PROJECT PROTEUS | SUPPORTING VICTIMS OF IDENTITY THEFT AND IDENTITY FRAUD

European Crime Prevention Award | Best Practices Conference

Tallin | 13-15 December 2017

CYBERCRIME

370 million victims per year

1 million per day

12 every second

CYBERCRIME

@ **lack of awareness of the general public**

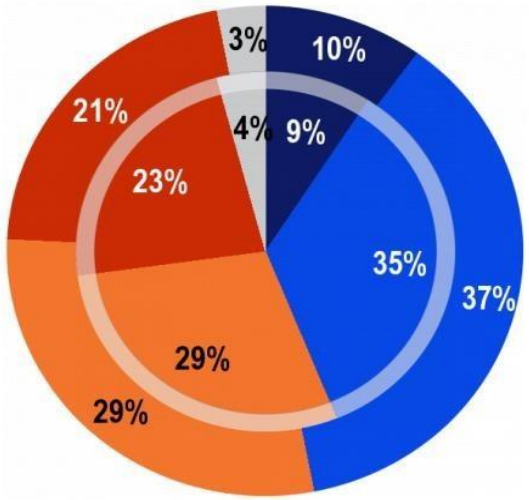
@ **insufficient preparation from services and even authorities**

@ **complexity of the cases and of *modi operandi***

what is your password?

CYBERCRIME

QB1. How well informed do you feel about the risks of cybercrime?



- Very well informed
- Fairly well informed
- Not very well informed
- Not at all informed
- Don't know

Inner pie : EB79.4 May-June 2013
Outer pie : EB82.2 Oct. 2014

EU28

TYPES OF CYBERCRIME

- @stalking
- @disseminating private contents
- @using malware
- @child sexual abuse
- @cyberbullying
- @phishing
- @romance scams

SHAME

IMPACT

CYBERCRIME

A NEW CHALLENGE FOR VICTIM SUPPORT

- gathering knowledge and expertise
- adopting best practices
- providing intensive training based on these best practices
- assessing the effectiveness of the intervention models

PROTEUS

With the financial support of the Prevention of and Fight against Crime Programme European Commission - DG Home Affairs

APAV
associação portuguesa de Apoio à Vítima

FORMAÇÃO APAV

SUPPORTING VICTIMS OF IDENTITY THEFT AND IDENTITY FRAUD

partners

Polícia Judiciária (Judiciary Police) (Portugal);

Procuradoria-Geral da República (General Prosecution) (Portugal);

Pärnu's Centre of Gender Based Violence (Estonia);

Ficalía General del Estado de España (Spain);

General Inspectorate of the Romanian Police (Romania)

PARTICIPANTS AND BENEFICIARIES

judicial authorities

law enforcement

victim support

private sector

SPECIFIC ISSUES ADDRESSED

underreporting

… derives from lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment, and perceived reputation risks for corporations…

impact on victims

… besides financial losses, the costs also include the time and hassle required sorting matters out. The psychological effects too are not inconsiderable, with victims reporting a variety of reactions: from fear, anger and distress, through to prolong cautiousness and suspicion …

lack of prevention and support

… forgotten victims …

OBJECTIVES

General objective

to contribute to the prevention of criminality and the protection of victims of crime

Core objective

to contribute to increase knowledge, skills, information and awareness on identity theft

Specific objectives

- capacitate professionals: exchange of knowledge, training and best practices
- information and prevention: raising awareness campaign

ACTIVITIES

best practices

Creation of a best practice guide (PT, RO, EE, ES) on the support to victims of identity theft

awareness raising campaign

raising awareness campaign with 40.000 leaflets, 6.000 posters, press/web adds, bus shelter adds and street furniture;

training

Design of a training course (PT, RO, EE, ES) on the support to victims of identity theft

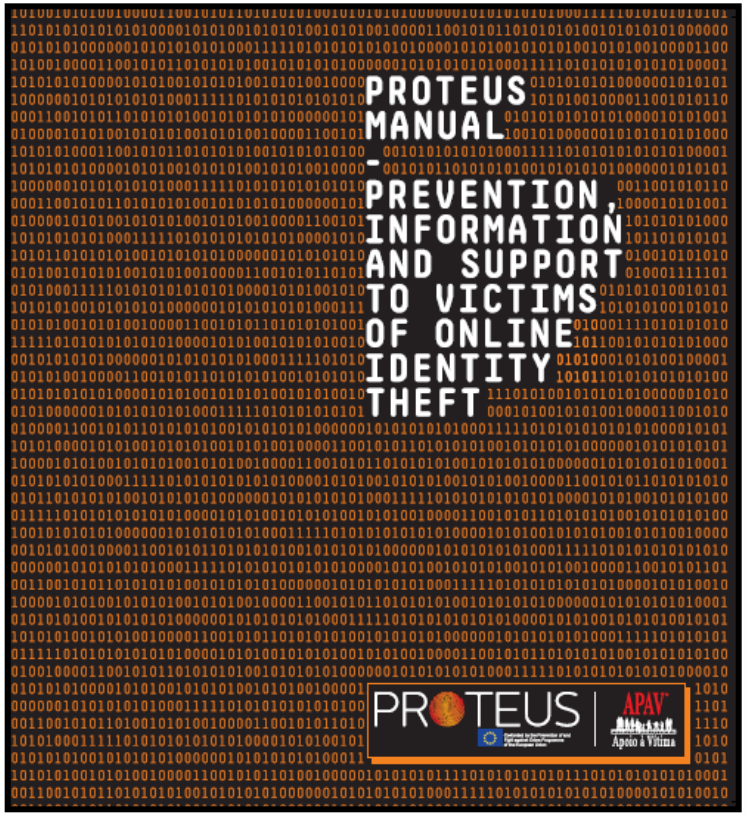
conference

1 final conference in Lisbon

workshops

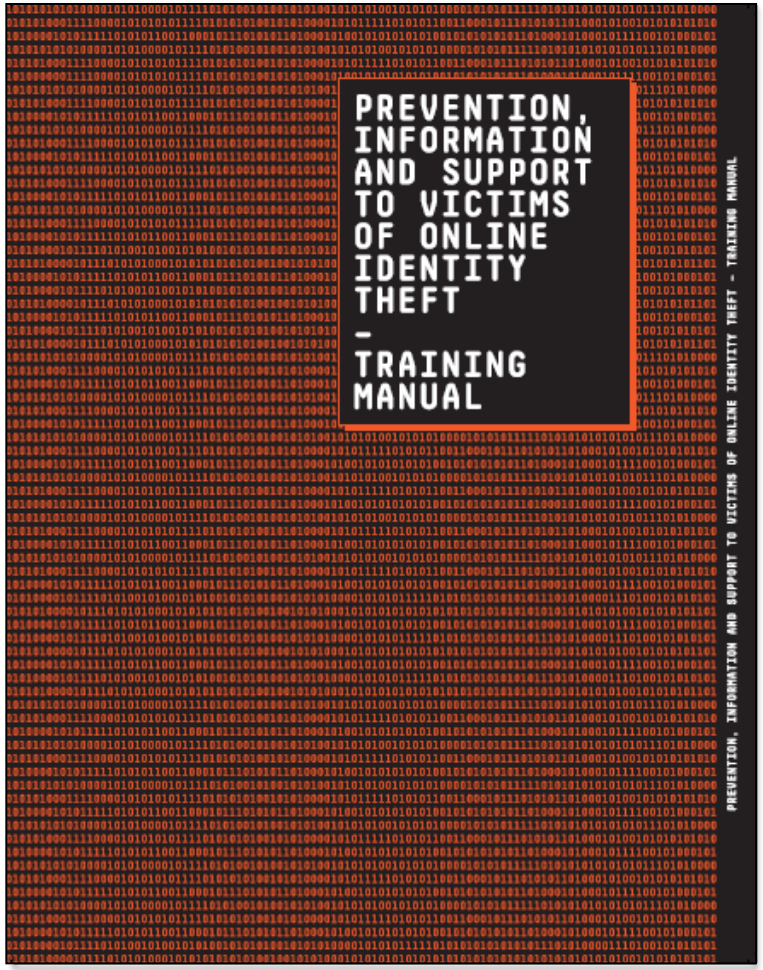
2 workshops (local experts + project team) in RO and ES: “Phishing: from origin to destination: using the banking system for money laundering”; “Social networks and identity theft”

BEST PRACTICES GUIDE



- cybercrime and identity theft
- modus operandi
- risk factors
- impact on victims
- difficulties for investigation
- national and international law
- prevention advice
- providing support
- glossary

TRAINING MANUAL



index

AWARENESS RAISING CAMPAIGN

AWARENESS RAISING CAMPAIGN

Küberkuritegevus

Küberkuritegevus (süüteod, mis on toime pandud kasutades arvuteid ja/või internetti) on kasvav ja pidevalt muutuv nähtus ning on seoses sellega muutumas üheks suurimaks ohuks inimestele, ettevõtetele ja ka riikidele. Järjest suurem hulk kurjategijaid kasutavad pidevalt arenevaid erinevaid info- ja kommunikatsioonitehnoloogia võimalusi, et panna toime kiireid, anonüümseid ja suuri inimhulki korraga haaravaid kuritegusid, millistel on olulised majanduslikud, praktilised, emotsionaalsed ja sotsiaalsed tagajärjed. See kõik saab aga juhtuda siis, kui me ei ole ise valmis ega oska end kaitsta.

PANGAANDMED

Andmepüük pannakse tavaliselt toime läbi suure hulga e-kirjade saatmise erinevatele saajatele (nn spämm) aadressilt, mis võib olla samane panga e-posti aadressiga. Nimetatud e-kiri sisaldab tavaliselt linki. Saajatel palutakse vajutada lingile ning tavaliselt on väidetavalt põhjuseks vajadus uuendada andmeid. Lingile vajutades avaneb panga veebilehele samane leheküg, kuid ei ole seda siiski. Lehele jõudes tuleks justnagu sisestada oma personaalsed internetipanga koodid. Sisestatud info võimaldab aga lehekülje loonud isikul saada ligipääsu konto omaniku rahalistele vahenditele ja kanda see edasi teisele kontole.

TÖÖALASED PETTUSED

Tegemist võib näiliselt olla üsna tavapärase tööpakkumisega, kuid tegelikkus on sellest väga kaugel. Ühendust võttes pakutakse suurepäraste tingimustega tööd. Kõik, mida tööotsija peab tegema, on tasuda koheselt värbajale teenuse eest või siis mingite väidetavate sertifikaatide, koolituste vms eest. Mõnel juhul soovitakse saada ka isikuandmeid ja pangadetaile väites, et seda on vaja protsessi paremaks sujumiseks. Igal juhul ei ole pakutud töökohta olemas. Halvimal juhul võidakse ohvrit veenda hoopis tegema ülekandeid ning seeläbi olema osa mõnest rahapesuga seotud skeemist.

SOTSIAALVÕRGUSTIKUD

Sotsiaalvõrgustikud on kurjategijatele eriti meelepärased, sest kasutajad postitavad enda kohta suurel hulgal infot. Üks sotsiaalmeedias sageli kasutatavatest skeemidest on erinevate linkide saatmine ja nn seinale postitamine ning nende juures on sellised loosungid nagu "Vaata, mida Sinu kohta on postitatud!" või inglise keeles "Don't miss this video!" vms. Samuti võidakse saata mängu- või sõbrakutseid. Igal juhul võib saadetud lingile vajutades oma seadmesse – olgu see siis kasutaja arvuti, telefon või tahvelarvuti – pahavara, mida kurjategijad hiljem kasutavad ohvrite andmete kogumiseks. Veel ühe variandina võidakse inimene juhatada edasi võltsleheküljele, kus palutakse sisestada uuesti oma kasutajatunnus ja salasõna. Info saab kurjategija ning seda saab hiljem kasutada mitmel erineval moel. Väga sage skeem on võltsi profiili loomise abil või olemasolevate profiilide ära kasutamine selleks, et saata erinevatele kontaktidele nn spämmi, mis on seotud kontaktide eelnevate eelistustega.

ROMANTIKA

Potentsiaalse ohvriga võetakse ühendust sotsiaalvõrgustiku või tutvumisportaali kaudu kellegi poolt, kes väidab end olevat nn rikka riigi kodanik, edukas, perekond puudub ning, et otsib omale hingesugulast. Nimetatud isiku profiili juures on tavaliselt ka kena mehe või naise pilt. Peale esimest kontakti algab võrgutamise osa ning pettur kasutab läheduse saavutamiseks ära kogu info, mis ta oma ohvri kohta leida suudab. Sellest hetkest alates, kui kurjategija tunneb, et suhe on loodud, ligub pettus edasi järgmisesse faasi, mis tähendab, et pettur küsib raha seoses mingi ootamatu ning tõsise sündmusega. Kuna emotsionaalne side on loodud, aitab aga ohver armastatut meelsasti...

10 ennetuslikku nõuannet

1	Lae oma seadmetesse kvaliteetne viirusetõrje ning uuenda seda regulaarselt.
2	Hoia oma salasõnad, internetipanga koodid ning muu isiklik info salajas ning ära avalda neid kellelegi.
3	Enne e-kirjaga saabunud manuste avamist või kirjas saadetud lingile klikkimist ole veendunud, et e-kiri on pärit sealt, kust väidetakse.
4	Internetti kasutades ole veendunud, et kasutad turvalist ühendust: kontrolli, kas aadressiribal on "https" mitte "http" ning et aadressiriba alguses on tabaluku kujutis.
5	Ülekandeid tehes pea meeles, mida Sinult pank tavaliselt küsib (koodi kolm viimast koodi, kalkulaatori pin jms) ning, et tavaliselt on see üks ja sama number, kui midagi esimesel sisestusel peaks valesti minema. Seega – kui küsitakse ka teisi koode või muud tavapärasest erinevat, siis on see märk sellest, et tegemist on võltsi lehekülgega.
6	Väldi oma kontodele logimist avalikus Wi-Fis olevatest või võõrastest seadmetest.
7	Ära avalda enda kohta käivat informatsiooni ei telefoni ega e-kirja teel enne, kui oled veendunud, kellega räägid või kellelt on saabunud e-kiri.
8	Ära jaga liiga palju enda kohta käivat informatsiooni sotsiaalvõrgustikes, eriti sünniaega, aadressi, telefoninumbrit, asukohta ning laste pilte ja videosid.
9	Ära vasta võõralt isikult tulnud sõbrakutsele.
10	Aktiveeri olemasolevad privaatsuse ja turvalisuse võimalused.

formacaoapav.pt

www.apav.pt/cibercrime

prevenir e formar

Obrigad@

mafaldavalerio@apav.pt

Rua José Estêvão, 135 A, Piso 2
1150-201 Lisboa
formacao@apav.pt
21 358 79 26/28