
Projekti number: 2020-1-LT01-KA203-078070

# O1-A2: Tulemused "Andmepüüdi äratundmine ja oskuste lüngad"

RAPORT

2021

# Partnerid

Vilnius University, Lithuania

Website: http://www.vu.lt

University of Tartu

Website: https://www.ut.ee/et

MECB - Macdac Engineering Consultancy Bureau LTD , Malta

Website: http://www.mecb.com.mt/eu

Altacom SIA, Latvia

Website: https://www.altacom.eu/

DOREA Educational Institute, Cyprus

Website: https://dorea.org/

ECDL- Information Technologies Institute, Lithuania

Website: http://www.ecdl.lt/

Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

# Sisukord



# Tabelite loend




Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

# Jooniste loend



# Lühendite loend

| | |
|---|---|
| **CEO** | Chief executive officer |
| **ENISA** | European Union Agency for Cybersecurity |
| **EU** | European Union |
| **EUROPOL** | The European Union Agency for Law Enforcement Cooperation |

Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

# 1. Sissejuhatus

## 1.1. Küberturvalisus Euroopa Liidus: reaalsus ja vajadused

Euroopa Komisjon on koostanud ja viinud läbi 2019. aastal spetsiaalse Eurobaromeetri uuringu[1], mille eesmärk on mõista ELi kodanike teadlikkust, kogemusi ja arusaamu küberturvalisusest. Ootuspäraselt näitasid tulemused, et Interneti kasutamine Euroopas kasvab jätkuvalt, eriti nutitelefonide kaudu. Tulemused[2] näitasid ka seda, et ELi kodanikud on rohkem teadlikud veebi kasutamise võimalikest ohtudest: 52% vastanutest väitis, et on küberkuritegevusest üsna hästi või väga hästi informeeritud (2017. aastal 46%). Uuringu tulemuste kohaselt on privaatsuse ja küberturvalisuse pärast rohkem kui üheksa Interneti-kasutajat kümnest muutnud oma veebikäitumist. Levinumad muutused on: tundmatute inimeste e-kirju ei avata, kasutatakse viirusetõrjetarkvara, külastatakse ainult teadaolevaid ja usaldusväärseid veebisaite ning logitakse sisse ainult isiklikku arvutisse.

Kuigi need tulemused on üsna julgustavad, satuvad paljud Interneti-kasutajad endiselt veebipettuste ja e-posti teel toimuvate õngitsusrünnete ohvriks. Eurostati andmete kohaselt teatas 2019. aastal üks kolmest ELi 16–74-aastastest isiklikuks tarbeks internetti kasutavast kodanikust turvalisega seotud juhtimist viimase 12 kuu jooksul.

2019. aastal oli andmepüük kõige sagedasem turvaintsident millest teatati[3]. 25% vastanutest väitis, et sai petusõnumeid, mida nimetatakse andmepüügiks või õngitsuseks (*phishing*), samas kui 12% vastanutest väitis, et nad suunati võltsveebisaitidele, kus küsiti isiklikku teavet (*pharming*). Internetti isiklikel eesmärkidel kasutavate inimeste osakaal, kes kogesid turvalisusega seotud probleeme, oli ELi liikmesriikides erinev. Kõrgeimat määra täheldati Taanis (50%), järgnesid Prantsusmaa (46%), Rootsi (45%), Malta ja Holland (mõlemad 42%), Soome (41%) ja Saksamaa (40%). Seevastu madalaim osakaal registreeriti Leedus (7%), Poolas (9%), Lätis (10%), Bulgaarias (13%) ja Kreekas (13%). Eestis ja Küprosel oli turvalisusega seotud probleeme kogenud inimeste osakaal vastavalt 32% ja 21%.

Eelnevat saab seletada erinevustega küberkuritegevuse alase teadlikkuse taseme vahel ELi riikides, ELi kodanike üldise enesekindluse vähenemisega ennast küberrünnakute eest kaitsta ning keerukamate küberrünnakutega, mida on raskem avastada ja vältida. Selliste rünnakute läbiviimiseks on kasutusel uued tehnikad ja uued platvormid.

Kui rääkida Euroopa ärisektorist, siis ka neid mõjutavad küberturvalisuse probleemid. Euroopa riigid ja ettevõtted on rünnakute sihtmärk üha sagedamini. 2017. aasta ülemaailmse infoturbe seisundi uuringu (*Global State of Information Security Survey*) kohaselt on umbes 80% Euroopa ettevõtetest kogenud sel aastal vähemalt ühte küberturvalisuse juhtumit ning töötajad põhjustavad 27% kõigist küberturbe intsidentidest.

Ülemaailmselt rünnati hiljutiste andmete põhjal 2019. aasta esimeses kvartalis ettevõtteid 120% sagedamini kui aasta varem, mille tulemusena põhjustati kahju koguni 22,2 miljardit eurot.

Üle 99% pahavara levitavatest e-kirjadest nõudis õnnestumiseks inimese sekkumist[4] – linkidele vajutamist, dokumentide avamist, turvahoiatuste aktsepteerimist ja muud käitumist. Seega on

1 EU Commission (2020): Special Eurobarometer 499: Europeans' attitudes towards cyber security, URL https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG (külastatud 11.02.2021)

2 European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020

3 EUROSTAT (2020): Is internet use safer today?, URL https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb/default/table?lang=en (külastatud 11.02.2021)

4 Proofpoint (2019): Human Factor Report 2019, URL https://www.proofpoint.com/us/resources/threat-reports/human-factor (külastatud 12.02.2021)

küberrünnakute pidurdamiseks või ennetamiseks võtmetähtsusega inimesed, olgu siis tööl või kodus, kes on teadlikud ohu märkidest ja oskavad õigeid tehnikaid, et rünnakuid ära tunda. Seetõttu on vaja ajakohastada olemasolevaid küberturvalisuse programme või luua uusi, et tugevdada ELi kodanike oskusi, haridust ja teadlikkust uusimatest esilekerkivatest küberturvalisuse probleemidest ja ohtudest.

Selliseid programme on vaja pakkuda ka kõigile üliõpilastele, arvestades, et ENISA andmetel on ülikoolides küberturvalisuse valdkonna teemad mitte tehnoloogilistes õppekavades alaesindatud.

## 1.2. Projekt "Andmepüügi vastu võitlemine 4. tööstusrevolutsiooni ajastul"

Küberturvalisusest saab digiajastu üks suurimaid väljakutseid, sest informatsioonist saab kallis vara, mis tegeleb tohutute andmemahtudega, parandades suhtlust digitaalse keskkonnaga. Digitaalsed seadmed ja infosüsteemid muutuvad küberrünnakute jaoks üha atraktiivsemaks.

Andmepüük on üks suurimaid probleeme, kuna küberkurjategijad kasutavad andmepüügi kampaaniate läbiviimiseks kiiremaid ja uuenduslikke tehnoloogilisi vahendeid. Seetõttu tuleks välja töötada laiale publikule vabalt kättesaadav inimpõhine andmepüügi kaitsesüsteem, mis kasutab inimese avastamisinstinkti ja tehnoloogiat üheskoos. Inimesest juhitud andmepüügikaitse loomiseks on vaja haridust, et kasutaja saaks õngitsemisrünnakud õigesti tuvastada ja neile reageerida.

Vilniuse Ülikooli Kaunase teaduskonna ja partnerite algatatud rahvusvaheline Projekt „Andmepüügi vastu võitlemine 4. tööstusrevolutsiooni ajastul“ („*CyberPhish*“) algas 2020. aasta novembri alguses ja kestab kaks aastat.

Projekti eesmärk on harida kõrgkoolide üliõpilasi, õppejõude, ülikoolide töötajaid (kogukonna liikmeid), hariduskeskusi, ärisektorit (tööandjaid ja töötajaid) ning julgustada osaliste kriitilist mõtlemist küberturvalisuse vallas.

Projekti partnerlus koosneb kuuest organisatsioonist viiest Euroopa riigist:

1. Vilniuse Ülikool, Leedu (koordinaator)
2. Infotehnoloogia instituut, Leedu
3. DOREA haridusinstituut, Küpros
4. Tartu Ülikool, Eesti
5. Altacom SIA, Läti
6. Macdac Engineering Consultancy Bureau Ltd (MECB), Malta

Lisateavet projekti ja projekti tegevuste kohta leiate projekti veebisaidilt: https://cyberphish.eu/ .

Co-funded by the Erasmus+ Programme of the European Union

# 2. ANDMEPÜÜK

## 2.1. Mis on andmepüük?

Andmepüük on petturite katse varastada kasutajate andmeid, näiteks sisselogimisandmeid, krediitkaardiandmeid või isegi raha, kasutades sotsiaalse ründe tehnikat. Seda tüüpi rünnak käivitatakse tavaliselt e-kirjade kaudu, mis näib olevat saadetud usaldusväärsest allikast, eesmärgiga veenda kasutajat avama pahatahtlik manusfail või vajutama petturlikku lingi peale[5]. Andmepüük on üks vanimaid küberrünnakute tüüpe, mis pärineb 1990. aastatest. Hoolimata sellest, et see on eksisteerinud aastakümneid, on see endiselt üks kõige levinumaid ja edukamaid küberrünnakuid[6].

Andmepüüki on palju erinevaid, kuid kõige tavalisemad on:

1) *Spray and pray* – pahatahtlikud e-kirjad, mis saadetakse mis tahes e-posti aadressidele tundliku teabe varastamise katseks;
2) *Cat phishing* - meelitamine väljamõeldud veebipõhise isiku abil;
3) *Advanced fee scam* – levinud rahvuslikkud pettused nö Nigeeria kodaniku abi palumine suure rahasumma liigutamisel;
4) *Spear fishing* - pahatahtlikud meilid, mis on spetsiaalselt loodud ja saadetud konkreetsele isikule või organisatsioonile, püüdes varastada tundlikku teavet;
5) *Whaling* - püüd varastada tundlikku teavet, kuid rünnak on sageli suunatud kõrgemale juhtkonnale;
6) *Vishing* - viitab andmepüügile, mis toimub telefoni teel;
7) *Smishing* - viitab andmepüügile, kasutades ohvri leidmiseks SMS-e, mitte e-kirju;
8) *Angler Phishing* – suhteliselt uus tüüp, mis viitab rünnakutele, mis esinevad sotsiaalmeedias, kasutades võltsitud URL-e, kloonitud veebisaite, postitusi, säutse ja kiirsõnumeid;
9) *Clone Phishing* – andmepüügi tüüp, kus originaalne ja varem edastatud e-kirja sisu ja väljanägemine võetakse aluses pahatahtlikku sisuga e-kirja loomisel;
10) *Malvertising* - see andmepüügitüüp kasutab veebireklaame või hüpikaknaid, et sundida inimesi klõpsama ausa välimusega lingil, mis seejärel arvutisse pahavara installib.

Viimase paari aasta jooksul on täheldatud andmepüügi kasvavat keerukust, kusjuures andmepüüki on üha raskem tuvastada, sest paljud andmepüügi meilid ja võltsitud veebilehed on peaaegu identsed tegelikega. Samal ajal on andmepüügikampaaniad muutunud kiiremaks ja automatiseeritumaks, sundides kaitsjaid senisest kiiremini tegutsema, kuna mõnel juhul kulub autentimise info lekkest rünnakuni vähem kui päev.

Europoli uuringute põhjal kasutavad küberkurjategijad andmepüügi jaoks terviklikumat strateegiat: näidates kõrgetasemelist pädevust nende poolt kasutatavate tööriistade, süsteemide ja haavatavuste kasutamisel; valeidentiteedi omandamises ja tihedas koostöös teiste küberkurjategijatega[7].

Ennustatakse, et e-post on jätkuvalt andmepüügi mehhanism number üks, kuid mitte kauaks. Eksperdid näevad sotsiaalmeedias, sealhulgas WhatsAppis ja teistes sotsiaalmeedia kanalites selliste rünnakute läbiviimisel üha enam kasutust. ENISA sõnul on kõige tõenäolisem muutus sõnumite saatmiseks kasutatavates meetodite keerukuse täiendav tõus, kui sõnumite ettevalmistamiseks ja saatmiseks võetakse kasutusele tehisintellekt (AI).

[5] European Union Agency for Cybersecurity (2020): Phishing - ENISA threat landscape 2019-20

[6] Deloitte (2019): Understanding Phishing Techniques URL https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf (accessed 112.02.2021)

[7] EUROPOL (2020): Internet Organised Crime Threat Assessment 2020

Co-funded by the Erasmus+ Programme of the European Union

## 2.2. Sotsiaalsed ründed ja andmepüük

Infoturbe kontekstis määratletakse sotsiaalne rünne (suhtlusrünne, *social engineering*) kui inimeste psühholoogiline manipuleerimine toimingute sooritamiseks või konfidentsiaalse teabe avaldamiseks. Sotsiaalsed ründed hõlbustavad ka muud tüüpi küberkuritegevust, kuna 84% küberrünnakutest toetub rünnakutele, kus ohver aitab kaasa enda tegevusega rünnaku edukusele (ENISA). Andmepüügi ohvrite arv kasvab jätkuvalt, kuna see kasutab inimest kui kõige nõrgemat lüli.

Inimese nõrkuse suunamine sotsiaalse ründe abil mõjutab ühiskonda suuresti ja võimaldab enamikku küberkuritegudest, alates petuskeemidest kuni tundliku teabe hankimise ja arenenud pahavara rünnakuteni. Küberkurjategijad kasutavad sotsiaalset rünnet veenmaks kasutajaid teadmatult pettusskeemide ohvriks langema, kuid andmepüügi eesmärk on saada volitused ja juurdepääs tundlikele kontodele / süsteemidele (EUROPOL).

Küberkurjategijad on õppinud ja saanud sotsiaalseteks ekspertideks, kasutades inimloomuse alustõdesid pettuste sooritamiseks. Kõige tavalisemad manipuleerimismeetodid tuginevad tavaliselt hirmule, hirmutamisele, pakilisuse tundele, ahnusele, uudishimule, looduse usaldamisele ja empaatiale. Küberkurjategijad teavad, et hoolikalt ettevalmistatud ja isikupärastatud e-post, kõnesõnum/kõne või tekstsõnum võivad inimesi panna inimesi tundlikku teavet avalikustama, raha üle kandma või pahavara sisaldava faili alla laadima ettevõtte võrku.

Sotsiaalse ründe mõiste paremaks mõistmiseks võiksime heita pilgu 6 veenmise põhimõttele, mida dr Robert B. Cialdini oma raamatus “Influence: The Psychology of Persuasion”[8] selgitas. Kui algselt kasutati neid põhimõtteid turunduses, võeti need hõlpsasti omaks ja hakati kasutama ka sotsiaalseteks rünneteks ja andmepüügi valdkonnas[9]:

1) ***Vastutasu*** – “anna ja võta". E-kirjas pakuti mõnele ostule allahindlust või kupongi vastutasuks teabe jagamise või konto registreerimise eest; e-kirjas lubati anda juurdepääs konfidentsiaalsele teabele, kui teatud manusfail on alla laaditud või link avatud on klassikalised näited.
2) ***Defitsiit*** – inimloomuses on tahta seda, mida on raske kätte saada. Andmepüügimeilid, mis rõhutavad, et konkreetne eelis on kättesaadav ainult siis, kui midagi tehakse lühikese aja jooksul (kiirustades). „Konto deaktiveeritakse 24 tunni jooksul, kui te ei klõpsa lingil, et probleem lahendada.” on näide sellest põhimõttest.
3) ***Autoriteet*** – inimesed kalduvad järgima autoriteeti ja usaldusväärseid eksperte üldiselt. Seetõttu püütakse paljudes andmepüügimeilides esineda kohalikeks juhtideks, tegevjuhtideks, kõrgemateks ohvitserideks, personalijuhtideks jne. Näiliselt tegevjuhi e-kiri, milles palutakse rahandusosakonnal viivitamatult osakonnale tundmatule kontole teatud summa raha suunata, on levinud näide.
4) ***Järjepidevus*** – inimesed on ühel või teisel viisil harjumuspärased olendid. Ametlikuks suhtluseks tunduvad andmepüügimeilid kasutavad seda fakti, lootes, et adressaat jätab tähelepanuta ebatavalise taotluse, mis sellises e-kirjas sisaldub. Amazoni logoga e-kiri, milles öeldakse, et saadetis on kinni ja palutakse saajal oma kodune aadress kinnitada, ei pruugi ohumärki tuvastada isegi siis, kui saadetist pole oodata - see on laialt tunnustatud kaubamärgi jõud.
5) ***Üksmeel*** – inimesed kipuvad järgima teisi inimesi, eriti kui nad pole milleski kindlad. Andmepüügimeil, milles mainitakse näiteks „544 töötajat 800-st on tarkvara värskendanud, klõpsake allalaadimiseks sellel lingil” kasutab seda suundumust ära.

[8] Dr Robert B. Cialdini is a Psychology and Marketing professor in the Arizona State University in USA

[9] NCC group (2020) :Psychology of the Phish: Leveraging the Seven Principles of Influence, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433 (accessed 12.02.2021)

6) ***Meeldiv*** – see on üsna lihtne põhimõte – Olukorras kus inimesed tahavad teistele meeldida, ütlevad nad kõige tõenäolisemalt „jah“. IT-osakonna e-kiri (väidetavalt), kus palutakse uuel töötajal turvasüsteemi värskendamiseks tema isikuandmeid / paroole.
7) ***Ühtsus*** – see põhimõte lisati hiljem. Idee on selles, et mida rohkem me ennast teistega samastame, seda rohkem mõjutavad nad meid. Andmepüügimeilil, mille on saatnud väidetavalt saajaga samad huvid, teave, mida saab hõlpsalt hankida sotsiaalmeedia kaudu, võib suure tõenäosusega õnnestuda. Näiteks kui inimene armastab koeri, on teise (väidetava) koeraarmastaja e-kiri koos armsate koerapiltide manustega suurem tõenäosus avada.

Inimloomusele rõhuvad meetodid viivad tihti edukate andmepüügi rünnakuteni, kasutades rünnakute osana pahatahtlikke linke või pahavara. Seega on inimeste jaoks ülioluline teadvustada neid põhimõtteid ja strateegiaid enda kaitsmiseks, kuid see on üsna keeruline, kuna see põhineb inimeste olemusel - viisil, kuidas me mõtleme ja käitume.

## 2.3. Andmepüük COVID-19 ajal

Kriisi ja katastroofide ajal kipume töötamiseks, teiste inimestega ühenduse loomiseks, teabe leidmiseks, jagamiseks ja teabe saamiseks, ostlemiseks jne lootma liialt arvutitele, mobiilseadmetele ja internetile[10].

COVID-19 pandeemia on rõhutanud meie haavatavust ja näidanud küberkuritegevuse kahetsusväärset mõju meie igapäevaelule kogu maailmas. Kuna füüsiline isoleeritus muutus normiks ning üha rohkem inimesi jäi kodukontorisse tööle, muutusid küberkuritegevused senisest laialdasemaks. Barracuda[11] teadlased täheldasid andmepüügi pettuste arvu suurenemist 667% võrra vaid ühe kuu jooksul pärast pandeemia algust 2020. aasta alguses.

On tõendeid selle kohta, et küberkurjategijad kasutavad inimeste heatahtlikkust ja haavatavusi jätkuvalt enda kasuks. Küberkurjategijad on olemasolevaid küberkuritegevuse vorme kohandanud pandeemilise narratiiviga sobivaks, kuritarvitanud olukorra ebakindlust ja üldsuse vajadust usaldusväärse teabe järele. Kurjategijad on kasutanud COVID-19 kriisi sotsiaalsete rünnakute korraldamiseks, nimelt õngevõtmise e-kirjad rämpspostikampaaniate kaudu ja sihipärasemad katsed, näiteks ettevõtte e-posti ohustamised (BEC – *business e-mail compromise*)[12]:

- Andmepüügikampaaniaid ja pahavara levitamist näiliselt ehtsate veebisaitide või dokumentide kaudu, mis pakuvad teavet või nõuandeid COVID-19 kohta, kasutatakse arvutite nakatamiseks ja kasutajate kontode ülevõtmiseks.
- Kurjategijad saavad juurdepääsu kaugtööd tegevatele töötajatele mõeldud ettevõtete või muude organisatsioonide süsteemidele.

EUROPOLi andmetel on küberrünnakute arv märkimisväärne ja eeldatavasti kasvab see veelgi. Küberkurjategijad jätkavad uuendusi mitmesuguste COVID-19 pandeemia ja eriti vaktsiinide teemaliste pahavara- ja lunavara pakettide juurutamisel.

Küberkurjategijad püüavad tõenäoliselt kasutada üha suuremat arvu rünnakutehnikaid, kuna paljud tööandjad kasutavad ja jätkavad kaugtööd ning võimaldavad distantsiol ühendusi oma organisatsiooni süsteemidega.[13]

[10] Council of Europe (2020): Cybercrime and COVID-19, URL https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (accessed 12.02.2021)
[11] Barracuda Networks is the worldwide leader in Security, Application Delivery and Data Protection Solutions
[12] Council of Europe (2020): Cybercrime and Covid, URL: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (accessed 12.02.2021)
[13] EUROPOL (2020): Pandemic profiteering - how criminals exploit the COVID-19 crisis

# 3. KÜSITLUS ÜLIÕPILASTELE, TÖÖTAJATELE JA TEGEVJUHTIDELE

## 3.1. Andmete kogumise metoodika

Välitööde osana koostasid CyberPhishi projekti konsortsiumi partnerid uuringu[14], mis oli suunatud Leedu, Läti, Eesti, Malta ja Küprose üliõpilastele, ettevõtete esindajatele ja tegevjuhtidele. Partnerite eesmärk oli kaasata igas partnerriigis vähemalt 70 osalejat (sealhulgas 20 äriesindajat ja 10 tegevjuhti).

Varasemate teadusuuringute ja kõigi partnerite tagasiside põhjal koostati küsimustiku ingliskeelne versioon, mis hiljem lokaliseeriti ja laaditi internetti täitmiseks inglise, leedu ja läti keeles. Uuring käivitati 2020. aasta detsembri keskel ja viidi lõpule 2021. aasta jaanuari lõpuks.

Uuringu peamised eesmärgid olid:

- teha kindlaks inimeste **teadlikkus** andmepüügist ja erinevatest andmepüügi liikidest;
- teha kindlaks, **kuidas** inimesed õngitsemise rünnakud ära tunnevad;
- selgitada välja oskuste puudujäägid.

Küsimustik sisaldas psühholoogiliste ja IT-alaste teadmistega seotud küsimusi, kriitilise mõtlemise lähenemist ning pakkus vastajatele andmepüügi näiteid, et hinnata oma teadmisi "praktikas". Iga andmepüüginäide põhines dr Robert B. Cialdini väljatöötatud kuuel veenmise põhimõttel. Kokkuvõttes jagati küsimustik mitmeks osaks ja koguti andmeid, mis käsitlevad:

- Isiklik teave - sealhulgas sugu, haridustase ja töökoha info;
- üldised teadmised ja käitumine andmepüügi valdkonnas;
- isiklik kogemus andmepüügiga;
- andmepüügirünnakute äratundmine - peamiste ohukohtade märkimine;
- praktilised andmepüügi näited;
- kriitilise mõtlemise oskuse enesehindamine;
- andmepüügirünnakute vältimine - miks õngitsemisrünnakud on edukad, sotsiaalsed ründed (ründajate poolt ära kasutatud inimlikud emotsioonid), tegevused vältimaks ohvriks langemist;
- enesehinnang enesekindlusele andmepüügirünnakute vältimiseks vajalike oskuste kasutamisel.

Kogutud andmeid kasutatakse oskuste puudujääkide väljaselgitamiseks ja soovituste koostamiseks uue õppekava jaoks, et tugevdada internetikasutajate oskusi, haridust ja teadlikkust uusimatest esilekerkivatest küberturvalisuse probleemidest ja ohtudest, eelkõige andmepüügist.

Selle uuringu tulemuste ja olemasolevate küberturvalisuse õppekavade analüüsi põhjal töötab partnerite konsortsium välja õppematerjali, teadmiste enesehindamise ja teadmiste kontrollimise testid ning simulatsiooni stsenaariumid koolituse jaoks.

## 3.2. Tulemuste kogumine

Küsimustiku tulemused kanti riiklikule tulemuste tabelile (struktureeritud riigiti - Leedu, Läti, Eesti, Malta ja Küpros). Sellesse tabelisse lisasid partnerid kõige asjakohasemad kogutud tulemused, edastades teavet järgneva kohta:

- uuritava (küsimustikule vastanud) sihtrühmade iseloomustus;
- uuringute tulemuste analüüs graafikute ja teksti abil;
- vastajate peamised järeldused ja ettepanekud;

[14] CyberPhish projekti veebileht: https://cyberphish.eu/

- Partnerite tehtud järeldused ja soovitused, et toetada partnereid muude projekti tulemuste määratlemisel ja väljatöötamisel.
- Tabelid andsid ülevaate vastajate teadmistest ja käitumisest küberturvalisuse, eriti andmepüügi teemal. Nende tabelite tulemused võimaldasid konsortsiumil võrrelda riike, tehes kindlaks oskuste lüngad ja vajadused.

## 3.3. Uuringute tulemused ja analüüs

### 3.3.1. Ülevaade küsimustikule vastanutest

Vaatamata lühikesele perioodile, mil küsimustikku levitati, ületasid kõik riigid minimaalse 70 vastaja piiri. Kokku koguti Küproselt, Eestist, Lätist, Leedust ja Maltalt 514 vastust.

| | Leedu | Läti | Eesti | Malta | Küpros |
|---|---|---|---|---|---|
| Vastajaid riigi kohta | 93 | 76 | 165 | 104 | 76 |

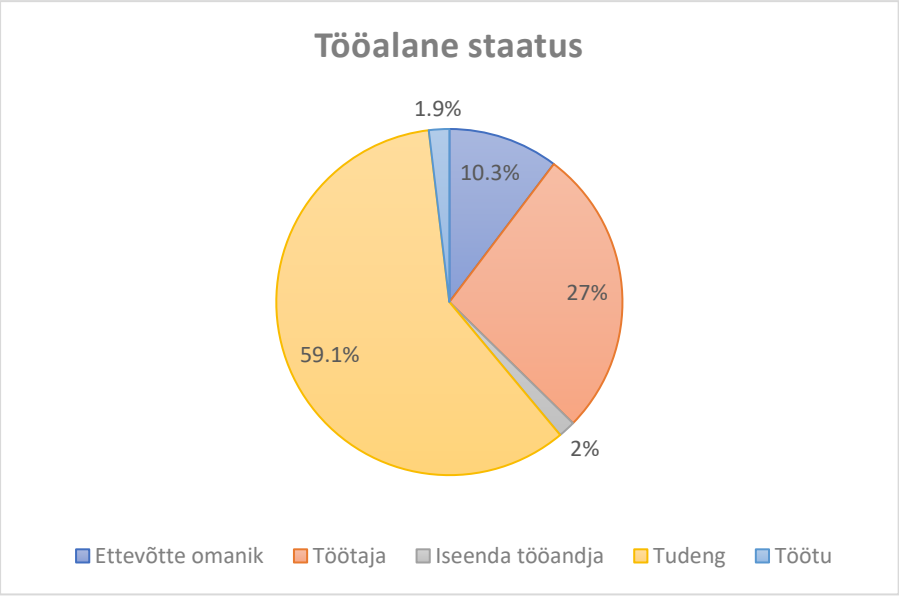
*Tabel 1. Küsimustikule vastajate arv riigiti*

514 vastajast - 259 olid naised, 248 mehed ja 7 vastajat eelistas oma sugu mitte avalikustada. Kõigis partnerriikides, välja arvatud Eesti, oli naissoost vastajate arv suurem meestest.

| | Leedu | Läti | Eesti | Malta | Küpros |
|---|---|---|---|---|---|
| Naine | 63,4% | 57,9 % | 34,6% | 54,8% | 55,3% |
| Mees | 36,6% | 40,8% | 63% | 45,2% | 42,1% |
| Eelistan mitte öelda | - | 1,3 % | 2,4% | - | 2,6% |

*Tabel 2. Küsimustikule vastajate sooline jaotus*

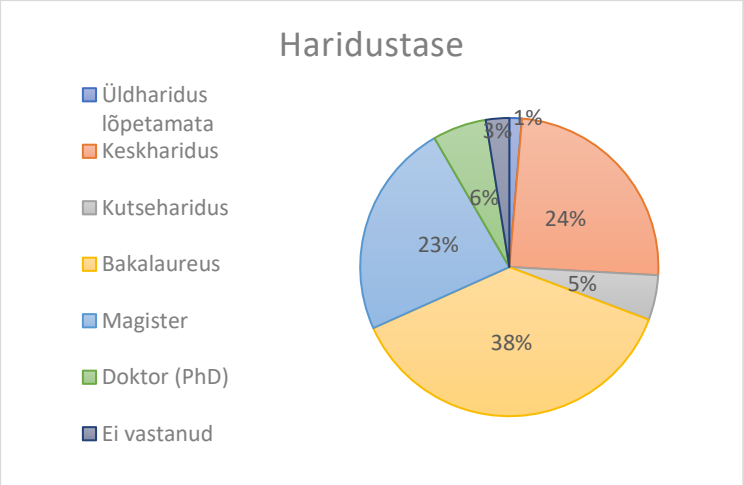
Enamik vastanutest on üliõpilased (59%), neile järgnevad töötajad (27%), ettevõtete omanikud (10%), töötud (2%) ja füüsilisest isikust ettevõtjad (2%).




*Joonis 1. Uuringus osalenute tööhõive staatus*

Co-funded by the Erasmus+ Programme of the European Union

Uuringus osalenud on hästi haritud - enamikul vastanutest (38%) on bakalaureusekraad, millele järgnevad magistrikraad (23%) ja doktorikraad (6%).

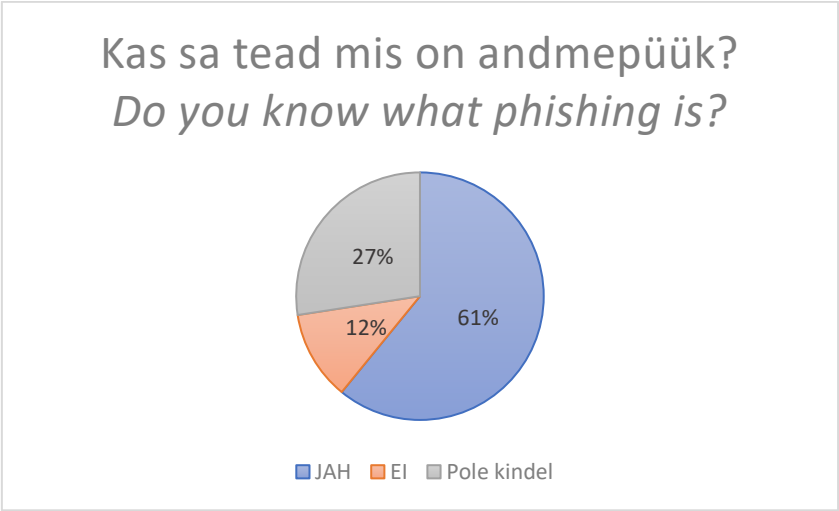



*Joonis 2. Uuringus osalenute haridustase*

### 3.3.2. Üldteadmised ja käitumine

Ehkki kõige rohkem vastajaid (74%) on märkinud, et pole kunagi osalenud spetsiaalsetes küberturvalisuse või andmepüügi koolitustel / töötubades / uuringutes, on üle poole vastanutest (56%) seda teemat ise uurinud. Need tulemused võivad viidata sellele, et küberjulgeoleku ja andmepüügi teemad on asjakohased kõigis küsitletud riikides ning kuigi vastajatel ei pruugi olla võimalust seda teemat ametlikus keskkonnas õppida, on nad oma teadmiste ja oskuste täiendamiseks valmis aega kulutama teema uurimisele iseseisvalt.

61% küsitlenutest vastas, et neil on teadmised andmepüügist, 27% pole kindel ja 12% ei tea, mis on andmepüük. Kui palutakse valida õige andmepüügi määratlus, on 72% küsitletud inimestest valinud selle õigesti. Maltal ja Eestis on vastajate arv, kes väidavad, et teavad, mis on andmepüük ja nende tegelikud teadmised samas suurusjärgus. Leedus, Küprosel ja Lätis on õige vastuse valinud rohkem inimesi kui neid, kes arvasid, et teavad, mis on andmepüük. Need tulemused viitavad sellele, et rohkem vastajaid Leedus, Küprosel ja Lätis on andmepüügist teadlikud, kuid nad pole oma teadmistes kindlad.




*Joonis 3. Uuringus osalenute teadlikkus „Mis asi on andmepüük?“*

Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

Pea pooled vastanutest (46%) märkisid, et kardavad sageli e-kirjas olevat linki või manust avada, arvates, et see võib olla võlts, samas kui 13% kardab alati. Ainult 3% vastanutest ei karda kunagi linke / manuseid avada ja 8% kardab harva.
Peaaegu kolmandik vastanutest (32%) kardab sageli saada andmepüügi rünnakute sihtmärgiks ja 19% on alati hirmul. Vaid 5% vastanutest märkis, et nad ei karda kunagi saada andmepüügi rünnaku sihtmärgiks, samas kui 17% kardab harva.

Eelnevad tulemused näitavad, et enamik vastanutest on teadlikud küberrünnakute võimalusest ja häkkerite peamistest tööriistadest (pahatahtlikud lingid ja manusfailid). Isegi kui 39% vastanutest märkis, et nad ei tea või pole kindlad, mis on andmepüük, kardab 51% vastajatest sageli või alati saada andmepüügi rünnakute sihtmärkideks. Need tulemused võivad tähendada, et isegi neil vastajatel, kes on teatanud, et teavad, mis on õngitsemine, pole tingimata vajalikke teadmisi enda kaitsmiseks või enesekindlust oma oskuste vastu.

Küsimusele erinevate tuttavate andmepüügiliikide kohta märkisid kõigi küsitletud riikide vastajad, et nad on kõige rohkem teadlikud nendest andmepüügiliikidest: „*Spray and Pray*“, „*Cat phishing*“ ja „*Malvertising*“. Kõigi küsitletud riikide, välja arvatud Leedu, vastajad on samuti kõige paremini teadlikud andmepüügiliigist “*Advanced fee scam*”.


*Joonis 4. Andmepüügi tüübid millest vastanud kõige rohkem kuulnud on*

Teiselt poolt on vastajad kõige vähem teadlikud nendest andmepüügiliikidest: “Whaling”, “Clone phishing” ja “Smishing”[15] (välja arvatud Küproselt pärit vastajad). Ka Malta, Küprose, Leedu ja Läti vastajad on kõige vähem teadlikud „Content injection” (andmesüst), samas kui Eesti vastajad märkisid, et nad on sellest kalapüügist enamasti teadlikud.


*Joonis 5. Andmepüügi tüübid millest vastanud kõige vähem kuulnud on*

Kui küsiti, millised tagajärjed tõenäoliselt või kindlasti tekivad pärast edukat andmepüügirünnakut isikule või ettevõttele, nimetas enamik küsitletud riikidest vastajaid järgmisi tagajärgi: „tundlike andmete vargus”, „krediitkaardipettus”, „kliendiandmete leke ”, „mainekahjustus” ja „kasutajanimede ja paroolide kaotamine” (välja arvatud Malta vastajad). Kõigi küsitletud riikide, välja arvatud Küpros[16], vastajad kalduvad samuti arvama, et pärast edukat andmepüügirünnakut müüakse nende andmeid suure tõenäosusega kuritegelikele kolmandatele isikutele.

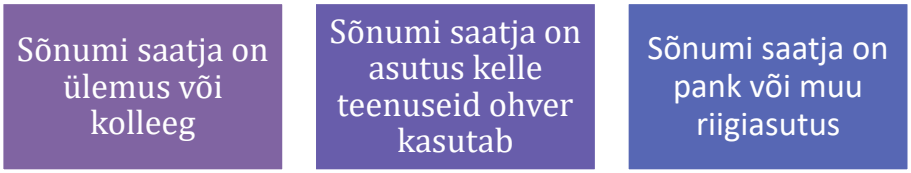
[15] Välja arvatud Küprose vastajad
[16] Välja arvatud Küprose vastajad

Co-funded by the Erasmus+ Programme of the European Union


*Joonis 6. Tagajärjed mis ilmnevad vastajate sõnul kõige tõenäolisemalt pärast edukat andmepüügirünnakut*

Teiselt poolt usuvad kõigi küsitletud riikide vastajad, et pärast edukat andmepüügirünnakut ei toimu tõenäoliselt „intellektuaalse omandi kaotust“. Leedu, Malta ja Eesti vastajad on skeptilised ka andmepüügirünnaku järgse “ettevõtte / kliendi kontolt vahendite varguse” suhtes.

Arvestades inimeste sotsiaalset loomust, klõpsavad vastajad kõige tõenäolisemalt e-kirjas või kirjas oleval lingil või manusel ning esitavad tundlikku teavet, kui selle: „saadab nende ülemus või kolleeg”, „saadab ettevõte, mille teenuseid nad kasutavad”, „saadab pank või riigiasutus”. Küprosel täidavad päringu tõenäolisemalt ka siis, kui e-kiri / sõnum „palub neil täpsustada üksikasju, näiteks nende tellimuse posti-aadressi (nn. *Amazon* tellimus)“. Samal ajal Lätis ja Maltal arvamused lahknevad, peaaegu sama arv vastajaid vastasid väga tõenäoline ja väga ebatõenäoline. Eesti ja Leedu vastajate seas pole lahkarvamusi ning enamik väga tõenäoliselt päringule oma saatmise aadressi täpsustada ei vastaks.




*Joonis 7. e-kirjade tüübid, milles vastajad kõige tõenäolisemalt lingile või manusele vajutavad ja/või jagavad tundlikku teavet*

Tulemused pole üllatavad, kui heidame pilgu eelnevalt kirjeldatud seitsmele veenmispõhimõttele. Nagu varem mainitud, kipuvad inimesed järgima ja usaldama suuremat autoriteeti või eksperte. Seega on paljude häkkerite eesmärk esineda usaldusväärsete valitsusasutuste / ametiasutuste ning pankade esindajana või tegevjuhtidena. See tendents oli nähtav ka uuringus, kus 34% vastanutest väitis, et usaldab väga sageli või alati sõnumeid, mis näivad pärinevat oluliselt üksuselt või tunduvad olulised, samas kui 30% teevad seda mõnikord.

Olulist rolli mängib ka “Meeldimise põhimõte”, mis tähendab, et inimesed reageerivad ebatavalistele päringutele palju tõenäolisemalt kui need tulevad näiliselt kolleegilt või ülemuselt.

Lisaks on inimesed harjumuspärased olendid ja neile meeldib järjepidevus. Oletame, et e-kirja saatis ettevõte, mida nad teavad ja milliseid teenuseid nad kasutavad ning tõenäoliselt on nad neilt varem e-kirju või teateid saanud. Sel juhul avavad nad selle suurema tõenäosusega, klõpsavad linkidel / manustel jne, kui nad teeksid ettevõttega, milliseid teenuseid nad ei kasuta.

Kõigis partnerriikides klõpsavad vastajad kõige vähem tõenäoliselt e-kirjas või kirjas oleval lingil või manusel ja/või esitavad tundlikku teavet, kui see: „pakub neile konfidentsiaalset teavet (nt teavet konkurentide kohta)”, „palub neil täita küsitlus ja esitage oma e-posti aadress või telefonikontaktid, et auhinnavõistlusel osaleda“ või „sõnumi saadab ettevõte/organisatsioon, keda nad tunnevad, kuid ei kasuta oma teenuseid“.

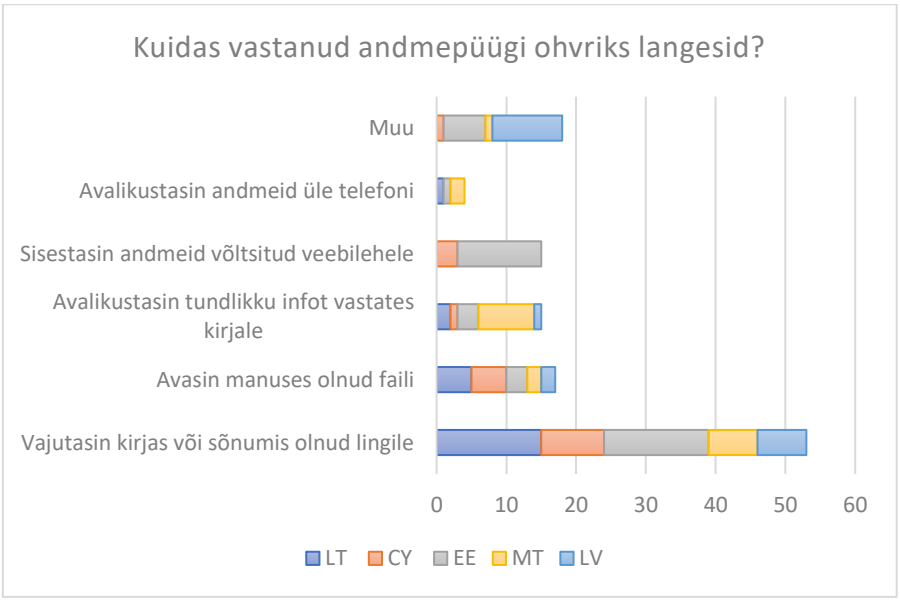
Co-funded by the Erasmus+ Programme of the European Union


*Joonis 8. e-kirjade tüübid, milles vastajad ebatõenäolisemalt lingile või manusele vajutavad ja/või jagavad tundlikku teavet*

Enamik vastajaid Eestist, Küproselt ja Maltalt avaldaks tõenäoliselt tundlikku teavet, kui e-kiri või sõnum „paluks neil aidata või annetada kohalikele või rahvusvahelistele heategevusorganisatsioonidele“. Küproselt pärit vastajad vajutaksid tõenäoliselt ka lingil/manusel ja edastaksid tundlikku teavet, kui see „kutsub neid konkreetsele üritusele (nt Zoom koosolekule). Vastupidiselt Küprosele, Leedu, Läti, Eesti ja Malta vastajad üritusele kutsega kirjale pigem ei reageeriks.

### 3.3.3. Isiklik kogemus andmepüügirünnakutega

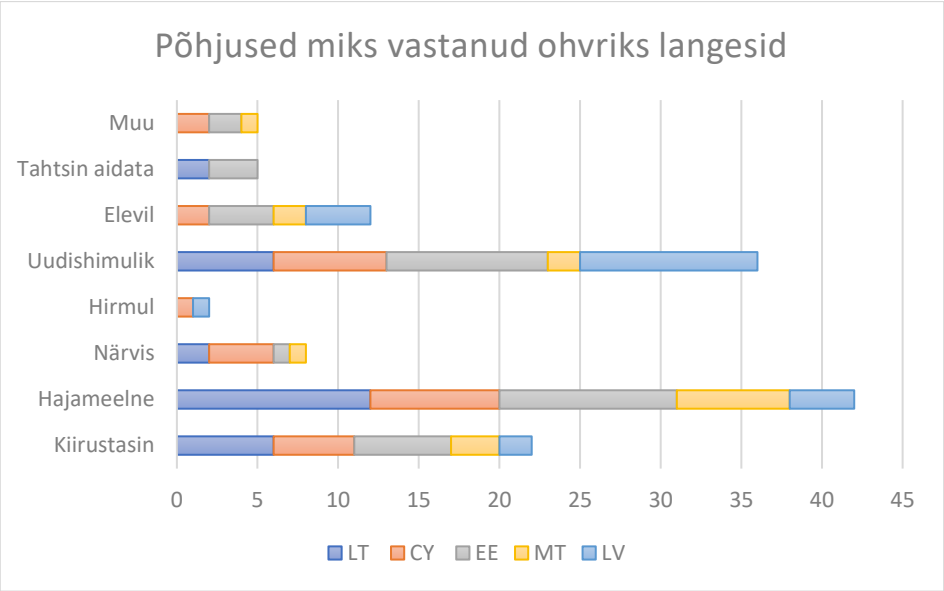
19,8% vastanutest või peaaegu iga viies vastajast on varem andmepüügi ohvriks langenud. Kõige levinum viis vastajate hulgas andmepüügiks on klõpsamine meilis või sõnumis oleval lingil, millele järgneb manusfailide avamine ning e-kirjale või sõnumile vastamine ja tundliku teabe edastamine. Üllataval kombel on ainult Eesti ja Küprose vastajad märkinud, et nad on andmepüügi käigus sisestanud sisselogimisandmeid võltsveebilehele. Muude vastuste hulgas olid kõige populaarsemad „mitme andmepüügitehnika kombinatsioon” ja „võltsküsitlusele vastamine ja personaalse info avalikustamine”.




*Joonis 9. Kuidas vastanud andmepüügi ohvriks langesid*

Kui paluti vastata, miks nad on nende arvates andmepüügi ohvriks langenud, märkis enamik vastanutest, et nad olid hajameelsed, uudishimulikud või kiirustasid. “Muude” vastuste hulgas oli levinud, et vastajad olid noored ja/või ei teadnud andmepüügist.

Co-funded by the Erasmus+ Programme of the European Union




*Joonis 10. Põhjused miks vastanud ohvriks langesid*

### 3.3.4. Andmepüügi rünnakute äratundmine

Uuringus paluti vastajatel hinnata ja märkida kahtlase e-posti, tekst- või telefonikõne ning sotsiaalmeediasõnumi tuvastamisel kõige olulisemad kriteeriumid.

***E-kiri***

Kahtlaste meilide äratundmise osas oli kõigi riikide vastajatel ühtne arvamus olulisemate kriteeriumide kohta, mida arvestada. Peamised märgitud kriteeriumid on järgmised: 1) saatja domeen (e-posti aadress) ei tundu ehtsana (ei vasta organisatsioonile, sisaldab varjatud kirjaviga, lisanumbreid, tähti selles jne); 2) e-kirja nähtavad lingid on erinevad tegelikust hüperlingist; 3) saatja palub kinnitada/edastada tundlikku teavet e-posti teel (kasutajatunnus ja parool, pangaandmed); 4) e-posti aadressides, linkides ja domeeninimedes on nähtavaid vastuolusid; 5) E-kiri sisaldab ootamatut/ebatavalist manust.

Vastajate poolt märgitud kõige vähem olulised kriteeriumid olid 1) umbisikuline tervitus e-kirjas; 2) puudub saatja info ega sisalda kontaktandmeid; 3) e-kiri tekitab uudishimu; 4) E-kiri on liiga hea, et olla tõsi. Maltalt pärit vastajad valisid samuti vähemtähtsaks kirjutamisstiili ning õigekirja- ja grammatikavead.

***Teksti sõnum või telefonikõne***

Peaaegu ühtset arvamust nähti ka kõigi küsitletud riikide vastajate vahel, kui tuli tuvastada olulisemad kriteeriumid kahtlase tekstisõnumi või telefonikõne tuvastamisel. Kõigi riikide vastajad leppisid kokku kõige olulisemates ohumärkides - 1) saatja / helistaja palub kontrollida üksikasju või esitada tundlikku teavet või saata raha; 2) erineva riigikoodiga number; ja 3) helistaja ei tutvusta ennast korralikult (nimi, ametikoht, ettevõte). Ka kõigi küsitletud riikide, välja arvatud Eesti, vastajad nõustusid, et ebatavaliselt pikk helistaja number on üks olulisemaid “ohumärke”. Lisaks sellele märkisid kõik uuringu vastajad, et hoiatust sisaldav sõnum (nt konto aegumine) ja vastuvõtjale surve avaldamine kiireloomulise otsuse tegemiseks on üks olulisemaid ohumärke (välja arvatud Küproselt vastanud).

Vähem oluliseks kriteeriumiks, mille vastajad märkisid Maltal, Eestis, Leedus ja Küprosel, olid õigekirja- ja grammatikavead. Vastupidi, Läti vastajad valisid õigekirja- ja grammatikavead üheks olulisemaks kriteeriumiks. Samuti vastasid küsitletud riikide vastajad, et see pole nii oluline, kui

helistaja ei viita neile nime ja perekonnanime järgi, välja arvatud Küproselt pärit vastajad, kelle arvates oli see kahtlase kõne äratundmisel üks olulisemaid kriteeriume.

***Sotsiaalmeedia kanalite sõnumid***

Ka sotsiaalmeedias kahtlaste sõnumite tuvastamisel oli vastajatel peaaegu ühtne arvamus. Enamik vastanutest nõustus järgmiste olulisemate kriteeriumide osas: 1) sõnumis küsitakse raha; 2) sõnumis palutakse kontrollida üksikasju või esitada tundlikku teavet; 3) sõnum sisaldab kahtlast linki ja 4) saatja sotsiaalmeedia profiil tundub kahtlane (nt uus konto, sõpru pole jne). Vastajad, välja arvatud Malta päritolu, usuvad samuti, et sõnum, milles palutakse teil mõni programm installida, on üks peamisi kahtlast tegevust tähistavaid märke. Õigekirja- ja grammatikavead, saatjaga ärisuhete puudumine või saatja mittetundmine tunnistati vastajate kõige vähem oluliseks kriteeriumiks.

| Andmepüügi rünnakute tuvastamine | Olulised kriteeriumid | Vähemolulised kriteeriumid |
|---|---|---|
| **E-kiri** | • saatja domeen (e-posti aadress) ei tundu ehtne;<br>• e-kirja nähtavad lingid on erinevad tegelikust hüperlingist;<br>• saatja palub kinnitada / edastada tundlikku teavet;<br>• e-posti aadressides, linkides ja domeeninimedes on nähtavaid vastuolusid;<br>• e-kiri sisaldab ootamatut/ebatavalist manust. | • umbisikuline tervitus;<br>• puudub saatja info ega sisalda kontaktandmeid;<br>• e-post ise tekitab uudishimu, vajadus rohkem teada saada. |
| **Tekstisõnum või telefonikõne** | • saatja/helistaja palub kontrollida üksikasju, esitada tundlikku teavet või saata raha;<br>• erineva riigikoodiga number;<br>• helistaja ei tutvusta ennast korralikult (nimi, ametikoht, ettevõte);<br>• ebatavaline pikk telefoni number[17];<br>• sõnum sisaldab hoiatust[18]. | • õigekirja- ja grammatikavead[19];<br>• helistaja ei viita teile eesnime, perekonnanime järgi[20]. |
| **Sotsiaalmeedia kanalite sõnumid** | • sõnumis küsitakse raha;<br>• sõnumis palutakse täpsustada üksikasju või esitada tundlikku teavet;<br>• sõnum sisaldab kahtlast linki;<br>• saatja sotsiaalmeedia profiil tundub kahtlane (nt uus konto, sõpru pole jne);<br>• sõnumis palutakse teil mõni programm installeerida[21] | • õigekirja- ja grammatikavead;<br>• saatjaga ärisuhete puudumine;<br>• tundmatu saatja. |

*Tabel 3. Kõige olulisemad ja vähem olulised kriteeriumid andmepüügirünnakute tuvastamisel*

[17] Välja arvatud Eesti vastajad
[18] Välja arvatud Küprose vastajad
[19] Välja arvatud Läti vastajad
[20] Välja arvatud Küprose vastajad
[21] Välja arvatud Malta vastajad

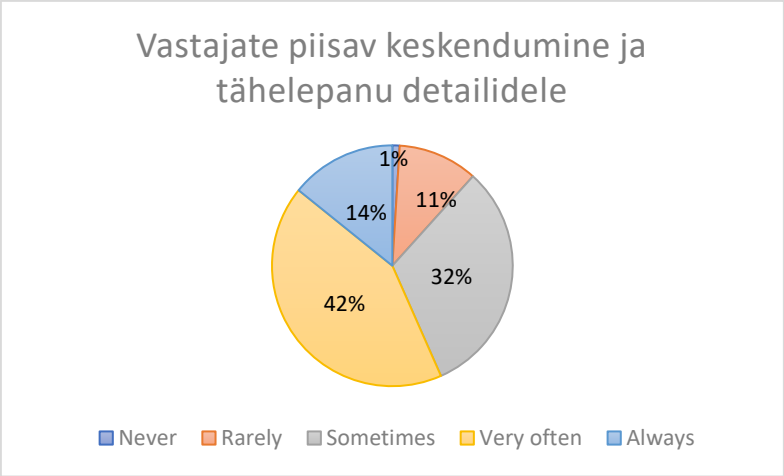
Co-funded by the Erasmus+ Programme of the European Union

Põhikriteeriumide märkimisel keskenduvad vastajad kahtlaste e-kirjade tuvastamisel peamiselt „tehnilistele kriteeriumidele“, näiteks linkidele, domeenidele, manustele, riigikoodile jne, mitte inimese emotsioonidele (sotsiaalsed ründed). Õigekirja- või grammatikavead või üldine tervitamine on viimaste punktide seas, mida vastajad peavad oluliseks.

Siiski on oluline märkida, et kuigi „tehnilised kriteeriumid“ on esimesed punktid, millele vastajad tähelepanu pööravad ja neid kontrollivad, ei tähenda need, et nad ei arvesta e-kirjade ja sõnumite hindamisel sotsiaalseid aspekte. Kui paluti tuvastada andmepüügi meilid / sõnumid ja uuriti peamisi ohumärke, valis enamik küsitletud riikidest vastanutest nii tehnilised kriteeriumid kui ka inimeste emotsioonidele keskendunud kriteeriumid (sotsiaalse ründe osad).

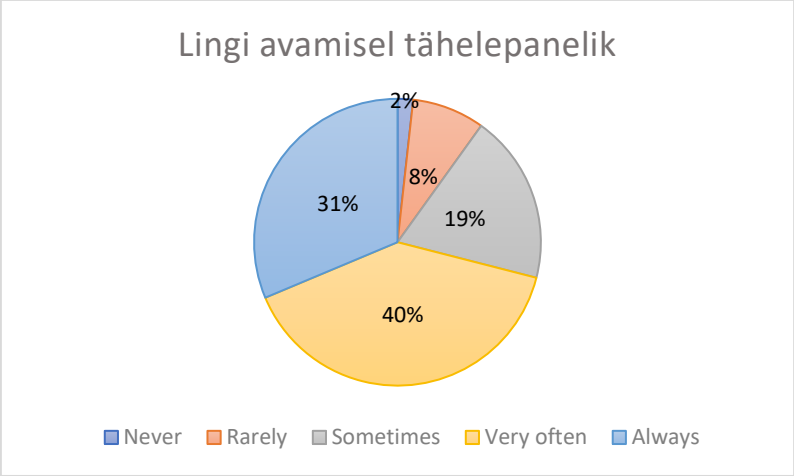
### 3.3.5. Kriitilise mõtlemise oskus

Enamik vastanutest suhtub oma kriitilise mõtlemise oskustesse üsna positiivselt. Enam kui pooled vastanutest (57%) väitsid, et nad on e-kirja või sõnumi avamisel väga sageli või alati piisavalt keskendunud ja tähelepanu detailidele. Võrdluseks märkis 12%, et neil pole kunagi olnud piisavalt või on harva piisavalt tähelepanu.




*Joonis 11. Vastajate piisav keskendumine ja tähelepanu detailidele e-maili/sõnumi avamisel*

71% vastanutest väidab, et on lingil või manusel klõpsamisel sageli tähelepanelik, samas kui 11% väitis, et pole seda tehes kunagi või on harva meeles.




*Joonis 12. Vastanute jaotus kui tähelepanelik on keegi lingi avamisel*

Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

67% vastanutest väitis, et kahtlase väljanägemisega meili või sõnumi saamisel suudavad nad tõendite põhjal väga sageli või alati visualiseerida oma otsuste võimalikke tagajärgi, samas kui ainult 5% vastanutest väitis, et ei suuda seda kunagi või harva visualiseerida.

77% vastanutest suudab kahtlase välimusega meili või sõnumi saamisel ka tõendite põhjal järeldusi teha väga sageli või alati, samas kui ainult 3% vastanutest ei saa seda kunagi teha või saavad harva. Tuvastati erinevus vastajate protsendi vahel, kes suudab tagajärgi visualiseerida ja suudab järeldusi teha. Seevastu pole kõik vastajad teadlikud andmepüügi tagajärgedest. Nad suudavad endiselt teha järeldusi ja tuvastada andmepüügi e-posti/sõnumi.

Siiski on oluline rõhutada, et vaatamata üsna headele tulemustele suudab umbes kolmandik vastanutest siiski vaid mõnikord tagajärgi visualiseerida ja järeldusi teha.

### 3.3.6. Andmepüügi rünnakute vältimine

Uuringu vastajatel paluti välja tuua ka peamised põhjused, mis nende arvates edukatele andmepüügi rünnakutele kaasa aitavad. Kõigi riikide vastajad valisid viis peamist põhjust: 1) inimesed ei ole teadlikud sellistest rünnakutest ja nende ennetamisest; 2) ründajad kasutavad ära inimloomust, nad toetuvad suhtlemise vajadusele ning inimeste emotsioonidele mängimisele; 3) ründajad suudavad hästi korrata legitiimsete ettevõtete sõnumeid ja kirju, muutes need väga usutavaks ja veenvaks; 4) inimesed ei pööra piisavalt tähelepanu/on asjatundmatud[22]; 5) ründajad on arenenumad ja sihivad konkreetseid inimesi, mistõttu on meilid isikupärastatud ja kasutavad spetsiifilist teavet[23].

Vastajate poolt olid kõige vähem valitud põhjused: 1) inimesed kasutavad vananenud tarkvara; 2) andmepüügi vahendid on odavad ja laialt levinud; ja 3) pahavara ise muutub keerukamaks[24].


*Joonis 13. Peamised põhjused, miks andmepüügi rünnakud on vastajate sõnul edukad*

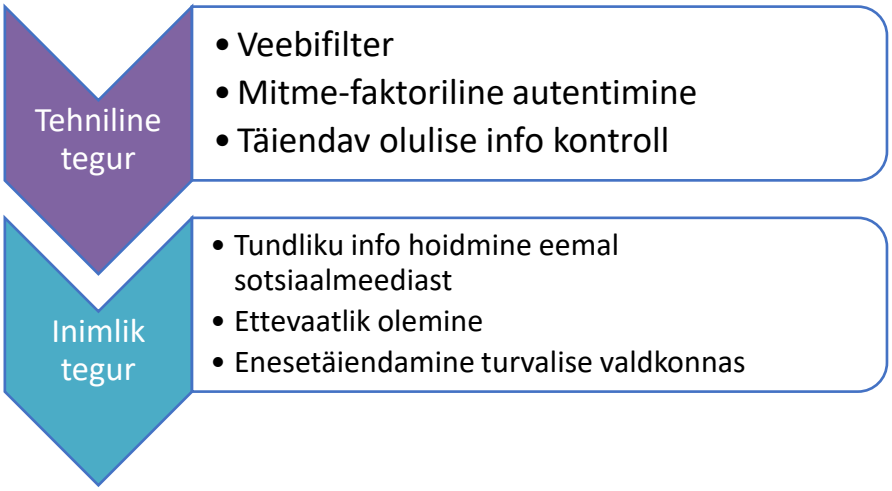
Vastajad nõustusid, et häkkerid kasutavad tavaliselt ära inimeste emotsioone, tahtmisi ja soove. Ohvreid meelitatakse pakkudes neile kingitusi või tasuta vautšereid, tõstes nende uudishimu ja tekitades hirmu / ärevust.

Enamik vastanutest usub, et andmepüügi rünnakute vältimiseks on oluline läheneda sellele küsimusele erinevatest vaatenurkadest: 1) tehniline tegur - kasutades veebifiltrit pahatahtlike veebisaitide blokeerimiseks, mitme-faktorilist autentimist / paroolide sagedast vahetamist ja täiendavat kontrolli ülitähtsates üksikasjades (saatjate e-post, lingid, manused jne) ja 2) inimlik tegur - hoides enda kohta tundlikku teavet sotsiaalmeedias eemal, olles ettevaatlik e-kirjade / sõnumite avamisel / telefonile vastamisel ja pidevalt harides ennast turvalisuse valdkonnas. Enamik Läti ja Küprose vastanutest peab turvatarkvara kasutamist oluliseks.

[22] Välja arvatud Malta vastajad
[23] Välja arvatud Küprose vastajad
[24] Välja arvatud Malta vastajad

Co-funded by the Erasmus+ Programme of the European Union

Vastajate arvates on kõige vähem olulised toimingud andmepüügi rünnakute vältimiseks uuendatud veebilehitseja kasutamine, kõige uuema olemasoleva tarkvara ja tööriistadega kursis olemine või uuendatud operatsioonisüsteemi kasutamine[25], samuti regulaarsed küberturvalisuse koolitused / töötoad.




*Joonis 14. Tegurid mis on olulised andmepüügi rünnakute vältimiseks vajalikud*

Valdkonnad, kus enamik vastanutest tunneb ennast kindlalt, on järgmised: on võimelised veebis leidma asjakohast ja usaldusväärset teavet, tuvastada andmepüügi rünnakuid ning kasutada turvatarkvara, mitme faktorilist autentimist ja veebifiltrit.

Vähem vastajaid tunneb end enesekindlalt oma teadmistega küberturvalisuse / andmepüügi terminoloogias ja selle kasutamisel ning ettevõtte tundliku teabe krüptimises.


*Joonis 15. Teemad, kus vastajad tunnevad end kõige enesekindlamalt*

[25] Välja arvatud Eesti vastajad

# 4. KOKKUVÕTE JA TULEMUSED

**Vastajate demograafiline jaotus**

- Uuringus osales 514 inimest, kellest 259 on naised, 248 meest ja 7 inimest eelistavad oma sugu mitte tuvastada.
- Enamik vastanutest on üliõpilased (304), neile järgnevad töötajad (139), ettevõtete tegevjuhid (53), töötud (10) ja füüsilisest isikust ettevõtjad (8).
- Enamik küsitlusele vastanutest on kõrgelt haritud - (38%) vastanutest on bakalaureusekraad, millele järgnevad magistrikraad (23%) ja doktorikraad (6%).

**Üldteadmised ja käitumine**

- Ehkki 74% vastanutest pole kunagi ametlikult osalenud ühelgi küberturvalisuse koolitusel / töötoas ega õppusel, on üle poole vastanutest (54%) seda teemat ise uurinud (artikleid lugenud, videosid vaadanud jne). Need tulemused näitavad, et kuigi vastajatel ei pruugi alati olla võimalust andmepüügi teemat ametlikus keskkonnas õppida, on neil motivatsioon oma teadmisi ja oskusi iseseisvalt täiendada.

- 61% vastanutest väitis, et teab, mis on andmepüük, samas kui 27% ei olnud kindel ja 12% ei teadnud. Kui paluti valida õige andmepüügi määratlus, valis rohkem vastajaid Leedust, Lätist ja Küproselt õige vastuse. Samas nad ei olnud kindlad vastamisel küsimusel, mis on andmepüük. Need leiud viitavad sellele, et rohkem vastajaid Leedust, Lätist ja Küproselt on andmepüügist teadlikud, kuid neil ei ole piisavalt teadmisi ega enesekindlust.

- 59% küsitletud inimestest kardab linki või manust avada väga sageli või arvab, et see võib olla pahatahtlik. Võrdluseks võib öelda, et 51% kardab väga sageli või alati andmepüügi rünnakute sihtmärgiks saada. Küsimustiku tulemused näitavad, et isegi need vastajad, kes väitsid, et teavad, mis on andmepüük, kardavad andmepüügi ohvriks langeda, viidates ebapiisavatele teadmistele või usalduse puudumisele oma oskuste suhtes.

- Vastajad on enamasti teadlikud andmepüügi tüüpidest “Spray and pray”, “Cat phishing” ja “Malvertising”. Teistpidi, neil on vähem teadmisi “Whaling”, “Clone phishing” ja “Smishing” rünnetest.

- Kui küsiti, millised tagajärjed tõenäoliselt või kindlasti tekivad pärast edukat andmepüügirünnakut isikule või ettevõttele, nimetas enamik küsitletud riikidest vastajaid neid tagajärgi: „tundlike andmete vargus”, „krediitkaardipettus”, „kliendiandmete leke ”, „mainekahjustus” ja „kasutajanimede ja paroolide kaotamine” (välja arvatud Malta vastajad). Kõigi küsitletud riikide, välja arvatud Küpros, vastajad kalduvad samuti arvama, et pärast edukat andmepüügirünnakut müüakse nende andmeid suure tõenäosusega kuritegelikele kolmandatele isikutele. Teistpidi, vastajad usuvad, et intellektuaalse omandi vargus on vähetõenäoline andmepüügi tulemusena.

- Leedu, Malta ja Eesti vastajad on skeptilised ka andmepüügi rünnaku tagajärjel „ettevõtte / kliendi kontolt raha varguse” suhtes.

- Vastajad vajutavad tõenäolisemalt e-kirjas või kirjas olevale lingile või manusele, kui selle on saatnud ülemus või kolleeg, ettevõte, mille teenuseid saaja kasutab,

Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

pank või riigiasutus. Veenmise põhimõtted "meeldimine" ja "autoriteet" on need, millele vastajad kõige tõenäolisemalt reageerivad.

- Vastajad ei klõpsa tõenäolisemalt e-kirjas või kirjas oleval lingil või manusel, kui see pakub konfidentsiaalset teavet, palub avalikustada isiklikke andmeid auhinnavõistlusel osalemiseks või kui ettevõte, mille teenust nad ei kasuta, saadab kirja. Tundub, et veenmise põhimõte „vastutasu“ on see, millele vastajad reageerivad kõige tõenäolisemalt.

**Vastajate kogemus andmepüügiga**

- Iga viies vastaja on sattunud andmepüügi ohvriks. Peamised meetodid, millega vastanud olid kokku puutunud olid: linkide avamine ja privaatse info avaldamine e-kirjaga ning veebilehtedel. Ainult Küprose ja Eestis vastajad andsid teada, et nad on kokku puutunud andmepüügiga, kus tuli sisestada oma andmed võltsitud veebisaidile.

- Peamised põhjused miks ohvriks langeti olid: hajameelsus, uudishimulikkus või kiirustamine. Mõni vastaja mainis ka seda, et ei olnud teadlik andmepüügist.

**Andmepüügi rünnakute tuvastamine**

- Andmepüügi rünnakute tuvastamisel keskenduvad vastajad peamiselt „tehnilistele kriteeriumidele“, näiteks linkidele, domeenidele, manustele, riigikoodile jne, mitte inimese emotsioonidele (sotsiaalsed ründed). Üheks kahtlust äratavaks asjaoluks on kindlasti ka kui teine osapool küsib tundlikku privaatset infot. Õigekirja- või grammatikavead või üldine tervitamine on viimaste punktide seas, mida vastajad peavad oluliseks.

- Siiski on oluline märkida, et kuigi „tehnilised kriteeriumid“ on esimesed punktid, millele vastajad tähelepanu pööravad ja neid kontrollivad, ei tähenda need, et nad ei arvesta e-kirjade ja sõnumite hindamisel sotsiaalseid aspekte. Kui paluti tuvastada andmepüügi meilid / sõnumid ja uuriti ohumärke, valis enamik küsitletud riikidest vastanutest nii tehnilised kriteeriumid kui ka inimeste emotsioonidele keskendunud kriteeriumid (sotsiaalse ründe osad).

**Kriitilise mõtlemise oskus**

- Enamik vastanutest suhtub oma kriitilise mõtlemise oskustesse üsna positiivselt. Enam kui pooled vastanutest (57%) väitsid, et nad on e-kirja või sõnumi avamisel väga sageli või alati piisavalt keskendunud ja tähelepanu detailidele. Võrdluseks 71% vastanutest väidab, et on lingil või manusel klõpsamisel sageli tähelepanelik.

- 67% vastanutest väitis, et kahtlase väljanägemisega meili või sõnumi saamisel suudavad nad tõendite põhjal väga sageli või alati visualiseerida oma otsuste võimalikke tagajärgi. 77% vastanutest suudab kahtlase välimusega meili või sõnumi saamisel ka tõendite põhjal järeldusi teha väga sageli või alati. Tuvastati erinevus vastajate protsendi vahel, kes suudab tagajärgi visualiseerida ja suudab järeldusi teha. Seevastu pole kõik vastajad teadlikud andmepüügi tagajärgedest. Samas nad suudavad endiselt teha järeldusi ja tuvastada andmepüügi e-posti/sõnumi.

- Siiski on oluline rõhutada, et vaatamata üsna headele tulemustele suudab umbes kolmandik vastanutest siiski vaid mõnikord tagajärgi visualiseerida ja järeldusi teha.

Co-funded by the Erasmus+ Programme of the European Union

**Andmepüügi rünnakute vältimine**

- Vastajad tõid välja järgmised põhjused, mis nende arvates viivad edukate andmepüügirünnakuteni: inimesed pole teadlikud andmepüügist ja selle vältimisest, ründajad kasutavad inimloomust ära. Samuti on neil kerge korrata legitiimsete ettevõtete e-kirju ja sõnumeid sest inimesed ei pööra piisavalt tähelepanu või on asjatundmatud. Vähem vastajaid usub, et vananenud tarkvara kasutavad inimesed, õngitsemisvahendid on odavad või laialt levinud ning keerukam pahavara on põhjused, miks andmepüügirünnakud toimuvad.

- Vastajad usuvad, et häkkerid kasutavad peamiselt ära inimese uudishimu, hirmu või ärevust ning kasutavad stiimuleid nagu „tasuta kingitused“ või „vautšerid“.

- Andmepüügirünnakute vältimiseks on vastajate arvates oluline läheneda sellele kahest erinevast vaatenurgast: „tehniline tegur” ja „inimtegur”, kasutades mõlema kajastamiseks sobivaid tööriistu ja strateegiaid. Näiteks hõlmab „tehniline tegur“ veebifiltri kasutamist, mitmikautentimine ja oluliste üksikasjade, näiteks saatja e-posti aadressi, linkide ja manuste jms kontrollimist. Inimtegur seisneb tundliku teabe mitte avaldamises sotsiaalmeedias, ettevaatlik olemises ja enda pidevas harimises.

- Huvitav on see, et kuigi enamus vastajaid on seisukohal, et on oluline ennast andmepüügi valdkonnas pidevalt harida, usub vähem vastajaid, et vaja on regulaarset küberturvalisuse koolitust või töötuba. See on seletatav tulemustega, kus peaaegu pooled vastanutest uurivad seda teemat iseseisvalt.

- Üldiselt rõhutavad vastajad inimese võimet hinnata ja tuvastada andmepüügirünnakuid, selle asemel et loota arvuti operatsioonisüsteemile, tarkvarale ja saadaolevatele tehnilistele tööriistadele.

- Valdkondades, kus enamik vastanutest tunneb end kõige kindlamalt on järgmised: veebis asjakohase ja usaldusväärset teabe leidmine, tuvastada andmepüügirünnakuid ning kasutada turvatarkvara, mitme teguri autentimist ja veebifiltrit.

- Vähem vastajaid tunneb end enesekindlalt oma teadmistega küberturvalisuse / andmepüügi terminoloogias ja selle kasutamisel ning ettevõtte tundliku teabe krüpteerimisel ja sellega ümber käimisel.

Co-funded by the Erasmus+ Programme of the European Union

# 5. Kasutatud kirjandus


1. EU Commission (2020): Special Eurobarometer 499: Europeans' attitudes towards cyber security, URL https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG
2. European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020
3. EUROSTAT (2020): Is internet use safer today?, URL https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb/default/table?lang=en (külastatud 11.02.2021)
4. Proofpoint (2019): Human Factor Report 2019, URL https://www.proofpoint.com/us/resources/threat-reports/human-factor (külastatud 12.02.2021)
5. European Union Agency for Cybersecurity (2020): Phishing - ENISA threat landscape 2019-2020
6. Deloitte (2019): Understanding Phishing Techniques, URL https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf (külastatud 112.02.2021)
7. EUROPOL (2020): Internet Organised Crime Threat Assessment 2020
8. NCC group (2020) :Psychology of the Phish: Leveraging the Seven Principles of Influence, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433 (külastatud 12.02.2021)
9. Council of Europe (2020): Cybercrime and Covid, URL: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (külastatud 12.02.2021)
10. EUROPOL (2020): Pandemic profiteering - how criminals exploit the COVID-19 crisis



Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

# Lisa 1. Projektis kasutatud inglise keelne küsimustik (Survey “Evaluation of skills and recognition of phishing attacks”)

## SECTION 1: Personal data

1. **Name:**…… *(optional)*

2. **E-mail address:**…….. *(optional - If you would like to receive the updates about the project and participate in the pilot testing of the training programme please submit your email.)*

3. **Gender**

- Male
- Female
- Prefer not to say

4. **Education Level**

- No Schooling Completed
- High School Diploma
- Professional Degree (Technical/ Vocational Training)
- Bachelor's Degree
- Master's Degree
- Doctoral degree
- Prefer not to say
- Other:……

5. **Employment Status**

- Business Owner
- Employed
- Self Employed
- Student
- Retired
- Unemployed
- Other:……

## SECTION 2: General knowledge & behaviours

6. **How likely are you to click on the link or attachment in the email or message and/or provide sensitive information if it:**

Co-funded by the Erasmus+ Programme of the European Union

| | Very unlikely | Unlikely | Neutral | Likely | Very likely |
|---|---|---|---|---|---|
| Offers voucher or discounts on some purchases | | | | | |
| Offers you access to some exclusive offers | | | | | |
| Invites you to specific event online or offline (e.g., zoom meeting) | | | | | |
| Asks you to fill in the survey/ provide your email or phone contacts in order to participate in the contest to win a prize | | | | | |
| Offers you confidential information (e.g., information about your competitors) | | | | | |
| Asks you to clarify your personal and/or account details for it not be closed/deactivated ( e.g., bank account, Netflix account, Facebook account, etc.) | | | | | |
| Ask you to clarify your details such as your address for your order shipment (e.g., Amazon deliver) | | | | | |
| Updates you on the newest developments regarding important social issues and natural disasters (e.g., updates on COVID-19 situation) | | | | | |
| Asks you to help/ donate to local or international charities' | | | | | |
| Includes information about your hobbies | | | | | |
| Is sent by the bank or any governmental institution | | | | | |
| Is sent by your boss or colleague | | | | | |
| Is sent by the company which services you use | | | | | |
| Is sent by the company/organisation you know but don't use their services | | | | | |

7. **Have you ever participated in any formal training/workshop/studies on cybersecurity or phishing specifically?**

- Yes
- No

'

Co-funded by the Erasmus+ Programme of the European Union

8. **Have you researched/ studied cybersecurity or phishing specifically by yourself? (read an article, watched videos, etc.)**
- Yes
- No

9. **Do you know what phishing is?**
- Yes
- No
- Not sure

10. **Which of these examples do you think fits the phishing definition?**
- A cybercrime in which a target is contacted by email to lure an individual into providing sensitive data about his accounts
- It is a kind of sport for pleasure or competition
- Unwanted and/or repeated emails by an individual or company offering products or services
- A cybercrime in which a target is contacted by email, telephone or text message to lure an individual into providing sensitive data.

11. **Are you aware of these types of phishing?'**

*1) Spray and pray – malicious emails that are sent to any and all email addresses in attempt to attempt to steal sensitive information;*
*2) Advanced fee scam – common fraud associated with nationals from Nigeria, e.g. asking for assistance in moving large amount of money;*
*3) Cat phishing – luring someone in relationship by adopting a fictional online persona;*
*4) Spear fishing - malicious emails that are specially crafted and sent to specific individual or organization in attempt to steal sensitive information*
*5) Whaling - an attempt to steal sensitive information and is often targeted at senior management;*
*6) Vishing - refers to phishing scams that take place over the phone;*
*7) Smishing - refer to phishing by using SMS messages as opposed to emails to target individuals;*
*8) Clone Phishing - type of phishing where a legitimate and previously delivered email is used to create an identical email with malicious content.*
*9) Content Injection - cybercriminals hack a familiar website and include a fake website login page or pop-up that directs website visitors to a fake website.*
*10) Malvertising - This phishing type uses online advertisements or pop-ups to compel people to click a valid-looking link that then installs malware on their computer.*

| | Not at all aware | Slightly aware | Moderately aware | Very aware | Extremely aware |
|---|---|---|---|---|---|
| Spray and pray | | | | | |
| Advanced fee scam | | | | | |
| Cat phishing | | | | | |
| Spear phishing | | | | | |
| Whaling | | | | | |
| Whishing | | | | | |
| Smishing | | | | | |
| Clone phishing | | | | | |
| Content Injection | | | | | |
| Malvertising | | | | | |

Co-funded by the Erasmus+ Programme of the European Union

**12. What kind of consequences are likely to occur after a successful phishing attack on a person or company?**

| | Definitely not | Probably not | Probably | Very probably | Definitely |
|---|---|---|---|---|---|
| Identity theft | | | | | |
| Credit card fraud | | | | | |
| Theft of sensitive data | | | | | |
| Loss of usernames and passwords | | | | | |
| Installation of malware and ransomware | | | | | |
| Loss of intellectual property | | | | | |
| Theft of client information | | | | | |
| Theft of funds from business and client accounts | | | | | |
| Access to systems to launch future attacks | | | | | |
| Data sold on to criminal third parties | | | | | |
| Reputational damage | | | | | |

## SECTION 3- Personal experience

**13. Have you ever feared to open a link in an e-mail or message, thinking that it could be fake?**

1 – Never
2 – Rarely
3 – Sometimes
4 – Often
5 – Always

**14. Are you, in general, afraid of becoming a target of a phishing attack?**

1 – Never
2 – Rarely
3 – Sometimes
4 – Often
5 – Always

**15. Have you ever been phished?**

*Description: By phished we mean - clicked on the malicious link/ attachment/ provided sensitive data, etc.*

- Yes
- No

Co-funded by the Erasmus+ Programme of the European Union

## SECTION 4 - Phishing attack (only for those who answered 'yes' in question 15)

**16. How have you been phished?**

- By clicking the link in the email or message
- By answering the email or message and providing sensitive information (e.g., login details)
- By opening attachment in the email
- By providing sensitive information by phone
- Other……

**17. Why do you think it happened?**

- I was in a hurry
- I was distracted/not paying attention
- I was stressed/nervous
- I was intimidated
- I was curious
- I was excited/happy (e.g., thought I won the prize)
- I wanted to help
- Other……

## SECTION 5 - Recognising phishing attack

**19. How important are these criteria in recognising a suspicious email?**

| | Not important | Slightly important | Moderately important | Important | Very important |
|---|---|---|---|---|---|
| Generic greeting in the email (e.g., Dear customer) | | | | | |
| The sender is asking you to confirm/ provide sensitive information (login credentials, bank details) via email or phone | | | | | |
| The sender's domain (email) does not look genuine (does not match the organisation, contain a concealed spelling mistake, extra numbers, letters in it, and etc.) | | | | | |
| The embedded links in the email is not the same as real hyperlink | | | | | |
| There are visible inconsistencies in email addresses, links & domain names | | | | | |
| The email contains an unexpected/unusual attachment | | | | | |
| There are spelling and grammar mistakes in the email | | | | | |
| The style of the writing in the email does not match a | | | | | |

Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

| | | | | | |
|---|---|---|---|---|---|
| person/company that usually sends you such emails | | | | | |
| There is no signature or contact information | | | | | |
| The email message creates a sense of urgency, demands immediate action, and makes you panic and feel stressed | | | | | |
| The email message creates curiosity, need to find out more | | | | | |
| The email message is too good to be true | | | | | |

**20. How important are these criteria in recognising a suspicious text message/phone call?**

| | Not important | Slightly important | Moderately important | Important | Very important |
|---|---|---|---|---|---|
| Unusually long number | | | | | |
| Number with the different country code | | | | | |
| Sender/Caller asks you to verify details or provide sensitive information or send money | | | | | |
| Caller does not introduce himself/herself properly (name, position, company) | | | | | |
| Caller does not refer to you by name, surname | | | | | |
| Text message contains a link | | | | | |
| You are not client of the sender/caller (company) | | | | | |
| You do not have any relationship or business relations with the sender/caller | | | | | |
| Message contains another phone number to call | | | | | |
| Spelling/grammar mistakes | | | | | |
| Message itself contains a warning (e.g. expiring account) and puts pressure on receiver to make an urgent decision | | | | | |

**21. How important are these criteria in recognising a suspicious message in Social Media channels?**

| | Not important | Slightly important | Moderately important | Important | Very important |
|---|---|---|---|---|---|
| The message asks you to verity details or | | | | | |

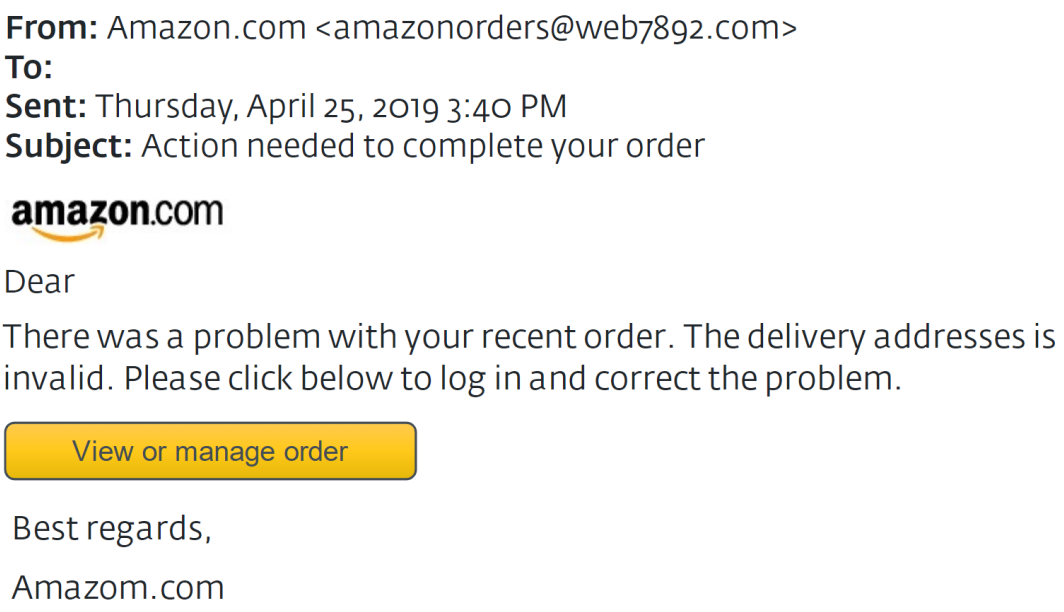
Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

| | | | | | |
|---|---|---|---|---|---|
| provide sensitive information | | | | | |
| The message asks you for money | | | | | |
| The message asks you to install some programme | | | | | |
| Message contains a doubtful link | | | | | |
| You do not know the sender | | | | | |
| You do not have any business relations with the sender | | | | | |
| The social media profile of the sender looks suspicious (e.g. new account, no friends, etc.) | | | | | |
| Message contains attention-grabbing title (e.g. You won't believe this video!) | | | | | |
| The message style does not match the sender (too formal/informal, etc.) | | | | | |
| Spelling/grammar mistakes | | | | | |

## SECTION 6 – Phishing examples

*Phishing Example 1*



**From:** Amazon.com <amazonorders@web7892.com>
**To:**
**Sent:** Thursday, April 25, 2019 3:40 PM
**Subject:** Action needed to complete your order

amazon.com

Dear

There was a problem with your recent order. The delivery addresses is invalid. Please click below to log in and correct the problem.

View or manage order

Best regards,

Amazom.com

**22. Is the image above a real email or phishing email?**

- Real Email
- Phishing Email

## SECTION 7

*Example 1 (only if answered 'Phishing Email' in previous question)*

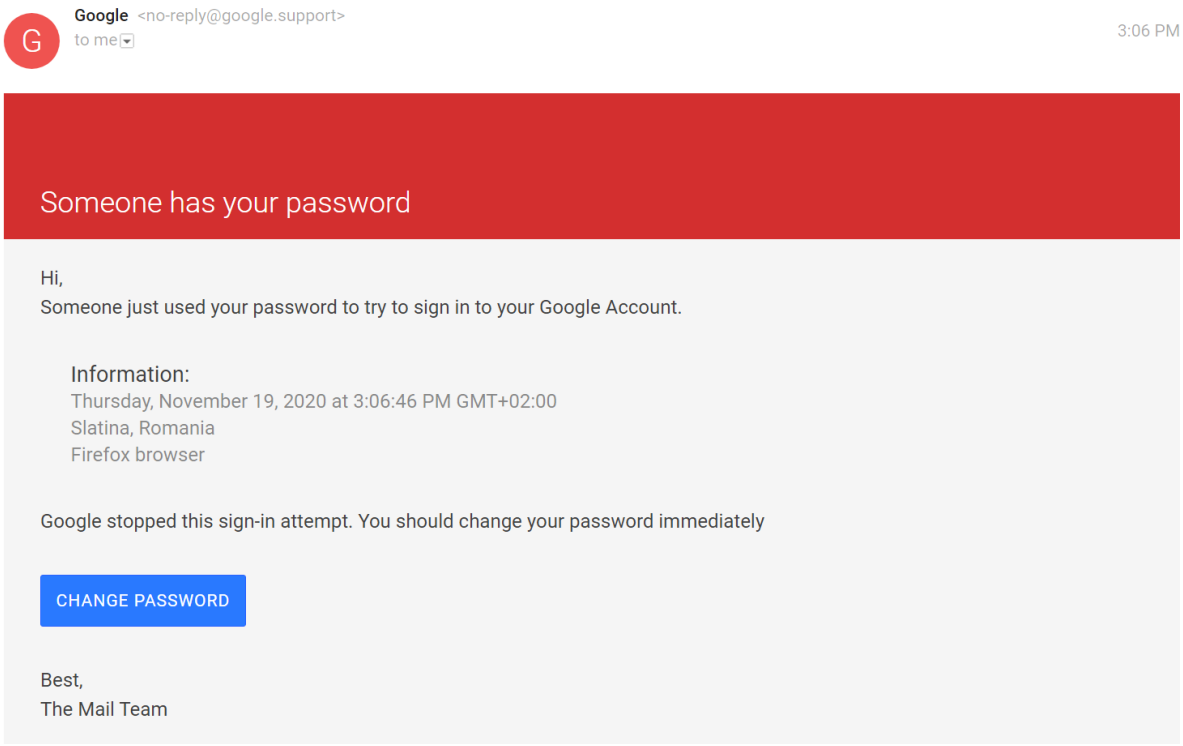
**23. Why have you decided that this is a phishing email? Choose the "red flags"**

- Generic greeting
- Request for confirmation/verification/details of sensitive information
- The sender's domain/email
- Suspicious links
- Inconsistencies in email addresses, links & domain names
- Spelling and grammar mistakes
- Suspicious style of writing
- Sense of urgency/need for immediate actions
- Too good to be true

Other……

## SECTION 8

*Phishing Example 2*




**24. Is the image above a real email or phishing email?**

- Real email
- Phishing email

## SECTION 9

*Example 2 (only if answered 'Phishing Email' in previous question)*

**25. Why have you decided that this is a phishing email? Choose the "red flags"**

- Generic greeting
- Request for confirmation/verification/details of sensitive information

Co-funded by the Erasmus+ Programme of the European Union

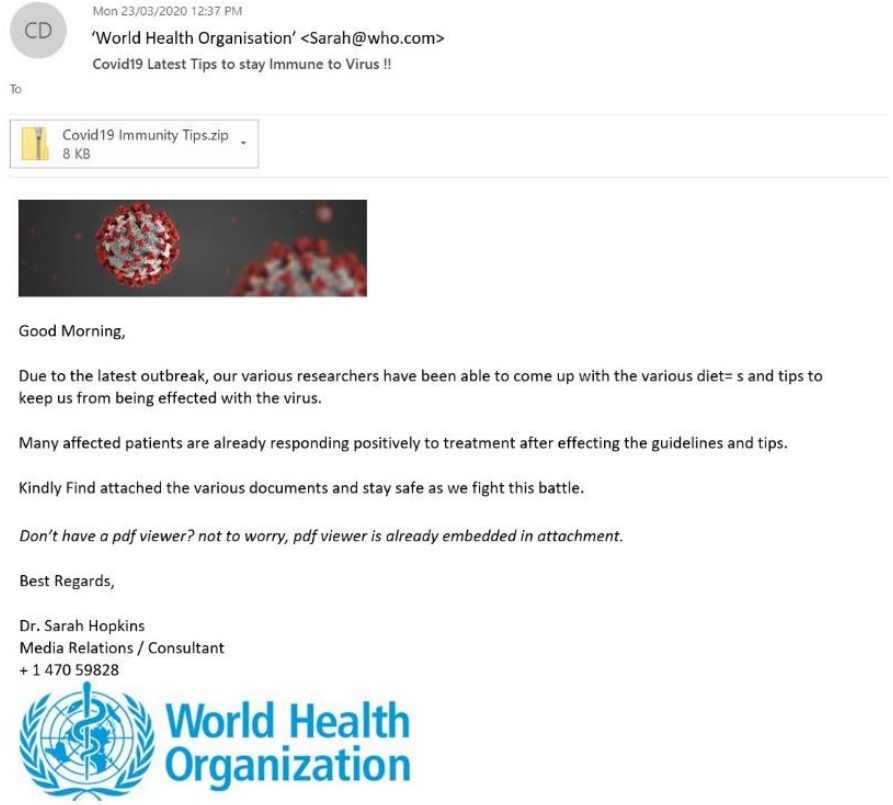
Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

- The sender's domain/email
- Suspicious links
- Inconsistencies in email addresses, links & domain names
- Spelling and grammar mistakes
- Suspicious style of writing
- Sense of urgency/need for immediate actions
- Too good to be true

Other……

## SECTION 10

*Phishing Example 3*




**26. Is the image above a real email or phishing email?**

- Real email
- Phishing email

## SECTION 11

*Example 3 (only if answered 'Phishing Email' in previous question)*

**27. Why have you decided that this is a phishing email? Choose the "red flags"**

- Generic greeting
- Request for confirmation/verification/details of sensitive information
- The sender's domain/email
- Suspicious links
- Inconsistencies in email addresses, links & domain names
- Spelling and grammar mistakes
- Suspicious style of writing
- Sense of urgency/need for immediate actions
- Too good to be true

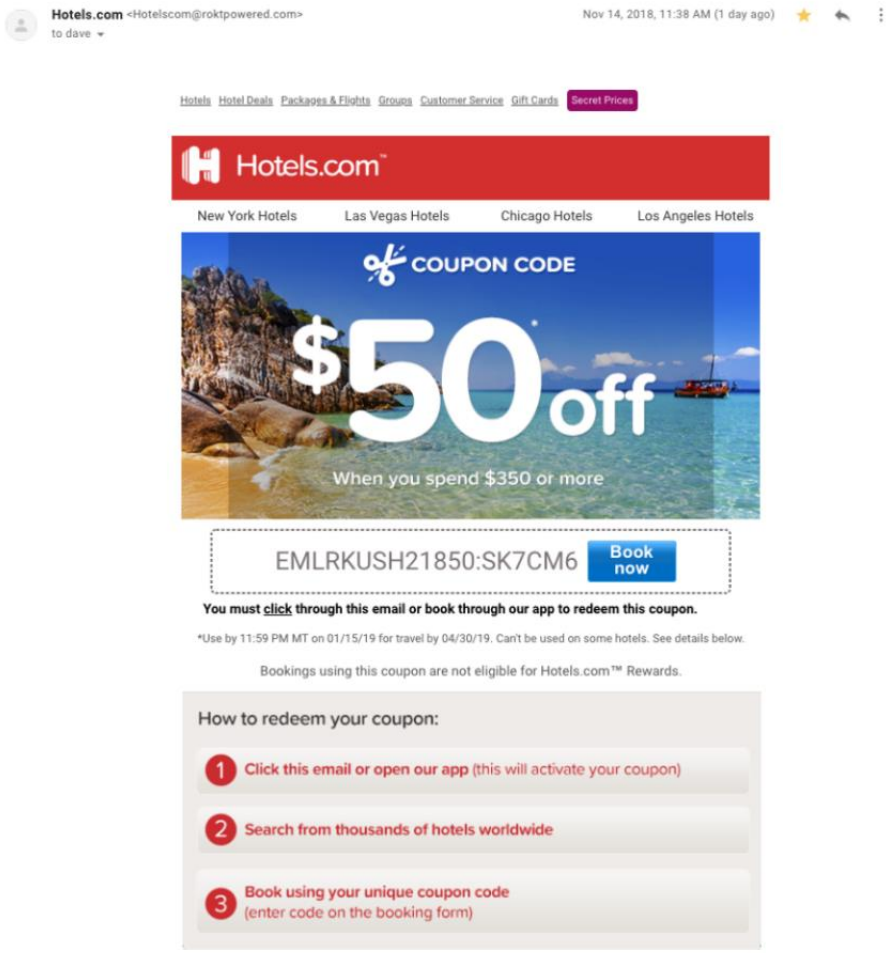
Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

Other……

## SECTION 12

*Phishing Example 4*




**28. Is the image above a real email or phishing email?**

- Real email
- Phishing email

## SECTION 13

*Example 4 (only if answered 'Phishing Email' in previous question)*

**29. Why have you decided that this is a phishing email? Choose the "red flags"**

- Generic greeting
- Request for confirmation/verification/details of sensitive information
- The sender's domain/email
- Suspicious links
- Inconsistencies in email addresses, links & domain names
- Spelling and grammar mistakes
- Suspicious style of writing
- Sense of urgency/need for immediate actions
- Too good to be true

Other ……

Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

## SECTION 14

*Phishing Example 5*

From: **Markus** <markusceo@eco1focus.com>
Date: Mon, Dec 7, 2020 at 11:38 AM
Subject: Invoice to be paid
To: Finance department <financedept@ecofocus.org>

Hi Gwen,

Could you do me a favour? Theres pending invoice from one of our providers and because I'm on holiday I need you to take care of it for me bec ause I can't access the accounts from here.
They contacted me and I told them to send through the email to you as well (check spam filter incase it's accidentally blocked!) Just click on the link in their email and transfer the amount to the account they specify.

This needs to be done TODAY so make it high priority.

If you do this for me it would be a huge favour.

Any questions then reply to this email. I can't take calls right now so just stick to replying to this email.

Thanks,
Markus
CEO

**30. Is the image above a real email or phishing email??**

- Real email
- Phishing email

## SECTION 15

*Example 5 (only if answered 'Phishing Message' in previous question)*

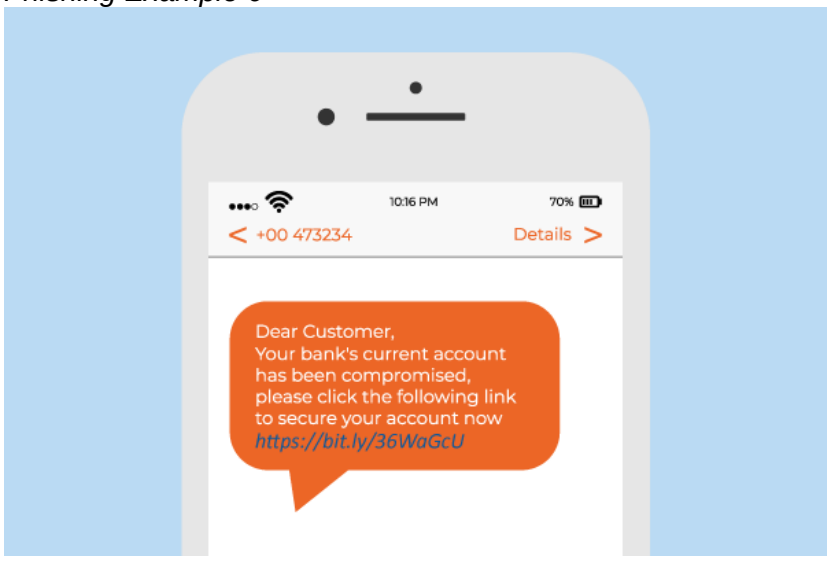
**31. Why have you decided that this is a phishing email? Choose the "red flags"**

- Generic greeting
- Request for confirmation/verification/details of sensitive information
- The sender's domain/email
- Suspicious links
- Inconsistencies in email addresses, links & domain names
- Spelling and grammar mistakes
- Suspicious style of writing
- Sense of urgency/need for immediate actions
- Too good to be true

Other ……

## SECTION 16

*Phishing Example 6*




Co-funded by the Erasmus+ Programme of the European Union

**32. Is the image above a real text or phishing text?**

- Real text
- Phishing text

## SECTION 17

*Example 6 (only if answered 'Phishing Text' in previous question)*

**33. Why have you decided that this is a phishing text message? Choose the "red flags"**

- Generic greeting
- Request for confirmation/verification/details of sensitive information
- The sender's domain/email
- Suspicious links
- Inconsistencies in email addresses, links & domain names
- Spelling and grammar mistakes
- Suspicious style of writing
- Sense of urgency/need for immediate actions
- Too good to be true

Other……

## SECTION 18 - Self-evaluation: Critical thinking

**34. Use the scale from 1 till 5 to evaluate:**

1) Never
2) Rarely
3) Sometimes
4) Very Often
5) Always

| | Never | Rarely | Sometimes | Very often | Always |
|---|---|---|---|---|---|
| Do you normally trust messages that appear to come from an important entity or look important? | | | | | |
| When you open an email/ message do you have a sufficient focus and attention to detail? | | | | | |
| Are you mindful of what you click on when you receive an email/message with the link/ attachment? | | | | | |

**35. When you receive a suspiciously looking email, do you evaluate:**

| | Never | Rarely | Sometimes | Very often | Always |
|---|---|---|---|---|---|
| Who is sender | | | | | |
| Sender's email | | | | | |
| Subject line | | | | | |
| Style of email (formal, non-formal, words used) | | | | | |

Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)

| | | | | | |
|---|---|---|---|---|---|
| Images | | | | | |
| Grammar and spelling mistakes | | | | | |
| Links/attachments | | | | | |
| Signature and credentials | | | | | |

**36. When you receive a suspicious looking email/message, are you able to visualise possible implications/consequences of your decision, based on evidence?**

- Never
- Rarely
- Sometimes
- Very Often
- Always

**37. When you receive a suspicious looking email/message, are you able to draw the conclusions, based on evidence?**

- Never
- Rarely
- Sometimes
- Very Often
- Always

## SECTION 19 - Avoiding phishing attacks

**38. Why phishing attacks are successful? (Choose top 5 reasons)**

- Attackers are really good at replication of messages and emails from legit companies, making them very believable and convincing
- Attackers exploit human nature, they rely on interaction and playing human emotions and needs
- Attackers can easily access personal details and information about the specific person or company in social media/company webpages, press, etc.
- Attackers are becoming more advanced, targeting specific individuals while using emails are highly personalized and use specific information
- People are not paying enough attention/are ignorant
- People are not aware/ have no knowledge on such attacks and how to prevent them
- People are using outdated software
- Organisations/Companies are not doing enough to prevent these attacks
- There is a lack of training provided in regard to cybersecurity and phishing
- Phishing tools are low-cost and widespread
- Malware itself is becoming more sophisticated
- Other……

**39. What emotions, needs and desires are usually exploited by attackers?**

- Fear
- Concern/Anxiety
- Panic
- Curiosity
- Greediness
- Motivation (Gift / Free voucher)
- Desire for emotional fulfilment
- Trusting nature

Co-funded by the Erasmus+ Programme of the European Union

- Helpfulness
- Other……

**40. What actions are important to take in order to avoid phishing attacks?**

| | Not important | Slightly important | Moderately important | Important | Very important |
|---|---|---|---|---|---|
| Using up-to-date browser | | | | | |
| Using up-to-date operational system | | | | | |
| Keeping up with the newest software & tools available | | | | | |
| Using security software | | | | | |
| Keeping sensitive information about yourself out of social media | | | | | |
| Using multi-factor authentication/changing passwords frequently | | | | | |
| Using web filter to block malicious websites | | | | | |
| Having regular cybersecurity trainings/workshops | | | | | |
| Develop a security policy | | | | | |
| Encrypting all sensitive company information | | | | | |
| Being cautions when opening the emails/messages/answering the phone | | | | | |
| Double-checking all-important details (senders' email, links, attachments, etc.) | | | | | |
| Trusting your instincts and using good judgement | | | | | |
| Continuously educating yourself on the topic | | | | | |

**41. To what extent do you agree with the statements. I feel confident in:**

| | Not confident at all | Slightly confident | Somewhat confident | Fairly confident | Completely confident |
|---|---|---|---|---|---|
| Knowing cybersecurity/phishing terminology and using it | | | | | |
| Finding the relevant & trustworthy information online | | | | | |

Co-funded by the Erasmus+ Programme of the European Union

| | | | | | |
|---|---|---|---|---|---|
| Taking right actions/measures to prevent phishing attacks | | | | | |
| Identifying phishing attacks | | | | | |
| Keeping my software/programmes up to date | | | | | |
| Using multi-factor authentication | | | | | |
| Using the security software | | | | | |
| Using web filter to block malicious websites | | | | | |
| Encrypting all sensitive company information | | | | | |

**42. Other comments/ suggestions**

Co-funded by the Erasmus+ Programme of the European Union

Euroopa Komisjoni toetus selle dokumendi koostamiseks ei tähenda sisu kinnitamist. Dokument kajastab ainult autorite seisukohti ning Euroopa Komisjon ei vastuta dokumendis sisalduva teabe võimalike kasutamise tagajärgede ega väidete eest. (Projekt number.: 2020-1-LT01-KA203-078070)