

PROTEUS

JUHENDMATERJAL

INTERNETIS

TOIME

PANDUD

ERINEVATE

IDENTITEEDIVARGUSE

VORMIDEGA

TEGELEMISEKS

PROTEUS

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

APAV[®]
associação portuguesa de
apoio à vítima

[illegible]

ISBN	Sundeksemplarid
978-972-8852-70-2	

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

Pealkiri

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

Kirjanik
2015 © APAV
Associação Portuguesa de Apoio à Vítima

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

SISUKORD

SISSEJUHATUS	5	3.4.2. Ühiskonnale	35
1. JUHTUMID	9	3.5. Menetluslikud raskused	35
< Juhtum 1 >	11	4. JURIIDILINE RAAMISTIK	37
< Juhtum 2 >	11	4.1. Rahvusvaheline tasand	39
< Juhtum 3 >	12	4.2. Eesti seadusandlus	40
< Juhtum 4 >	12	4.3. Identiteedivargus, seadusandlus ja	45
< Juhtum 5 >	13	Küberkuritegevuse konventsioon	
< Juhtum 6 >	13	5. JUHTUMITE LAHENDAMISEKS KASUTATUD SEADUSED	47
< Juhtum 7 >	13	< Juhtum 1 >	49
< Juhtum 8 >	14	< Juhtum 2 >	49
< Juhtum 9 >	14	< Juhtum 3 >	49
< Juhtum 10 >	14	< Juhtum 4 >	50
2. IDENTITEEDIVARGUS	15	< Juhtum 5 >	50
2.1. Küberkuritegevus	17	< Juhtum 6 >	50
2.1.1. Globaliseerumine	17	< Juhtum 7 >	50
2.1.2. Küberkuritegevuse defineerimine	17	< Juhtum 8 >	50
2.2. Identiteedivargus	19	< Juhtum 9 >	51
2.2.1. Terminoloogilised raskused	19	< Juhtum 10 >	51
2.2.2. Defineerimine	20	6. ENNETUS	53
2.3. <i>Modi operandi</i>	21	6.1. Ennetusmeetmed	55
3. IDENTITEEDIVARGUS - REAALSUS	27	6.2. Märgid pahavaraga nakatumisest	60
3.1. Tavapärasemaid internetipõhiseid	29	6.3. Kuidas saada aru, et olete sattunud	60
identiteedivargusi		identiteedivarguse ohvriks?	
3.2. Ohver ja teo toimepanija	30	7. OHVRI TOETAMINE	63
3.3. Riskifaktorid	31	7.1. Pahavaraga nakatumisel	65
3.4. Identiteedivarguse tagajärjed	32	7.2. Identiteedivarguse korral	65
3.4.1. Ohvrile	32	LISAD	69
a. MAJANDUSLIKUD	33	Sõnaseletusi	71
b. ÕIGUSLIKUD	33	Pankade jt seotud asutuste kontaktid	73
c. EMOTSIONAALSED	33		
d. IGAPÄEVARUTIINILE	34		



SISSEJUHATUS

[illegible]

SISSEJUHATUS

2013. aastal toimunud uuringu tulemusena, milles osales 13 022 isikut vanuses 18 - 64 eluaastat 24 erinevast riigist, jõuti järeldusele, et küberkuritegevuse ohvriks langeb igal aastal 378 miljonit inimest, 1 miljon ohvrit päevas ja 12 ohvrit sekundis¹.

Inimeste arv, kes langeb interneti abil ja e-maili kontode kaudu identiteediga seotud süütegude ohvriks, varieerub 1%-st 17%-ni 21-s erinevas riigis maailmas. Samal ajal satub varguste ohvriks samades riikides 1-5% rahvastikust².

Küberkuritegevuse ohvrid on aga eriti haavatavas seisus ning on alakaitstud. Kuna tegemist on võrdlemisi uue kuritegevuse haruga, on teadmised sellest väga üldised ning selle tagajärjed on alahinnatud nii defineerimise, seadusandluse kui ka menetluse seisukohalt.

Internetipõhiste identiteedivarguste juhtumid võivad olla väga keerukad, mistõttu ohvrid vajavad personaalset tuge oma tasakaalu taastamiseks. Sageli on vaja abi ka nakatunud seadme käsitlemisel, mida ohver enam ise ei kontrolli.

Internetis toimepandavate süütegude hulk kasvab pidevalt ja seega kasvab ka politseisse pöördumiste ning ohvrite hulk, mis omakorda tekitab vajaduse parandada toe ja abi andmist.

Nimetatud põhjusel on valminud ka käesolev juhendmaterjal, mis keskendub eriliselt internetipõhiste identiteedivarguste erinevatele vormidele ning toetab ohvreid abistavaid organisatsioone ning teiste valdkondade spetsialiste abistades neil toimuvat mõista ning ohvrite informeerimiseks ja toetamiseks parimal võimalikul moel.

1 Norton Cyber-crime Report, 2013.

2 United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime - Draft*, February 2013, p.3.

1.

JUHTUMID

[illegible]

1. JUHTUMID

< Juhtum 1 >

Teet on 50-aastane politseinik. Ühel ilusal suvepäeval läks ta kauplusesse, et soetada puhkuse jaoks tarvilikke varusid. Kassa juurde jõudes pakkus kassiir talle võimalust omandada kliendikaart, millel olid ka krediitkaardi võimalused. Liikmestaatusega kaasnenuks 20% allahindlus just neile kaupadele, mille Teet oli välja valinud ning muid kohustusi ei kaasnenu ja seega leidis Teet, et tegemist on väga soodsa tehinguga. Kuu peale ülalkirjeldatud poodlemist sai Teet arve, mis oli igati korrektne - tema poolt tehtud tehing ning maha arvestatud 20%. Ta maksis arve ning ei kasutanud kaarti enam. Kaks aastat hiljem aga tabas Teetu suur üllatus, kui ta sai 6000€ suuruse arve. Arve järgi oli ta võlgu tundmatule kindlustusfirmale sõidukikindlustuse eest, kusjuures Teet oli viimased 20 aastat kasutanud kogu aeg ühte ja sama kindlustusfirmat.

< Juhtum 2 >

Kreete on 32-aastane konsultant rahvusvahelises ettevõttes. Ta on kasutanud oma tööarvutit üle 10 aasta. Ettevõtte IT osakond on vastutav arvutite korrasoleku eest ning Kreetel pole iial enne olnud probleeme arvutiga seotud turvalisusega. Kreete ise tunneb, et ta on üsna hästi kursis küberkuritegevuse ohtudega ning on kasutusele võtnud abinõud arvuti kaitsmiseks. Näiteks ei teosta ta ostusid interneti teel, et mitte avaldada oma krediitkaardi andmeid, perekonna ja sõpradega vahetab ta teateid ja e-maile ainult oma isikliku arvuti abil, samuti teostab ta selle abil isiklikke otsinguid ning teeb pangatehinguid. Ühel päeval, kui Kreete on lugenud artiklit küberkuritegevuse kasvu kohta, otsustas ta uurida, milline on parim antiviiirus ning see oma isiklikku arvutisse ka soetada. Selleks kasutas ta populaarset otsingumootorit ning leidis paljude hulgast ka kahtlase lehekülje, mis pakkus väidetavalt võimsat kaitset viiruste eest. Ta otsustas seda mitte installeerida, kuna ta teadis, et alla

1. JUHTUMID

tohib laadida tarkvara ainult usaldusväärsetest allikatest. Sel õhtul teostas Kreete internetipanga abil ka mõned ülekanded. Kaks nädalat hiljem kontrollis Kreete oma kontojääki ning avastas, et tema arvel ei olnud enam peaaegu üldse raha.

< Juhtum 3 >

36-aastane abiõpetaja Heli ostis oma esimese arvuti 3 aastat tagasi ning talle meeldib sõpradega e-kirju vahetada ja hoida end kursis viimaste moeuudistega. Ta kasutab selleks tuntud otsingumootorit. Tal on ka kaks last - 6- ja 8-aastased, kes kasutavad samuti sama arvutit.

Viimase kuu jooksul on muutunud Heli arvuti nii aeglaseks, et nii Heli kui ka tema lapsed on sootuks loobunud selle kasutamisest. Eelmisel esmaspäeval sai Heli ReidosHackers'i nimeliselt saatjalt e-kirja milles öeldi, et tema arvuti on üle võetud ning nõuti 600€, et ta saaks omaenda arvuti taas enda kasutusse.

< Juhtum 4 >

Leili on kogu oma eelneva elu kokana töötanud 65-aastane naine, kes naudib auga välja teenitud pensionipõlve. Ta sai oma vanimalt pojalt jõuludeks arvuti.

Talle meeldib väga vahetada e-kirju oma sõpradega, kellest osad elavad ka välismaal.

Ühel päeval, kui ta parasjagu kontrollis oma e-posti lootuses, et on saanud oma Soomes elavalt sugulaselt kirja, leidis ta eest e-kirja oma pangalt milles sooviti, et ta klikiks e-kirjas olnud lingil ning täidaks avaneva vormi. Leili otsis kohe üles oma pangaga seotud dokumendid ning täitis ankeedi viivitamatult, kuna rahaasjadega ei tohi ju venitada.

Kuu hiljem võttis temaga ühendust kliendihaldur pangast, kuna pangale oli silma jäänud, et suur summa oli Leili arvelt kantud tundmatule arvele ning tehingut otsustati kontrollida võttes naisega ühendust.

1. JUHTUMID

< Juhtum 5 >

Tõnu on 45-aastane õpetaja, kelle käest hakkasid hiljuti töökaaslased ja sõbrad uurima, mis tema elus toimub, sest ta on saatnud neile e-kirju, milles palub rahalist abi.

< Juhtum 6 >

17-aastane Joel kohtus samas koolis õppiva 15-aastase Eliisega ning armus temasse jäägitult. Ta otsustas võita Eliise südame kingituste ja muude tähelepanuavaldustega ning see tal ka õnnestus. Nende suhe kestis 5 kuud, kuid siis muutus Eliise eemalolevaks ning ütles lõpuks Joelile, et ei armasta teda enam. Joel vihastas ning teatas Eliisele, et ta ei leia enam kunagi kedagi ning et ta veel kahetseb seda, et Joeli maha jättis. Eliise ei muretsenud Joeli poolt öeldu pärast.

Kahe päeva pärast, kui Eliise oli kooli jõudnud, tundis Eliise, et tema klassikaaslased vaatasid teda imelikult, sosis-tasid omavahel ja naersid. Klassi jõudes küsis ta oma pinginaabrilt Erikalt, kas tema teab, mis toimub? Erika vastas, et Facebook'is on Eliise nime ja pildiga konto, kus ta kuulutab, et on huvitatud seksist raha eest.

< Juhtum 7 >

22-aastane majandustudeng Marten õppis ühel juunikuu hommikul nädala pärast toimuvaks statistikaeksamiks. Kui ta uksekella helina peale ukse avas, sai ta postiljonilt kutse 2 päeva pärast toimuvale kahtlustatavana ülekuulamisele seoses kelmusega.

1. JUHTUMID

< Juhtum 8 >

Mare, 50-aastane lasteaiaõpetaja, oli just väljunud bussist, kui sai kõne kelleltki, kes väitis end olevat SEB panga esindaja ning, et tal on vaja kontrollida mõningaid Mare andmeid. Kahe kuu pärast sai Mare krediitkaardi arve võõralt pangalt, mille klient ta pole kunagi olnudki.

< Juhtum 9 >

Aare on 39-aastane arst, kellega võtsid paar päeva enne teise lapse sündi ühendust kahe krediitdiasutuse esindajad küsimaks, kas tema taotlused on ikka kehtivad. Aare, kes polnud kunagi elus laenu võtnud, eitas taotluste esitamist. Teda üllatas, kui palju isiklikku infot kelmid tema kohta olid omanud. Taotlused tühistati. Kuu hiljem pöördus Aare oma panga poole sooviga võtta eluaseme-laenu seoses suurenenud perega. Laenust keelduti, kuna Aare oli väidetavalt eelnevatel kuudel teinud hulgaliselt laenutaotlusi.

< Juhtum 10 >

Gerdo on 16-aastane 11. klassi õpilane, kes on olnud kooli-kiusamise ohver alates ajast, mil ta kooli läks. Tema koolikaaslased teevad tema üle nalja seetõttu, et ta on häbelik, hea õpilane ning saab hästi läbi Priiduga, kelle üle õpilased samuti naeravad, kuna ta olevat naiselik.

Ühel päeval tuli Gerdo koolist koju ning logis end oma Facebook'i kontole sisse lootuses vestelda mõne inimesega oma sõbralis-tist, keda ta polnud kunagi kohanud ning kes võtsid teda sel-lisena nagu ta oli. Tema süda aga pidi peaaegu seisma jääma, sest ajajoonel oli mitu fotot temast aluspesus koos tekstiga "Kas ma pole mitte kuum?"

Gerdot valdas meeleheide, kui talle meenus, et ainus inimene, kes teadis tema Facebook'i salasõna ja kasutajatunnust, oli Priit.

2.

IDENTITEEDIVARGUS

[illegible]

2. IDENTITEEDIVARGUS

2.1. Küberkuritegevus

2.1.1. Globaliseerumine

2011. aastal omas ligipääsu internetile vähemalt 2,3 miljardit inimest ehk rohkem, kui 1/3 maa-
kera elanikkonnast. on ennustatud, et aastaks 2020 on igal inimesel kuus võrguga ühenduses
olevat seadet. See on ka põhjus, miks tänapäeva kuritegevus nõ toitub internetist.

Info- ja kommunikatsioonitehnoloogia (IKT) abil leitakse hulgaliselt uusi mooduseid kuritegu-
de toimepanemiseks. Interneti levik ja uute tehnoloogiate kasutamine aitavad kaasa erinevate
kuriteoliikide levikuks.

IKT vahendid võimaldavad kuritegudel globaliseeruda. See tähendab, et autor saab kerge vae-
vaga panna toime kuriteo Brasiilias portugallase vastu ning see juhtubki tavaliselt andmepüügi
juhtumite puhul, mis oli kirjeldatud juhtumis 4.

Seega küberkuritegevus kasvab - sealhulgas läbi sotsiaalsete võrgustike – ning seda panevad
toime kas kuritegelikud ühendused või üksikud kurjategijad, kes otsivad võimalusi saada kasu
või muid hüvesid.

2.1.2. Küberkuritegevuse defineerimine

Küberkuritegevuse definitsiooni osas ei ole ühtset seisukohta. Erinevate riikide ja rahvusvaheli-
ne seadusandlus ei ole suutnud kehtestada teemaüleseid ühtseid seisukohti.

ÜRO Uimastite ja Kuritegevuse Büroo kohaselt sõltuvad küberkuritegevuse erinevad mõisted
sellest, millist nähtust üritatakse defineerida.

Sama asutus proovib kirjeldada mõistet läbi selle alla kuuluvate tegevuste. Kirjeldatud on neli-
teist tegevust, mis on omakorda jagatud kolme kategooriasse:

2. IDENTITEEDIVARGUS

Konfidentsiaalsuse, väär- kuse, arvutisüsteemide ja info vastu suunatud teod	Arvuti abil toime pan- dud teod saamaks isik- likku või ainelist infot	Arvuti abil toime pandud teod saamaks kuritegelikku kasu
> Ebaseaduslik sisene- mine arvutisüsteemi; > Ebaseaduslik juur- depääs andmetele või andmete omandamine; > Ebaseaduslik arvuti- süsteemi või andmetesse sekkumine; > Arvutite väärkasuta- miseks mõeldud vahendi- te omamine, levitamine või tootmine; > Andmete kaitse va- hendite või privaatsuse rikkumine.	> Kelmus või informaa- tika pettus; > Identiteediga seo- tud süüteod, millised on toime pandud arvuti vahendusel; > Arvuti vahendusel toime pandud süüteod autoriõiguse ja kauba- märkide suhtes; > Rämpsposti saatmi- ne või selle saatmise kontrollimine; > Arvuti vahendusel toime pandud teod, mis põhjus- tavad isiklikku kahju; > Laste seksuaalne väärkohtlemine (nn groo- ming ja meelitamine).	> Arvuti vahendusel vaenule õhutamine; > Lapsporno tootmine, levitamine või omamine; > Terroriaktide soorita- mine arvuti vahendusel.

Suhtluses Euroopa Parlamendiga defineerib Euroopa Nõukogu küberkuritegevust kui “kriminaalkorras karistatavaid tegevusi, mis on toime pandud kasutades elektroonilisi suhtlusvõrgustikke ja infosüsteeme, või seesuguste süsteemide vastu”.

Tundub, et seesugune lähenemine annab üsna hea ülevaate käesolevast teemaderingist. Laiem konseptsioon hõlmab kõiki kuritegusid, mis võivad olla toime pandud elektrooniliste vahendite abil. Kitsamas väljenduses võetakse arvesse ainult süüteod, milles digitaalne komponent on osa kuri- või väärteost.

2. IDENTITEEDIVARGUS

2.2. Identiteedivargus

2.2.1. Terminoloogilised raskused

Väljendi „identiteet“ ümber on palju segadust ja seega tuleb juba alguses öelda, et käesoleva juhendmaterjali kontekstis viitame antud väljendi puhul ühe inimese isiklikule infole mida kasutab teine isik selleks, et panna toime kuritegusid.

Väljend „identiteedivargus“ - olenemata sellest, et on valitud käesolevasse juhendmaterjalis kasutatavaks - ei defineeri korrektselt fenomeni. Tegelikult ei ole päris õige ükski väljend, mida tavaliselt käesolevas kontekstis kasutatakse.

Tõsi on see, et tutvustavates juhtumites viitame sellele, et kurjategija peab pääsema ligi isikliku informatsioonile või salasõnadele või nt koodikaartidele selleks, et kuritegu toime panna.

Erinevate riikide seadusandluses on kasutusel erinevad väljendid. Näiteks on Ameerika Ühendriikides kasutusel väljend *identity theft* samal ajal, kui Ühendatud Kuningriigis kasutatakse väljendit *identity fraud*. Eesti Vabariigi seadusandluses on kasutusel väljend “teise isiku identiteedi ebaseaduslik kasutamine”. Karistusseadustik § 157 sätestab, et teist isikut tuvastavate või tuvastada võimaldavate isikuandmete tema nõusolekuta edastamise, nende juurdepääsu võimaldamise või nende kasutamise eest eesmärgiga luua teise isikuna esinemise teel temast teadvalt ebaõige ettekujutus, kui sellega on tekitatud kahju teise isiku seadusega kaitstud õigustele või huvidele, või varjata kuritegu – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

Ühendatud Kuningriigis prooviti piiritleda väljendi tähendust. Võimalusena kaaluti võtta peamise väljendina kasutusele “identiteedivargus”, sest “identiteedipettus” ei anna asja olemusest piisavat ülevaadet ning väljend “identiteedirööv” ei sobi seetõttu, et mõiste rööv on seotud vägivallaga, mida antud kuritegude puhul ei esine.

Seega paistab siiski olevat sobivaim väljend “identiteedivargus”, sest kirjeldab kõige paremini nimetatud nähtust ning selle erinevaid väljendusvorme.

2. IDENTITEEDIVARGUS

2.2.2. Defineerimine

Käesoleval juhul on defineerimisega sarnane lugu nagu eelmises peatükis küberkuritegevusele ühtse mõiste leidmisega. Proovime defineerida nähtust nii, et see sobituks käesoleva juhendmaterjali mõttega.

Alustuseks tuleb toonitada, et identiteedivargus ei ole sugugi mitte igas riigis kriminaalkorras karistatav tegu. Näiteks Portugalis ei ole identiteedivargus iseenesest kuritegu, kuid kriminaaliseeritavad on mõningad selle tulemuseni viivad nn alltegevused.

Ameerika Ühendriikide Föderalse Kaubanduskomisjoni kohaselt on identiteedivargusena käsitletav selline tegu, kus keegi kasutab ilma vastavate volitusteta kellegi teise isiklikku infot selleks, et panna toime kelmusi ja teisi kuritegusid.

Euroopa Komisjoni juurde kuuluva ekspertgrupi hinnangul on fenomeni tuumaks kellegi isikliku informatsiooni kasutamine selleks, et panna toime kuritegusid.

Euroopa Nõukogu majanduskuritegude divisjoni seisukoht on, et väljend “identiteedivargus” kirjeldab tegevusi, milles teo toimepanija saavutab valedel alustel kontrolli teiste isikute identiteedi üle. Seesugused teod saab toime panna ka ilma tehnikavahenditeta, kuid samuti arvuti vahendusel.

Riigiti eristatakse identiteedivargust keskendudes näiteks rohkem tegevusele, mis kulub info hankimisele samal ajal, kui teised pööravad rohkem rõhku tegevuse eesmärgile, mis omakorda viib ebaseaduslike tagajärgedeni.

Erinevate defineeringute ühine element on see, et kirjeldatud tegevused hõlmavad ühte või enamat kolmest faasist – faas, milles hangitakse ohvri kohta isiklikku informatsiooni, faas, milles omatakse ja edastatakse saadud informatsioon (teades, et seda kasutatakse ära kuriteo toimepanemiseks) ja kolmandas faasis kasutatakse informatsiooni kuriteo/kuritegude toimepanemiseks.

Selleks, et formuleerida võimalikult laiapõhjaline definitsioon, saab öelda, et identiteedivargus hõlmab ohvri kohta isikliku ja/või salajase informatsiooni hankimist, selle omamist või edastamist kuritegelikul eesmärgil ning info kasutamist kuritegude toimepanemiseks.

Kuna käesolev juhendmaterjal viitab interneti teel toime pandud identiteedivargustele on rõ-

2. IDENTITEEDIVARGUS

huasetus sellel, kas ohvri andmed saadi interneti teel või mitte (juhtumid 2 ja 4) või on saadud muul moel, kuid edastatud interneti vahendusel, või on kuritegu toime pandud interneti teel (juhtumid 1,8 ja 10). Kui kuritegu seisneb ainult ühes kolmest kirjeldatud faasist, siis peab see olema toime pandud interneti teel.

Nagu eespool mainitud – kui ohvri info on kord saadud, siis saab kurjategija seda kasutada ka edaspidi kuritegude toimepanemiseks. Neid kuritegusid on üldiselt kolme tüüpi: kuriteod, mis ei ole otseselt ohvri vastu suunatud, kuid on tehtud tema nimel (juhtumid 5 ja 7), teod, mis on suunatud kurjategija või kolmanda isiku rikastumisele ning põhjustavad otseselt kahju ohvrile (juhtumid 1,2,4,8 ja 9) ja teod, mis on suunatud ohvri laimamisele (juhtumid 6 ja 10).

2.3. *Modi operandi*

Ohvri andmete omandamine võib toimuda väga erineval moel. Käesolevas kontekstis on eesmärk, kasutades uusi vahendeid, juhtida eksiteele nii kasutaja kaitsemeetmeid kui ka -võime. Seetõttu peab lähenemine olema ka üldisem, et see ei aeguks liiga kiiresti.

On olemas traditsioonilisi meetodeid hankimaks kellegi kohta isiklikku informatsiooni, näiteks kellegi prügikastis sorimine, postkast, varastades isikut tõendavaid dokumente jms, mis sisaldab nt inimese varalist seisut. Samuti saab kellegi kohta informatsiooni teeseldes end olevat nt nn kaablikutt, tööandja või keegi teine, kes võib mingit informatsiooni vajada. Samuti võidakse infot välja peilida ohvrile lähedastelt isikutelt, kontakteerudes ohvriga või pangaga valedel ettekäändetel ja eesmärgiga saada vajalikku informatsiooni (juhtum 8), ostes soovitud informatsiooni korrumppeerunud ametnikelt või jälgides ohvrit, kui viimane teeb mingeid toiminguid (nt raha väljavõtt).

Kõiki neid meetodeid võib võtta arvesse internetipõhise identiteedivarguse puhul ka käesolevas juhendis, sest eelpool loetletud moel saadud informatsiooni abil saab edaspidi toime panna kuritegusid interneti vahendusel.

Veel üks võimalus ohvri kohta info hankimiseks ning mis ei ole eriti levinud, on mingi andmekandja, nt mobiiltelefoni, vargus, milles on ainult isikule kuuluv ja kolmandatele osapooltele mitte avaldatav informatsioon.

Olles nüüd põgusalt vaadelnud traditsioonilisi interneti teel toimepandavate kuritegude meetodeid

2. IDENTITEEDIVARGUS

läheme selliste mooduste juurde, kus kasutatakse nõ uusi tehnoloogiaid, täpsemalt internetti.

Üks näide on nn „nigeerlaste kirjad“. Need levisid esmalt tavaposti ja faksi teel. Nüüd saadetakse neid peamiselt laiali e-posti abil. Siin kasutatakse nii traditsioonilisi meetodeid kui ka internetti info hankimiseks.

E-kiri saabub tavaliselt halvas inglise keeles või siis käesoleval ajal juba veelgi halvemas eesti keeles. Algselt saadeti neid kõrgetel kohtadel olevatele ametnikele ja firmajuhtidele, kuid täna-seks on saajate ringi kaasatud juba põhimõtteliselt kõik inimesed. Sageli väidab saatja end olevat mõne riigi valitsejate ringi kuuluvaks või sellele lähedalseisvaks isikuks (nt surnud kuninga eksiilis olev abikaasa).

Algaastatel saabusidki nimetatud kirjad peamiselt Nigeeriast, kuid siis levis skeem ka naaberriikidesse ja viimasel ajal on nimetatud põhimõttel toimivaid kirju välja saadetud näiteks Lõuna-Aafrikast.

Selline kiri sisaldab tavaliselt ettepanekut. Saatja väidab end valdavat suurt summat raha, mille ta on omandanud seoses oma privilegieeritud staatusega.

Kurjategija väidab, et teda ei tohi avalikult raha päritoluga seostada ning seetõttu on vaja antud raha kanda üle välismaale. Kurjategija pakub kirja saajale, et vastutasuks tehingu eest saab viimane kogusummast 20% - 35%. Selleks küsib kirja saatja saajalt hulgaliselt isikuandmeid – arveldusarve, isiklikud andmed, asutuse andmed jne.

Kõiki neid andmeid ei pruugita küsida kohe esimeses kirjas või e-kirjas. Kurjategija ootab vastust, mis võimaldaks dialoogi jätkumist.

Kui petised on saanud piisavalt infot erinevate isikute kohta, siis saavad nad toime panna erinevaid rahvusvahelisi kuritegusid.

Ajalehtedes ja veebis avaldatavad töökuulutused võivad samuti olla pettused ning on disainitud ohvrite tähelepanu tõmbamiseks saamaks teada nende isikuandmeid ning sooritamaks selle infoga edasisi süütegusid. Need on nn tööpettused.

On oluline märkida ka abipalveid, mis on saadetud läbi e-posti või Facebook'i. Andmepüük selleks, et saada ligipääs kellegi e-postile tekib siis, kui (abi-)palvele vastatakse ja saadetakse

2. IDENTITEEDIVARGUS

kurjategijale küsitud informatsioon (juhtum 5). Facebook'is toimib sama skeem. Abipalve võib olla postitatud kas ohvri nn seinale või saadetud privaatsõnumina.

Facebook'i saab kasutada selleks, et leida uusi identiteedivarguse ohvreid. Seda saab teha paigaldades ohvri arvutisse nuhkvara. Selle abil postitavad kurjategijad ohvri seinale linke, mis suunavad ohvri mingile lehele, kus küsitakse neilt isikuandmeid. Näiteks postitatakse kellegi lehele video ning selleks, et sõbralistis olijad saaksid seda "like"-ida, peavad nad sisestama mingit infot enda kohta, kuid tegelikkuses kontrollib seda kurjategija.

Otsingumootoreid nagu Google, mis võimaldavad teostada otsinguid miljonitelt lehtedelt sekundis, saab samuti kasutada lubamatutel eesmärkidel.

Google hacking on termin, mida kasutatakse kirjeldamaks kompleksotsinguid otsingumootorites, mille eesmärk on leida kaitsmata ohvreid ja tundlikku informatsiooni erinevatelt saitidelt. *Google Hacking Database* muudab selle ülesande lihtsamaks. See on andmebaas otsingutest, mis tuvastab sensitiivse informatsiooni. See identifitseerib serveri haavatavust ja veateateid, mis sisaldavad omakorda liiga palju informatsiooni – faile, mis sisaldavad salasõnu, tundlikke juhendeid; lehekülgi, mis sisaldavad sisselogimise portaale, tulemüüri logisid ning kuigi Google blokitab mõningaid tuntumaid *Google hacking* päringuid, on äärmiselt keeruline peatada hakerit tungimast sinu lehele ja käivitamast eelpoolnimetatud andmebaasi.

On juhtumeid, kus erinevate asutuste ja organisatsioonide töötajad omavad ligipääsu klientide ja koostööpartnerite tundlikule informatsioonile ning omandavad seda kuritegelike kavatsustega – sageli kavatsusega nimetatud info edasi müüa kuritegelikele ühendustele. See juhtus tõenäoliselt Teeduga juhtumis 1. Töötaja, kellele ta andis oma andmed krediitkaardi taotlemiseks, müüs krediitkonto kohta käivad andmed edasi ning neid kasutati hiljem omakorda kindlustusettevõttes.

Üks kõige tavapärasemaid meetodeid saamaks ohvri kohta käivaid isikuandmeid identiteedivarguse sooritamiseks ning mis on pälvunud ka hulgaliselt tähelepanu, on nn andmepüük.

Nimetatud tehnika koosneb suure hulga e-kirjade saatmisest (nn rämpspost ehk spämm), mis sisaldab endas linki. Nimetatud lingile vajutades leiab end tõenäoliselt lehel, mis on äärmiselt sarnane näiteks teie internetipanga esilehega ning seal on ka kõik vajalik sisselogimiseks. Tegemist on siiski petuskeemiga. Kui ohver kasutab linki antud lehele minemiseks, siis peab ta sellel lehel end identifitseerima kasutades selleks oma internetipanga koode. See info võimal-

2. IDENTITEEDIVARGUS

dab lehe loojal siseneda ohvri internetipanka ning kanda kontrol olevad vabad vahendid teisele kontole. Taoline juhtum on kirjeldatud juhtumis 4.

Andmepüügi puhul on võimalik jälgida nelja staadiumi: algfaas koosneb rämpsposti massilisest saatmisest, mis sisaldab endas linki. Teises faasis edastab ohver oma isikuandmed pahaaimamatult kurjategijale, kolmandas faasis siseneb kurjategija saadud informatsiooniga ohvri kontole ning kannab sellel leiduvad vahendid edasi. Neljandas faasis toimub nn rahapesu, kus ebaseaduslikult omandatud raha muudetakse erinevate tegevuste abil taas legaalseks.

Rääkides uutest moodustest isikuandmete saamiseks, tuleb pöörata tähelepanu ka nähtusele nimega *pharming*. Tegemist on seesuguse meetodiga, mis kasutab pahavara levitamiseks samuti rämpsposti – e-kiri sisaldab varjatud faile, mis varjatult ja automaatselt paigaldavad ohvri arvutisse pahavara. Kui see on kord juhtunud, siis ilma arvutiomaniku teadmata muudavad need Lemmikute kaustas olevaid faile ning nn *cooki'ide* ehk “küpsiste” registreerumist. Selliste muudatuste tulemusel suunab arvuti isiku, kes enda arvates siseneb tavapäraselt oma internetipanka, hoopis teisele lehele, mis on disainitud andmepüügiks.

Veel üks tehnika, mida on oluline mainida, on *sniffing*. Ühes võrgus olevad arvutid jagavad erinevaid kommunikatsioonikanaleid. Jagatud kanalite puhul saavad arvutid ka seda infot, mis saadetud teisele arvutile. Sellist info püüdmist nimetatakse *sniffing'uks*.

Lõpetuseks vaatame ka nn häkkimist ja kräkkimist. Mõlemad on moodused, kuidas siseneda ebaseaduslikult arvutisüsteemidesse ning on seega tegemist meetoditega, mille abil on võimalik saada juurdepääs kellegi isiklikule informatsioonile. Käesolevas kontekstis viitavad mõlemad tegevustele, mis on seotud erinevate koodide murdmisega või ebaseaduslikult litsentside omandamisega, mis võimaldavad teistesse arvutitesse luba küsimata sisenemist. Juhtum 3 kirjeldab pahavaraga nakatumist, mida iseloomustab arvuti aeglus. Tihti nakatavad kurjategijad ohvri arvuti ja küsivad nn lunaraha – s.t., et nad lubavad teatud summa eest lahendada nende endi poolt tekitatud probleemi. Käesoleval juhul aga ei ole tegemist internetipõhise identiteedivargusega, välja arvatud juhul, kui kurjategija sai ohvri arvutisse sisenedes tema kohta konfidentsiaalset informatsiooni.

Andmete kaevamine (*data mining*) koosneb informatsiooni analüüsist, mustrite ja seaduspärade ning nendevaheliste seoste loomises. Sellist tehnikat kasutatakse tavaliselt uuringutega seotud aladel. On olemas arvutiprogrammid - nn andmekaevajad, mis koguvad internetist või

2. IDENTITEEDIVARGUS

ohvri arvutist informatsiooni ilma selleks õigust omamata ning analüüsivad saadud teavet ja loovad seoseid. See võimaldab näiteks ettevõtetel ennustada tarbijate käitmist ja identiteedivargust silmas pidades muudab võimalikuks korrastada ohvri isikuandmeid selliselt, et kurjategija saab neid kasutada.

Vaatleme põgusalt ka nähtust, mida kutsutakse klahvisalvestiks (*keylogging*). Selleks on loodud programmid, mis salvestavad kõik tegevused mida klaviatuuril on tehtud. Nimetatud olukorda kirjeldab ka juhtum 2 eespool. Kõik, mis ohver tegi oli see, et ta avas lehekülje, mis pakkus anti-viirust ning pahavara, mis sisaldas endas klahvisalvestit, installeeris ennast ise tema arvutisse. See omakorda võimaldas koguda infot tema panga kohta ning kurjategija kasutas seda infot tema konto tühjendamiseks.

3.

IDENTITEEDIVARGUS - REALSUS

[illegible]

3. IDENTITEEDIVARGUS - REAALSUS

3.1. Tavapärasemaid internetipõhiseid identiteedivargusi

Peamiselt kirjeldame käesolevas materjalis andmepüüki kui meetodit saamaks ligipääsu ohvri e-posti kontole (juhtum 5) või panka (juhtum 4) ning teise isiku laimamist sotsiaalsõrgustikes (juhtumid 6 ja 10), kuna nende näol on tegemist kõige tavapärasemate juhtumitega.

Esmalt vaatleme andmepüüki seoses e-posti konto ülevõtmisega. Olles juba mõnes eelmises peatükis kirjeldatud moel saavutanud kontrolli ohvri isikuandmete üle, võib saada kurjategija kontrolli ka oma ohvri e-posti konto üle selleks, et vaadata, missugust infot meilikonto sisaldab, loomaks kontakti ohvri pangaga (tavaliselt kliendihalduriga) või saatmaks e-postilt finantsasutustesse päringuid võimaluste erinevate krediitvõimaluste kohta.

Seega on e-postilt andmepüügi kaks peamist eesmärki saada ohvri kohta tundlikku informatsiooni panemaks toime petuskeeme panga kaudu või ohvri tutvavatega kontakteerumiseks ja neilt ohvri nimel raha välja petmiseks. Seega me näeme, et selline andmepüük on peamiselt seotud rahalise kasuga kurjategijale ning sellised kuriteod on kahjuks juba väga levinud.

Teistsuguses kontekstis saab rääkida identiteedivargusest siis, kui selle eesmärk on isikut laimata sotsiaalsetes sõrgustikes. Selline situatsioon tekib sageli inimeste isiklike suhete kontekstis ning tihti just teismeliste ja noorte omavahelistes suhetes.

Üldiselt saame öelda, et teise isiku laimamiseks sotsiaalsõrgustikes on kaks peamist moodust: ohvri andmetega libalehekülje loomine ohvri või au teotavate kommentaaride ja fotodega (vt juhtum 6) ning ohvri tegeliku konto abil solvavate fraaside, hinnangute ja pildimaterjali levitamine (juhtum 10).

Nende juhtumite puhul on vahel ohver see, kes on eelnevalt andnud enda kohta käiva info vabatahtlikult kurjategijale, mis hiljem võimaldab viimasel siseneda ohvri kontole või levitada alandavaid fakte või fotosid.

3. IDENTITEEDIVARGUS - REAALSUS

3.2. Ohver ja teo toimepanija

On oluline eristada erinevate kurjategijate profile. Selle kurjategija, kes üritab saada infot kelmuste toimepanemiseks, motiivid erinevad selle kurjategija omast, kes paneb toime laimuga seotud tegusid.

Esimesel puhul on hea teha vahet isiku vahel, kes tunneb ohvrit läbi erinevate seoste ning kellel on seeläbi lihtsam pääseda ligi ohvri isiklikule informatsioonile ning ohver ongi just seetõttu valitud. Teisel juhul leiab toimepanija oma ohvreid juhuslikult. Sel juhul on kurjategijat peaaegu võimatu tabada, sest sellised kuriteod pannakse sageli toime maakera teiselt poolelt ning ta kasutab alati ohvri identiteeti ja mistõttu teda ennast on praktiliselt võimatu tuvastada. Seetõttu ei ole antud valdkonnas nõ tuntud kurjategijaid ning neid on ka väga keeruline profileerida.

Alguses nähti nn küberkurjategijat kui meessoost isikut, kes on tudeng, tunneb hästi arvuteid ning kellel on üle keskmise IQ. Samuti arvati, et tegemist on introvertidega kellel on piiratud sotsiaalse suhtlemise oskus ning keda motiveeris võimalus nõ lüüa masinat ning seeläbi demonstreerida oma intellekti üleolekut ülejäänud ühiskonna suhtes.

Reaalsus on siiski teine – täna saab internetipõhise identiteedivarguse toimepanija olla kes iganes, kes soovib sel teel kasu saada. Seda põhjusel, et andmepüügiks on väga erinevaid võimalusi ning mitte kõik meetodid ei vaja erilisi teadmisi ja seega võib toimepanijaid leida igast nn ühiskonnakihist ning väga erinevate isiksuseomadustega.

Internetist võib leida ka mitmeid lehekülgi, kus õpetatakse arvutikuritegusid toime panema ning seega on need teadmised laialdaselt kättesaadavad igauhele, kes vajab raha.

Eraladi väärrib antud valdkonnas välja toomist isik, keda kutsutakse *insider´iks*. Me räägime siinkohal kõrge kvalifikatsiooniga töötajast, kes on pälvinud oma tööandja usalduse ning kes kasutab seda eelist ning teadmisi, et müüa informatsiooni kuritegelikele ühendustele või üksikutele kurjategijatele.

Kõige ohtlikumad selles valdkonnas ongi erinevad kuritegelikud ühendused, kes kontrollivad kogu identiteedivarguse protsessi alates info hankimisest kuni rahapesuni.

Mis puudutab ohvrit, siis ka siin ei ole võimalik tuua välja kindlat profiili. Kõige otsustavam

3. IDENTITEEDIVARGUS - REAALSUS

faktor ohvri valikul on tema infole ligipääsu lihtsus. See ei tähenda tingimata, et toimepanija on ohvrile lähedalseisev isik, kuigi see võib paljudel juhtudel tõepoolest nii olla.

UK-s tehtud uuringu põhjal saab siiski välja tuua, et kõige tavapärasem sihtmärk on 40 – 50 aastane töötav mees. Seega saab öelda, et kurjategijad otsivad konkreetset isikuid, kellel on tõenäoliselt raha ning hea finantsvõimekus (st on võimalus taotleda krediitkaarti jne).

Uuringud on näidanud, et USA-s on suurem tõenäosus sattuda seesuguse kuriteo ohvriks inimestel, kelle iga-aastane sissetulek ületab 75 000 USD-d ning isikutel vanuses 16 – 34 eluaastat.

Sageli on ohvriteks ka erinevad ettevõtted – pangad, kindlustusfirmad jt rahandusega seotud asutused, kuid nemad eelistavad intsidentidest mitte teavitada ning lahendada probleem ettevõtte siseselt. Seda põhjusel, et kardetakse oma maine pärast.

Sotsiaalsõrgustike kontekstis panevad identiteedivargusi toime isikud, kes on ohvrile lähedased ning kes mingil põhjusel on otsustanud ohvrile halba teha, näiteks luues libakonto ja avaldades ohvrit alandavaid postitusi. Selline olukord ilmneb sageli lõppenud suhte puhul, kus üks osapooltest otsustab teisele “kätte maksta”.

3.3. Riskifaktorid

Kuna ohvriks võib langeda igaüks, on väga oluline teada riske, mis muudavad internetikasutjad haavatavamaks ning mis seeläbi omakorda suurendab ohvriks langemise ohtu.

Inimeste eraelulised detailid on järjest enam kättesaadavad, eriti sotsiaalsõrgustikes ning küberkurjategijad teavad täpselt, kuidas seda enda kasuks tööle panna.

On olemas mõned identiteedivarguse ohvriks langemise riski suurendavad käitumistavad, mida inimesed kasutavad sotsiaalsõrgustikes. Nendeks on:

- › Privaatsussätete mitte aktiveerimine või oma profiili väga avatuna hoidmine;
- › Suure hulga info jagamine;
- › Tundmatute isikute sõbrakutsete aktsepteerimine;
- › Intiimsete fotode postitamine sotsiaalsõrgustikesse.

3. IDENTITEEDIVARGUS - REAALSUS

Töötades tundide kaupa veebis, kasvab küberkuritegevuse ohvriks langemise oht. Seda eriti siis, kui keegi töötab kodus ning kasutab isiklikku arvutit. Seda põhjusel, et erinevatel ettevõtetel ja asutustel on olemas oma IT-ga tegelevad osakonnad/töötajad, kelle töö on kaitsta arvuteid ja arvutisüsteeme samal ajal, kui vabakutselisel inimesel on lihtsalt tõenäoliselt vähem kaitsitud arvuti.

On olemas suur hulk tegevusi, mis kasvatavad ohvriks langemise riski. Näiteks:

- › Arvutisse ei ole paigaldatud viirusetõrjet ja nuhkvara leidvat tarkvara;
- › Tundmatutele linkidele klikkimine;
- › Täiskasvanutele mõeldud saitide külastamine;
- › Sotsiaalvõrgustikes sellistele sõnumitele vastamine, mille on saatnud tundmatud isikud. Sama kehtib ka e-kirjade kohta;
- › Rahakotis erinevate salasõnade ja PIN koodide kaasas kandmine või seesuguse info talletamine arvutis kaitsmata failis;
- › Isegi usaldusväärsetele inimestele oma salasõnade ja PIN koodide avaldamine;
- › Kasutades liiga lihtsaid salasõnu nagu näiteks sünniaeg või lemmiklooma nimi;
- › Hoides tähtsaid dokumente kolmandatele osapooltele liiga kättesaadavates kohtades;
- › Visates dokumente minema, mitte neid hävitades;
- › Saates konfidentsiaalset informatsiooni e-maili teel;
- › Mitte paigaldades oma arvutis olevatele programmidele uuendusi;
- › Kasutades vaba Wi-Fi võrku.

3.4. Identiteedivarguse tagajärjed

3.4.1. Ohvrile

Kuigi asjaolude kokkulangesdes võivad kõik sattuda küberkuriteo ohvriks, on enim ohustatud mõningad spetsiifilised grupid nagu näiteks madalama sissetulekuga inimesed, vähemused ja eakad, sest neil on vähem majanduslikke võimalusi, terviseprobleemid või keelebarjäär. Näiteks võib neil olla keerulisem pöörduda politseisse, probleemid erinevate vormide täitmisel või dokumentide lugemisel ning seetõttu raskusi ohvreid abistavate organisatsioonidega kontakteerumisel. Neil võib olla ka oluliselt keerulisem taastuda emotsionaalsest šokist ja majanduslikust kaotusest nii rahalises kui ka psühholoogilises mõttes.

3. IDENTITEEDIVARGUS - REAALSUS

a. MAJANDUSLIKUD

Majanduslik mõju saab olla kahesugune: otsene kahju, mis viitab summale, mille kurjategija omastas kasutades ohvri identiteeti, sh kaupade ja teenuste rahaline väärtus. Teine on kaudne kahju, mis sisaldab erinevaid kulusid ohvrile seoses ohvriks langemisega (õigusabikulud, kulud telefonile, postikulud jms). 2006. ja 2007. aastal läbiviidud uuringust selgus, et umbes 62% küberkuritegude ohvritest väidab, et seoses kuriteoga on neile tekitatud olulist rahalist kahju.

Samal perioodil oli antud kuritegevuse tagajärjel kogukulu USA kodanikest ohvritele umbes 17,3 mlrd dollarit ja 2011. aastal oli 24 riigi peale kokku kahju ohvritele 388 mlrd dollarit.

Kui on toime pandud krediitkaardi väärkasutusega seotud pettused, siis pangad eelistavad tagastada ohvrile kaotatud summa, kuna tavaliselt ei ole kahju nende jaoks suur ning nad ei soovi avalikku tähelepanu, mis võib nende mainet kahjustada. Samas võib neil olla ka kohustus kliendile kahjud kompenseerida.

Ohver võib kaotada oma elukoha, kui tema säästud on kadunud. Kui isik on sattunud kuriteo ohvriks, siis võib tal hiljem olla raskusi saada uut krediiti või laenu.

b. ÕIGUSLIKUD

Ohvrile võidakse esitada kahtlustus/süüdistus kuriteo eest, mida ta toime ei ole pannud (juhtum 7) ning tal võib olla probleeme tsiviilkohtus seoses võlgnevusega, mida ta ei ole tekitanud. Sama lugu on lepingukohustuste täitmisega, mida ohver ei ole sõlminud.

c. EMOTSIONAALSED

Olenemata sellest, et psühholoogilised tagajärjed inimeseti erinevad arvestades inimeste psüühika erisusi, on kõige tavapärasemad ohvriks langemise tagajärjed: hirm, ärevus, viha või kestav usaldamatus kõigi ja kõige suhtes, mida ohvrid ise sageli kirjeldavad kui "paranoiat". Identiteedivarguse emotsionaalset mõju kirjeldatakse sarnaselt vägivallakuriteo ohvrile. Paljud tunnevad, et nende privaatsust on rikutud, abitust, jõuetust ja

3. IDENTITEEDIVARGUS - REAALSUS

hirmu, et nad võivad uuesti sattuda sellise kuriteo ohvriks.

Majandusliku stabiilsuse kaotamisest tingitud turvalisuse kadu omab ohvritele väga suurt mõju. Samuti mõjub olukord nagu kirjeldatud juhtumis 7 ning vajadus tõestada oma süütust.

Paljud ohvrid süüdistavad juhtunust iseennast ning arutlevad, kas üldse kedagi saab usaldada ning kas süüdlane saab õiglase karistuse (või kas ta üldse karistuse saab).

Internetipõhise identiteedivarguse ja küberkuritegevuse ohvrid üldiselt tunnevad, et neid käsitletakse nagu “teisejärgulisi ohvreid”, kes saavad vähem tuge, kui teiste kuritegude ohvriks langenud inimesed. Seda põhjusel, et need süüteo on sotsiaalselt alahinnatud ning ohvrite toimetuleku taastamiseks on vähe meetmeid. Samuti peavad nende kuritegude ohvrid teadma, kuidas tulla toime pettumusega, sest paljudel juhtudel ei ole kurjategijat üldse võimalik tuvastada. Seda vajadust ei tohi alahinnata, sest iga kord, kui ohver puutub kokku uute võlgnevustega jt kuriteo tagajärgedega, reviktimiseerub ta uuesti.

Kuriteo tagajärjed on teistsugused, kui teo toimepanija on ohvrile lähedalseisev isik. Neil juhtudel võib ohver tunda survet võtta kuriteo toimumise eest vastutus selleks, et kaitsta kurjategijat tagajärgede eest. Ohvrid ei pruugi tahta kuriteost teatada, kui nad saavad teada, et teo taga on keegi lähedane ja eelnevalt usaldatud isik nagu näiteks sugulane või sõber. Neil võib olla ka häbi, et neid on “haneks tõmmatud”.

d. IGAPÄEVARUTIINILE

Identiteedivargus on tagajärgede likvideerimise mõistes väga tülikas ja aeganõudev, kui me räägime ohvri poolt selle teo tagajärgede likvideerimisega. USA-s on välja selgitatud, et keskmiselt kulutab iga ohver 97 tundi, et tegeleda kaasnenud kahjudega ning kulutades selleks keskmiselt 1884 USD-d (info on saadud USA organistasioonilt *Identity Theft Resource Center*). UK-s kulub isikul oma nime puhastamiseks 3 kuni 48 tundi.

40% ohvritest on öelnud, et ajakulu oli kuriteo kõige halvem külg.

3. IDENTITEEDIVARGUS - REAALSUS

3.4.2. Ühiskonnale

Ühendkuningriigis on välja arvatud, et identiteedivargusega põhjustatud kahjud riigi majandusele on hinnanguliselt 1,3 mlrd naela aastas. Austraalias on vastav summa 1 ja 3 mlrd vahel. USA-s aastal 2005 oli vastav kulu 56,5 mlrd dollarit. Lissaboni haldusalas ületas kulu majandusele aastal 2011 2 milj eurot.

Identiteedivargus põhjustab kasvavat kahju erinevatele institutsioonidele nagu pangad, kindlustusfirmad jt teenuseid pakkuvatele ettevõtetele. Need asutused võivad olla kohustatud korvama ohvrile kahju, v.a. juhul, kui on kindlaks tehtud, et kahju tekkis ohvri hooletusest. Nimeetatud asutuste kohustusi ei saa jätta tähelepanuta juba ainuüksi seetõttu, et tarbija peab selle lõppkokkuvõttes siiski kinni maksma.

Isegi asutuste identiteeti on võimalik kasutada ilma nende loata ja sel juhul on kaudsed kahjud seostavad töötajate otsingutega, ennetusega ja kindlustusega.

Samuti ei saa jätta tähelepanuta nende asutuste maine langust, kuna ka siin on tegemist mõjuga majandusele.

Riigid ja valitused võivad kannatada otseste kahjude all, kuna paljud teod on pandud toime avalike teenuste nime all. Samuti on kaudsed kulud ennetusele, väljaõppele ning õiguskaitse ressurssidele tegelemaks seda tüüpi kuritegevusega.

3.5. Menetluslikud raskused

Internetipõhiste identiteedivarguste ja küberkuritegevuse uurimine põhjustab probleeme nii politseile kui ka prokuratuurile. Kuriteo enda karakteristikud ja sellega seonduvad faktorid muudavad kurjategija väljaselgitamise väga keeruliseks, et mitte öelda – vahel ka võimatuks.

Identiteedivargus on rahvusvahelise haardega kuritegevuse liik. Kui kurjategija ja ohver ei ole samast riigist, on uurimine piiratud. Seda põhjusel, et lisaks vajadusele jälitada kurjategijat üle maailma, on vaja ka suurepärase koostööd erinevate riikide politsei jõudude ja prokuratuuride vahel. Suveräänsuse printsiip ei lase ühel riigil teises riigis uurimist läbi viia ilma kohaliku võimu nõusolekuta. Koostöö erinevate riikide ametkondade vahel nõuab formaalsusi ja aega, mis omakorda kahjustab menetluse tulemuslikkust.

3. IDENTITEEDIVARGUS - REAALSUS

Paljud küberkuritegevusele omased protsessid saavad olla automatiseeritud (näiteks rämpspositi saatmine), mistõttu ta kordab ennast pidevalt ja seega on püsiva iseloomuga.

Kurjategijad kasutavad tehnoloogiaid, mis võimaldavad jääda anonüümseks, nt krüpteerimisprogrammid.

Tehnilisuse kõrge tase nõuab küberkuriteo uurimisel mitmete erinevate ekspertide kaasamist ning väga suure sisemise ressursi kasutamist (nii logistilises kui ka inimressursi mõttes).

Lisaks nendele spetsiifilistele karakteristikutele kahjustavad menetlust ka üldisemad tegurid.

Arvestuslikult 80% ohvritest ei teavita toimepandud kuriteost politseid. Nimetatud fakt tuleneb teadlikkuse puudumisest antud valdkonnas ning samuti levinud veendumusest, et politsei ei suuda midagi ära teha. Ohvrid ei teavita kuriteost ka sel põhjusel, et tunnevad häbi juhtunu pärast.

Ettevõtted, pangad, kindlustusettevõtted jt finantsasutused tegelevad juhtumitega pigem sisemiselt, kuna nad ei soovi avalikkuse ees oma mainet kahjustada nii koostööpartnerite kui ka klientide ees.

Samal ajal kasvab igapäevaselt koos internetikasutajate arvuga ka ohvrite arv.

Veebist on leitavad leheküljed, kus õpetatakse toime panema erinevaid küberkuritegusid ning neid on lihtne leida – tuleb vaid kasutada levinud otsingumootoreid.

Igapäevaselt loovad kurjategijad uusi meetodeid saamaks ligipääsu inimeste isikuandmetele. Need uued meetodid ja tehnika levivad väga kiiresti mustal turul.

Üks suur takistus küberkuritegude uurimisel seisneb ka elektroonilise tõendusmaterjali hindamises. Leidmaks algallikat ehk teisisõnu IP aadressi, on vajalik siseneda nn registri ajalukku, mida haldavad internetiteenuse pakkujad ja seega on nende koostöö uurimisasutustega olulise tähtsusega.

Samuti on oluline digitaalse tõendusmaterjali nn elujõulisus. Seega sellele ligipääs, kogumine, säilitamine ja analüüsimine peavad alati olema läbi viidud protseduurireeglite järgi ning vastavate spetsialistide poolt. Tõendusmaterjali kogumine peab toimuma võimalikult kiiresti, sest seda on väga kerge hävitada.

4.

JURIIDILINE RAAMISTIK

[illegible]

4. JURIIDILINE RAAMISTIK

Õige seadusandluse kohaldamine mängib olulist rolli küberkuritegevuse ennetamisel ja sellega võitlemisel.

Seadusandluse olemasolu on oluline teatud tegude kriminaliseerimisel ning politseile võimaluste andmisel seesuguseid toiminguid uurida, elektroonilise tõendusmaterjali kogumisel ja säilitamisel, info vahetuses nii riigi siseselt kui rahvusvaheliselt ning teenusepakkujate kohustuses infot säilitada.

USA-s keskendutakse näiteks siseriiklikul tasemel peamiselt teole, kuid on vajadus arendada seadusandlust ka teiste küberkuritegevuse osade osas ning see suund on juba leidmas ka vajalikku tähelepanu ja tunnustust.

4.1. Rahvusvaheline tasand

Lähiaastad on paljastanud, et rahvusvahelisel tasandil tuntakse suurt muret küberkuritegevusega võitlemise osas. Euroopa Nõukogu, Euroopa Komisjon ja ÜRO on antud valdkonnas algatanud ja läbi viinud mitmeid tegevusi ning valdkonda oluliselt edasi arendanud.

Euroopa Nõukogu Küberkuritegevuse Konventsioon (ECCC) 23. novembrist 2011 on rahvusvaheliselt enim kasutatav raamdokument riikide poolt küberkuritegevusega seotud seadusandluse kohandamisel.

ECCC üritab pidevalt ja järjest enam internetistatud maailmas kaitsta ühiskonda küberkuritegevuse eest võttes vastu järjest paremini sobituvaid seadusi ja suuniseid ning erugtades rahvusvahelist koostööd. Allpool toome välja mõned kuriteod, mis on antud dokumendiga kinnitatud ja seaduste kohaldamist idetiteedivarguse erinevates staadiumites nii nagu me oleme seda siin defineerinud. ECCC on loonud ka protseduurilised ja koostööga seonduvad normid, mis on kohaliku seadusandluse aluseks.

Euroopa Liidu kontekstis tuleb tuua välja 2005/222/JHA raamdokument, mis käsitleb infosüsteemide vastu suunatud ründeid ja EL direktiiv 2013/40/EU, mis vahetas eelmise välja.

Esimene dokument oli suunatud parandama liikmesriikide politsei jt õiguskaitseorganite omavahelist koostööd ning ühtlustama küberkuritegevusega seotud norme.

4. JURIIDILINE RAAMISTIK

EL direktiiv 2013/40/EU vahetas niisiis eelmise välja ning selle peamine eesmärk on ühtlustada liikemsriikide karistusseadustikke küberkuritegevuse valdkonnas luues riikidele antud valdkonnas miinimumnõuded nii karistatavate tegude kui ka karistuste määrade osas parandamiseks osapoolte vahelist koostööd.

4.2. Eesti seadusandlus

Eesti Vabariigis kehtivas Karistusseadustikus (KarS) on mitmeid küberkuritegevusega seotud paragrahve. Mitmed neist on jõustunud alates 01.01.2015 ning seega on tegemist uute sätetega.

KarS 2. jaos (põhivabaduste rikkumised) on välja toodud alljärgnevad süüteod, milliseid võib toime panna nii arvutisüsteeme ja interneti abil kui ka ilma nendeta:

§ 156. Sõnumisaladuse rikkumine

- (1) Kirjavahetuse ja sidevahendi abil edastatud sõnumi saladuse rikkumise eest – karistatakse rahalise karistusega.
- (2) Sama teo eest isiku poolt, kes pääses sõnumi juurde oma tööülesannete tõttu, – karistatakse rahalise karistuse või kuni üheaastase vangistusega.
- (3) Käesoleva paragrahvi lõikes 1 või 2 sätestatud teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahalise karistusega.

[RT I, 23.12.2014, 14 - jõust. 01.01.2015]

§ 157. Isikuandmete ebaseaduslik avaldamine

[RT I, 12.07.2014, 1 - jõust. 01.01.2015]

- (1) Kutse- või ametitegevuses teatavaks saanud isikuandmete ebaseadusliku avaldamise eest isiku poolt, kellel oli seadusest tulenev kohustus andmeid mitte avaldada, ja kui puudub käesoleva seadustiku §-s 1571 sätestatud süüteoüksus, – karistatakse rahatrahviga kuni 300 trahviühikut.
- (2) Sama teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahatrahviga kuni 32 000 eurot.

[RT I, 12.07.2014, 1 - jõust. 01.01.2015]

§ 157. Delikaatsete isikuandmete ebaseaduslik avaldamine

- (1) Delikaatsete isikuandmete ebaseadusliku avaldamise või neile ebaseadusliku juurde-

4. JURIIDILINE RAAMISTIK

pääsu võimaldamise eest –

karistatakse rahatrahviga kuni 300 trahviühikut.

(2) Sama teo eest, kui see on toime pandud omakasu eesmärgil või kui sellega on tekitatud teisele isikule kahju, –

karistatakse rahalise karistuse või kuni üheaastase vangistusega.

(3) Käesoleva paragrahvi lõikes 1 sätestatud teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahatrahviga kuni 32 000 eurot.

(4) Käesoleva paragrahvi lõikes 2 sätestatud teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahalise karistusega.

[RT I, 12.07.2014, 1 - jõust. 01.01.2015]

§ 157. Teise isiku identiteedi ebaseaduslik kasutamine

Teist isikut tuvastavate või tuvastada võimaldavate isikuandmete tema nõusolekuta edastamise, nende juurdepääsu võimaldamise või nende kasutamise eest eesmärgiga luua teise isikuna esinemise teel temast teadvalt ebaõige ettekujutus, kui sellega on tekitatud kahju teise isiku seadusega kaitstud õigustele või huvidele, või varjata kuritegu – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

[RT I 2009, 51, 348 - jõust. 15.11.2009]

KarS käsitleb ka mitmeid spetsiifiliselt küberkuritegevust tegevusi. Nendeks on:

§ 206. Arvutiandmetesse sekkumine

(1) Arvutisüsteemis olevate andmete ebaseadusliku muutmise, kustutamise, rikkumise või sulustamise eest –

karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

[RT I, 12.07.2014, 1 - jõust. 01.01.2015]

(2) Sama teo eest, kui:

1) see on toime pandud paljudes arvutisüsteemides olevate andmete vastu ja selle toimepanemisel kasutati käesoleva seadustiku §-s 2161 nimetatud seadet või arvutiprogrammi;

2) see on toime pandud grupi poolt;

3) see on toime pandud elutähtsa valdkonna arvutisüsteemis olevate andmete vastu või;

4) sellega on tekitatud oluline kahju, –

karistatakse rahalise karistuse või kuni viieaastase vangistusega.

[RT I, 12.07.2014, 1 - jõust. 01.01.2015]

(3) Käesoleva paragrahvi lõikes 1 või 2 sätestatud teo eest, kui selle on toime pannud juriidiline isik, –

4. JURIIDILINE RAAMISTIK

karistatakse rahalise karistusega.

[RT I 2008, 13, 87 - jõust. 24.03.2008]

§ 206. Terminalseadme identifitseerimisvahendi ebaseaduslik kõrvaldamine ja muutmine

(1) Elektroonilise side võrgus kasutatavas terminalseadmes identifitseerimisvahendi ebaseadusliku kõrvaldamise või muutmise eest ärilisel eesmärgil –

karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

(2) Sama teo eest, kui selle on toime pannud juriidiline isik, –

karistatakse rahalise karistusega.

[RT I 2007, 13, 69 - jõust. 15.03.2007]

§ 207. Arvutisüsteemi toimimise takistamine

(1) Arvutisüsteemi toimimise ebaseadusliku häirimise või takistamise eest andmete sisetamise, edastamise, kustutamise, rikkumise, muutmise või sulustamise teel –

karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

(2) Sama teo eest, kui:

1) see on toime pandud paljude arvutisüsteemide vastu ja kui selle toimepanemisel kasutati käesoleva seadustiku §-s 2161 nimetatud seadet või arvutiprogrammi;

2) see on toime pandud grupi poolt;

3) sellega häiritakse või takistatakse elutähtsa valdkonna arvutisüsteemi toimimist või avalike teenuste osutamist või

4) kui sellega on tekitatud oluline kahju, –

karistatakse rahalise karistuse või kuni viieaastase vangistusega.

[RT I, 12.07.2014, 1 - jõust. 01.01.2015]

(3) Käesoleva paragrahvi lõikes 1 või 2 sätestatud teo eest, kui selle on toime pannud juriidiline isik, –

karistatakse rahalise karistusega.

[RT I 2008, 13, 87 - jõust. 24.03.2008]

Erinevatel põhjustel menetletakse Eestis mitmeid süütegusid ka üldiste paragrahvide järgi, see tähendab, et ei ole vahet, kas tegu on toime pandud kasutades arvutisüsteeme ja intrnetti või mitte. Sellisteks paragrahvideks on näiteks:

§ 120. Ähvardamine

(1) Tapmisega, tervisekahjustuse tekitamisega või olulises ulatuses vara rikkumise või hävitamisega ähvardamise eest, kui on olnud alust karta ähvarduse täideviimist, –

4. JURIIDILINE RAAMISTIK

karistatakse rahalise karistuse või kuni üheaastase vangistusega.

(2) Sama teo eest, kui selle on toime pannud juriidiline isik, –karistatakse rahalise karistusega.

[RT I, 23.12.2014, 14 - jõust. 01.01.2015]

§ 209. Kelmus

(1) Teisele isikule varalise kahju tekitamise eest tegelikest asjaoludest teadvalt ebaõige ettekujutuse loomise teel varalise kasu saamise eesmärgil –karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

[RT I, 12.07.2014, 1 - jõust. 01.01.2015]

(2) Sama teo eest, kui see on toime pandud:

1) isiku poolt, kes on varem toime pannud varguse, röövimise, omastamise, süüteo toimepanemise tulemusena saadud vara omandamise, hoidmise või turustamise, asja tahtliku rikkumise või hävitamise, kelmuse või väljapressimise;

2) ametiisiku poolt;

3) suures ulatuses;

4) grupi poolt või

5) avalikkuse poole pöördudes, –

karistatakse ühe- kuni viieaastase vangistusega.

[RT I, 12.07.2014, 1 - jõust. 01.01.2015]

(3) Käesoleva paragrahvi lõikes 1 või 2 sätestatud teo eest, kui selle on toime pannud juriidiline isik, –karistatakse rahalise karistusega.

(4) Kohus kohaldab käesoleva paragrahvi lõike 2 punktides 2 ja 3 sätestatud kuriteo eest kuriteoga saadud vara laiendatud konfiskeerimist vastavalt käesoleva seadustiku §-s 832 sätestatule.

[RT I, 12.07.2014, 1 - jõust. 01.01.2015]

Lisanduvad ka lastega seotud seksuaalvägivalla süüteod:

§ 178. Lapsporno valmistamine ja selle võimaldamine

(1) Nooremalt kui kaheksateistaastast isikut pornograafilises või nooremalt kui neljateistaastast isikut pornograafilises või erootilises situatsioonis kujutava pildi, kirjutise või muu teose või selle reproduktsiooni valmistamise, omandamise või hoidmise, teisele isikule ülevõtmise, näitamise või muul viisil kättesaadavaks tegemise eest –karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

(11) Sama teo eest, kui see on toime pandud isiku poolt, kes on varem toime pannud käes-

4. JURIIDILINE RAAMISTIK

olevas paragrahvis või §-s 175, 1751, 1781 või 179 sätestatud kuriteo, –
karistatakse ühe- kuni kolmeaastase vangistusega.

(2) Sama teo eest, kui selle on toime pannud juriidiline isik, –
karistatakse rahalise karistusega.

[RT I, 13.12.2013, 5 - jõust. 23.12.2013]

§ 178. Seksuaalse eesmärgiga kokkulepe lapseealisega kohtumiseks

(1) Nooremale kui kaheksateistaastasele isikule, kes ei olnud võimeline toimumust aru saama, või nooremale kui neljateistaastasele isikule kohtumisetepaneku tegemise või temaga kohtumiskokkuleppe sõlmimise eest ning kohtumist ettevalmistava teo tegemise eest, kui kohtumise eesmärk on panna nimetatud isiku suhtes toime käesoleva seadustiku §-s 133, 1331, 141–1451, 175, 1751, 178 või 179 sätestatud seksuaalse iseloomuga süütegu, –
karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

[RT I, 13.12.2013, 5 - jõust. 23.12.2013]

(11) Sama teo eest, kui see on toime pandud isiku poolt, kes on varem toime pannud käesolevas paragrahvis või §-s 175, 1751, 178 või 179 sätestatud kuriteo, –
karistatakse ühe- kuni kolmeaastase vangistusega.

[RT I, 13.12.2013, 5 - jõust. 23.12.2013]

(2) Sama teo eest, kui selle on toime pannud juriidiline isik, –
karistatakse rahalise karistusega.

[RT I 2010, 10, 44 - jõust. 15.03.2010]

§ 179. Lapseealise seksuaalne ahvatlemine

(1) Nooremale kui neljateistaastasele isikule pornograafilise teose või selle reproduktsiooni üleandmise, näitamise või muul viisil teadvalt kättesaadavaks tegemise või sellisele isikule seksuaalse kuritarvitamise näitamise või sellise isiku nähes suguuhtesse astumise või muul viisil teadvalt tema seksuaalse ahvatlemise eest –
karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

[RT I, 13.12.2013, 5 - jõust. 23.12.2013]

(11) Sama teo eest, kui see on toime pandud isiku poolt, kes on varem toime pannud käesolevas paragrahvis või §-s 175, 1751, 178 või 1781 sätestatud kuriteo, –
karistatakse ühe- kuni kolmeaastase vangistusega.

[RT I, 13.12.2013, 5 - jõust. 23.12.2013]

(2) Sama teo eest, kui selle on toime pannud juriidiline isik, –
karistatakse rahalise karistusega.

4. JURIIDILINE RAAMISTIK

4.3. Identiteedivargus, seadusandlus ja Küberkuritegevuse konventsioon

Esimeses faasis – kellegi identiteedi kohta info hankimisel, mis võimaldab identiteedivargust toime panna – on võimalik kohaldada erinevaid rahvusvahelisi seaduseid. Näiteks CL paragrahv 3 – arvutitega seotud pettused – ja samaväärne on ka ECCC (European Computer Crime Centre) paragrahv 7, CL paragrahv 6 – lubamatu juurdepääs – ja ECCC paragrahv 2, CL paragrahv 7 - ebaseaduslik sekkumine – ning samalaadsed ECCC paragrahvid 3,4, ja 5, mis samuti käsitlevad andmete ja süsteemide väärkasutamist.

Igasugune tegevus, mis hõlmab sekkumist süsteemidesse, privaatsusesse, jälitamist, salajast salvestamist jne ei ole lubatud, kuna tegemist on ohvrit puudutava eraelulise info kogumisega ebaseaduslikult. Samamoodi ei ole lubatud avada kellelegi teisele erineval moel edastatud dokumente, kirju, e-posti jne.

Samuti saab lugeda ebaseaduslikuks kellegi eravestluse sisu salvestamist, pildistamist ja filmimist, mille avaldamine laiemale publikule ei ole ette nähtud.

Samuti on võimalik dokumentide varguse abil saada teada isiku kohta olulist informatsiooni panemaks toime identiteedivargust. Antud valdkonnas oluline osa on ka arvuti abil informatsiooni välja petmine.

Keelatud on privaatse info edastamine ja omamine selleks mitte ettenähtud isikutel.

Seitsmendas juhtumis – Marteni “identiteedivaras”, kes pani toime kuriteo noormehe isiklikku informatsiooni kasutades ning kus ohver võeti antud teo eest vastutusele, peaks võetama vastutusele ilmselt see, kes reaalset need teod toime pani. Samuti oleks oluline võtta nimetatud kurjategija vastutusele ka noormehe isikliku informatsiooni hankimise eest.

Samuti peaks olema võimalik karistada teo toimepanijat eravestluste avalikustamise eest, isikute intiimsete fotode jms edastamise/avalikustamise, eraeluliste andmete avalikustamise eest, sh arvuti abil, isiku poliitiliste, usuliste ja filosoofiliste tõekspidamiste avalikustamise eest.

Pettus on kriminaliseeritav, sh kasutades arvutisüsteeme.

5.

JUHTUMITE LAHENDAMISEKS KASUTATUD SEADUSED

[illegible]

5. JUHTUMITE LAHENDAMISEKS KASUTATUD SEADUSED

< Juhtum 1 >

Teedu juhtumi puhul, milles tema krediitkaardi andmed tõenäoliselt edastas kurjategijatele kaupluse töötaja, on Eestis võimalik menetleda Karistusseadustiku (KarS) § 209 ehk kelmuse järgi, mis sätestab, et Teisele isikule varalise kahju tekitamise eest tegelikest asjaoludest teadvalt ebaõige ettekujutuse loomise teel varalise kasu saamise eesmärgil karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

< Juhtum 2 >

32-aastase Krete puhul, kes installeeris oma koduses se arvutisse kogemata pahavara, saab politsei alustada menetluse samuti KarS § 209 järgi või ka KarS § 213 järgi, mis käsitleb arvutikelmusi. Antud paragrahvis on sätestatud, et (1) teisele isikule varalise kahju tekitamise eest arvutiprogrammi või andmete ebaseadusliku sisestamise, muutmise, kustutamise, rikkumise, sulustamise või muul viisil andmetöötlusprotsessi ebaseadusliku sekkumise teel varalise kasu saamise eesmärgil karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

< Juhtum 3 >

36-aastase abiõpetaja Heli juhtumi puhul, kes ostis endale meelelahutuseks arvuti 3 aastat tagasi ning millega mängivad ka tema 6- ja 8-aastased lapsed ja kelle arvuti nn võeti üle eesmärgiga nõuda kannatanult kahjutasu, saab samuti rakendada KarS § 206, samuti teatud tingimustel saab kasutada ka KarS § 1572, mis käsitleb teise isiku identiteedi ebaseaduslikku kasutamist. St, et teist isikut tuvastavate või tuvastada võimaldavate isikuandmete tema nõusolekuta edastamise, nendele juurdepääsu võimaldamise või nende kasutamise eest eesmärgiga luua teise isikuna esinemise teel temast teadvalt ebaõige ettekujutus, kui sellega on tekitatud kahju teise isiku seadusega kaitstud õigustele või huvidele (siinkohal nt teenuse tõkestamine), või varjata kuritegu karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

5. JUHTUMITE LAHENDAMISEKS KASUTATUD SEADUSED

< Juhtum 4 >

65-aastase pensionäri Leili juhtumit, kes täitis püüdlikult e-posti teel isikuandmete ankeedi ning seeläbi saadi andmepüügi abil teada tema isiklik informatsioon, mille ta arvas olevat pangast ning kelle arvelt seejärel kanti suur hulk raha tundmatule arveldusarvele, saab samuti lahendada kelmust ja arvutikelmust puudutavate paragrahvide abil.

Käesoleval juhul on modus operandi ehk toimepanemise viis õn- gitsemine.

< Juhtum 5 >

Õpetaja Tõnu puhul, kelle nimelt hakkas tuttavate e-postile saabuma e-kirju milles küsiti raha, on kvalifitseeritavad nii arvutikelmuse- sena kui ka teise isiku identiteedi ebaseadusliku kasutamisenä.

< Juhtum 6 >

17-aastane Joel pani kättemaksu teostamiseks Eliise suhtes toi- me teise isiku identiteedi ebaseadusliku kasutamise.

< Juhtum 7 >

Marteni suhtes, kes kutsuti kahtlustavana ülekuulamisega seo- ses kelmusega, oli aga ise sattunud kelmuse ohvriks.

< Juhtum 8 >

50-aastane Mare, kes andis telefoni teel enda kohta käivat infot isikule, kes väitis end olevat SEB panga esindaja, sattus nn vahen- dusründe abil kelmuse ohvriks.

5. JUHTUMITE LAHENDAMISEKS KASUTATUD SEADUSED

< Juhtum 9 >

Aare, kelle nimel oli tehtud krediidiasutustesse mitmeid taotlusi, sattus nii kelmuse kui ka teise isiku identiteedi ebaseadusliku kasutamise ohvriks.

< Juhtum 10 >

16-aastase kiusamise ohvrilt Gerdo sõber Priit pani tema suhtes toime teise isiku identiteedi ebaseadusliku kasutamise.

6.

ENNETUS

[illegible]

6. ENNETUS

Vastavalt 2012. aastal Euroopa Komisjoni poolt läbi viidud uuringule, oli 70% elanikkonnast kuulnud või näinud informatsiooni küberkuritegevuse kohta, 31% vastanutest pidas end üsna hästi informeerituks nimetatud kuritegevuse osas ning 7% pidas end väga hästi antud valdkonnas kursis olevaks.

Teine uuring, mis hõlmas enam, kui 13 000 internetikasutajat 24 riigis näitas, et 90% kustutab kahtlased e-kirjad ning 80% kasutab erinevaid antiviruse programme ega ava tundmatute saatjate poolt saadetud lisasid ega linke.

Samas sotsiaalsõrgustike kasutajast ainult 50% ütles, et nad kasutavad privaatsussätteid ja 35% kasutajatest aktsepteerivad võõraste poolt saadetud sõbrakutseid.

Uuringud laste ja noorte seas vähem arenenud riikides näitavad, et nemad on suuremas riskis sattuda küberkuritegevuse ohvriks. Uuringus, milles osales enam kui 25 000 koolilast Kesk- ja Lõuna-Ameerikas näitas, et 45% lastest, kellel oli kodus internetiühendus, kasutas ainult 10% viirusetõrjet või veebi filtreerimist.

Riigid peavaad kasutama oma võimalusi harimaks oma kodanikke enne, kui nad satuvad küberkuritegevuse ohvriks. Kõige efektiivsem on selles valdkonnas inimeste teavitamine küberkuritegevuse ohtude osas.

6.1. Ennetusmeetmed

Kasutades sotsiaalseid võrgustikke peab kasutaja:

- › Olema ettevaatlik info osas, mida ta seal jagab. Tundlikku informatsiooni ei tohiks avaldada;
- › Olema ettevaatlik info osas, mida teised enda kohta jagavad;
- › Valima hoolikalt, kellele ta jagab isiklikku informatsiooni;
- › Olema tähelepanelik tundmatute isikute suhtes;
- › Olema skeptiline ega mitte uskuma kõike, mida ta onlineis loeb või kuuleb;
- › Olema teadlik tingimustega, mida ta aktsepteerib, kui liitub sotsiaalsõrgustikuga, kuna see võib tähendada, et ta kaotab õigused sinna sisestatud informatsiooni üle.

6. ENNETUS

Kasutades e-posti peab kasutaja:

- › Võtma arvesse, et e-kirjad, mis on kirjutatud halvas eesti keeles ning võimalik, et ka näiteks eesti – soome või ka eesti – inglise segakeeles, on tõenäoliselt seotud andmepüügiga, isegi siis, kui e-kiri tuleb tuttavalt;
- › Võtma arvesse, et selline olukord tekib eriti nende e-kirjadega, mille sisuks on nt suur lotovõit vms, on probleeme e-posti kontoga või on vaja uuendada andmeid panga jaoks;
- › Mitte laadima alla lisasid, mitte “klikkima” linkidel ning mitte vastama tundmatutele e-kirjadele;
- › Uurima välja, kas e-kiri, mis väidetavalt tuleb pangast või koostööpartnerilt, on ikka sealt saadetud;
- › Kui e-mail on tulnud tundmatult asutuselt, siis uurima välja, kas kiri on ikka nende poolt saadetud;
- › Liigutama nn hiirt üle lingi enne sellele klikkimist vaadates brauseri vasakut alumist nurka, mis aadressi seal näidatakse;
- › Kui lingi domeen on teine, kui e-postis väidetakse, siis ei tohi antud lingile minna;
- › Võtma alati ühendust pangaga saades sealt e-kirja, kuna pangad ei kontakteeru kliendiga tavaliselt ew-posti kaudu;
- › Saades ebahariliku e-kirja tuttavalt, kus palutakse abi või isikuandmeid, olema ettevaatlik, kuna tegemist võib olla andmepüügiga;
- › Mitte kasutama tööga seotud e-posti isiklikuks otstarbeks;
- › Mitte saatma konfidentsiaalset informatsiooni e-posti teel;
- › Hoidma oma e-postiga seotud tarkvara uuendatuna;
- › Lülitama välja programmi võimalused, mille abil saavad e-postiga seotud failid automaatselt end alla laadida;
- › Lülitama välja Java.

Kaitsmaks arvutit ja mobiilset seadet, peab kasutaja:

- › Vältima erinevate seadmete jätmist kohtadesse, kus on neid kerge varastada (nt auto);
- › Kaitsma arvutit pahatahtlike kasutajate eest kasutades salasõna ja lukustama arvuti töö lõppedes ning pausi ajal;
- › Arvutit välja laenates tuleb arvestada selles sisalduva informatsiooniga ning sellega, et kõvakettale salvestatud teabele on siiski võimalik ligi pääseda ka siis, kui tegemist on salasõnaga kaitsitud kasutajakontoga;

6. ENNETUS

- › Kustutama kogu isikliku informatsiooni seadmest, kui see müüakse või vistakase ära;
- › Hoidma alati arvutis leiduva viirusetõrje ja nuhkvara programmi uuendatuna, samuit tulemüüri ja spämmivastase tarkvara;
- › Konfigureerima kasutatava brauseri selliselt, et see ei salvestaks nn küpsiseid ja hüpikaknaid;
- › Tõstma brauseri turvalisuse taseme keskmisele või kõrgele tasemele;
- › Pöörama tähelepanu installeeritud programmidele ja nende päritolule;
- › Hoidumast sisse logimast veebilehtedele, kus isiklikku informatsiooni jagatakse avalike võrgustikega või avatud Wi-Fi võrkudega või tundmatutesse arvutitesse;
- › Olema erilisel tähelepanelik veebilehtedele, kus jagatakse isiklikku informatsiooni, eriti pangandusega seotud lehekülgedel, samuti hoiduma lehekülgedest, kus on palju kirja- ja keelisi vigu;
- › Veenduma alati, et veebilehe aadressi eest on “https”, mis on turvaline, aga mitte “http”, mis on ebaturvaline. Samuti olema kindel, et ilmuks võtmekujuline kujutis;
- › Kasutama ainult oma panga ametlikku lehekülge;
- › Lugema läbi finantsasutuste jt isiklikku informatsiooni käitlevate asutuste privaatsuspoliitika;
- › Mobiiliseadmetes peab ekraanikuva olema aktiveeritud ja kaitstud;
- › Tee oma seadme sisust regulaarselt koopiaid ning ole selle infoga ettevaatlik ning võimalusel krüpteerima see ning loo tugev ja turvaline salasõna;
- › Seadmesse erinevaid nn äppe ehk rakendusi installeerides tuleb veenduda, et alla laadimine tuleb usaldusväärsest allikast ning pööra tähelepanu ka erinevate lubade küsimisele – näiteks kui rakendus, mis ei peaks küsima luba ligipääsuks Sinu e-maili kontole seda siiski küsib, siis ei tohiks nimetatud tarkvara alla laadida.

Kaitsmaks isikuandmeid sisaldavaid dokumente, peab kasutaja:

- › Kandma endaga kaasas ainult igapäevaselt olulisi dokumente;
- › Hoidma oma rahakotti töö olles turvalises kohas;
- › Kodus hoidma oma dokumente kindlas kohas, näiteks seifis;
- › Hävitama kehtivuse kaotanud füüsilised ja digitaalsed dokumendid, mis võivad sisaldada isiklikku informatsiooni, et muuta võimatuks selle informatsiooni kasutamine;
- › Tee kindlaks isik, kes küsib isiklikku informatsiooni telefoni teel, e-posti kaudu või muul moel ning nimetatud isiku põhjus info küsimiseks:
 - » Küsi helistajalt tema andmeid ning esindatava asutuse peamiseid andmeid;
 - » Proovi mõelda, mida isik võib vajada teada saada: finantsasutus võib teada nt

6. ENNETUS

kasutaja ema neiu põlve nime ning seda võib küsida. Samasl ajal kui keegi kontakteerub küsimaks näiteks ema neiu põlve nime väitega, et võtab ühendust finantssasutusest, tuleb meele pidada, et selline asutus ei vaja seesugust informatsiooni – seesuguse kõne eesmärk on õngitseda informatsiooni;

- » Kui võõras isik helistab või saadab e-kirja, milles teavitatakse nt võidust ning küsib isiklikku laadi informatsiooni, siis peab kasutaja paluma saata kirjalik teade. Kui dokument saadetakse, siis peab kasutaja lugema seda hoolikalt ning informatsiooni saates adresseerima selle tuntud ja hea mainega asutusele;
- › Olles reisil ning jagades detailset infot telefoni teel usaldusväärsele isikule tuleb veenduda, et kedagi ei ole lähedal ja kuulmas;
- › Teavitama erinevaid asutusi, et tema kohta käivat informatsiooni ei ole lubatud jagada;
- › Hoidma olulist informatsiooni salasõnaga kaitsitud failides;
- › Krüpteerima eriti olulise informatsiooni.

Kasutades tavaposti peab kasutaja:

- › Kindlustama oma postkasti ligipääsmatuse kasutades head lukku;
- › Võtma posti ära piisavalt tihti, et välistada selle kuhjumist ning seeläbi vältima võimalust, et võõras isik saab postkastist siiski posti kätte;
- › Reisides paluma, et võimalusel hoiustatakse posti lähimas postiasutuses või paluma usaldusväärselt isikult, et ta võtaks posti postkastist ja hoiustaks enda juures;
- › Proovima kontrollida oodatavate kirjade saabumist, mis sisaldavad krediit- või deebetkaarte, panga teateid või arveid;
- › Võimalusel saata isiklikku informatsiooni sisaldavad dokumendid tähitud postiga;
- › Kolides uude elukohta teavitama postkontorit oma uuest aadressist.

Tegemaks turvalisi finantstehinguid peab kasutaja:

- › Teostama ülekandeid ainult turvaliste veebilehtede kaudu, milliste aadressid algavad “https”-ga;
- › Pidama meeles, et veebitehingute puhul küsivad pangad ainult teatud osa numbritest krediitkaardil vm;
- › Pidama meeles, et pangad ei vaja lisaprogrammide installerimist suurendamaks tehingute turvalisust – sellised programmid on reeglina pahavara;
- › Küsimuste korral kontakteeru pangaga telefoni teel;

6. ENNETUS

- › Hoia Java ja Flash uuendatuna;
- › Kaitse kõiki kontosid salasõnaga.

Vestlemaks erinevate programmide abil online turvaliselt, peab kasutaja:

- › Kasutama valenime, mis ei võimalda tema tuvastamist;
- › Kasutama selliseid vestlusportaale, millistel on moderaator;
- › Hoidma enda kohta käivat informatsiooni salajas;
- › Salvestama vestlusi;
- › Mitte avama erinevaid manuseid, mis saadetakse vestluse kaudu.

Koostamaks turvalisi salasõnu, peab kasutaja:

- › Vältima aimatavaid sõnu ja numbreid;
- › Vältima klaviatuuril järjestikuste tähtede kasutamist salasõnana. Lisaks sellele, et see on suhteliselt levinud võte, on sellist kombinatsiooni ka lihtne ära arvata;
- › Salasõna luues mitte kasutama isiklikku infot, mis on teada paljudele (nt sünniaeg, nimi, selle osa, aadress jne);
- › Looma salasõnad maksimaalses lubatud pikkuses;
- › Kombineerima tähti, numbreid ja sümboleid;
- › Olema loominguline (nt erilise tähtsusega fraas millest salasõnaks kasutada iga sõna esimest tähte vms);
- › Salasõna koostamisel kasutama nii suuri kui ka väikeseid tähti ning kasutada tähtede asemel numbreid vm sümboleid);
- › Loo erinevatele kontodele erinevad salasõnad (kui pead neid üles märkima, siis ära tee seda arvutis);
- › Muuda salasõnu regulaarselt.

MÄRKUS: Vanemad peavad pidevalt jälgima oma laste ja noorte tegevusi arvutis kindlustamaks, et lapsed ja noored kasutavad ülalkirjeldatud meetodeid.

6. ENNETUS

6.2. Märgid pahavaraga nakatumisest

Töenäosus sattuda identiteedivarguse ohvriks suureneb, kui arvuti on nakatunud pahavaraga. Seega on oluline tunda märke, et arvuti on sellega nakatunud:

- › Aeglus;
- › Sagedased blokeeringud;
- › Hüpiksõnumite ja –piltide ilmumine, veidrad helid või ilma loata instaleerunud programmid;
- › Kaitsemehhanismide (nt viirusetõrje) iseeneslik seiskumine;
- › Süsteemi võimetus tunda ära suurtähti;
- › Internetiühenduse pidev ja seletamatu tegevus;
- › Kodulehekülje või eelistatud brauseri iseeneslik muutumine;
- › Pidev iseeneslik suunamine võõrastele internetilehekülgedele;
- › Uute lemmikute ilmumine nn lemmikute nimekirja või brauseri ülaossa;
- › Kommentaaride iseeneslik avaldamine sotsiaalsõrgustikes;
- › Vestluste iseeneslik tekkimine nt Skype's, Facebook Messenger'is, Google Talk'is jne;
- › Palju tagasisaadetud e-kirju, mille vastuvõõt nurjus ning milliseid saatja ise saatnud ei ole;
- › Java ikooni teke tööriistaribale ilma, et kasutaja ühtegi sellepõhjalist programmi teadlikult kasutaks.

6.3. Kuidas saada aru, et olete sattunud identiteedivarguse ohvriks?

Identiteedivarguse tagajärjed võivad olla seda tõsisemad, mida hiljem see avastatakse. Seega, et hoida ära tõsisemaid tagajärgi, on oluline olla teadlik sellele viitavatest märkidest. Seega vaatleme järgnevalt mõningaid tegevusi, mis sellisele olukorrale viidata võivad:

Selleks, et avastada õigeaegselt identiteedivargus, peab kasutaja:

- › Olema valvas igasuguse ebahariliku tegevuse osas oma e-posti ja sotsiaalsõrgustike kontodel;
- › Hoidma pidevalt oma erinevatel võimalikel panga-, krediidi ja investeerimiskontodel nõ silm peal:

6. ENNETUS

- » Kontrollima oma kontoväljavõtetelt pidevalt viimased tehinguid;
- » Märkama tehinguid, mida ta ise ei ole teinud;
- › Kontrollima krediitkaardiväljavõtet märkamaks tehinguid, mida ta ise ei ole teinud;
- › Ühinema finantsasutuste erinevate ohu tõrjumiseks mõeldud tegevustega;
- › Uurima põhjuseid, miks keeldutakse väljastama laenu või krediitkaarti vms (tegemist võib olla kurjategijate eelneva ohvri andmete väärkohtlemisega);
- › Võtma ühendust krediitdiasutusega, kui ei ole saabunud igakuist väljavõtet (kui selline teenus on tellitud);
- › Kui saadakse info selle kohta, et panga jt finantsasutuste info saadetakse aadressile, mida konto omanik ei ole lubanud ega teatanud ning, et keegi võib kontot kasutada ebaseaduslikult. Sellises olukorras on oluline küsida koopiaid kõigist makstud arvetest ning alates eelmisest kontrollitud väljavõttest kõiki kontol teostatud tehinguid.

7.

OHVRI TOETAMINE

7. OHVRI TOETAMINE

7.1. Pahavaraga nakatumisel

Pahavaraga nakatumisel peab kasutaja:

- › Katkestama internetiühenduse, et see ei nakataks võimalikke teisi arvutied;
- › Puhastama arvuti sisu – see võib tähendada kogu süsteemi uuesti paigaldamist ja seda võib teha nii spetsialist kui ka kasutaja ise, kui tal on ka tegeliike teadmisi, kuidas selliseid protseduure tehakse;
- › Panema tööle arvuti puhastamiseks ettenähtud programmi nn “safe mode”is või CD-lt;
- › Muutma kõik salasõnad.

7.2. Identiteedivarguse korral

Peale internetipõhise identiteedivarguse ohvriks sattumist peab kasutaja teadma võimalusi, kuidas peatada kahju tekkimine ning vähendada mõju oma isiklikule ja sotsiaalsele elule ning suhtlusele ning rahalistele vahenditele.

Identiteedivarguse korral peab kasutaja:

- › Võtma koheselt ühendust oma panga vm finantsasutusega;
- › Tühistama kõik krediit- ja deebetkaardid ning paluma väljastada endale uued kaardid, muutma kõik PIN-koodid, kui kurjategijal võis olla ligipääs erinevatele kontodele või salajasele informatsioonile;
- › Sulgema kõik kontod, millele kurjategijal võis olla ligipääs;
- › Tühistama internetipanga juurdepääsud ning paluma uusi, kui küberkurjategijal võis olla ligipääs;
- › Taotlema finantsasutuselt vajalikke taotlusvorme vaidlustamiseks tehinguid, mis võisid olla teostatud kurjategija poolt kasutaja nimel;
- › Kui ei ole kindlaks määratud taotlusvorme, siis peab kasutaja saatma kirja kõne all oleva asutuse tugiteenuseid osutavale aadressile;
- › Küsima kõiki krediitkaardi ja deebetkaardi tehingute väljavõtteid ning otsima neilt tehinguid, mis on kurjategija poolt tehtud ning selliste tehingute leidmisel sellest viivitamatult finantsasutust;

7. OHVRI TOETAMINE

- › Valede tehingute tuvastamisel tuleb paluda finantsasutusel nimetatud konto ja kaardi kasutamise kohta teha nõuettehing.
- › Paluda finantsasutusel mitte saata väljavõtteid oma kontaktidele (e-post, kodune jm aadress);
- › Peale identiteedivarust tuleb aastaid hoolikalt jälgida kontoga tehtud tehinguid;
- › Kontrollida Maksehäireregistrit;
- › Teavitama kuriteost politseid või prokuratuuri;
- › Edastama kaebuse finantsasutusele;
- › Küsima enda kohta infot karistusregistrit kontrollimaks, kas sealne info on õige;
- › Muutma enda e-posti konto salasõna, kuna kurjategijal võis olla sellele ligipääs;
- › Teavitama teenuseosutajat, postiasutust, sotsiaalsüsteemi (toetused) ja Maanteeametit (lubadega ningsõidukite ost/müük jms seonduv);
- › Hoiatama tööandjat, et ta võib olla identiteedivaruse ohver juhaks, kui neile laekub mingit infot ohvri osas;
- › Hoidma alles kõik e-kirjad, SMSid ja kirjad võimaliku teo toimepanijaga. Samuti on oluline hoida alles kirjavahetus finantsasutusega kasutamaks neid vajadusel tõendusmaterjalina.

1. Kui oled sattunud identiteedivaruse ohvriks sotsiaalvõrgustikus Facebook seoses käitumissuga, et avaldada laimavat informatsiooni, siis peab:

- › Teavita loodud kontost tehes järgmist:
 - » Vajuta märgil “...” “Sõnum” või “Message” nupu kõrval, mis asub kontol profiili ülemises paremas nurgas;
 - » Avaneb neli võimalust, millest tuleb valida “Teavita” ehk “Report”;
 - » Siis valida variant “Teavita sellest kontost” ehk “Report this account”;
 - » Ilmub küsimus “Mis on valesti?” ehk “What’s wrong with this account?” ning seal tuleb valida “This timeline is pretending to be me or someone I know” ehk antud konto teeskleb mind vi kedagi, keda ma tunnen;
 - » Seejärel ilmub küsimus “Who are they pretending to be?” ehk keda antud konto teeskleb, millel tuleb teha valik “Me” ehk mind;
 - » Avaneb teade “Based on what you chose, here are a few things you can do.” ehk arvestades, mida sa valid, saab nii mõndagi teha ja siis tuleb valida “Submit to Facebook for review” ehk saada Facebook’ile läbi vaatamiseks;
 - » Lõpetamiseks valida “Done” ehk tehtud.

7. OHVRI TOETAMINE

- › Teavitamiseks avaldatud infost tuleb:

- » Vali noolekujutis, mis näitab suunaga alla, mis asub postituse ülemises paremas nurgas ning vali “I don’t like this post” ehk mulle ei meeldi see postitus.

2. Kui toimepanija loob vale lehekülje ohvri nimega selleks, et jagada laimavat informatsiooni, siis peab sellest teavitamiseks:

- » Valima “...” “Message” nupu kõrval lehekülje ülal paremas nurgas;
- » Avaneb viis võimalust, millistest tuleb valida “Report Page” variant;
- » Seejärel tuleb valida valik “Is troubling me or someone I know”;
- » Avaneb sõnum “We’re sorry you had to go through this experience. Here are some things you can try to solve this.” ning seejärel tuleb valida “Submit to Facebook for review”;
- » Lõpuks vajuta “Done”.

3. Kui on kasutatud ohvri õiget lehekülge avaldamks laimavat infot:

- › Vaheta parooli, milleks:

- » Vajuta taba kujutisega märki lehekülje ülal sinisel ribal paremal nurgas;
- » Sealt vali “See more settings”;
- » Järgnevalt vali variant “General” avaneva lehe üleval vasakus nurgas;
- » Seejärel avaneb ekraanil «General account settings» ja variandil “Password” tuleb vajutada “Edit”;
- » Seejärel tuleb sisestada vana parool ja uus parool kaks korda;
- » Järgnevalt tuleb valida “Save changes”;
- » Ilmub teade: «Your password has been changed. Log out of other devices?» ja tuleb valida «Log me out of other devices», mis logib sinu kasutaja välja kõigis arvutites ja seadmetes, kus oled või on keegi Sinu nime alt end sisse loginud;
- » Lõpuks vajuta “Submit”.

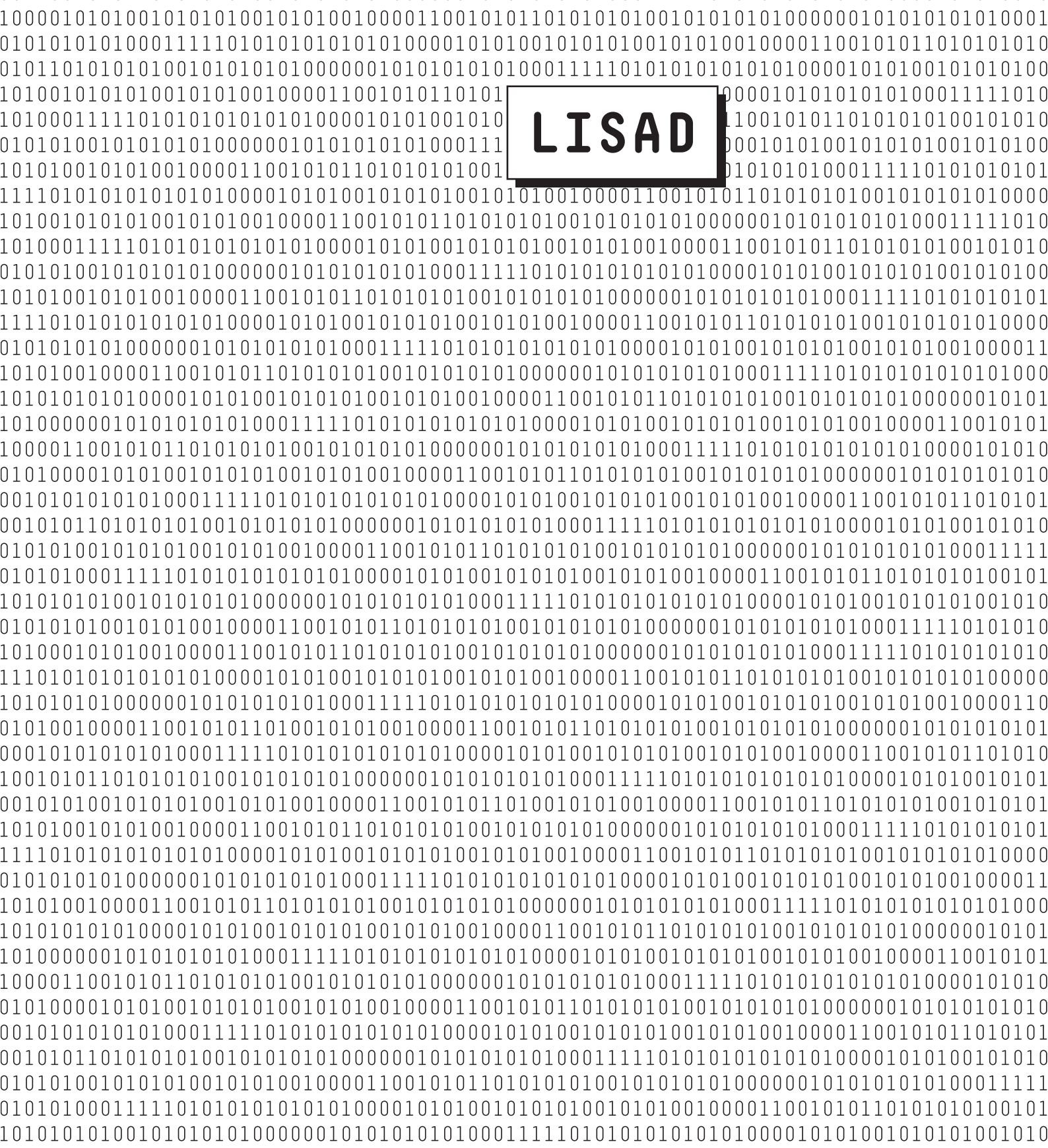
- › Avaldatud teadete kustutamiseks tuleb:

- » Vajutada noolt alla, mis asub postituse üleval paremas nurgas ning valida “Delete”;
- » Avaneb teade “Are you sure you want to delete this?” ning tuleb uuesti vajutada “Delete”.

7. OHVRI TOETAMINE

4. Igal juhul:

- › Blokeeri teo toimepanija, et tal ei oleks enam ligipääsu sinu postitustele. Selleks tuleb:
 - » Vajutada "...", "Message" nupu kõrval profiili üleval paremas nurgas isiku kontol, keda soovid blokeerida;
 - » Avaneb neli võimalust, millistest valida "Block";
 - » Küsitakse "Are you sure you want to block ...?" ning seejärel tuleb vajutada "Confirm".
- › Tee avaldus politseisse või prokuratuuri õigusliku seisukoha võtmiseks.



LISAD

[illegible]

LISAD

Sõnaseletusi

Bot ja botnet – Väljend tuleneb sõnast robot. Kurjategijad jagavad pahavara, mis saab muuta kasutaja arvuti nn bot'iks ehk robotiks, vahel kasutatakse sel puhul ka väljendit zombi. Kui see juhtub, teeb kasutaja arvuti internetis automaatseid toiminguid. Kurjategijad kasutavad tavaliselt bot'e selleks, et nakatada võimalikult suurt hulka arvutied. Nakatatud arvutid moodustavad võrgustiku ehk botnet'i, mida omakorda kasutatakse spämmi ehk rämpsposti saatmiseks, viiruste levitamiseks, teiste arvutite ja serverite ründamiseks ning erinevate kuritegude (nt kelmus(toimepanemiseks. Kui kasutaja arvuti on osa botnet'ist, muutub see väga aeglaseks ning selle kasutaja võib tahtmatult osutada kurjategijatele nende tegevuses kaasabi;

Brauser ehk **veebilehitseja** – Programm, mida kasutatakse interneti kasutamiseks;

Chat – Vestlus internetis;

Cooky ehk **nn küpsis** – Küpsis on fail, mis on loodud veebilehekülje poolt talletamaks informatsiooni kasutaja arvutis, sh selle arvuti eelistuste osas lehekülje külastamisel. Minnes leheküljele, mis kasutab "küpsiseid", võib külastatav lehekülg küsida veebilehitsusprogrammilt luba salvestada/paigaldada arvuti kõvakettale nn küpsiseid. Hiljem sama lehte külastades saadab brauser selle leheküljega puutumuss olevaid küpsiseid, mis võimaldab leheküljel pakkuda kasutajale tema huvidest lähtuvat informatsiooni. On olemas küpsiseid, mis on loodud lehekülje poolt ja võimaldavad kasutajal mitte sissestada igakordselt salasõna samal ajal, kui teised leheküljed jätavad kasutaja valikud meelde.

Arvuti andmed – igasugune teave, mida arvutisüsteem suudab töödelda, sh programmid, mis toetavad arvutisüsteemi poolt info töötlemist. Väljendi "arvutisüsteem" definitsoon ECCC kohaselt katab kõikvõimaliku tehnoloogia, sh uuemad mobiiltelefonid, nutitelefonid, tahvelarvutid jne.

Arvutisüsteem – Seade või omavahel ühenduses olevate seadmete kogum, millest üks või mitu tegelevad sarnaste andmete automaatse töötlemisega;

Download/allalaadimine – Mingi dokumendi või interneti sisu üle kandmine internetist kasutaja seadmesse;

E-mail/E-post – Elektrooniline post;

Flash (laiendiga .flv failid) – Failid, mis on genereeritud Adobe Flash Player'i poolt ning mis on teatavat tüüpi tarkvaraliik, mida kasutatakse interaktiivsete animatsioonide loomiseks;

Java – Programmeerimiskeel;

Link – Viide veebilehele;

Login ehk **sisselogimine** – Protsess, mille abil sisenetakse arvutisüsteemi ning süsteem on kasutaja poolt kontrollitav kasutades selleks autoriseerimist ning identifitseerimist salasõna jm vahendite abil;

Pahavara – Tarkvara, mis on loodud ebaseaduslikuks siseneamiseks võõrasse seadmesse või seadmete süsteemi eesmärgiga tekitada kahju, muutusi või varastada informatsiooni (nii konfidentsiaalselt kui ka mitte konfidentsiaalselt). Arvutiviiruseid, nn ussiviirust ja nuhkvara nimetatakse pahavaraks;

LISAD

Pop-up ehk hüpikaken – Lisaaken brauseris, mis avaneb sisenedes veebilehele või avades mingi ühenduse;

Remote wipe ehk üle võrgu puhastus – Turvalisusega seotud meede, mis võimaldab võrguadministraatoril või seadme omanikul saata seadmele kaugkäsk info kustutamiseks;

Teenusepakkuja – Iga juriidiline või füüsiline isik, kes pakub kasutajatele arvuti abil suhtlemise teenust. Samuti isik, kes protsessib või hoiab kasutajate informatsiooni;

Spoofing (eesti keeles tüssamine) – Selline rünne on olukord, kus isik või programm teeskleb olevat keegi/miski teine ning saab seeläbi informatsiooni või eeliseid, mille saamiseks tal õigus puudub.

Nuhkvara – Automaatne arvutprogramm, mis kogub informatsiooni kasutaja internekäitumise kohta ning edastab selle informatsiooni interneti vahendusel kolmandale isikule ilma kasutaja teadmata. Ühelt poolt saab nuhkvara arendada ettevõtetes, kes soovivad kasutajate harjumis ning seeläbi kasutada kliendile suunatud reklaami. Teisalt kannavad paljud viirused endas nuhkvara, mille eesmärk on omandada kasutaja isiklikke andmeid, nt pangadetaile.

Andmeside – Andmed, mis on seotud arvutisüsteem abil suhtlusele ning mis on loodud arvutisüsteemi poolt, mis on osa suhtlusest ning mis viitab ka andmeside päritolule, sihtmärk, teekon-nale, kellaajale, kuupäevale, suurusele, kestvusele ja teenusele.

Website/Site ("sait") – Veebilehekülje asukoht internetis;

Wi-fi – Juhtmevaba internetiühendus;

World Wide Web/WWW/Web – See on süsteem, mis on ühenduses nn hüpermeedia dokumentidega, mis on seotud internetiga.

LISAD

Pankade jt seotud asutuste kontaktid

SEB Pank

(+372) 6 655 100

Sampo Pank

(+372) 6 812 300

BIG Pank

(+372) 7 311 333 (1333)

Swedbank

(+372) 6 310 310

Krediidipank

(+372) 6 690 900

Finantsinspektsioon

(+372) 6 680 500

Nordea Pank

(+372) 6 283 300

LHV Pank

(+372) 6 800 400

Eesti Pangaliit

(+372) 6 116 567

[illegible]

[illegible]

APAV[®]

 associação portuguesa de
Apoio à Vítima



FISCALÍA GENERAL DEL ESTADO



**PÄRNU CENTRE
FOR GENDER
BASED VIOLENCE**



Procuradoria-Geral da República

1110Käesoleva materjali paljundamine ja tsiteerimine on lubatud mittetulunduslikel1010
0100eesmärkidel ning allikale viidates.0101010100000010101010101000111101010010101
1010Käesolev trükkis väljendab autori seisukohti. Euroopa Komisjon ei vastuta1110101
0001selles sisalduva informatsiooni ning selle kasutamise eest.01010101000101011001
0100001010100100001100101011010101010010101001010101010100000010101010101000111110101
0100Projekti eestvedaja on Portugali ohvriabi organisatsioon ning seda kaasrahastati0101
1010Euroopa Komisjoni kuritegevuse ennetamise ja selle vastu võitlemise programmi1001
0101raames.101010010100010101010100011111010101010101010000101010010101010010001010
01011001010101010010100011111010101010101010000101010010101010010101001000011001010
01000011001010110101010100101010101000000101010101010001111101010101010101000010101
1010100101010101010000001010101010100011111010101010101010000101010010101010010101001