Funded by the
Erasmus+ Programme
of the European Union

Küberrünnakud: andmepüük ja sotsiaalsed ründed

Juhtumiuuringud

Safeguarding against Phishing in the age of 4th Industrial Revolution
www.cyberphish.eu
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CyberPhish
Safeguarding your digital future

Õppe-eesmärgid

Tutvustada erinevaid andmepüügirünnakute tüüpe ja õppida neid ära tundma

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Õpilase töökoormus

Loengud	1,5 h
Audio- ja videomaterjal	0,5 h
Juhtumiuuringud	4,5 h
Lisalugemine	0,5 h
Eksamiks valmistumine	2 h

Sisukord:

Funded by the
Erasmus+ Programme
of the European Union

Sisukord:

- **Valletta pank**
- Küprose postkontor
- Smart-ID
- Isikuandmete lekked
- Emoteti pahavara
- Andmepüügirünnaku simulatsioon

Tutvustab, kuidas turvariskid võivad kahjustada infrastruktuuri ja mõjutada inimeste elu

Funded by the Erasmus+ Programme of the European Union

Valletta pank

Juhtumi kirjeldus

Valletta panka oli häkitud ja häkkerid deponeerisid välismaistele kontodele 13 miljonit eurot. Põhjusele keskendumiseks sulges pank sularahaautomaatide, sõnumisüsteemide, mobiilipangateenuste ja kontorite töö. Seetõttu jäid paljud inimesed mõneks tunniks või isegi mõneks päevaks ilma rahata. Inimestel tekkisid probleemid sest ei saanud igapäevaseid kaupu osta ega teenuseid tarbida.

Valletta pank

Juhtumi kirjeldus

- Raha kanti välismaistele kontodele
- Pank oli petturlikele tehingutele jälile saanud ja üritas neid tühistada
- Rünnak sai alguse välismaalt
- Pank tegi rünnaku tühistamiseks tihedat koostööd rahvusvahelise politseiga
- HSBC teatas, et nende teenused toimisid tõrgeteta
- Maksed neljale riigile blokeeriti
- Häkkerid üritasid saata raha Ühendkuningriiki, USA-sse, Tšehhi ja Hongkongi, pank hoiatas peaministrit ja alustas tegingute tagasipööramist
- MFSA hoiab silma peal
- Poeomanikud olid teenuste puudumise tõttu teadmatuses

https://timesofmalta.com/articles/view/bank-of-valletta-goes-dark-after-detecting-cyber-attack.701896

Funded by the Erasmus+ Programme of the European Union

Küsimused aruteluks

- Mida võiks sellest rünnakust õppida?

  Seoses:

  - *kaitstud vara*
  - *turvarisk*
  - *riski mõju*
- Kuidas oleksite käitunud?
  - *Panga kliendina*
  - *Pangaametnikuna/juhina*
  - *Süsteemiadministraatoritena*

Küsimused aruteluks

- Mis oleks võinud ära hoida järgmisi olukordi?
  - *Turvariski tekkimist*
  - *Kriis pärast julgeolekusündmust*
- Kui sa oleksid panga juht:
  - *Kuidas oleksite olukorda rahustanud?*
  - *Kuidas saaksite tagasi kaotatud raha ja panga maine?*

Funded by the Erasmus+ Programme of the European Union

Sisukord:

- Valletta pank
- **Küprose postkontor**
- Smart-ID
- Isikuandmete lekked
- Emoteti pahavara
- Andmepüügirünnaku simulatsioon

Tutvustab veenmise põhimõtteid ja võimalikke tegevusi andmepüügirünnakute mõju vähendamiseks

Funded by the Erasmus+ Programme of the European Union

Küprose postkontor

Juhtumi kirjeldus

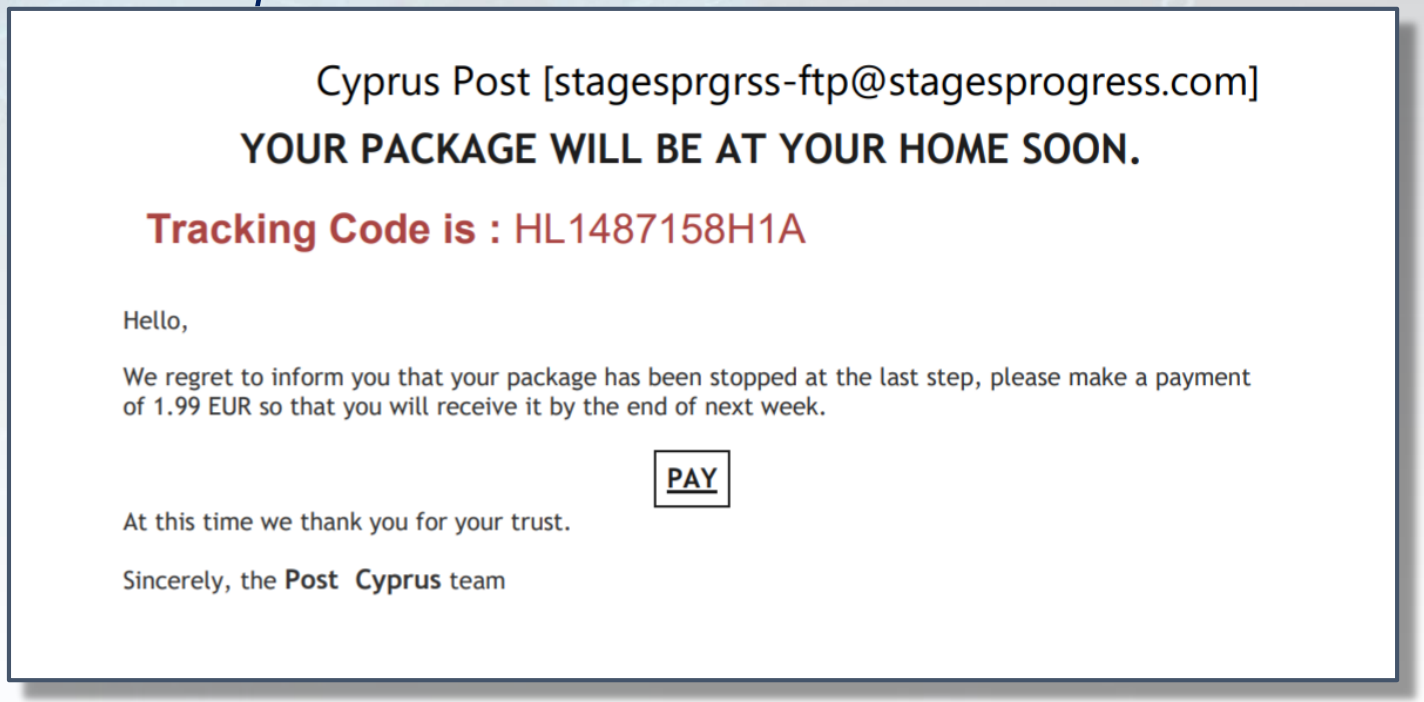
- Küprose postkontor on strateegiline organisatsioon, mis tegutseb Küprose valitsuse alluvuses. Enamik Küprose inimesi kasutab postiteenuseid, eriti pakkide kättetoimetamist (veebiostlemine) – teenus, mis on pärast COVID-19 pandeemia algust tohutult kasvanud.
- See pole esimene kord, kui petturid on sihikule seadnud/kasutanud Küprose postkontori oma kelmuse ohvriks. Enne seda, 2018. aastal, on petturid saatnud tekstisõnumeid erinevatest allikatest, sealhulgas Facebooki sõnumitest, inimestele, väites, et Cyprus Post on valinud paki tellijale võimaluse võita kõrgtehnoloogiline telefon. Sõnumid, mille eesmärk on kasutajaid mitmel viisil eksitada, sealhulgas isikuandmete vargus, juurdepääs isiklikele elektroonilistele kontodele ja võrguteenustele ning teave Interneti-pangaandmete kohta.

Küprose postkontor

Juhtumi kirjeldus

Sõnumipettus 2018. aastal:

Sõnumipettus 2021. aastal:



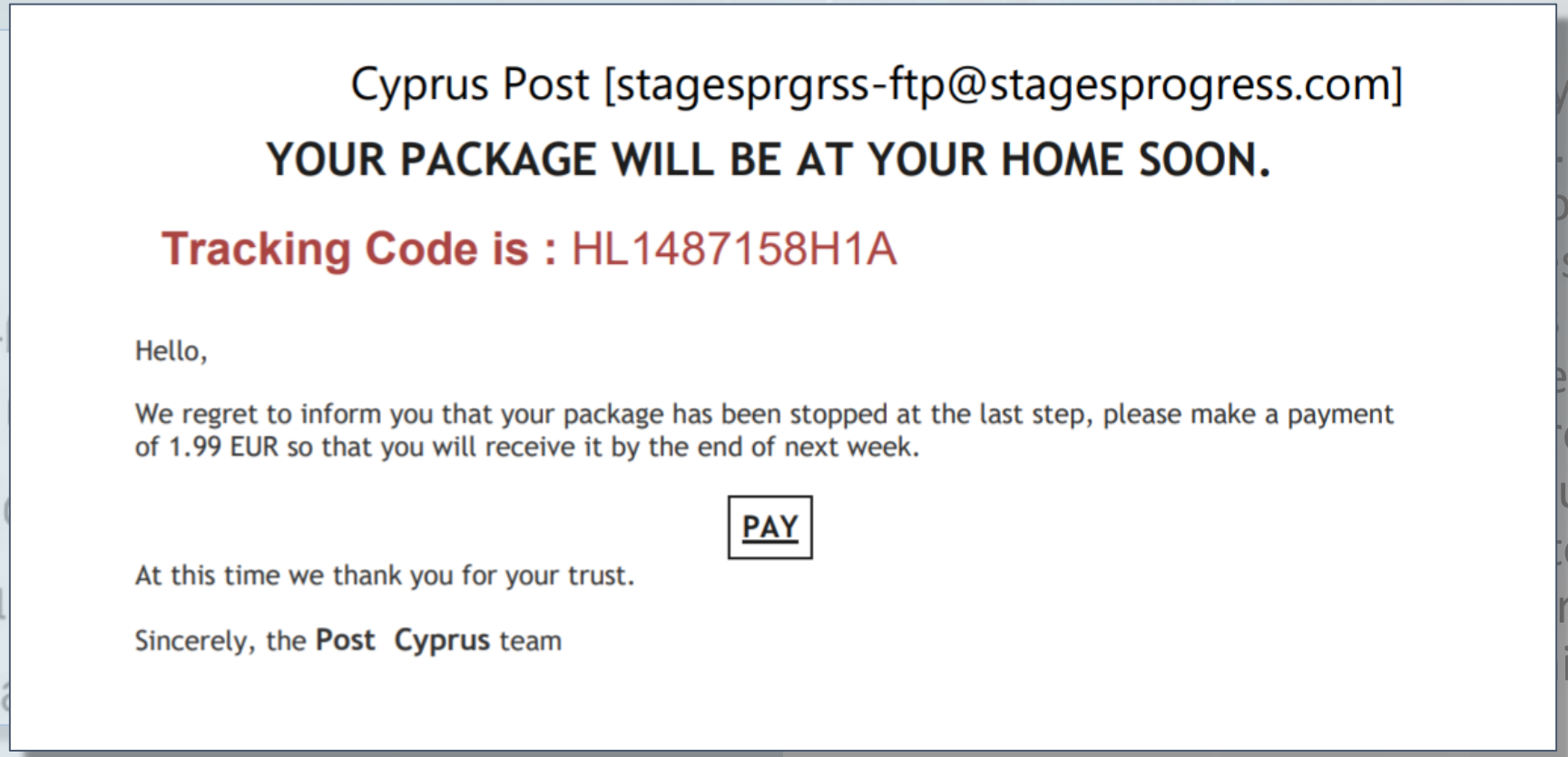
Küprose post hoiatas avalikkust, et klientidele saadetakse e-posti teel võltsitud sõnumeid, milles nõutakse tollimaksu tasumist.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Küprose postkontor

Juhtumi kirjeldus



Cyprus Post [stagesprgrss-ftp@stagesprogress.com]

YOUR PACKAGE WILL BE AT YOUR HOME SOON.

Tracking Code is : HL1487158H1A

Hello,

We regret to inform you that your package has been stopped at the last step, please make a payment of 1.99 EUR so that you will receive it by the end of next week.

PAY

At this time we thank you for your trust.

Sincerely, the **Post Cyprus** team

Küsimused aruteluks

- Milliseid veenmispõhimõtteid võiks Küprose postkontori juhtumis tuvastada?
- Miks tuleks Küprose postkontori juhtumit pidada andmepüügirünnakuks?
- Miks teesklevad petturid, et nad on pärit "tuntud" riigiasutustest ja/või organisatsioonidest?
- Kuidas peaksid "tuntud" riigiasutused ja/või organisatsioonid ise petuskeemidele reageerima?

Funded by the Erasmus+ Programme of the European Union

Sisukord:

- Valletta pank
- Küprose postkontor
- **Smart-ID**
- Isikuandmete lekked
- Emoteti pahavara
- Andmepüügirünnaku simulatsioon

Arutage, kuidas ohuagendid kasutavad kaitstud varade kahjustamiseks kaasaegseid autentimistehnikaid.

Funded by the Erasmus+ Programme of the European Union

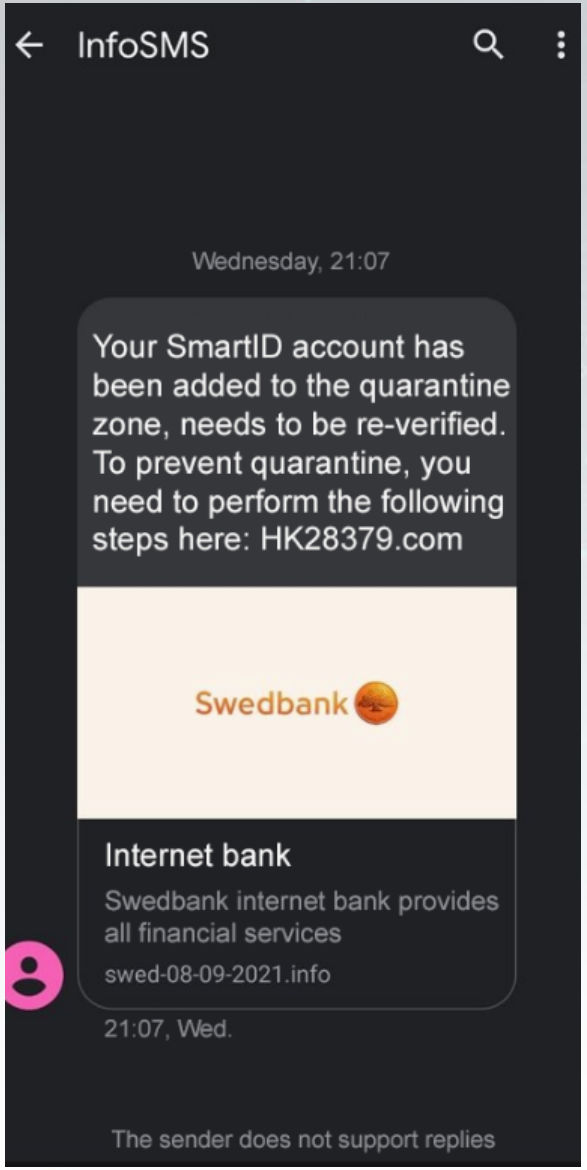
Juhtumi kirjeldus

Smart-ID on lihtsaim, turvalisem ja kiireim viis end veebis autentida, e-teenustes registreeruda ja dokumente allkirjastada. Smart-ID võimaldab inimesel oma eelistatud nutiseadmega turvaliselt ja mugavalt siseneda interneti- või mobiilipanka ja teistesse e-teenustesse. Smart-ID ei ole seotud SIM-kaartide ega mobiilioperaatoritega; on vaja ainult juurdepääsu Internetile.

https://www.smart-id.com

Funded by the Erasmus+ Programme of the European Union

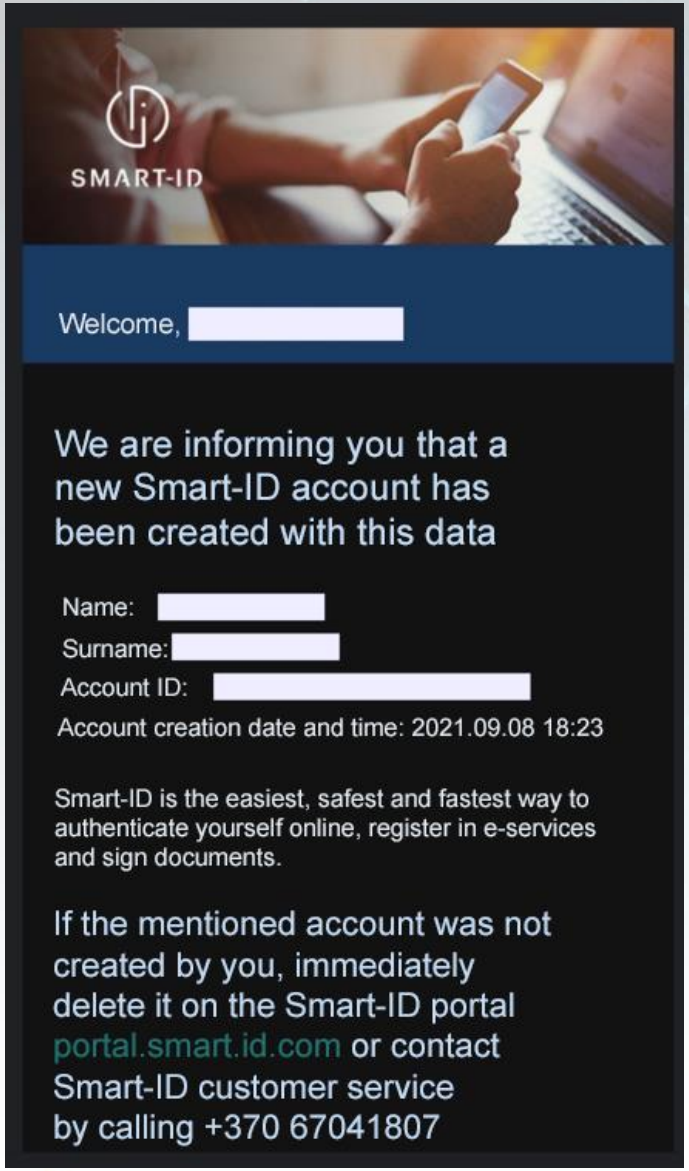
Juhtumi kirjeldus



2021. aasta septembris saatsid petturid Leedu kodanikele erineva sisuga SMS-sõnumeid, mille eesmärk on vaid üks asi: juhtida kodanike tähelepanu nende raha, isikliku Smart-ID või internetipangakonto väidetavale turvalisusele. Sõnumites palutakse klõpsata aktiivsel Interneti-lingil ja anda riski neutraliseerimiseks isiklikud sisselogimisandmed.

Funded by the Erasmus+ Programme of the European Union

Juhtumi kirjeldus



Kui ohver lingil klõpsab, avaneb võltsveebisait, kus kasutaja peab esitama isikuandmed või „aktiveerima“ konto.

Küsimused aruteluks

- Kuidas saaks turvalisi autentimisvahendeid, nagu Smart-ID, kasutada kodanike raha röövimiseks?
- Milliseid toiminguid tuleks teha pärast sellise SMS-i saamist?
- Mis on andmepüügi SMS-i tähistavad ohu märgid?
- Milliseid toiminguid peaksite tegema, kui teid häkitakse?
- Kas kaotatud raha on võimalik tagasi saada?
- Mida võiks sellest olukorrast õppida?

Funded by the Erasmus+ Programme of the European Union

Sisukord:

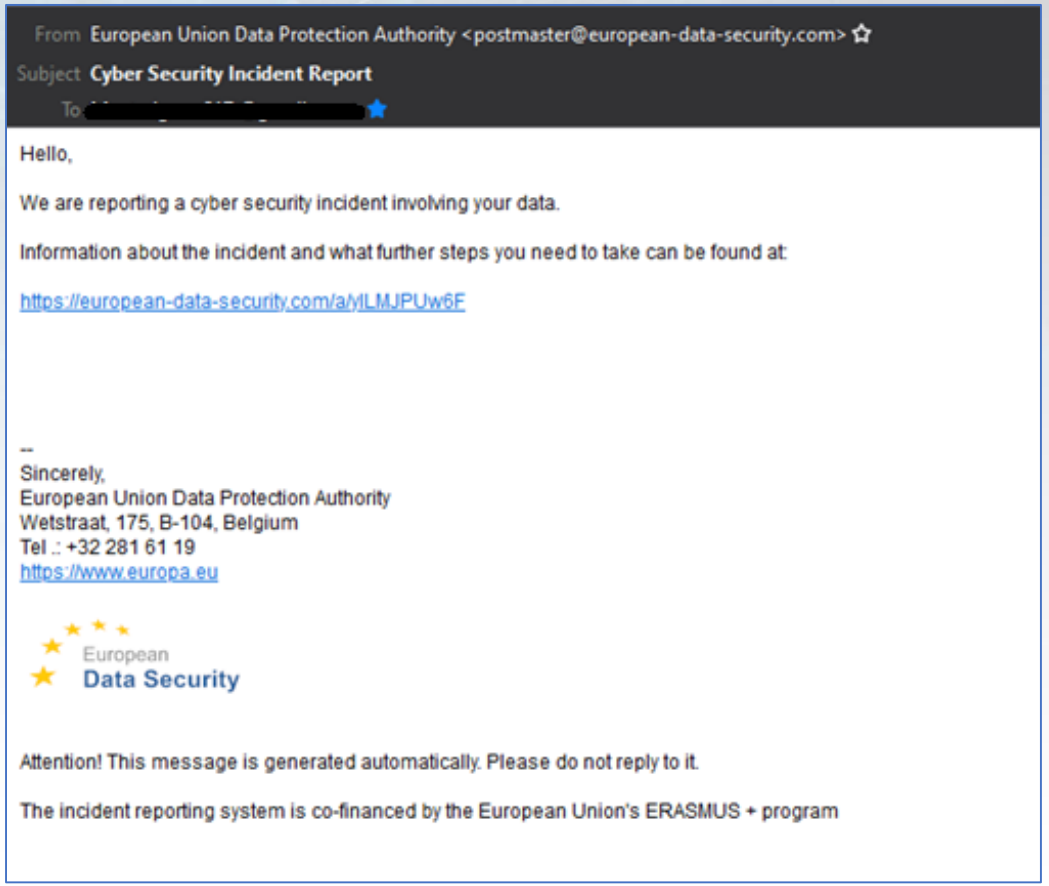
- Valletta pank
- Küprose postkontor
- Smart-ID
- **Isikuandmete lekked**
- Emoteti pahavara
- Andmepüügirünnaku simulatsioon

Arutage, kuidas ära tunda võltsitud e-kirju, mis pakuvad erinevaid teenuseid ebausaldusväärsetelt organisatsioonidelt

Funded by the Erasmus+ Programme of the European Union

Juhtumi kirjeldus

Kolme nädala jooksul 2021. aasta kevadel avalikustati Leedus vähemalt neli suurt isikuandmete vargust. Need sündmused tekitasid massilise meedia tähelepanu ja palju arutelusid. Petturid on olukorda ära kasutanud ja saatnud võltsitud kirju. Nendes kirjades julgustati adressaate liituma olemasoleva organisatsiooni veebilehega ja kontrollima, kas nende isikuandmeid avalikustati.



From: European Union Data Protection Authority <postmaster@european-data-security.com>
Subject: Cyber Security Incident Report
To: [redacted]

Hello,

We are reporting a cyber security incident involving your data.

Information about the incident and what further steps you need to take can be found at:

https://european-data-security.com/a/yILMJPUw6F

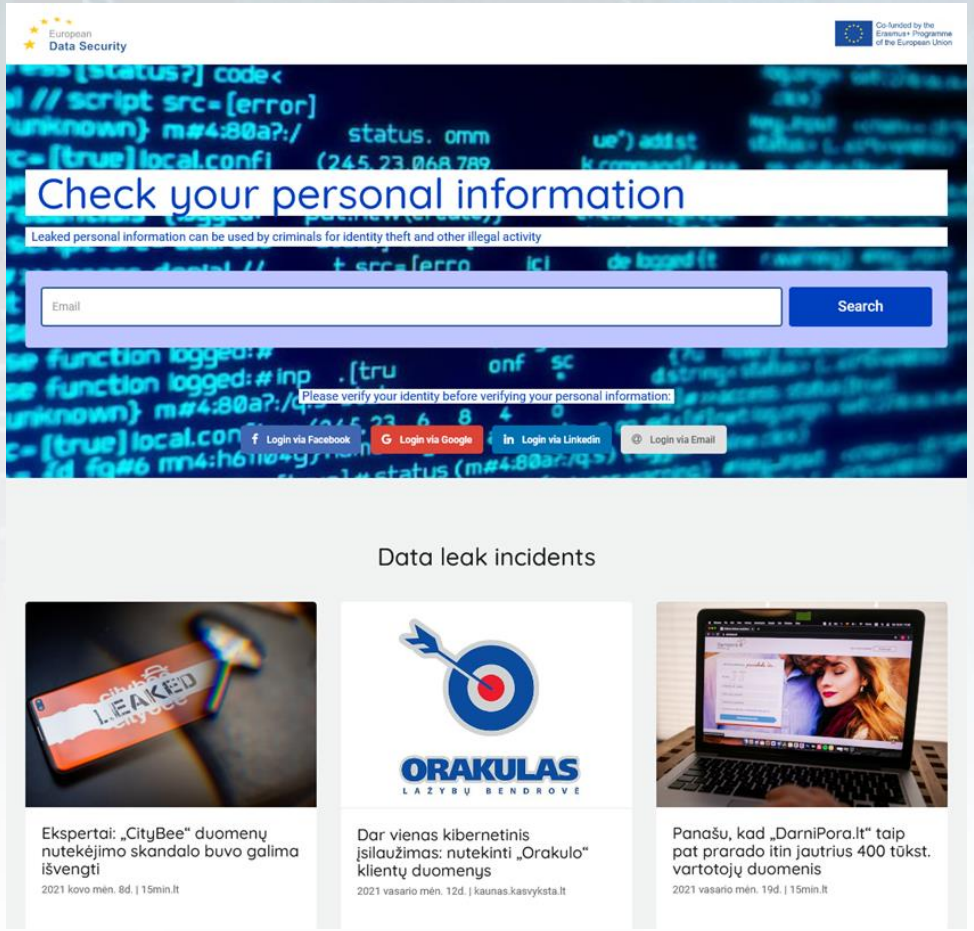
--
Sincerely,
European Union Data Protection Authority
Wetstraat, 175, B-104, Belgium
Tel .: +32 281 61 19
https://www.europa.eu

European
Data Security

Attention! This message is generated automatically. Please do not reply to it.

The incident reporting system is co-financed by the European Union's ERASMUS + program

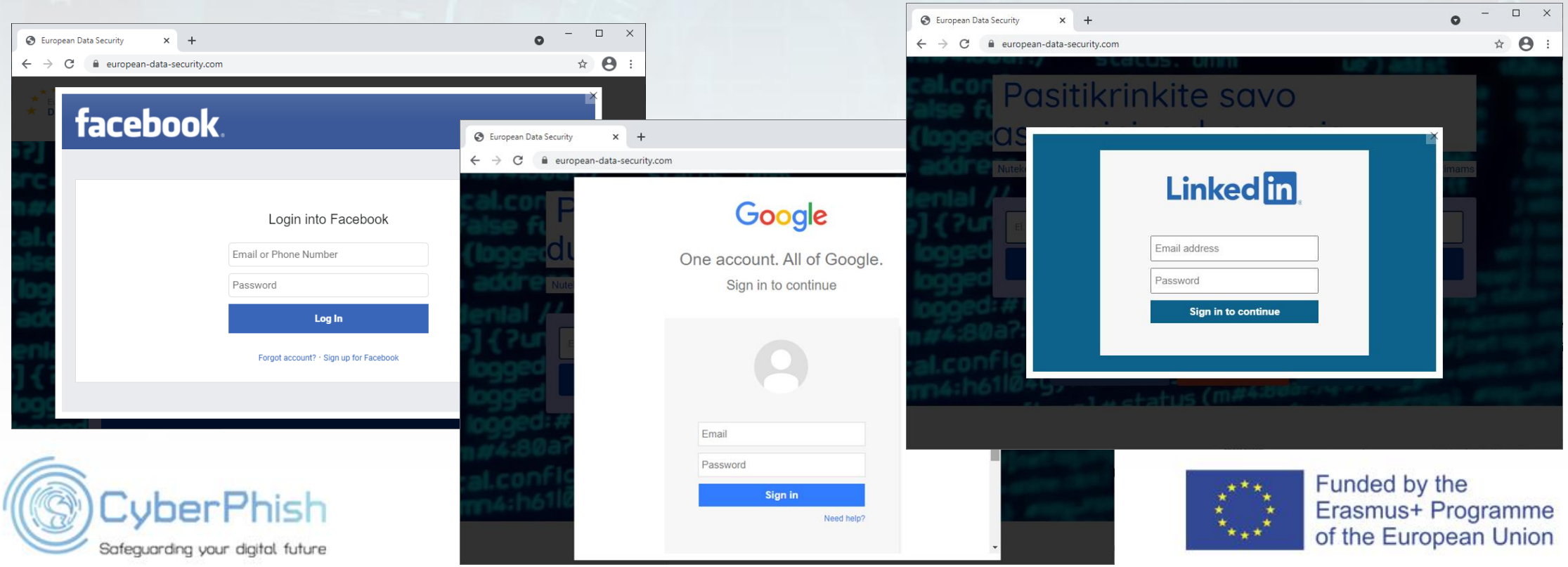
Juhtumi kirjeldus



Kui rünnaku ohver linki vajutas, suunati ta olematu organisatsiooni veebilehele. Sellel lehel paluti ohvril ühte sotsiaalvõrgustikku sisse logida.

Juhtumi kirjeldus

Kui ohver valis ühe kontodest, avanesid võltsitud liitumisaknad. Nendesse akendesse sisestatud teave (nt sisselogimisandmed – sisselogimisnimi ja parool) varastati.



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Küsimused aruteluks

- Mida teha, kui teie konto sisselogimisandmed on ohus?
- Mida teha sellise meili saamisel?
- Millised on ohu märgid andmepüügimeilide ja sisselogimisvormide kohta?
- Milliseid õppetunde te sellest juhtumist õppisite?

Funded by the Erasmus+ Programme of the European Union

Sisukord:

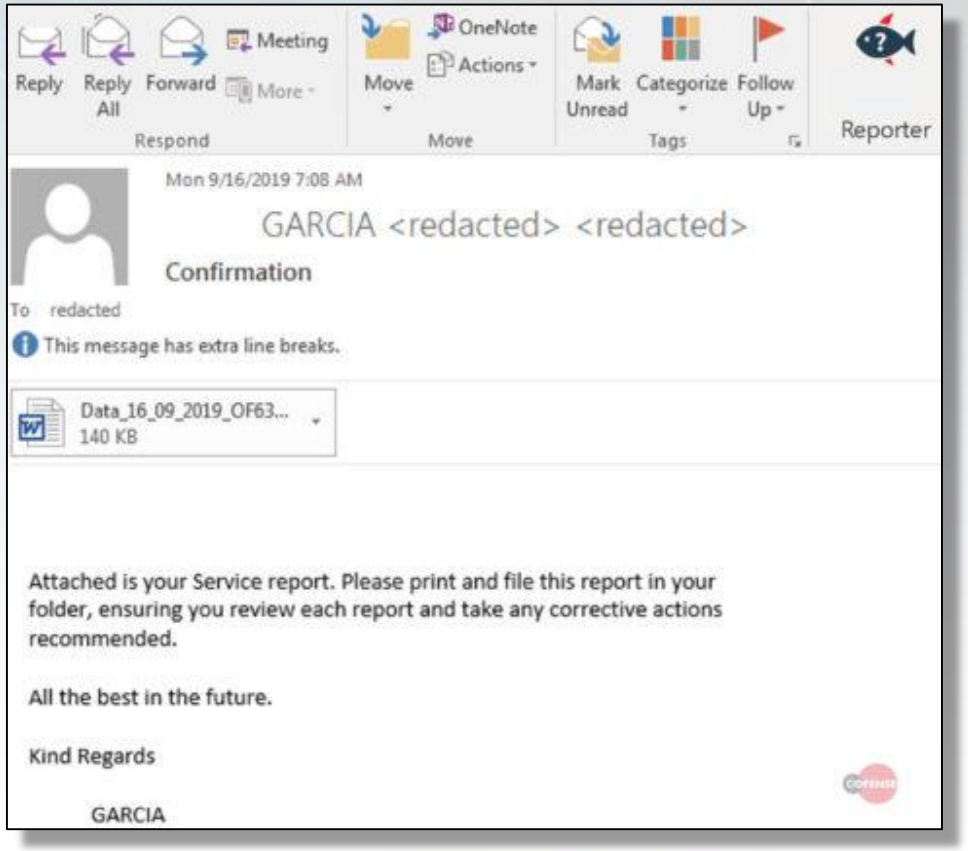
- Valletta pank
- Küprose postkontor
- Smart-ID
- Isikuandmete lekked
- **Emoteti pahavara**
- Andmepüügirünnaku simulatsioon

Arutage usaldusväärsetelt saatjatelt saadud potentsiaalselt pahatahtlike meilide mõju

Funded by the Erasmus+ Programme of the European Union

Juhtumi kirjeldus

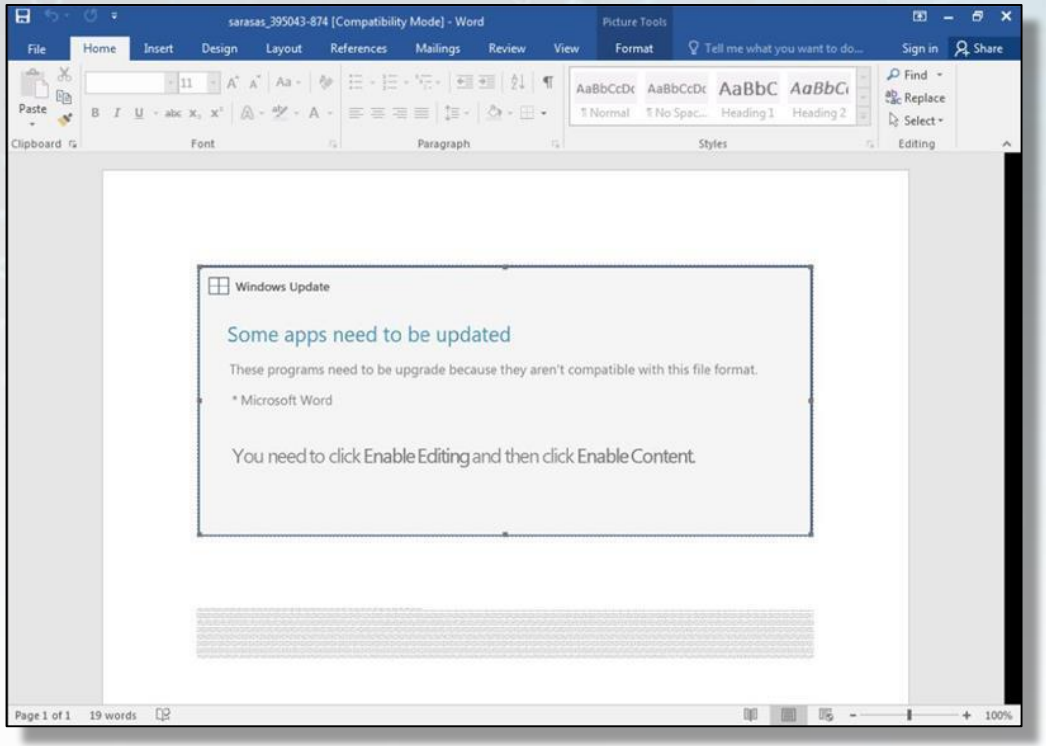
- Pahatahtlik rämpspost (malspam), mis edastab **Emoteti** pahavara, on kõige levinum meilipõhine oht. See kasutab "lõime kaaperdamise" tehnikat, mis kasutab nakatunud arvutite meiliklientidelt varastatud seaduslikke sõnumeid. See rämpspost võltsib õiget kasutajat ja kehastub vastuseks varastatud meilile. Lõime kaaperdatud rämpspost saadetakse algses kirjas olevatele aadressidele.



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Juhtumi kirjeldus



See tehnika on tõhusam kui vähem keerukad meetodid, mida paljud inimesed on nüüdseks õppinud märkama. See lähenemisviis on edukam veenma potentsiaalseid ohvreid klõpsama lisatud failil või klõpsama lingil, et laadida alla pahatahtlik Wordi dokument koos makrodega, mis on loodud kasutaja Emotetiga nakatamiseks.

Funded by the Erasmus+ Programme of the European Union

Küsimused aruteluks

- Kuidas saaks inimene veel kord kontrollida, kas e-kiri pärineb seaduslikust allikast, isegi kui see näib olevat vastus vestlusele?
- Kas inimene peaks selliseid faile oma igapäevatöös vastu võtma?
- Kas antiviirust on vaja ka siis, kui ta (arvab, et ta) ei surfa kunagi võõrastel veebisaitidel või kasutab seadet ainult tööga seotud tegevusteks?
- Kas inimene peaks manuse avama, kui e-kiri tundub oluline ja töötegevusega seotud, kuid manused tunduvad kahtlased?

Funded by the Erasmus+ Programme of the European Union

Sisukord:

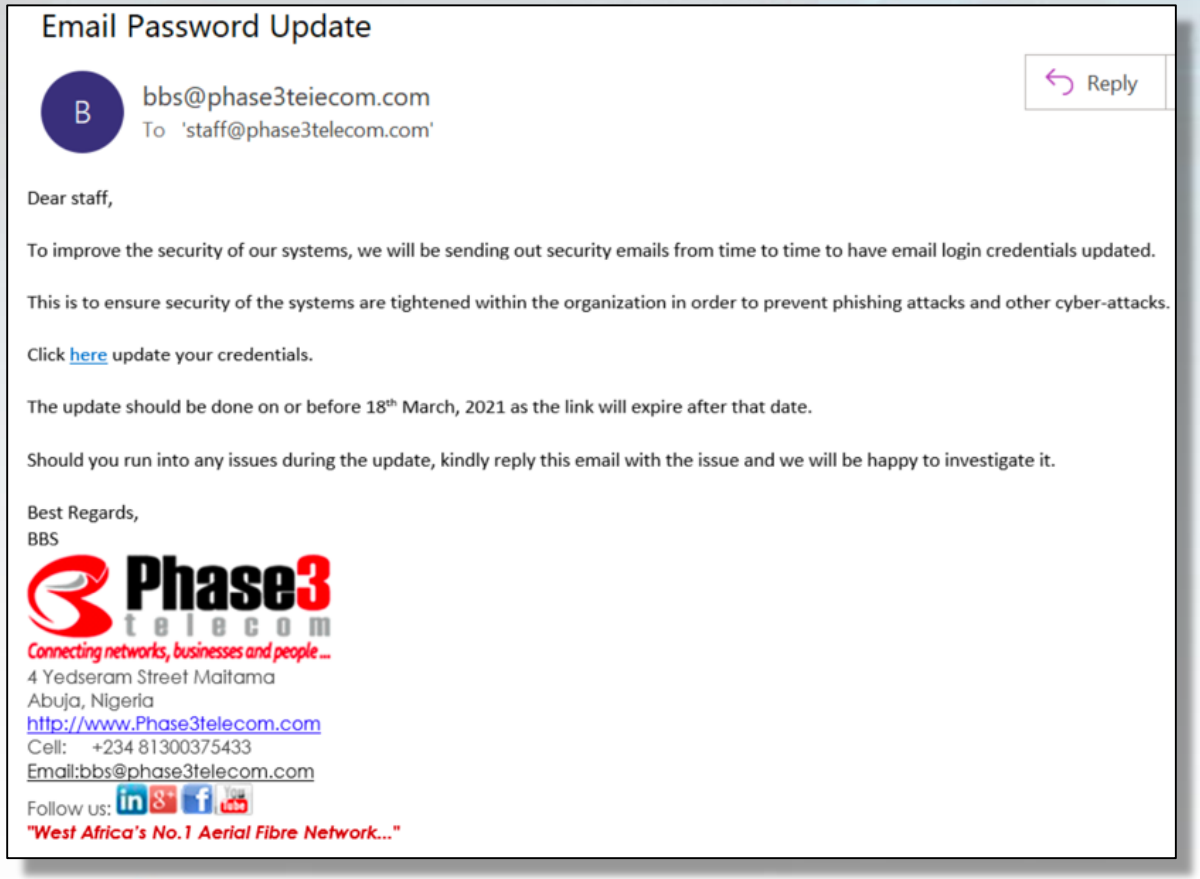
- Valletta pank
- Küprose postkontor
- Smart-ID
- Isikuandmete lekked
- Emoteti pahavara
- **Andmepüügirünnaku simulatsioon**

Arutage andmepüügirünnakute mõju organisatsioonile

Funded by the Erasmus+ Programme of the European Union

Andmepüügirünnaku simulatsioon

Juhtumi kirjeldus



Email Password Update

B bbs@phase3teiecom.com
To 'staff@phase3telecom.com'

Reply

Dear staff,

To improve the security of our systems, we will be sending out security emails from time to time to have email login credentials updated.

This is to ensure security of the systems are tightened within the organization in order to prevent phishing attacks and other cyber-attacks.

Click here update your credentials.

The update should be done on or before 18th March, 2021 as the link will expire after that date.

Should you run into any issues during the update, kindly reply this email with the issue and we will be happy to investigate it.

Best Regards,
BBS

Phase3 telecom
Connecting networks, businesses and people...
4 Yedseram Street Maitama
Abuja, Nigeria
http://www.Phase3telecom.com
Cell: +234 81300375433
Email:bbs@phase3telecom.com
Follow us:
"West Africa's No.1 Aerial Fibre Network..."

Üks telekommunikatsioonieettevõte otsustas käivitada kontrollitud simulatsiooni, et uurida, kuidas nende töötajad on andmepüügirünnakutest teadlikud. Simulatsioon viidi läbi varajastel kellaaegadel. Andmepüügimeil saadeti 17. märtsil 2021 kell 8.26. Kellaaja valiku eesmärk oli töötajaid üllatada, kuna see on üks esimesi selle päeva e-kirju. Andmepüügi e-posti sisu nõudis turvavärskendust, mis sisaldas linki, mis oli väidetavalt volituste värskendamiseks (lingil klõpsamisel suunas see kasutaja ostetud domeeninimele kasutades loodud sarnase väljanägemisega võltsitud veebisaidile)

Olorunshe T. E., Recognition of Phishing Attacks and its Impact: A Case Study, Master thesis, University of Tartu, 2021
URL: https://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=72801&year=2021

Funded by the Erasmus+ Programme of the European Union

Juhtumi kirjeldus

Simulatsiooni tulemused

- Simulatsioon oli suunatud ligikaudu **250** töötajale.
- Kokku jälgiti **179** lingiklikki ettevõtte võrgust ja **40** klikki väljastpoolt ettevõtte võrku.
- Andmepüügirünnakust teatas **3 inimest**. Ülejäänud **4** helistasid, et saada kinnitust, kas meil oli õige. **2** töötajat helistasid, et kaevata mittetöötava lingi üle.

Päev	Ettevõtte võrgust tehtud klikkide arv	Välisvõrgust tehtud klikkide arv
1	161	>30
2	18	>10
kokku	179	>40

Olorunshe T. E., Recognition of Phishing Attacks and its Impact: A Case Study, Master thesis, University of Tartu, 2021
URL: https://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=72801&year=2021

Funded by the Erasmus+ Programme of the European Union

Juhtumi kirjeldus

Ohvrite analüüs

- **Finantsmeeskonna liige**
  - *Saabus mõni minut pärast andmepüügimeili saatmist*
  - *Vastaja palus linki parandada*
  - *Juurdepääs kliendiandmetele, makseprotsessidele/andmetele, raamatupidamisandmetele*
- **Üksuse juht**
  - *Juurdepääs erinevat tüüpi andmetele*
  - *Võimalik kahju organisatsiooni mainele*
- **Mitteinsenerimeeskonna liige**
  - *Juurdepääs kolleegide andmetele samas üksuses*
  - *Avab värava tulevaste rünnakute jaoks*
- **Inseneriüksuse liige erinevast piirkonnast**
  - *Juurdepääs andmetele piirkonnaüksuses*
  - *Võimalik kahju teenustele piirkonnas*
- **Inseneriüksuse liige**
  - *Juurdepääs organisatsiooni sisevõrgule*

CyberPhish
Safeguarding your digital future

Olorunshe T. E., Recognition of Phishing Attacks and its Impact: A Case Study, Master thesis, University of Tartu, 2021
URL: https://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=72801&year=2021

Funded by the Erasmus+ Programme of the European Union

Küsimused aruteluks

- Määratlege andmepüügirünnak
  - *Mis on andmepüüdja profiil?*
  - *Mis on andmepüügi rünnaku meetod?*
  - *Mis on haavatavus?*
  - *Mis on mõju?*
- Millised on ohu märgid, mis näitavad, et meil on andmepüügirünnak?
- Milline on selle andmepüügirünnaku mõju vaadeldavale ettevõttele?
- Kuidas vaadeldavas ettevõttes andmepüügi teadlikkust tõsta?

Funded by the Erasmus+ Programme of the European Union

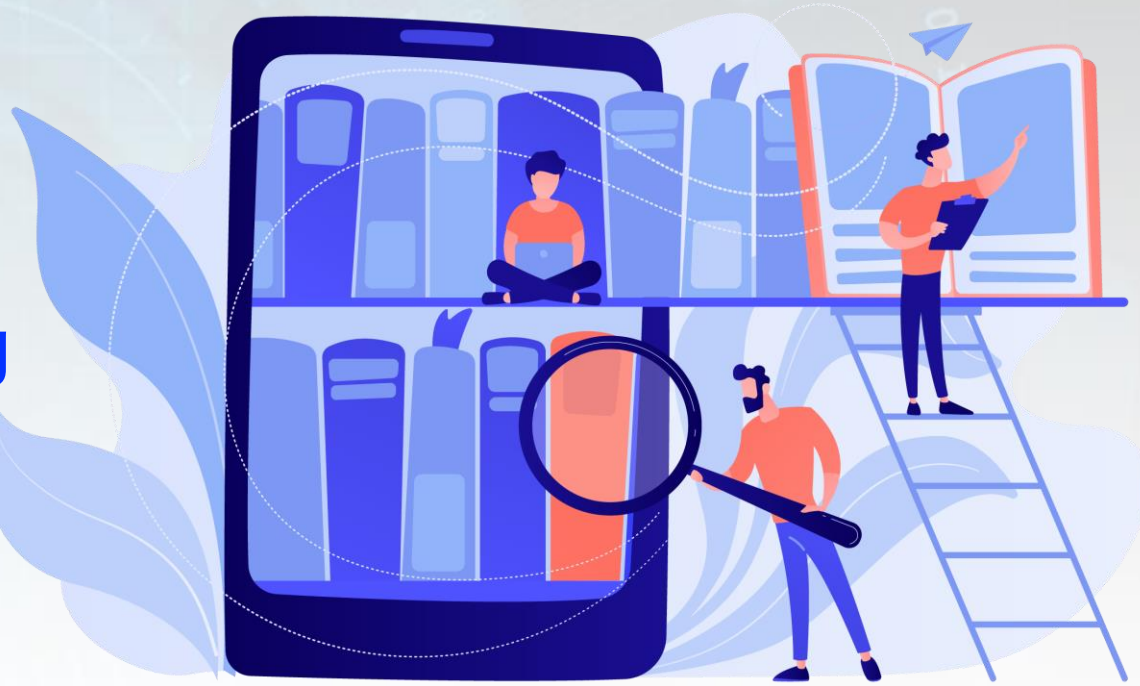
Kokkuvõte

- Kuidas turvariskid kahjustavad infrastruktuuri ja mõjutavad inimeste elu.
- Andmepüügirünnaku mõju vähendamiseks veenmise ja tegevuse põhimõtted.
- Kuidas ohuagendid kasutavad kaitstud varade kahjustamiseks kaasaegseid autentimistehnikaid.
- Kuidas ära tunda võltsitud e-kirju, mis pakuvad erinevaid teenuseid ebausaldusväärsetelt organisatsioonidelt.
- Usaldusväärsetelt saatjatelt saadud pahatahtlike meilide mõju.
- Andmepüügirünnakute mõju organisatsioonile.

Funded by the Erasmus+ Programme of the European Union

Lisalugemine

- **Kevin D. Mitnick and William L. Simon** (*2002*):
  The Art of Deception, Controlling the Human Element of Security, *Willey Publishing, Inc.*



Lühivideod

- Bank Security Breach
  https://youtu.be/kkc3nkCXUk0
- Cyber Attack on Banks and Post Office
  https://youtu.be/yB3N9U6V3c4
- Smart-ID Registration with ID-card
  https://youtu.be/m9t4PY0DROM
- Emotet - the Evolution of Malware
  https://youtu.be/CkwKTBifXJg
- Phishing Attack Simulator
  https://youtu.be/hh25C0cdop0

Tänan kuulamast!