ASISTENȚĂ PENTRU VICTIME

7.1. Infectarea cu malware

În cazul unei infectări cu malware, utilizatorul trebuie:

- › Să deconecteze computerul de la rețea pentru a nu infecta alte computere (dacă se aplică);
- › Să curețe computerul: acest lucru poate presupune reinstalarea întregului sistem și se poate face de către un specialist sau chiar de victimă dacă aceasta din urmă cunoaște procedurile;
- › Să opteze pentru dezinfectare, să ruleze programul de cleanup în “safe mode” sau de pe un CD sau flash drive cu un anti-virus de pe un computer sigur;
- › Să schimbe toate parolele.

7.2. Furtul identității

Atunci când este victima unui furt de identitate pe internet, utilizatorul trebuie să cunoască modalitățile prin care poate limita efectele infracțiunii și să reducă impactul asupra vieții sale personale, sociale și financiare.

În cazul furtului identității, utilizatorul trebuie:

- › Să contacteze imediat instituția financiară cu care lucrează;
- › Să anuleze toate cardurile de credit și debit, să solicite emiterea altor carduri și să schimbe toate codurile PIN dacă există posibilitatea ca infractorul să fi avut acces la conturile respective sau la alte date confidențiale;
- › Să anuleze conturile la care infractorul a avut acces sau pe care a intrat;
- › Să anuleze accesul prin homebanking și să ceară noi coduri în dacă există posibilitatea ca infractorul să fi avut acces la acest serviciu;
- › Să solicite instituției financiare să pună la dispoziție formularele necesare pentru a putea demonstra faptul că actul infracțional a fost comis de utilizator;
- › În absența formularelor specifice, victima ar trebui să transmită o scrisoare la adresa indicată de serviciul suport al instituției;
- › Să discute cu banca despre posibilitatea de a i se restitui banii;
- › Să solicite băncii toate extrasele de cont de credit sau debit și să caute erori sau operațiuni pe care nu le-a efectuat, apoi să informeze instituția dacă descoperă o problemă

7. ASISTENȚĂ PENTRU VICTIME

- și să conteste acțiunile infractorului;
- › În cazul în care descoperă erori, utilizatorul ar trebui să solicite instituției să lanseze o alertă de fraudă a cardului de credit;
- › Să solicite instituției financiare să împiedice ca datele conținute în raportul de credit să fie făcute publice;
- › După ce s-a produs furtul identității, utilizatorul va citi cu atenție rapoartele cardului de credit în anii care urmează;
- › Să verifice dacă există obligații de credit asumate în numele său la “Banco de Portugal” – Registrul Central de Credit;
- › Să raporteze infracțiunea la biroul procurorului general sau la poliție;
- › Să transmită instituției financiare raportul plângerii;
- › Să solicite un cazier judiciar și să verifice dacă informațiile conținute sunt corecte;
- › Să schimbe parola contului de e-mail dacă există posibilitatea ca infractorul să fi avut acces la acesta;
- › Să anuleze documentele de identitate la care a avut acces infractorul;
- › Să anunțe furnizorii de servicii cu care lucrează, oficiul poștal din apropierea locuinței, sistemul de asigurări sociale și autoritatea de conducere despre furtul identității;
- › Să atenționeze angajatorii că a fost victima unui furt al identității în cazul în care întâlnesc informații incorecte despre utilizator;
- › Să salveze e-mailurile, SMS-urile, scrisorile sau alte comunicări dintre utilizator și suspect sau dintre utilizator și instituțiile financiare, care pot fi folosite ca dovezi, dacă este nevoie.

În cazul furtului identității în vederea defăimării pe Facebook, utilizatorul trebuie:

1. Dacă infractorul creează un profil fals al victimei pentru a publica un conținut defăimător, victima va proceda după cum urmează, folosind rețeaua Facebook:
 - › Raportarea contului - pentru a face acest lucru:
 - » Click pe opțiunea “...” lângă butonul “Mesaj” în colțul din dreapta sus pe profilul contului;
 - » Vor apărea patru opțiuni și se va selecta opțiunea “Raportare”;
 - » Selectarea opțiunii “Raportarea acestui cont”;
 - » Mesajul “Care este problema cu acest cont?” va fi afișat; în acest moment utilizatorul va face click pe opțiunea “Acest timeline pretinde a fi persoana mea sau o persoană cunoscută mie”;

7. ASISTENȚĂ PENTRU VICTIME

- » Va apărea pe ecran întrebarea “Cine pretind că sunt?”, la care victima trebuie să facă click pe “Eu”;
- » Va apărea acest mesaj “Pe baza selectărilor dvs., iată câteva lucruri pe care le puteți face” iar utilizatorul trebuie să selecteze opțiunea “Supuneți spre analiză de către Facebook”;
- » În fine, utilizatorul va face click pe opțiunea “Terminat”.

› Pentru raportarea unui conținut publicat, victima trebuie să facă următoarele:

- » Click pe săgeata întoarsă din colțul dreapta sus al unei postări și selectarea opțiunii “I don’t like this post”.

2. Dacă infractorul creează o pagină falsă pe numele victimei pentru a posta un conținut defăimător:

› Pentru raportarea paginii și a conținutului postat, victima trebuie să facă următoarele:

- » Click pe opțiunea “...” lângă butonul “Mesaj” în colțul din dreapta sus pe profilul contului;
- » Vor apărea cinci opțiuni iar victima va selecta opțiunea “Raportează pagină”;
- » Apoi, victima va selecta opțiunea “mă deranjează pe mine sau pe cineva cunoscut”;
- » Va apărea apoi mesajul “Ne pare rău că a trebuit să treceți prin această experiență. Iată câteva lucruri pe care le puteți încerca pentru a rezolva situația”; selectați atunci opțiunea “Supuneți spre analiză de către Facebook”;
- » În fine, click pe opțiunea “Terminat”.

3. În cazul în care infractorul a utilizat profilul real al victimei pentru a publica un conținut defăimător:

› Schimbați parola de acces; pentru a face acest lucru, victima va proceda după cum urmează:

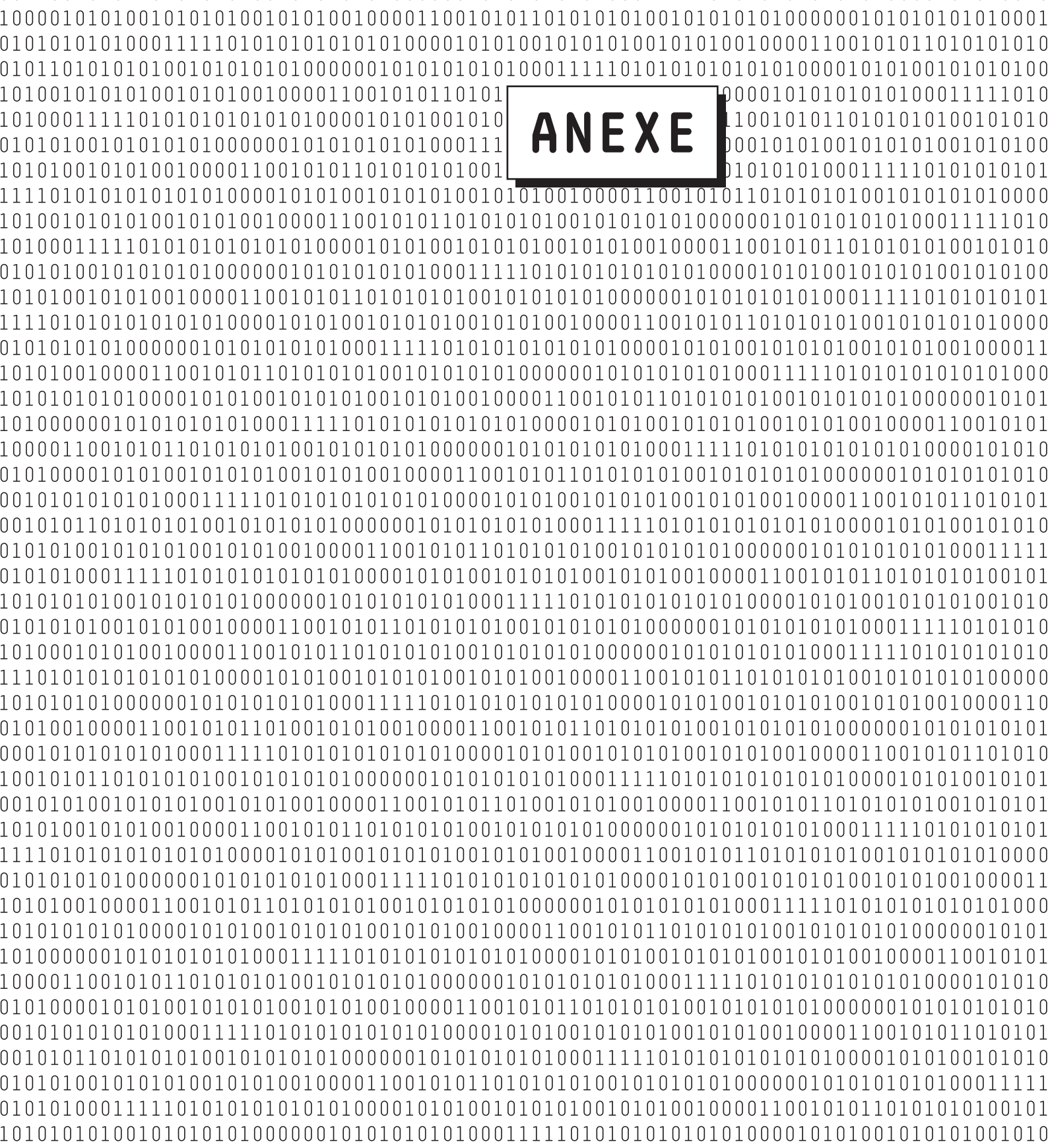
- » Apăsați icon-ul cu un dispozitiv de siguranță din colțul dreapta sus al barei albastre din partea de sus a paginii;
- » Selectați apoi opțiunea “Mai multe setări”;
- » Ulterior, victima va face click pe opțiunea “General” din colțul stânga sus al paginii care apare;
- » Apoi, va apărea pe ecran «Setări generale ale contului» iar pe opțiunea “Parolă”

7. ASISTENȚĂ PENTRU VICTIME

- victima trebuie să facă click pe “Editare”;
 - » Ulterior, victima trebuie să introducă vechea parolă și apoi să introducă parola nouă de două ori;
 - » Victima va selecta apoi opțiunea “Salvează schimbările”;
 - » Va apărea următorul mesaj: «Parola dvs. a fost modificată. Vă delogați din alte dispozitive?» iar victima trebuie să facă click pe opțiunea «Deloghează-mă din alte dispozitive»;
 - » În fine, victima va face click pe “Transmite”.
- › Pentru a șterge un conținut postat, victima va proceda astfel:
 - » Click pe săgeata întoarsă din colțul dreapta sus al unei postări și selectarea opțiunii “Ștergere”;
 - » Apoi, va apărea următorul mesaj “Ești sigur că vrei să ștergi?” iar victima va selecta din nou opțiunea “Ștergere”.

4. În orice situație:

- › Trebuie blocat infractorul, în așa fel încât acesta să nu mai aibă acces la postările victimei, ca și toți ceilalți utilizatori de Facebook care sunt deranjați. Pentru a face acest lucru, victima va proceda astfel:
 - » Click pe opțiunea “...”, lângă “Mesaj”, în colțul din dreapta sus al profilului utilizatorului pe care dorește să-l blocheze;
 - » Vor apărea patru opțiuni și va fi selectată opțiunea “Blocare”;
 - » Va apărea atunci mesajul “Ești sigur că vrei să blochezi ...?” iar victima va selecta opțiunea “Confirmare”.
- › Plângere la biroul procurorului general sau la poliție.



[illegible]

ANEXE

Glosar

Bots e botnets – Expresia *bot* este o formă presurtată de la *robot*. Infractorii distribuie un *malicious software* (*malware*) care poate transforma computerul utilizatorului într-un *bot* (robot) sau zombie, deoarece poate fi de asemenea denumit. Atunci când se întâmplă acest lucru, computerul poate rula sarcini automate pe internet, fără cunoștința utilizatorului respectiv. Infractorii folosesc aceste computere *bots* pentru a infecta un mare număr de computere. Aceste computere formează o rețea sau *botnet*. Infractorii utilizează un *botnet* pentru a trimite spam-uri, a împrăștiia programe de virus, a ataca alte computere și servere și pentru a comite alte tipuri de infracțiuni și fraude. Dacă un computer devine parte a unui astfel de *botnet*, computerul respectiv devine mai lent iar utilizatorul său poate ajuta neintenționat infractorii.

Browser – Un program pentru accesarea Internetului, care vine deja prin definiție pe computer;

Chat – Conversație online;

Cookies – Un *cookie* este un fișier creat de un website pentru a stoca informațiile pe computerul utilizatorului, inclusiv preferințele acestuia la vizitarea site-ului respectiv. Atunci când intră pe un site care utilizează *cookies*, site-ul poate cere browser-ului instalat pe computer să plaseze unul sau mai multe *cookies* pe hard drive. Ulterior, la întoarcerea pe site-ul respectiv, browser-ul va trimite acele *cookies* care aparțin site-ului respectiv. Acest lucru permite site-ului să prezinte informații personalizate pe nevoile utilizatorilor săi. Acestea sunt *cookies* pe care website-urile le creează pentru ca utilizatorul să nu fie nevoit să introducă o parolă de exemplu când accesează site-ul respectiv pentru a doua oară. Alte site-uri folosesc *cookies* pentru a stoca preferințele utilizatorului.

Date computerizate – Orice reprezentare a faptelor, informațiilor sau conceptelor într-o formă care permite prelucrarea într-un sistem computerizat, inclusiv un program potrivit pentru a cauza realizarea unei funcții de către un sistem; definiția “sistem computerizat” conform ECCC acoperă toate formele de tehnologie care depășesc cadrul tradițional sau sistemele computerizate de tip desktop, cum sunt telefoanele mobile moderne, telefoanele mobile inteligente, PDA-urile, tabletele, altele similare.

Sistem computerizat – Orice dispozitiv sau grup de dispozitive relaționate sau interconectate care, conform unui program, realizează prelucrarea automată a datelor;

Download – Transfer de conținut de pe Internet pe echipamentul utilizatorului;

E-mail – Mesaj transmis prin intermediul poștei electronice;

Flash – Fișiere generate de Adobe Flash Player care este un tip de software utilizat pentru crearea de animații interactive;

Java – Limbaj de programare;

Link – Link la un website;

Login – Proces prin care accesul la un sistem computerizat este controlat prin identificarea și autentificarea utilizatorului, folosind informațiile de autorizare furnizate de respectivul utilizator;

ANEXE

Malware – Prescurtare de la “*malicious software*”; este un software care are scopul de infiltrare ilegală într-un sistem computerizat nerelaționat, cu intenția de a produce daune, modificări sau de a sustrage informații (confidențiale sau nu). Programe gen *virus*, *worms* și *spyware* sunt considerate a fi *malware*.

Pop-ups – O fereastră suplimentară care se deschide pe browser atunci când este accesată o pagină web sau la deschiderea unei anumite conexiuni.

Remote wipe – O caracteristică de securitate care permite unui administrator de rețea sau deținătorului unui dispozitiv să transmită o comandă către un dispozitiv computerizat și să șteargă date;

Provider de servicii – Orice entitate publică sau privată care furnizează utilizatorilor serviciilor sale abilitatea de a comunica prin intermediul unui sistem computerizat, precum și orice altă entitate care prelucrează sau stochează date computerizate în numele acestui serviciu de comunicare sau utilizatorilor acestui serviciu.

Spoofing – Un atac *spoofing* este o situație în care o persoană sau un program reușește să treacă drept altcineva prin falsificarea datelor și obținând astfel un avantaj ilegal.

Spyware – Program computerizat automat care colectează informații despre utilizator și obiceiurile sale pe Internet și le transmite către o entitate străină de pe Internet, fără cunoștința și permisiunea utilizatorului. Pe de altă parte, un spyware poate fi dezvoltat de companiile care doresc să monitorizeze obiceiurile utilizatorilor și să facă publicitate în mod customizat, cu scopu de a-și vinde mai bine produsele pe Internet. De asemenea, multe virusuri poartă spyware care intenționează să sustragă date confidențiale ale utilizatorilor, cum ar fi datele bancare.

Date de trafic – Orice date computerizate legate de comunicare prin intermediul unui sistem computerizat, generate de o un sistem computerizat care a făcut parte dintr-un lanț de comunicare, indicând originea comunicării, destinația, ruta, ora, data, dimensiunea, durata sau tipul serviciului care se află la baza acestuia.

Website/Site – Amplasare / loc pe Internet sau pagină web;

Wi-fi – Conexiune wireless la internet;

World Wide Web/WWW/Web – Un sistem de documente hypermedia conectate care sunt interconectate și rulează pe Internet.

[illegible]

[illegible]







