Funded by the
Erasmus+ Programme
of the European Union

Küberrünnakud: andmepüük ja sotsiaalsed ründed

Suhtlusrünnaku tüübid ja manipuleerimine

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

Selgitage erinevaid andmepüügirünnakute tüüpe ja õppida neid ära tundma

Andmepüügirünnakud:

- - GDPR seotud rünnakud; E-kirjad; Sõnumirakendused; Sotsiaalvõrgustik; Veebilehed; Loterii pettused; SMS; Telefoni kõned; Näost näkku suhtlus; Üle-õla ründed;

Tehnikate kombinatsioon:

- *Spray and Pray, Spear Phishing, Whaling, Vishing, Smishing, Angler Phishing, Clone Phishing, Malvertising*.

Õppija töökoormus

Loengud	4 h
Audio- ja videomaterjal	2 h
Juhtumiuuringud	2 h
Lisalugemine	2 h
Eksamiks valmistumine	2 h

Funded by the Erasmus+ Programme of the European Union

Scams via Emails

Fake Wins

Shoulder Surfing

Fake Surveys

Scams via SMS

Baiting

Fake Websites

Scams in Social Media

Vishing

Tailgating

Scams via Instant messaging

CyberPhish


Telefonikõned
SMS
E-mailid
Tulevad organisatsiooni sisse
CyberPhish

Eduka andmepüügirünnaku tulemused

- Tundlike andmete kadu
- Kontode (kasutajanimede ja paroolide) kaotamine
- Identiteedivargus
- Kliendi teabe vargus
- Raha kadu ettevõtte- ja kliendikontodelt
- Juurdepääs infrastruktuurile tulevaste rünnakute käivitamiseks
- Volitamata tehingud
- Intellektuaalomandi kaotus
- Kuritegelikele kolmandatele isikutele edastatud või müüdud andmed
- Igapäevategevuste häirimine
- Juhtumile reageerimine
- Likvideerimine ja taastumine
- Kaotatud töötunnid taastumiseks
- Maine kahjustamine
- Sissetuleku kaotus
- Trahvid, õiguskulud
- …

Funded by the Erasmus+ Programme of the European Union

Teemad:

Sündmuspõhine rünnak	E-mail	Tekstisõnum	Veebisait
Loterii pettus	Telefonikõne	Näost näkku	Üle-õla vaatamine

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Sündmuspõhised rünnakud

- Suuremahulised sündmused, sõjad, pandeemiad, nagu COVID-19, panevad inimesi käituma impulsiivsemalt kui tavaolukorras

- Enim kasutatavad tehnikad: meilid, andmepüük, SMS, tagaotsimine, telefonikalastus (*vishing)* jne.

Funded by the Erasmus+ Programme of the European Union

GDPR-iga seotud rünnakud

- **Andmekaitse üldmäärus (GDPR)** on määrus, mis alates 2018. aastast kehtib andmekaitse ja privaatsuse kohta Euroopa Liidus. GDPR kontrollib ettevõtteid ja organisatsioone isikuandmete töötlemise osas.
- Isikuandmete automatiseeritud või osaliselt automatiseeritud töötlemist teostavad ettevõtted peavad järgima GDPR-i
- 2018. aastal toimus palju GDPR-i rünnakuid, kuna kõik ettevõtted ja organisatsioonid pidid oma organisatsioonides GDPR-i rakendama

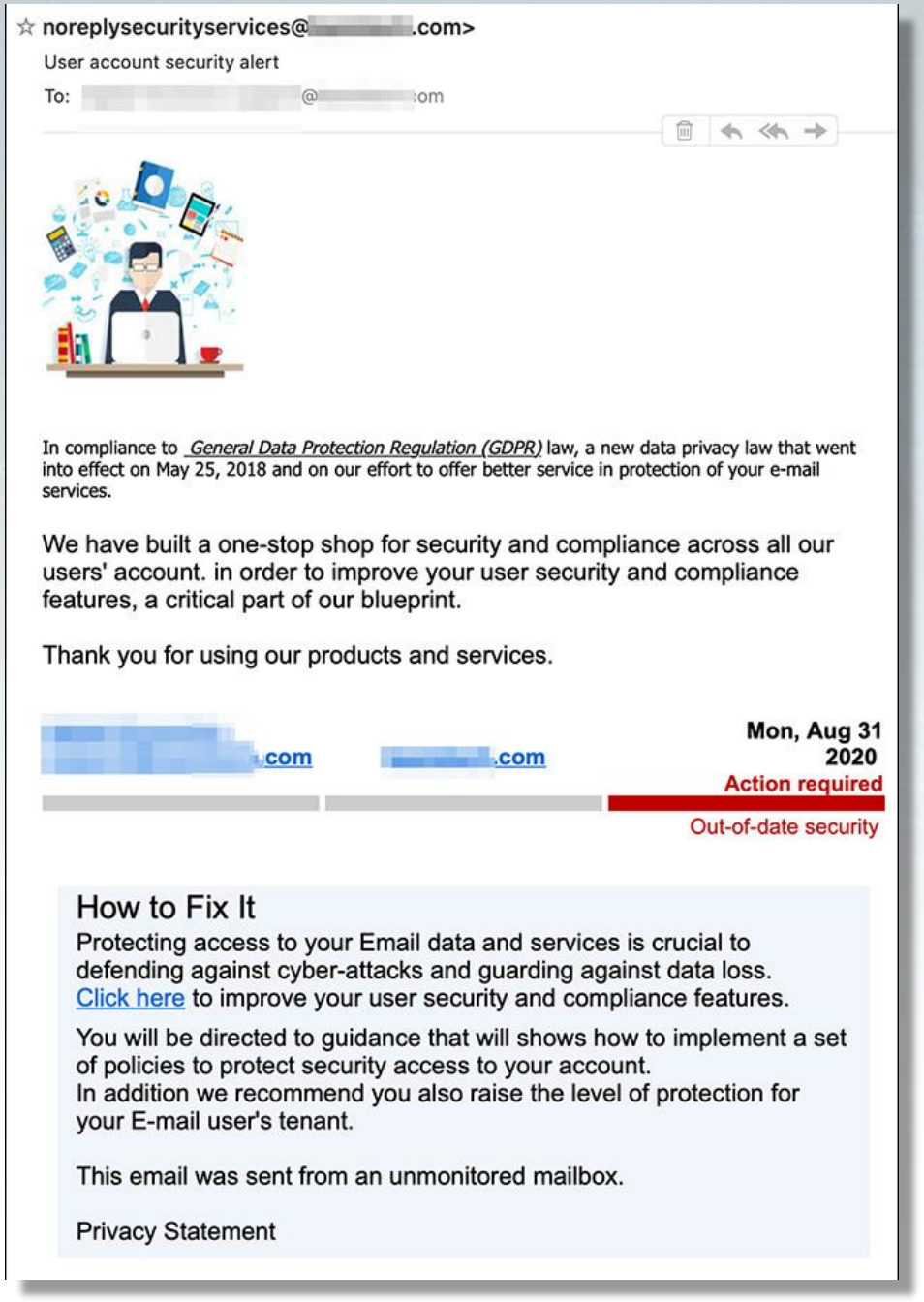
Funded by the Erasmus+ Programme of the European Union

GDPR-iga seotud rünnak organisatsioonidele

- **Miks seda tüüpi kinnitused on edukad?** Ettevõtetel ei olnud piisavalt teadmisi GDPR-ist.
- **Sihtrühm:** organisatsioonide töötajad,
  - Tavaliselt ettevõtte e/meilid, mis on saadaval Internetis või
  - otse ettevõtete juhtidele või kõrgematele juhtidele (kellel on loodetavasti juurdepääs kliendiandmetele või kes vastutavad GDPR-i järgimise eest)
- **Oht:** meilid turvaorganisatsioonidelt, kes pakuvad teenuseid kasutajate turvalisuse ja GDPR-i järgimise parandamiseks
- **Ründemeetod:** meilid (harpuunimine, *spear phishing*).
- **Taktika:** kujundatud ja vormindatud meilid näevad välja seaduslikud. Ründajad jätsid mulje, et meilid pärinevad ametlikest allikatest.
- **Tunnused:**
  - **Hirm seaduserikkumiste ees**
  - **Inspireeriv kiireloomulisuse tunne:** ründajad kasutasid võltsitud GDPR-i järgimise ajakava, mida ründajad regulaarselt värskendasid, et adressaadile avaldatavat survet suurendada.
- **Ohvrid:**
  - Mitte koolitatud isik (kes klõpsab meilis oleval lingil ja annab andmeid)

Funded by the Erasmus+ Programme of the European Union

GDPR-iga seotud rünnak: kasutajate turvalisuse ja GDPR-i järgimise parandamine



☆ noreplysecurityservices@[redacted].com>

User account security alert

To: [redacted]@[redacted]om

In compliance to *General Data Protection Regulation (GDPR)* law, a new data privacy law that went into effect on May 25, 2018 and on our effort to offer better service in protection of your e-mail services.

We have built a one-stop shop for security and compliance across all our users' account. in order to improve your user security and compliance features, a critical part of our blueprint.

Thank you for using our products and services.

[redacted].com [redacted].com

Mon, Aug 31 2020

Action required

Out-of-date security

How to Fix It

Protecting access to your Email data and services is crucial to defending against cyber-attacks and guarding against data loss. Click here to improve your user security and compliance features.

You will be directed to guidance that will shows how to implement a set of policies to protect security access to your account.
In addition we recommend you also raise the level of protection for your E-mail user's tenant.

This email was sent from an unmonitored mailbox.

Privacy Statement

- Andmepüügi veebisait avaneb, kui ohver lingil klõpsab
- Veebisait isikupärastatkse ohvrite e-posti aadressidega
- Ohvril võidakse paluda sisse logida (sisselogimisandmeid esitades) võltsveebisaidile, mis näeb välja nagu päris veebisait.

Tulemus:

- Varastatud ohvrite e-posti sisselogimisandmed, et pääseda ligi e-kirjadele
- Ohvri meilidest võidakse varastada tundlikke andmeid või varastatud kontakte võidakse kasutada edasisteks küberrünnakuteks

Source: https://www.inspiretosecurity.com/2020/08/24/phishers-targeting-employees-fake-gdpr-compliance-reminders/

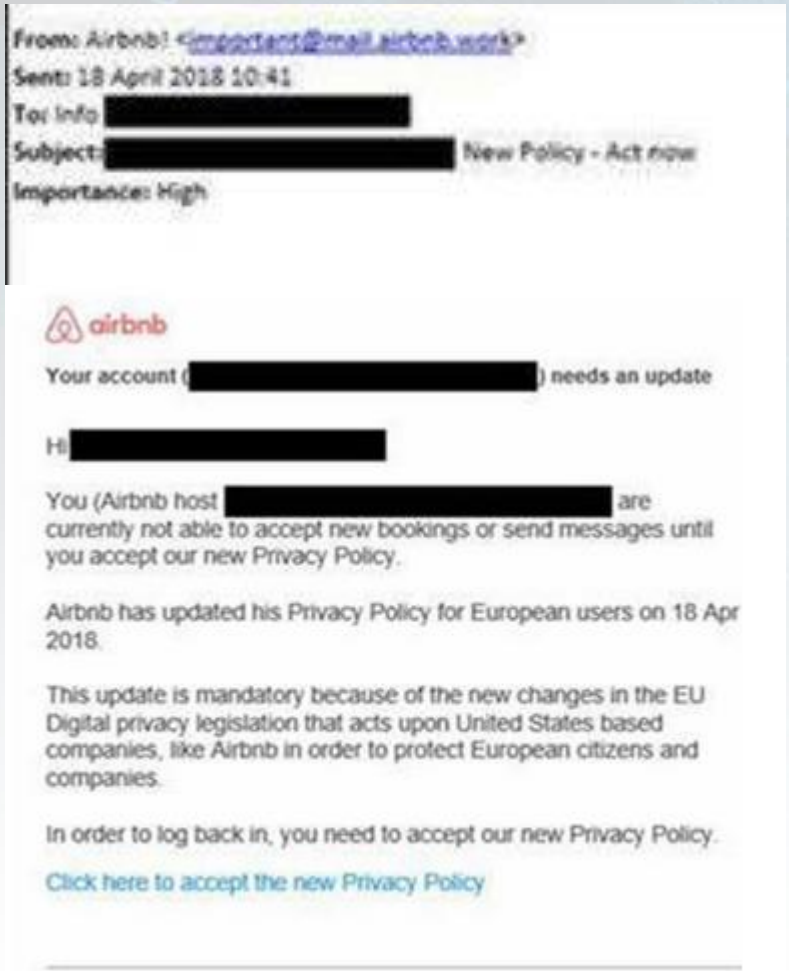
GDPR-iga seotud rünnak klientidele

- **Miks seda tüüpi rünnak on edukas??** Ettevõtted saatsid klientidele e-kirju seoses GDPR-i värskendustega semis kutsusid üles tutvuma /nõustuma “uue” privaatsuspoliitikaga.
- **Sihtrühm:** erinevate organisatsioonide kliendid, tavaliselt IT-teenuste pakkujad, finantsorganisatsioonide kliendid.
- **Oht:** e-kirjad "organisatsioonidelt", milles palutakse kinnitada luba isikuandmete salvestamiseks ja töötlemiseks
- **Ründe meetod:** e-kirjad.

- **Taktika:**
  - kujundatud ja vormindatud meilid näevad välja nagu päris organisatsiooni meilid. Ründajad jätsid mulje, et meilid pärinevad ametlikust allikast.
  - ründajad kasutavad usaldusväärseid kaubamärke
- **Tunnused:**
  - **Pühendumus ja järjekindlus**
  - **Lojaalsus organisatsioonile**
- **Ohvrid:**
  - Kliendid, kellel on andmepüügist piiratud või puuduvad teadmised (kes klõpsab meilis oleval lingil ja edastab andmeid)

Funded by the Erasmus+ Programme of the European Union

GDPR-iga seotud rünnak: nõustuge uute privaatsuseeskirjadega



From: Airbnb! <important@mail.airbnb.work>
Sent: 18 April 2018 10:41
To: Info [redacted]
Subject: [redacted] New Policy - Act now
Importance: High

airbnb

Your account ([redacted]) needs an update

Hi [redacted]

You (Airbnb host [redacted] are currently not able to accept new bookings or send messages until you accept our new Privacy Policy.

Airbnb has updated his Privacy Policy for European users on 18 Apr 2018.

This update is mandatory because of the new changes in the EU Digital privacy legislation that acts upon United States based companies, like Airbnb in order to protect European citizens and companies.

In order to log back in, you need to accept our new Privacy Policy.

Click here to accept the new Privacy Policy

- Andmepüügi veebisait avaneb, kui ohver lingil klõpsab.
- Ohvril võidakse paluda esitada oma isiklikud andmed, sealhulgas kasutaja info ja maksekaardi andmed võltsveebisaidile, mis näeb välja nagu päris veebisait .
- **Tulemus**:
  - Varastatud ohvrite e-posti sisselogimisandmed, et pääseda e-kirjadele. Tundlikke andmeid võidakse varastada ohvri meilidest või varastatud kontakte kasutada edasisteks küberrünnakuteks.
  - Varastatud finantsandmed.
  - Nakatunud seadmed (nt klahvilogijad, lunavara jne)

Source: https://www.zdnet.com/article/phishing-alert-gdpr-themed-scam-wants-you-to-hand-over-passwords-credit-card-details/, Redscan

COVID-iga seotud rünnakud

- COVID-19 pandeemia ajal töötasid paljud inimesed kodus. Töötajad kasutasid kaugrežiimis tööülesannete täitmiseks personaalarvuteid, põhisuhtlus toimus meili teel – see tähendab, et töötajad muutusid küberrünnakute suhtes haavatavamaks.
- COVID-19 ajal märgati pandeemiaga seotud petuskeemide tõusu, nagu võltsitud haiguste tõrje ja ennetamise keskused (CDC) või tervishoiuorganisatsioonide meilid, meilid vaktsiiniga hõlmatuse kohta, kust saate vaktsiini, vaktsiinide statistikat, töötajate vaktsineerimise staatust. jne.

Funded by the Erasmus+ Programme of the European Union

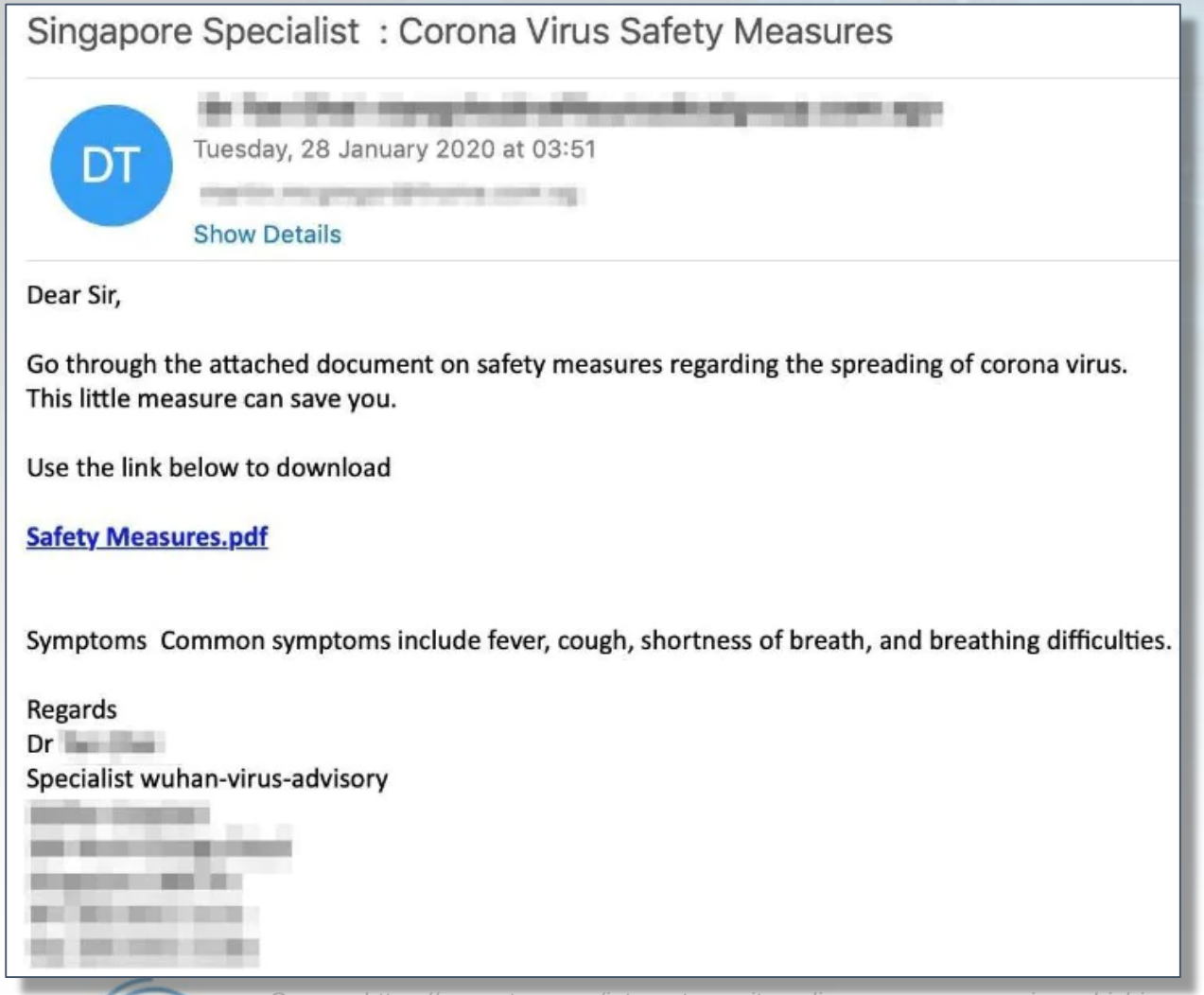
Covidi rünnakud: e-kirjad

- **Miks seda tüüpi rünnak on edukas?** COVID-19 tekitas inimestes ebastabiilsuse ja ebakindlustunde, poliitikute sagedased muudatused karantiini, vaktsineerimise, vaktsineerimist tõendavate dokumentide jms osas.
- **Sihtrühm:** kõik inimesed
- **Oht:**
  - meilid, milles palutakse esitada võltsveebisaidil tundlikku teavet
  - meilid, milles palutakse lingil klõpsata
- **Ründe meetod:** e-kirjad.

- **Taktika:**
  - kujundatud ja vormindatud meilid näevad välja nagu päris organisatsiooni meilid
  - ründajad soovitavad tavaliselt alla laadida dokumenti, e vaadata üle COVID-19 statistika, laadida alla COVID-i vorm, täita veebivormi või täita allalaaditud dokumente vaktsineerimise oleku kohta, laadida üles negatiivne test jne. .
- **Tegurid:**
  - **Inspireeriv kiireloomulisuse tunne**
  - **Inspireeriv hirmutunne**
  - **Palub järgida mittestandardset protsessi**
- **Ohvrid:**
  - kodanikud, kelle teadmised andmepüügist on piiratud või puuduvad (kodanikud, kes sooritavad andmepüügimeilides küsitud toiminguid)

Funded by the Erasmus+ Programme of the European Union

Covidi rünnakud: terviseealane nõuanne



Singapore Specialist : Corona Virus Safety Measures

DT

[redacted]

Tuesday, 28 January 2020 at 03:51

[redacted]

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus. This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

- Andmepüügi veebisait avaneb, kui ohver klõpsab lingil, mis näeb välja nagu link PDF-failile
- Ohvril võidakse paluda esitada oma isikuandmed, sealhulgas konto andmed ja maksekaardi andmed, et võltsveebisaidil "identiteeti tuvastada".
- **Tulemus**:
  - Varastatud ohvrite e-posti sisselogimisandmed, et pääseda e-kirjale.
  - Varastatud finantsandmed.
  - Nakatunud seadmed (nt klahvilogijad, lunavara jne)

Source: https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

Funded by the Erasmus+ Programme of the European Union

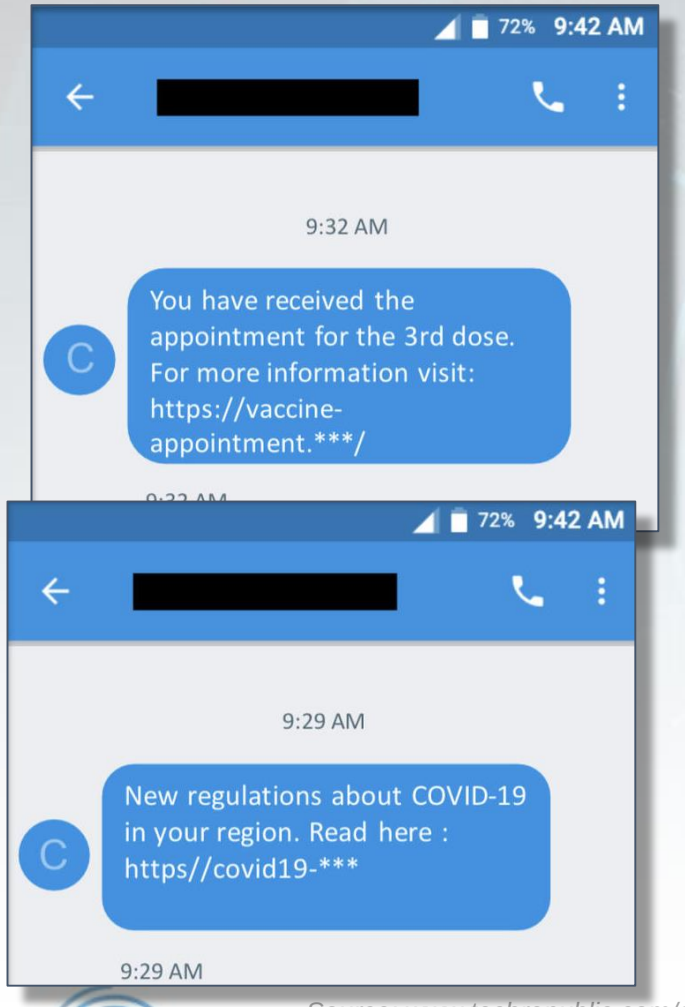
Covidi rünnakud: SMS

- **Miks seda tüüpi rünnak on edukas?**
  COVID-19 tekitas inimestes ebastabiilsuse ja ebakindluse tunde, sagedased poliitikute otsused muutused karantiinis, vaktsineerimise, vaktsineerimist tõendavate dokumentide jms osas. Suuremahulised sündmused, sõjad, pandeemiad, nagu COVID-19, panevad inimesi käituma impulsiivsemalt kui nad seda teeksid. tavaolukorras.
- **Sihtrühm:** kogu rahvastik
- **Oht:**
  - meilid, milles palutakse esitada võltsveebisaidil tundlikku teavet
  - meilid, milles palutakse lingil klõpsata
- **Ründe meetodid:** tekstisõnumid (SMS).

- **Taktika:**
  - kujundatud ja vormindatud sõnumid näevad välja nagu päris organisatsiooni sõnumid
  - ründajad soovitavad tavaliselt alla laadida dokumenti, et vaadata üle COVID-19 statistika, laadida alla COVID-i vorm, täita veebivormi või täita allalaaditud dokumente vaktsineerimise oleku kohta, laadida üles negatiivne test jne..
- **Tunnused:**
  - **Inspireeriv kiireloomulisuse tunne**
  - **Inspireeriv hirmutunne**
  - **Palub järgida mittestandardset protsessi**
- **Ohvrid:**
  - kodanikud, kelle teadmised andmepüügist on piiratud või puuduvad (kodanikud, kes sooritavad andmepüügimeilides küsitud toiminguid)

Funded by the Erasmus+ Programme of the European Union

Covidi rünnakud: teave vaktsiinide kohta SMS-i teel



- **Miks seda tüüpi rünnak on edukas?** Asutused saadavad kodanikele vaktsineerimise kohta SMS-e.
- **Sihtrühm:** kõik einimesed
- **Oht:**
  - SMS palub klõpsata antud lingil
- **Ründe meetod:** SMS.
- **Taktikad:**
  - SMS-id on lühikesed. Üks või kaks lauset. Tavaliselt antakse SMS-is link võltsitud veebisaidile
- **Tunnused:**
  - ebastabiilsuse ja ebakindluse tunne
- **Ohvrid:**
  - kodanikud, kelle teadmised andmepüügist on piiratud või puuduvad (kodanikud, kes sooritavad andmepüügimeilides küsitud toiminguid)

Source: www.techrepublic.com/article/new-sms-malware-targets-android-users-through-fake-covid-messages

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Teemad:

Sündmuspõhine rünnak	E-mail	Tekstisõnum	Veebisait
Loterii pettus	Telefonikõne	Näost näkku	Üle-õla vaatamine

Funded by the Erasmus+ Programme of the European Union

Andmepüügikirjad

- Üks tuntumaid andmepüügi tüüpe
- Ründajad võivad kasutavad järgmisi taktikaid andmepüügimeilides:
  - Palub saata tundlikku teavet meili teel
  - Palub klõpsata meilis antud lingil
  - Küsib manuse avamist, tavaliselt PDF- või DOC-vormingus
- Andmepüügimeilide tavapärased teemad:
  - Konto probleemid
  - Tehnilise toe probleemid
  - Romantiline suhe
  - Andmepüügimeilid tegevjuhtidele ja juhtidele
  - Raha tagasi saamiseks või asutuselt rahalise toetuse saamiseks

Funded by the Erasmus+ Programme of the European Union

Andmepüügikirjad

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) **Advanced fee scam** – levinud rahvuslikkud pettused nö Nigeeria kodaniku abi palumine suure rahasumma liigutamisel;

3) **Spear fishing** - pahatahtlikud meilid, mis on spetsiaalselt loodud ja saadetud konkreetsele isikule või organisatsioonile, püüdes varastada tundlikku teavet;

4) **Whaling** - püüd varastada tundlikku teavet, kuid rünnak on sageli suunatud kõrgemale juhtkonnale;

5) **Angler Phishing** – suhteliselt uus tüüp, mis viitab rünnakutele, mis esinevad sotsiaalmeedias, kasutades võltsitud URL-e, kloonitud veebisaite, postitusi, säutse ja kiirsõnumeid;

6) **Clone Phishing** – andmepüügi tüüp, kus originaalne ja varem edastatud e-kirja sisu ja väljanägemine võetakse aluses pahatahtlikku sisuga e-kirja loomisel;

7) **Malvertising** - see andmepüügitüüp kasutab veebireklaame või hüpikaknaid, et sundida inimesi klõpsama ausa välimusega lingil, mis seejärel arvutisse pahavara installib.

Funded by the Erasmus+ Programme of the European Union

Andmepüügimeilid: taotlused saata tundlikku teavet meili teel

- **Miks seda tüüpi ründed on edukad?** Andmepüügirünnakud näivad veenvamad, kui jätvad mulje et on usaldusväärsest allikast. Organisatsioonid ei teosta piisavat hoolsuskohustust. Ründajad kasutavad keerukamaid andmepüügirünnakuid, mida on raske tuvastada jne.
- **Sihtrühm:** kõik inimesed
- **Oht:**
  - meilid, milles palutakse saata vastus
  - meilid, milles palutakse kirja teel tundlikku teavet esitada
- **Taktikad:**
  - otsib partnereid, annab ohvrile häid uudiseid, pakub raha, annab teada võidust, keegi teeskleb sõpra ja palub ootamatu katastroofi tõttu raha laenata jne.
  - pakub raha, annab teada konkursi võitjast jne.
- **Tunnused:**
  - **Jätab ohvrile mulje, et saatja on kasulik**
  - **Sisendab ahnust**
- **Ohvrid:**
  - kodanikud, kellel on andmepüügist piiratud või puuduvad teadmised (kodanikud, kes vastavad andmepüügimeilis küsitud või sooritavad toiminguid)
- **Tulemus:**
  - Identiteedivargus, raha kaotamine

Funded by the Erasmus+ Programme of the European Union

Andmepüügimeilide näited: tundliku teabe e-posti teel saatmise taotlused

Sender: eduardorodriguez <andreasjohnson874@gmail.com>

To: andreasjohnson847@gmail.com

Subject:

Hello My Friend

I am ANTONI FELIKS from Poland, I have a good news for you CONGRATULATIONS!!!
Contact me now on this email: homebankpln@gmail.com or homebankpln@polandmail.com to receive a good news

Sender: administrator <admin@www-professionals.online>

To:
Subject: Congratulations!!!

We are pleased to inform you that your email has won $ 7,500 from www online lottery award. In order to get this award you are required to provide such information:
Beneficiary name and surname:_____
Beneficiary address:_____
Beneficiary country: _____
Beneficiary credit card number: _____
Beneficiary credit card CVC2: _____

NOTE: keep your winning information confidential.

Signed
CEO: Luis Andres Jonson

Sender: Ava Williams <avawilliamsj@gmail.com>

To: avawilliamsj@gmail.com

Subject: Hi…

Greetings to you

I know that you will be surprised to receive this message from me because we have not met before. I got your email from Google research. I am writing to you from a hospital where I have been undergoing medical treatment because I am very sick now as a result of cancer.

I contacted you today because I need your help to invest the funds I inherited from my late husband.
I will compensate you with 30% of the money if you agree to help me with this.
I will tell you more about myself and my plans when I hear back from you.

Regards
Mrs. Ava Williams

Sender: manyrib7@gmail.com

To:

Subject: Hi…

My name is Rihab Manyang, I am here to find a business partner or friend to help me invest my fund in your country.

Funded by the Erasmus+ Programme of the European Union

Andmepüügimeilid: palub klõpsata meilis pakutud lingil

- **Miks seda tüüpi rünnak on edukas?** Andmepüügirünnakud näivad veenvamad, kui jätvad mulje et on usaldusväärsest allikast. Organisatsioonid ei teosta piisavat hoolsuskohustust. Ründajad kasutavad keerukamaid andmepüügirünnakuid, mida on raske tuvastada: nad saavad kasutada sisu, konteksti ja emotsionaalsete motivaatorite kombinatsiooni, mis on andmepüügi rünnaku edukuse taga jne.
- **Sihtrühm:** kõik inimesed
- **Oht:**
  - andmepüügirünnakud kopeerivad meie olemasolevaid töövooge
  - ründajad paluvad meilis antud linki klõpsatal
- **Taktika:**
  - Meilid, mis puudutavad ohustatud e-posti aadresse või paroole
  - Meilid koostööks jagatud dokumentide kohta
  - Tehnilistest probleemidest teavitavad meilid
- **Tunnused:**
  - **Inspireeriv kiireloomulisuse tunne**
  - **Inspireeriv hirmutunne**
  - **Ründajad kasutavad ohvri emotsioone ja instinkte**
- **Ohvrid:**
  - kodanikud, kellel on andmepüügist piiratud või puuduvad teadmised (kodanikud, kes vastavad andmepüügimeilis küsitud või sooritavad toiminguid)
- **Tulemus:**
  - Identiteedivargus, raha kaotamine

Funded by the Erasmus+ Programme of the European Union

Andmepüügimeilide peamised omadused

- Kasutatakse mainekate organisatsioonide või isikute nimesid
- Kasutatakse usaldusväärsete allikate andmeid
- Küsitakse tundlikku teavet
- Meilidel võib olla manuseid
- Tavaliselt teadmata saaja (umbisikulised)
- Lingid veebisaitidele (linke võib lühendada)
- Lingid suunavad traditsiooniliselt pahatahtlikele veebisaitidele
- Kasutatakse hirmu või väljendatakse kiireloomulisust
- Ebausutav info, mis ei saa olla tõsi (loterii, allahindlused, pärandus jne)

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Andmepüügimeilides kasutatavad lingid

- Andmepüügimeilide ründajad kasutavad tavaliselt linke võltsitud veebilehekülgedele:
  - Ründajad võivad registreerida võltsdomeeni. URL-i nimi võib olla sarnane tegelikule organisatsioonile, nad muudavad domeeninimes lihtsalt ühte või mitut tähte, näiteks tähe “l” asemel võivad nad kasutada tähte “i” või “m” asemel “rn” jne. Näiteks võivad nad registreerida sellise võltsdomeeninime www.exarnple.com (päris URL www.example.com)
  - Ründajad saavad domeeni registreerida, kasutades URL-is organisatsiooni tegelikku nime, näiteks www.sales-organization.com (päris URL www.organization.com)
  - Ründajad võivad kasutada lühendatud URL-e, nagu Bitly, TinyURL, Short.io (lisateavet leiate jaotisest Lühendamisteenused)
  - Ründajad võivad kasutada häkitud veebisaidi linki (kasutades päris domeeninime, kuid teise osa URL-ist loovad häkkerid)
  - Ründajad sisaldavad seaduslikul veebilehel pahatahtlikku koodi (injection attack). Kui ohver selle veebisaidi avab, käivitatakse pahatahtlik skript. Sellise rünnaku tulemuseks on andmete vargus, klahvilogimine, küpsiste vargus jne.

Funded by the Erasmus+ Programme of the European Union

Saatja: NB Online Fraud Prevention <info@nat1onalbank.com>

Saaja: undisclosed-recipients

Pealkiri: Your National Bank account has been suspended

CyberPhish

National Bank

Dear Customer,

We recently noticed that different devices from different locations tried to login to your National Bank account.

We provide the list of IP addresses with recent attempt to login to your account :
12.55.155.6:8080
32.44.789.99:3128
54.22.124.44:8080
78.44.457.14:80

Currently your account is SUSPENDED. You need to activate it within 7 days, otherwise account will be blocked.

To confirm that you are original user and activate account, please click HTTP://WWW.NAT1ONALBANK.COM?PROFILE
More information here.

http://www.nat1onalbank.com/?PROFILE

Sincerely,
National Bank Online Fraud Prevention Manager
JohnBank@gmail.com

ZIP **Report-of-attempts-to-login.zip**

Manuse või faili allalaadimisega andmepüügimeilid

- **Miks seda tüüpi rünnak on edukas?**
  Andmepüügirünnakud näivad veenvamad, kui jätvad mulje et on usaldusväärsest allikast. Organisatsioonid ei teosta piisavat hoolsuskohustust. Ründajad kasutavad keerukamaid andmepüügirünnakuid, mida on raske tuvastada: nad saavad kasutada sisu, konteksti ja emotsionaalsete motivaatorite kombinatsiooni, mis on andmepüügi rünnaku edukuse taga jne. .
- **Sihtrühm:** kõik inimesed
- **Oht:**
  - andmepüügirünnakud kopeerivad meie olemasolevaid töövooge
  - ründajad paluvad avada lisatud pilte, muusikat, filme, dokumente (nt PDF, DOC, ZIP), millele on manustatud pahatahtlikku tarkvara
  - ründajad lisavad HTML-faile, mis on täiesti töökorras – neil on kõik andmepüügiks vajalikud elemendid, ründajad ei pea neid Internetis avaldama
- **Taktika:**
  - Manustega meilid: äri- või üksikettepaneku fail, "konfidentsiaalse" või "väga olulise" teabe fail, müügi- või finantsteave (maksmata arved, ostutellimus), kiireloomulised kõnemeilid, uuendatud organisatsioonipoliitika, tehniliste probleemidega failid, aja- spetsiifiline teave, näiteks pandeemia jne.
  - Meilid, milles palutakse täita manustatud dokument oluliste töövoogude jaoks
- **Tunnused:**
  - **Inspireeriv kiireloomulisuse tunne**
  - **Ründajad kasutavad ohvri emotsioone ja instinkte**
- **Ohvrid:**
  - kasutajad, kellel on andmepüügist piiratud või puuduvad teadmised (kodanikud, kes avavad manuse)
- **Tulemus:**
  - Nakatunud arvutid, identiteedivargused, raha kaotamine

Andmepüügimeilide näited: manuse või faili allalaadimisega andmepüügimeilid

Ärge usaldage meilis leiduvaid linke ja manuseid, isegi kui see pärineb usaldusväärselt isikult

Saatja: Jaana Jordan<cdg446@comcast.net>

Saaja: Una Vilime <una.vilime@*organisationname.com*>

Pealkiri: hi Una

You need to process a Faster payment for an invoice urgently, kindly let me know if you are available asap.

Regards

Jaana Jordan

Sent from my iPhone

Saatja: ABC Bank<noreply@support-abcbank.com>

Saaja:

Pealkiri: ABC bank Account Support Department

Dear ABC Bank user,

We noticed unusual activity in your credit/debit account. As a result me have to limit access to your bank account. Your limited access will remain until the issue has been resolved.

We work to ensure your account safety, therefore we appreciate your understanding.

In order to ensure your safety we attached a document which you need to open in a web browser. Follow provided steps in the opened web page to restore your account.

Sincerely

ABC bank Account Support Department

Andmepüügimeilide näited: manuse või faili allalaadimisega andmepüügimeilid

Saatja: WeTransfer <noreply@wetransfering-files.net>

Saaja:me

Pealkiri: info@wetransfering-files.net **sent you policy.doc via WeTransfer**

we

info@wetransfering-files.net sent you policy.doc via WeTransfer

1 item, 25.6 KB in total · Expires after 2 days

Important information for staff!

Please find attached confidential file - updated organisational policy. Please download it and read it carefully, otherwise you won't be able to access your workplace premises or information systems. System Security Team

Get your file

Download link https://bit.ly/2YI6BY6

Saatja: Microsoft Security Team<support@digi-support.com>

Saaja:

Pealkiri: Important: data security alert

Microsoft

Dear Microsoft User,

Taking care of your online safety, we send you a safety message. We noticed that your document with sensitive data is freely available on the Internet.

We remind you that by sharing sensitive information of other people, you are in breach of GDPR. This could result in a hefty fine.

Please download the document and change sharing options.

Download document.

Microsoft Security Team

Harpuunimine - *Spear Phishing*

- **Miks seda tüüpi rünnak on edukas?** Andmepüügisõnumid on suunatud spetsiaalselt kavandatavale ohvrile, andmepüügi rünnakud toimuvad aja jooksul, andmepüük kasutab nullpäeva rünnakuid, ettevõtetel puuduvad arvutikasutuspoliitikad või need ei jõusta neid, iga andmepüügimeil näeb autentne välja, ohver täidab nõuded jne.
- **Sihrühm:** töötajad: Arvuti-meeskonna personaliülemad, raamatupidajameeskond, personalimeeskond, palgaarvestusmeeskond jne.
- **Oht:**
  - andmepüügirünnakud kopeerivad olemasolevaid töövooge
- **Taktika:**
  - Manustega meilid: äri- või üksikettepaneku fail, "konfidentsiaalse" või "väga olulise" teabe fail, müügi- või finantsteave (maksmata arved, ostutellimus), kiireloomuline kõnemeil jne.
  - Meilid linkidega võltsitud veebisaidile
- **Tunnused:**
  - **Inspireeriv kiireloomulisuse tunne**
  - **Ründajad kasutavad ohvri emotsioone ja instinkte**
- **Ohvrid:**
  - töötajad, kellel on andmepüügist piiratud või puuduvad teadmised
- **Tulemus:**
  - Konfidentsiaalse teabe kaotamine, intellektuaalomandi kadu, ärisaladuste kadu, nakatunud digitaalseadmed jne.

Funded by the Erasmus+ Programme of the European Union

Näide "Spear" andmepüügimeilidest (boss/ tegevjuht): andmepüügimeilid koos manuse või faili allalaadimisega

Saatja: CEO <bill.jonson99@hotmail.com>

Saaja: me

Pealkiri: Urgent payment

Hi, Jane,

I am at the meeting now for a few hours and have limited access to my work email and to my mobile phone. I just got a message informing that we are late with payment to our exclusive partner.

In order to get goods on time, **please do urgent payment today** to the partner's supplier directly.
Bank details indicated below:
AA 12 3000 9852 0001 0020.

Purpose of payment: for goods

Counting on you,
Bill Jonson

Saataja: Managing Director <Eva.Stivens53@yahoo.com>

Saaja: me

Pealkiri: Current Month Salaries

Hi, Tom,

I'm working from home today, therefore I'm writing from my personal email.

I updated salaries of current month and made several changes. I am sorry for this misunderstanding, hope you will be able to make the changes and all staff will be paid on time.

Contact me, if you have any questions.

Regards
Eva Stivens, Managing Director

Updated-Salaries.xls

Tehnilise toe andmepüügimeilid

CyberPhish
Safeguarding your digital future

Andmepüük: tehniline tugi

- **Miks seda tüüpi rünnak on edukas?**
  Digitaalseid seadmeid kasutades saavad kasutajad tavaliselt mitmesuguseid tõrkeid või hoiatusi. Seetõttu võivad petturid taotleda tehnilist tuge ja pakkuda abi turvarikkumiste lahendamisel kaugjuurdepääsutarkvara kaudu või e-kirjas oleval lingil klõpsates.
- **Sihtrühm:** kõik kodanikud, eriti digioskusteta inimesed, eakad
- **Oht:**
  - andmepüügirünnakud kopeerivad meie olemasolevaid töövooge
  - ründajad paluvad klõpsata meilis toodud linki või helistada antud telefoninumbril
- **Taktika:**
  - Meilid, mis puudutavad ohustatud e-posti aadresse või paroole
  - Meilid koostööks jagatud dokumentide kohta
  - Tehnilistest probleemidest teavitavad meilid
- **Tunnused:**
  - Inspireeriv kiireloomulisuse tunne
  - Inspireeriv hirmutunne
  - Ründajad röövivad ohvri emotsioone ja instinkte
- **Ohvrid:**
  - kodanikud, kellel on andmepüügist piiratud või puuduvad teadmised
- **Tulemus:**
  - Lunavara, nakatunud digiseade, pääse digiseadmele ligi, seadmele juurdepääsu omades saavad petturid seda kasutada hilisemateks rünneteks, muuta seadme sätteid, varastada tundlikke andmeid, kasutaja võib raha kaotada jne..

Ründajad võivad kasutada ka teist tüüpi tehnikaid:
Hüpiksõnumid (Pop-up messages)
Võltsveebisaidid (fake websites)
Ootamatud kõned (Vishing)

Funded by the Erasmus+ Programme of the European Union

Tehnilise toe andmepüügimeili näide

Saatja: Mail Settings <tech-support.954mail-delivery352477@cloud.website.com>

Saaja: Lucy Bradson

Pealkiri: Email Delivery Failure

Hello lucy.bradson

Email Server is having problem verifying your email.

You won't be able to receive new mails until you verify this mailbox.

Automatically Verify your mailbox now through below instruction.

UTO-VERIFY MAILBOX NOW

Your email account will be TERMINATED after 24hours if no valid action is taken.

Best Regards, Mailbox Administrator

Tehnilise toe andmepüügikõned

Näide tehnilise toe andmepüügi hüpikaknast

Microsoft Security Alert

X

Your computer may have a Virus.

You have immediately to call
1 877 00 11 00 145 for assistance.

Your IP address:
147.254.114.741

Date:
11th February 2021

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Andmepüügimeilid: romantiline suhe(Cat Phishing)

- **Miks seda tüüpi rünnak on edukas?** On inimesi, kes on üksikud või lahutatud. Nad võivad saada andmepüügimeile või sotsiaalmeediasõnumeid petturitelt või tutvumisveebisaitidelt.
- **Sihtrühm:** üksi, lahutatud, uut suhet otsivad inimesed, sotsiaalmeedia kasutajad
- **Oht:**
  - Võltsidentiteediga petturid lähevad kiiresti suhetesse ja saavad ohvri usalduse. Pärast seda küsivad petturid raha ja kaovad pärast selle saamist.
- **Taktika:**
  - E-kiri tundmatult isikult
  - Tekstsõnum sotsiaalmeedia kaudu, kiirsuhtlusprogramm
- **Tunnused:**
  - **Minnakse kiiresti suhtesse**
  - **Hankige võimalikult kiiresti ohvri usaldus**
- **Ohvrid:**
  - emotsionaalselt haavatavad kodanikud
- **Tulemus:**
  - rahaline kahju.

Funded by the Erasmus+ Programme of the European Union

Näide:
Romantiline suhe (Cat Phishing)

Sender: John John <john.19850215@gmail.com>

To: me

Subject: to my love

My Love,

I am very happy having the opportunity to find you, because only you in all the world could understand me. I feel that you are my second half. I believe that a thousand kilometers will not affect our close relationship.
I will make everything that I can to come to your country, change my workplace and spend the rest of my life in great happiness with you.

I look forward to your message.

Your Love, John

Illustration by Freepik Storyset

Sender: John John <john.19850215@gmail.com>

To: me

Subject: to my love

Hey, My Love,

You won't believe this, but I wanted to make you surprise and see you in your town. When I landed to Frankfurt, I had to wait for 18 hours for another plane. Therefore I went to the city hotel, and here my bag was stolen. Could you help me, please. I stayed in the hotel and tomorrow I need to cover Hotel invoice. Could you please cover my stay?

I look forward to see you asap, my Dear.

Your Love, John

Söötpüük (*Baiting*)

Söötpüük - *Baiting*

- **Miks seda tüüpi rünnak on edukas?** Inimesed kipuvad usaldama ja usuvad, et nad võiksid saada midagi tasuta, osta midagi allahindlusega, saada raha või auhindu.
- **Sihtrühm:** ***kõik inimesed***
- **Oht :**
  - petturid pakuvad midagi väga atraktiivset, näiteks muusika, filmide allalaadimist, ootamatuid võite või auhindu, suuri allahindlusi ja nii edasi.
- **Taktika:**
  - Väga ahvatleva pakkumisega meilid, hüpikaknad, tekstisõnumid, sotsiaalmeedia postitused
  - USB-draivid vedelevad kontoriruumide lähedalt

- **Tunnused:**
  - **Vale lubadus**
  - **Inspireeriv ahnuse tunne**
  - **Inspireeriv uudishimutunne**
- **Ohvrid:**
  - Ahned või uudishimulikud kodanikud, hoolimatud töötajad
- **Tulemus:**
  - Hankitakse tundlikku teavet, identiteedivargus, intellektuaalomandi vargus, sabotaaž, raha kaotamine, paigaldatud pahavara.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Baiting näited
Andmepüügi e-post: allahindluspettused

Saatja: Black Friday Proposal<Black-Friday-Proposal@trust-fridays.com>

Saaja: me

Pealkiri: Congratulations! You've landed Secret Prices

www.trust-fridays.com/discounts/sdtuyx5D7rtkh6

Väga tuntud kaubamärkide ja toodete uskumatult suured allahindlused või madalad hinnad

Baiting näited
Andmepüügimeil: maksutagastused ja Covid-19

Saatja: Government gateway <do-not-reply@online-gateway.com>
Saaja: me
Pealkiri: Government refund on COVID-19

To whom is it may concern

The government has taken actions helping citizens and organizations suffering from Covid-19.

We inform you that you are eligible to get a one-time refund for $2.500. In order to get this refund, you need to fill in this online form.

This message was generated automatically by Government gateway

Petturid võivad jälgida tegelikke sündmusi ja kasutada neid rünnakuteks, samuti võivad nad pakkuda nõutud tooteid või maksude tagastust, nagu selles näites.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Baiting näide.
Andmepüügimeil: võit, auhinnad

Saatja: Ade Goodchild <admin>

Saaja: me

Pealkiri: Dear Beloved

Dear Beloved,

Your E-mail was randomly picked by my foundation, you are to receive a donation 1,000.000.00 (One Million Pounds) which you must use at least 20% to touch the lives of the less privileged ones around you. I just kicked off foundation.

Read more details about how I became a millionaire.
https://www.bbc.cominews/uk-england-hereford-worcester-47637306

Kindly confirm the ownership of your email by sending your response to me immediately and I shall explain in detail you need to know.

Yours faithfully,
Ade Goodchild
Goodchild Foundation.

Peibutavad petturid võivad saata e-kirju, mis teavitavad ohvreid võidust, auhindadest ja kergest rahast.

Teemad:

Sündmuspõhine rünnak	E-mail	Tekstisõnum	Veebisait
Loterii pettus	Telefonikõne	Näost näkku	Üle-õla vaatamine

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Tekstsõnumid

- Telefonide, rakenduste või sotsiaalmeedia platvormide kaudu saadetud lühisõnumid.
- Ründajad võivad järgmisi taktikaid kasutada:
  - Taotleb tundliku teabe saatmist tekstsõnumis
  - Palub klõpsata tekstisõnumis antud lingil
  - Küsib manuse avamist
  - Helistada antud telefoninumbril
- Andmepüügi tekstisõnumite tavapärased teemad:
  - Värskendage isiklikku või kauba kohaletoimetamise teavet
  - Pakkuda tohutut allahindlust või osaleda auhinna saamiseks konkursil
  - Konto probleemid
  - Romantiline suhe
  - Pakkuge rahalist toetust

Funded by the Erasmus+ Programme of the European Union

Tekstisõnumid

- Tekstsõnumid võivad olla varjatud usaldusväärsetest allikatest pärinevateks
- Andmepüügi tekstisõnumid võivad tulla erinevate platvormide kaudu:
  - **Kiirsõnumid** (Hangouts, Skype etc.)
  - **Sotsiaalmeedia platvormid või rakendused** (Instagram, Facebook, LinkedIn, Snapchat, Twitter etc.)
  - **SMS andmepüük – smishing** (including WhatsApp, Telegram, Viber)
- Kasutavad lühendavaid URL-i teenuseid

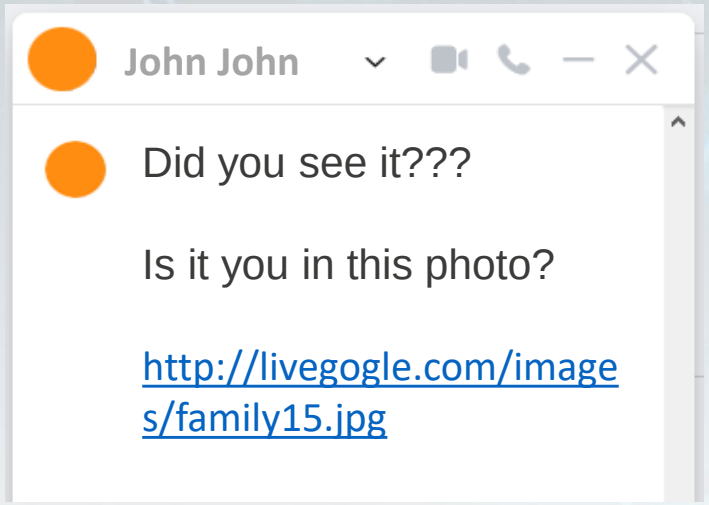
Funded by the Erasmus+ Programme of the European Union

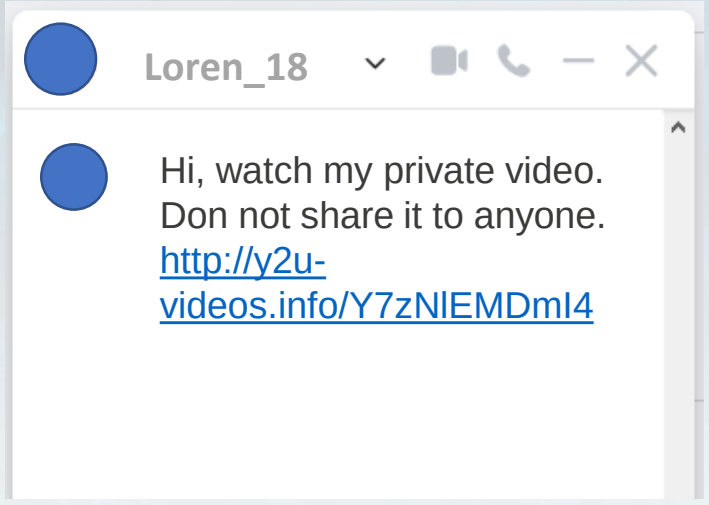
Tekstsõnumid: sotsiaalmeedia ja kiirsõnumid (IM)

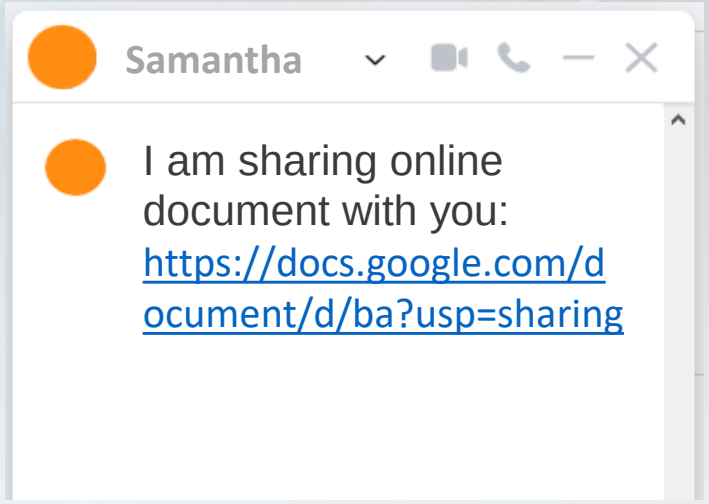
- **Miks seda tüüpi rünnak on edukas?** Petusõnumeid on tõelistest sõnumitest raske eristada (tavaliselt kasutavad petturid kiirsuhtlussi, mis nakatab seadmeid pärast lingil klõpsamist või manuse avamist) jne.
- **Sihtrühm:** kõik inimesed
- **Oht:**
  - sõnumid koos manustega, linkidega, sõnumid, mis paluvad rahalist toetust, sõnumid romantilistelt petturitelt jne.
- **Ründe meetod:** kiirsõnumite või sotsiaalmeedia kontaktide või tundmatute isikute tekstisõnumid.
- **Taktika:**
  - Lühisõnum (tavaliselt üks või kaks lauset) koos lingiga. Sõnumid paluvad uuendada kontot, muuta seadeid, avada dokumente või pilte, soovitada häid allahindlusi jne.
  - Lühisõnum (tavaliselt üks või kaks lauset) koos manusega.
  - Lühisõnumid, milles palutakse rahalist toetust
- **Tunnused:**
  - **Inspireeriv kiireloomulisuse tunne**
  - **Inspireeriv hirmutunne**
  - **Naiivsuse ärakasutamine**
- **Ohvrid:**
  - kodanikud, kellel on andmepüügist piiratud või puuduvad teadmised ja keda kiirsõnumite kaudu ei eeldata andmepüügiks
- **Tulemused:**
  - Nakatunud digiseadmed, identiteedivargus, volikirjade vargus, raha kaotamine

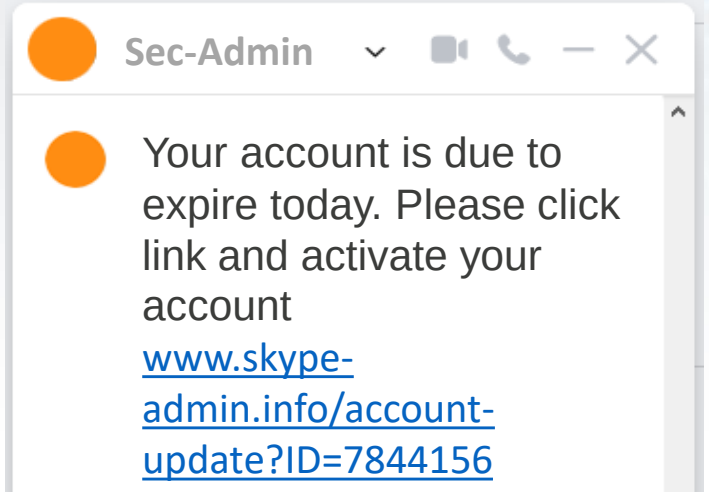
Funded by the Erasmus+ Programme of the European Union

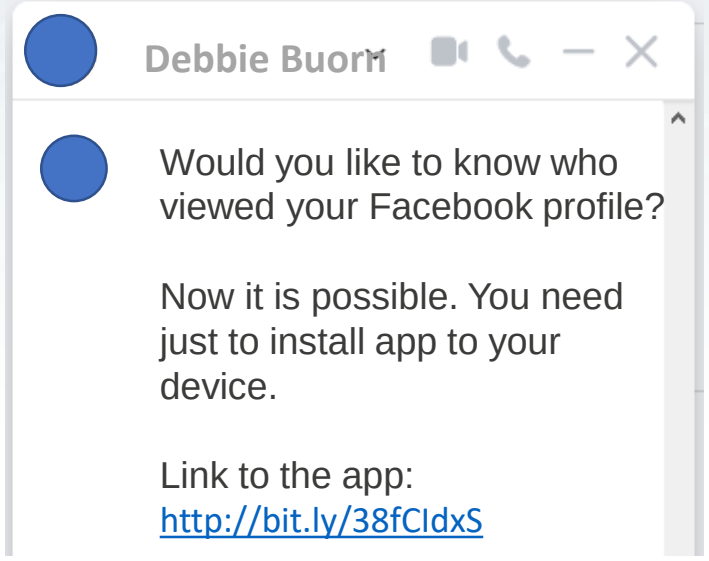
Tekstsõnumid: kiirsõnumite (IM) andmepüügi näited

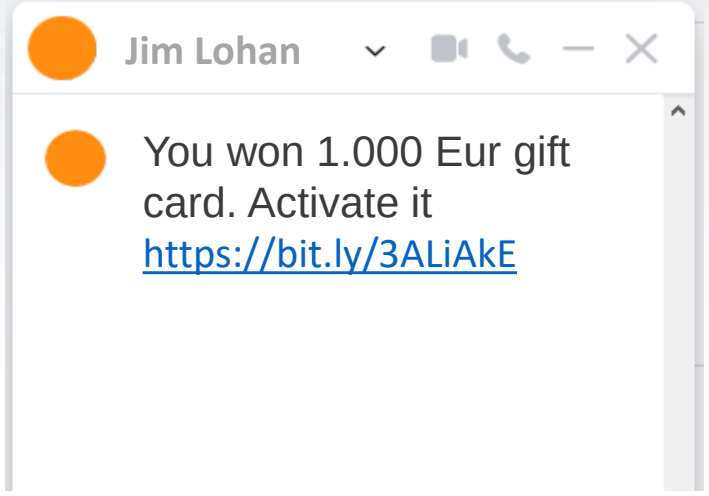












Tekstsõnumid
Sotsiaalmeedia andmepüügi näited

Instagram

Hi, someone tried to login to your account several times unsuccessfully. Due security reasons, your account is locked. In order to unlock please sign in here and provide this code: 753147

© Instagram. Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025

Instagram

We found that you posted content which is encountered copyright. Your account was deactivated.

Click here to activate your account.

© Instagram. Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025

Instagram

 https://www.livegogle.com/images/family15.jpg

© Instagram. Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025

SMS-kalastus
Smishing

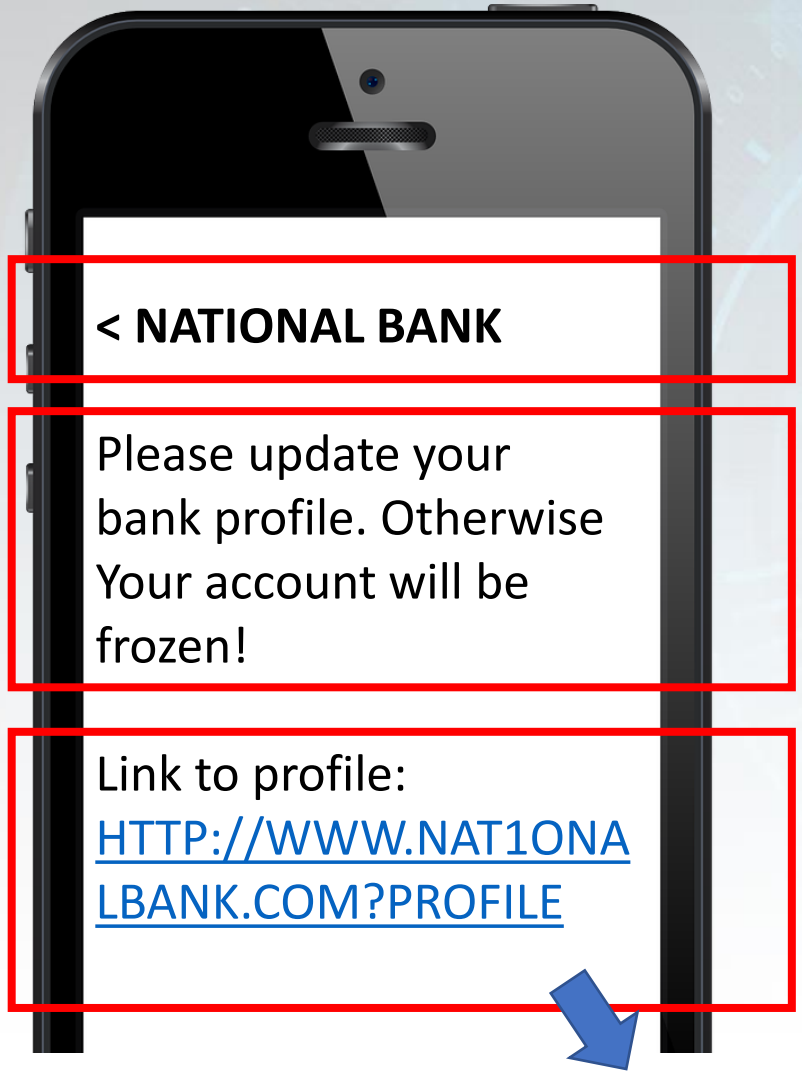
CyberPhish

Tekstsõnumid: SMS kalastus (Smishing)

- **Miks seda tüüpi rünnak on edukas?** Tõelistest sõnumitest on raske eristada (tavaliselt kasutavad petturid tõelisi asutuste nimesid).
- **Sihtrühm:** kõik inimesed
- **Oht:**
  - sõnumid linkidega, sõnumid, milles palutakse rahalist tuge, vastata või helistada
- **Ründe meetod:** SMS tekstisõnumid.
- **Taktika:**
  - Lühisõnum (tavaliselt üks või kaks lauset) koos lingiga. Sõnumid palub muuta seadeid, värskendada kontot, muuta saadetise andmeid jne.
- **Tunnused:**
  - **Inspireeriv kiireloomulisuse tunne**
  - **Inspireeriv hirmutunne**
  - **Naiivsuse ärakasutamine**
- **Ohvrid:**
  - kodanikud, kellel on andmepüügist piiratud või puuduvad teadmised ja keda ei eeldata SMS-i teel andmepüügiks
- **Tulemused:**
  - Nakatunud digiseadmed, identiteedivargus, volikirjade vargus, raha kaotamine

Funded by the Erasmus+ Programme of the European Union

Tekstisõnumid: Smishing näide



http://www.nat1onalbank.com?profile

http://www.nat1onalbank.com?profile

National Bank

YOUR PROFILE NEEDS TO BE UPDATED!

Name

Surname

Email Address

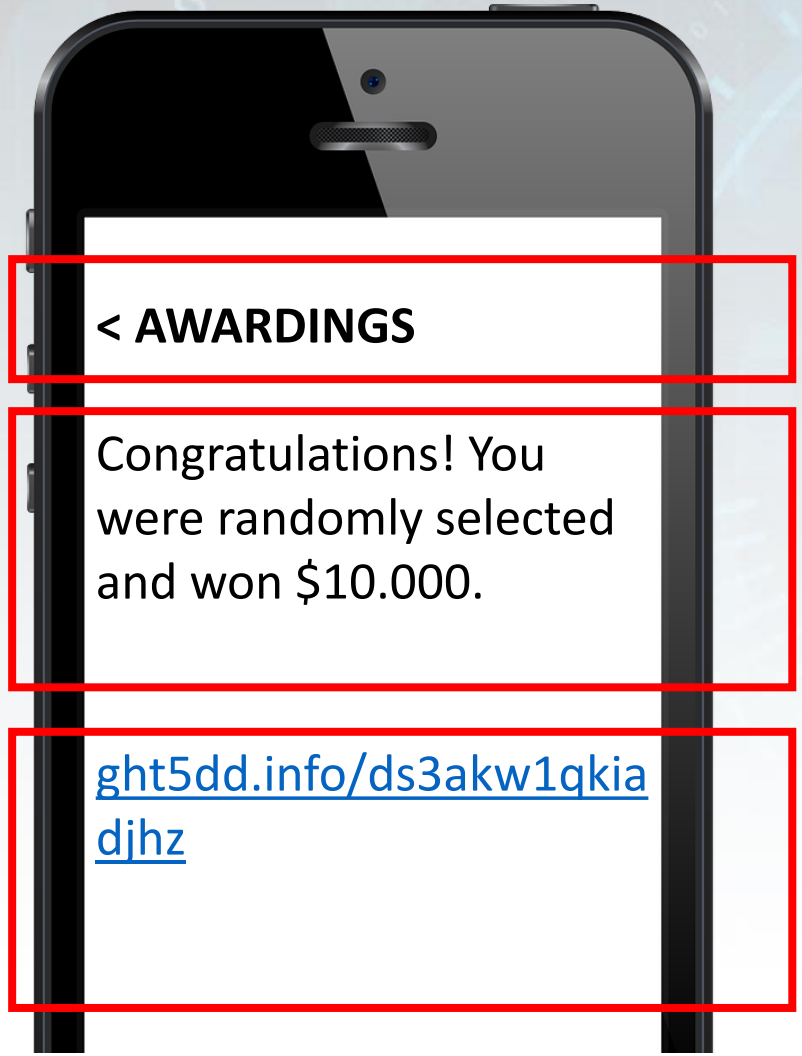
Email Address Password

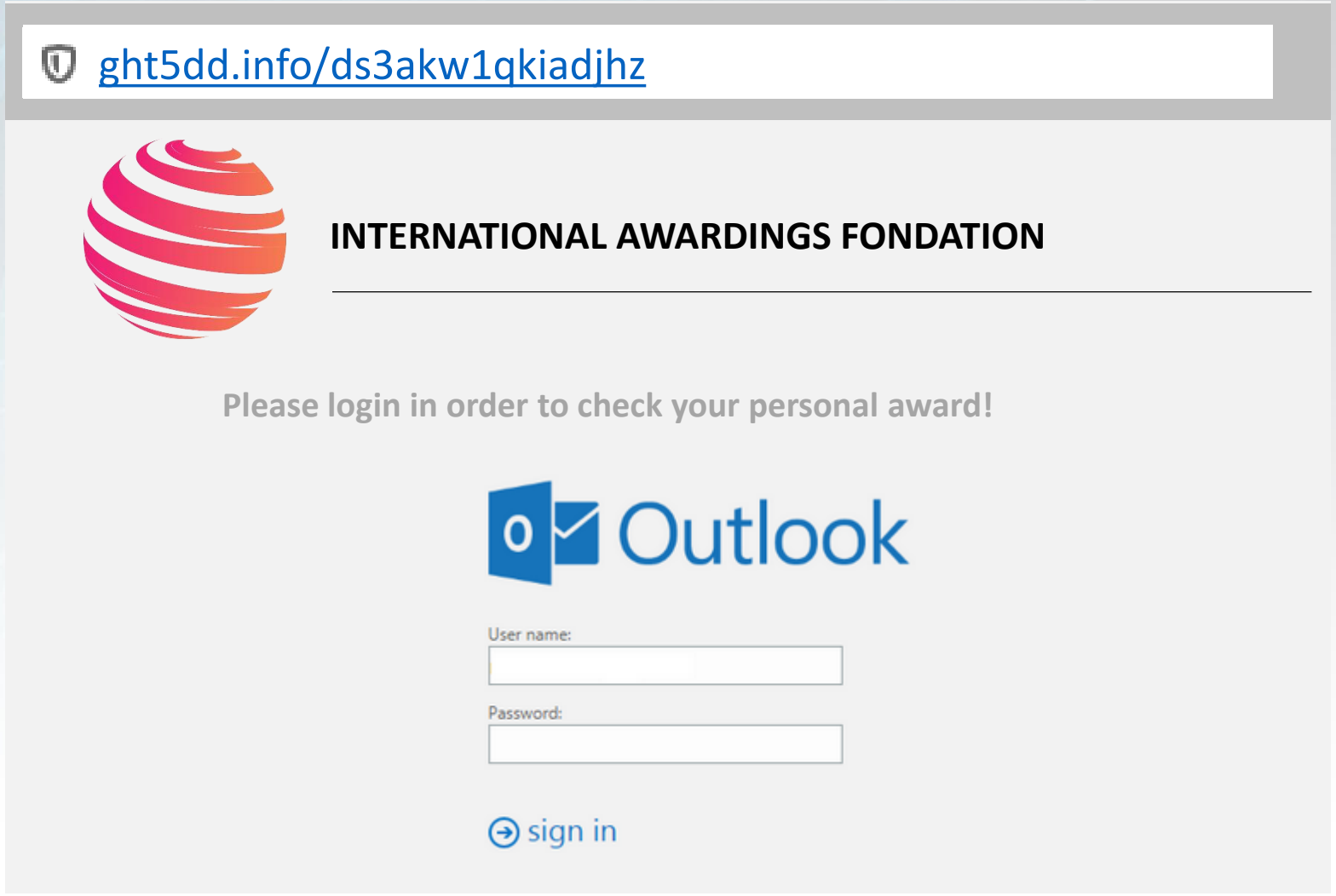
Credit Card Number

CSV Security Code

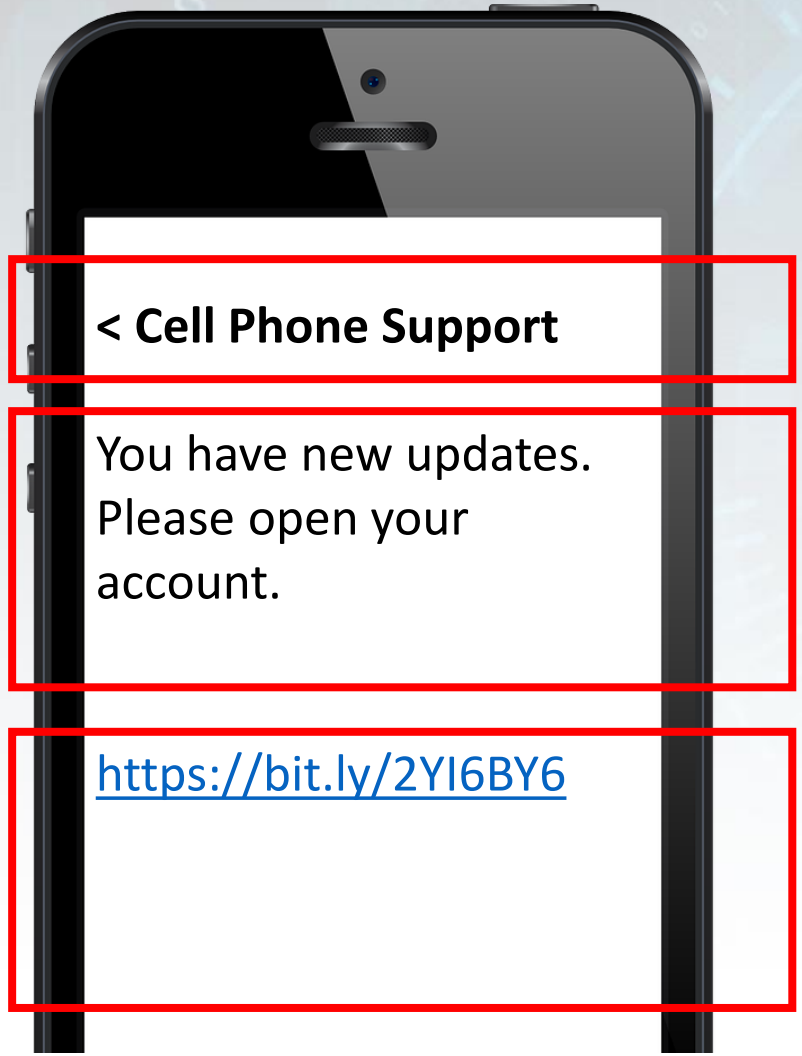
Update Your profile

Tekstisõnumid: Smishing näide

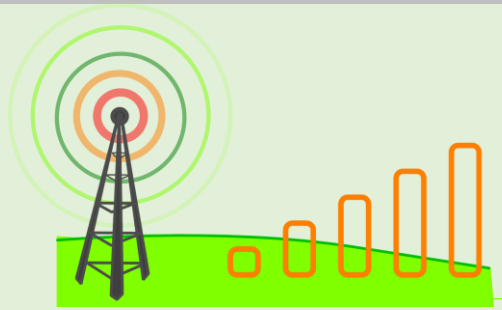




Tekstisõnumid: Smishing näide



https://bit.ly/2YI6BY6



Please provide login details in order to see updates dashboard

Username

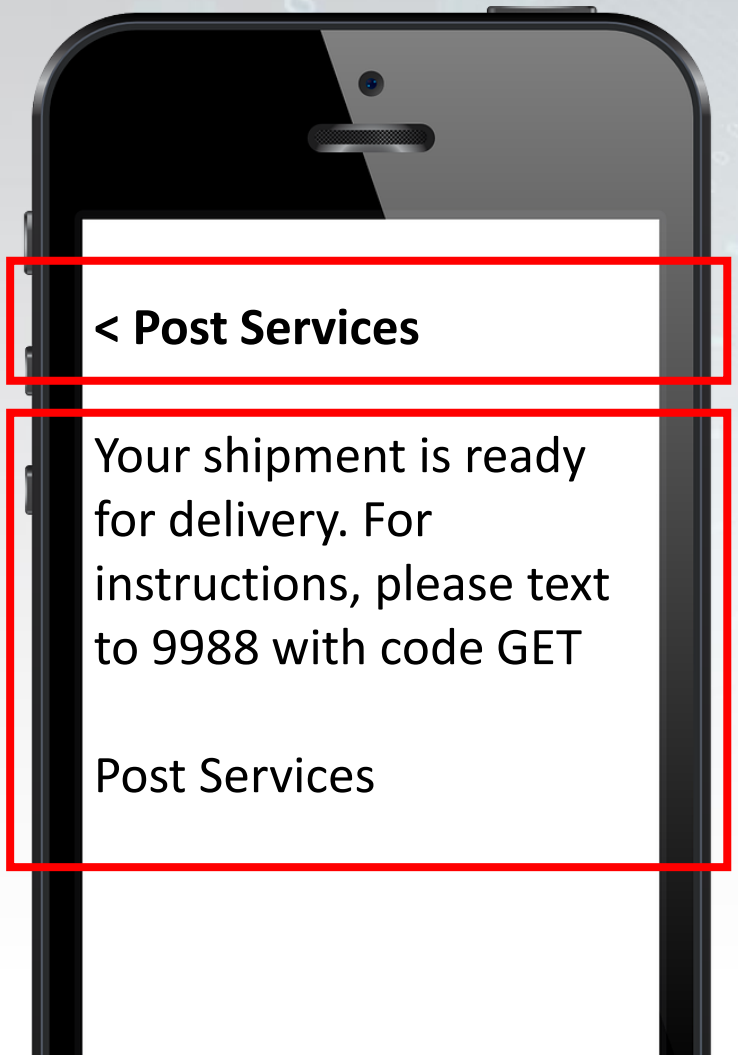
Password

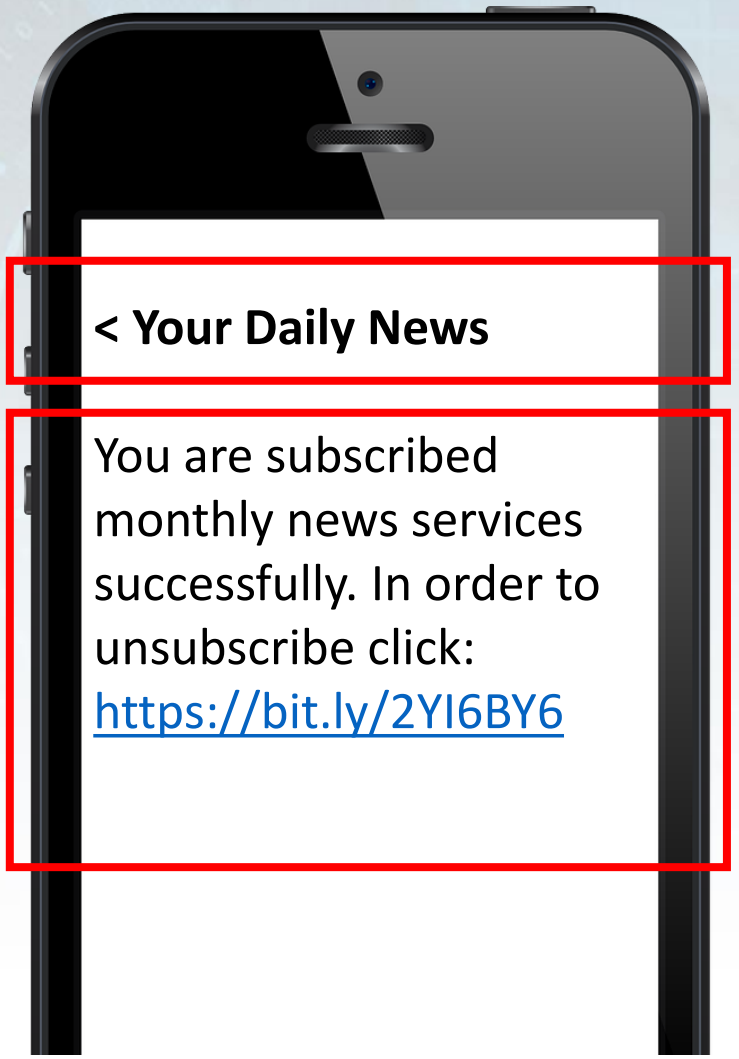
Please update your payment details

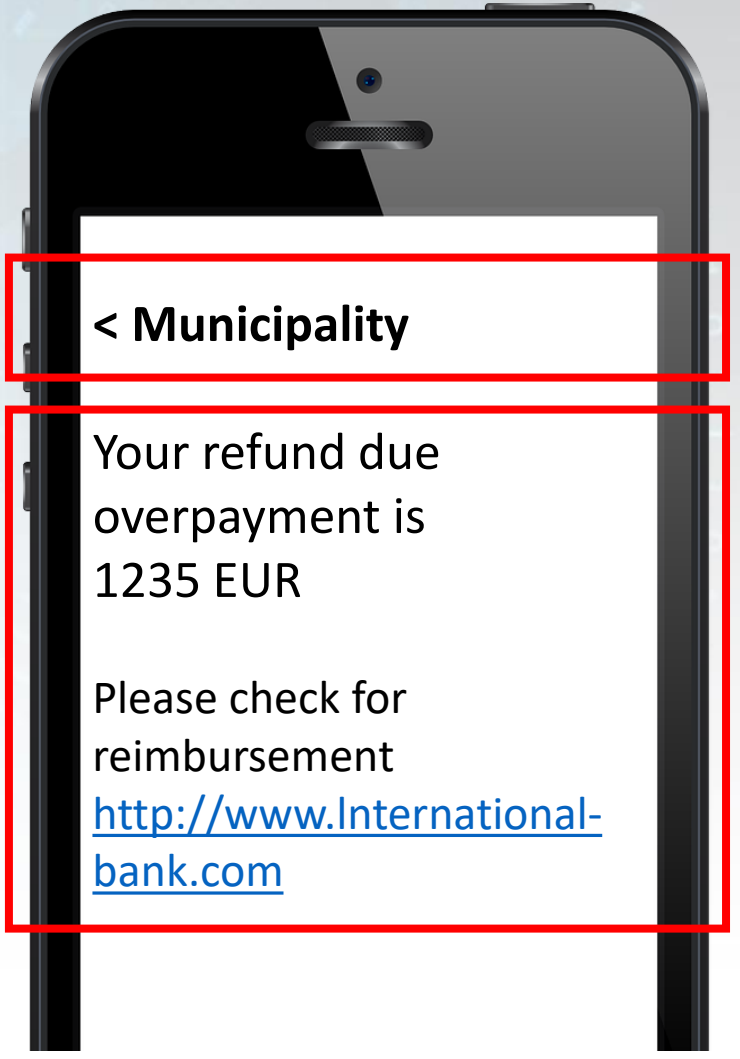
Credit Card Number

CSV Security Code

Tekstisõnumid: Smishing näide

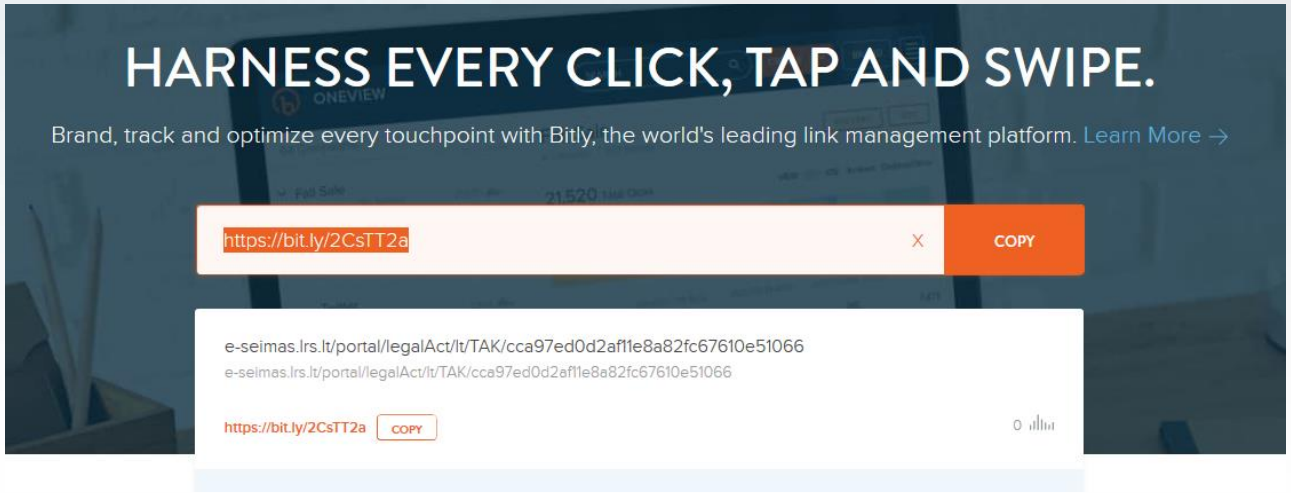






URL-i lühendamise teenused

- URL-i lühendamisteenuseid kasutatakse laialdaselt. Näited sellistest teenustest:
  - Bitly
  - youtu.be
  - Rebrandly
  - TinyURL
  - BL.INK
  - URL Shortener by Zapier
  - Shorby
  - Short.io



CyberPhish
Safeguarding your digital future

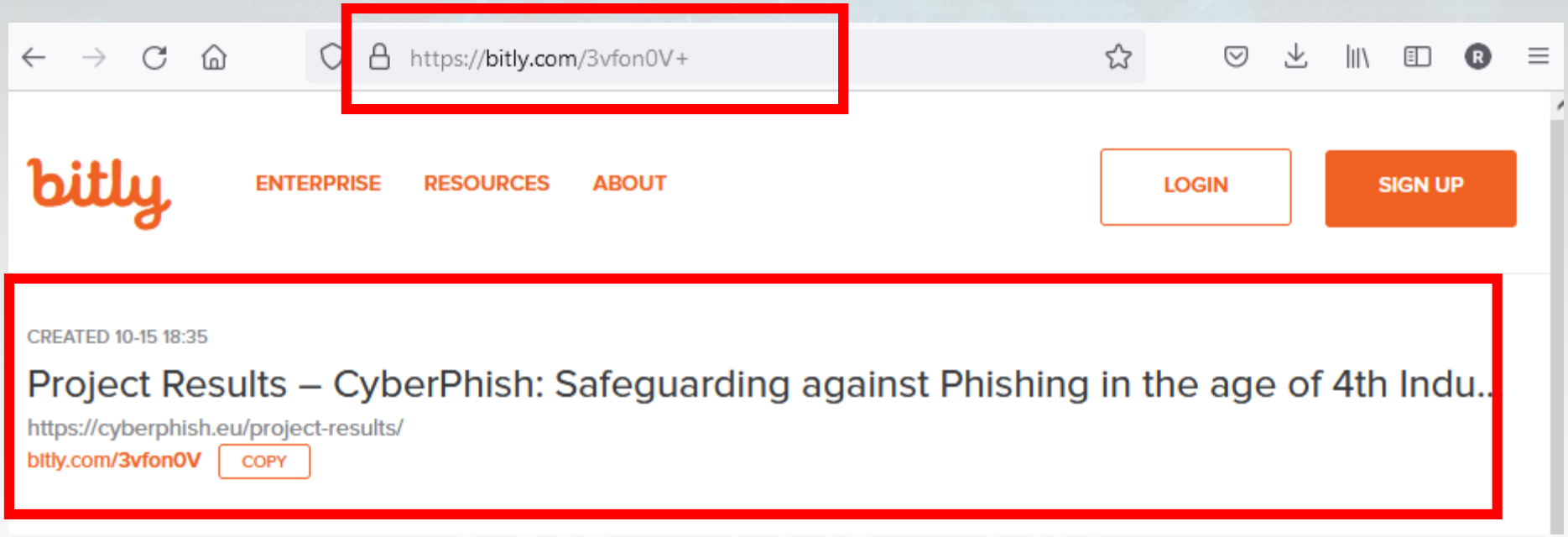
Funded by the Erasmus+ Programme of the European Union

URL-i lühendamisteenuste kasutamise eesmärgid

- Pikka URL-i on raske meelde jätta
- Mugav kasutamine veebisaitidel, sotsiaalmeedias, trükiväljaannetes
- Lühike URL on mugav SMS-ide, kiirsõnumite saatmisega
- On lühendamisteenuste pakkujaid, kes saavad luua inimloetavaid URL-e

Funded by the Erasmus+ Programme of the European Union

Kontrollige bit.ly linki: lingi lõppu saate kirjutada +



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kontrollige teavet veebisaidi kohta

http://checkshorturl.com

Get long URL from hundreds of URL shortening services

Ensure your safety and prevent unsuitable content while surfing on the World Wide Web

https://bitly.com/3vfon0V | Expand

Long URL	https://cyberphish.eu/project-results/
Delay	0.96 second(s)
Short URL	https://bitly.com/3vfon0V
Redirection	301
Search long URL on	Yahoo | Google | Bing
Check if safe on	Web Of Trust | SiteAdvisor | Google | Sucuri | Norton
Title	Project Results – CyberPhish: Safeguarding against Phishing in the age of 4th Industrial Revolution
Description	N/A
Keywords	N/A
Author	N/A

Kontrollige teavet veebisaidi kohta

- http://www.getlinkinfo.com: Tehke kindlaks, kas veebisait sisaldab ründetarkvara või on tuntud andmepüügisait

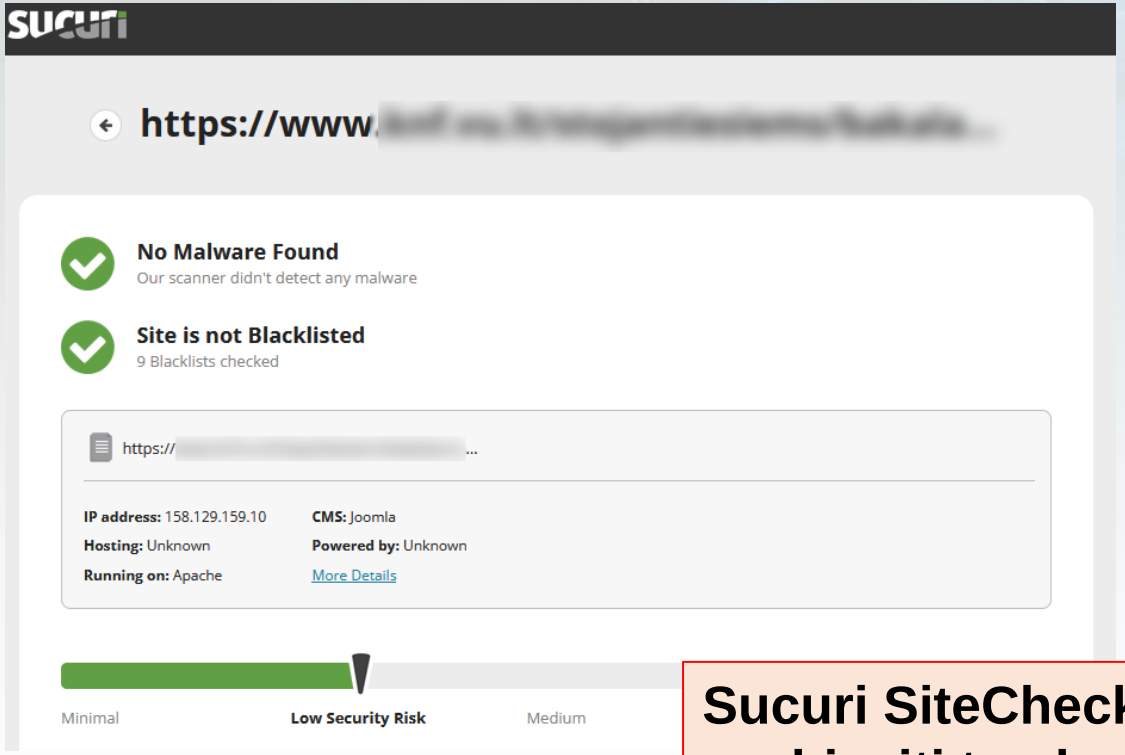
CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

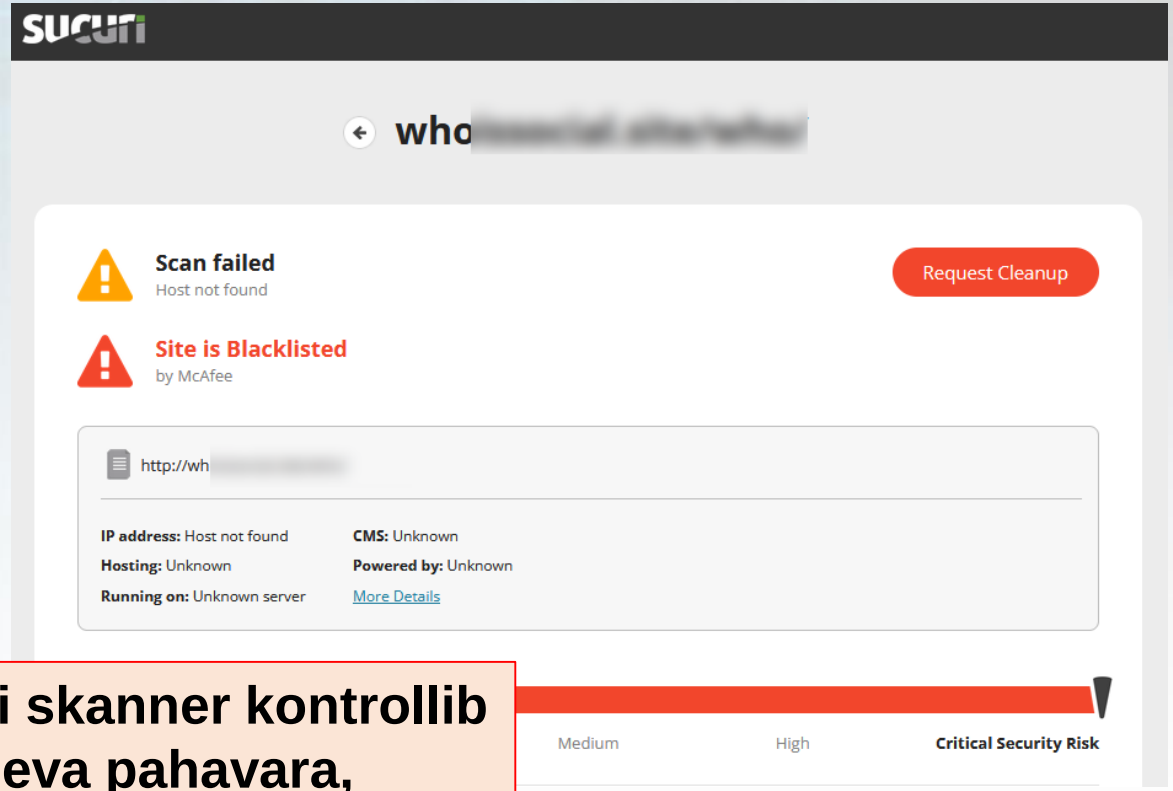
Kontrollige teavet veebisaidi kohta

https://sitecheck.sucuri.net

Turvaline skannitud veebisait



Ebaturvaliselt skannitud veebisait



Sucuri SiteChecki skanner kontrollib veebisaiti teadaoleva pahavara, viiruste, mustas nimekirja oleku, veebisaidi vigade, aegunud tarkvara ja pahatahtliku koodi suhtes.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Teemad:

Sündmuspõhine rünnak	E-mail	Tekstisõnum	Veebisait
Loterii pettus	Telefonikõne	Näost näkku	Üle-õla vaatamine

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Veebisaitide õngitsemine

- Veebisaitide andmepüüki nimetatakse ka võltsimiseks
- Veebisaitidel kasutavat andmepüüki on mitut tüüpi:
  - **Võltsitud URL-iga võltsveebisaidid –** väga tuntud asutuste või organisatsioonide veebisaitide võltskoopiad, mida kasutajad usaldavad*
  - **Ise käitatavad veebisaidid –** petturid töötasid välja oma veebisaidid, nagu võltsveebipood, investeerimisportaalid*
  - **Tasuta hostimisteenused**
  - **Hüpikaknad veebisaitidel**
  - **Reklaamiplokid,** mida kasutatakse portaalides, isegi usaldusväärsetel veebisaitidel
- Võltsveebisaitide linke kasutatakse andmepüügimeilides, SMS-ides, kiirsõnumites, sotsiaalmeedias jne.
- Otsingumootor võib pakkuda ka linke ohtlikele veebisaitidele*

** www.uni-mannheim.de/en/information-security/security-tips/spam-and-phishing/examples-and-current-warnings/#c230018*

Veebisaitide õngitsemine

- võltsveebisaitide peamised eesmärgid:
  - Hankida infosüsteemidesse sisselogimismandaate, meilid
  - Hankida finantsteavet, nagu pangakaardi andmed ja turvakoodid
  - Nakatada kasutajate seadmeid, kuna veebisaidid võivad sisaldada pahatahtlikku koodi
- Petturid võivad veebilehe seaduslikuks muutmiseks kasutada sarnaseid domeeninimesid, tavaliselt asendades domeeninimes ühe või mitu tähte, näiteks kasutada tähte „i” asemel l; näide:
  - Originaal veebileht www.website.eu
  - Pahalase veebileht www.webslte.eu

More about HTTPS:
https://www.cloudflare.com/learning/ssl/what-is-https
https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/

Funded by the Erasmus+ Programme of the European Union

Veebisaitide õngitsemine

- Võltsveebisaidid kasutavad sama kujundust, logosid ja värve nagu seaduslikud veebisaidid, mistõttu on neid raske ära tunda. Seetõttu tuleks kontrollida muid indikaatoreid, nt:
  - URL-aadress,
  - Kontaktandmed,
  - Olge mandaatide või finantsandmete esitamisel ettevaatlik, kui avate meilist lingi.

Funded by the Erasmus+ Programme of the European Union

Võlts veebisaidi aadress

- Võltsveebisaitide URL algab tavaliselt HTTP-ga
- Võltsveebisaidid võivad samuti alata HTTPS-iga
- HTTPS kasutab SSL-sertifikaati, kontrollib veebisaidi omandiõigust ja hoiab kasutajaandmeid turvalisena: tagab turvalise andmeedastuse kliendi ja serveri vahel, kuid ei näita veebisaidi legitiimsust.

More about HTTPS:
https://www.cloudflare.com/learning/ssl/what-is-https
https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/

Funded by the Erasmus+ Programme of the European Union

Veebisaitide õngitsemine

- **Miks seda tüüpi rünnak on edukas?** Võltsveebisaite on raske eristada päris veebisaitidest, kasutatakse muid andmepüügitegureid, et innustada kasutajaid veebisaite avama, teatud toiminguid tegema.
- **Sihtrühm:** kõik inimesed
- **Ründe meetod:** emails, SMS, instant messages, social media posts, combined methods.
- **Taktika:**
  - Meil või sõnum koos lingiga. Sõnumid paluvad uuendada kontot, muuta seadeid, avada dokumente või pilte, soovitada häid allahindlusi jne.
  - Võltsveebisaite leiavad kasutajad otsingumootori abil: tegemist võib olla heade allahindlustega veebipoe kaupadega
  - Petturid võivad helistada ohvritele ja kutsuda neid üles tegema edukaid investeeringuid

- **Tunnused:**
  - **Inspireeriv kiireloomulisuse tunne**
  - **Inspireeriv hirmutunne**
  - **Sisendab ahnust**
  - **Naiivsuse ärakasutamine**
- **Ohvrid:**
  - kodanikud, kellel on andmepüügist piiratud või igasugused teadmised ja keda ei eeldata andmepüügiks
- **Tulemus:**
  - Nakatunud digiseadmed, identiteedivargus, volikirjade vargus, raha kaotamine

Funded by the Erasmus+ Programme of the European Union

Veebisaidi õngitsemine: andmepüügiveebisaidi näide

http://sale-branding.store

Safe online shopping

BEST PRICES! ALL BRAND IN ONE PLACE WITH 90% DISCOUNT ONLY TODAY!

Funded by the Erasmus+ Programme of the European Union

Veebisaidi õngitsemine: andmepüügiveebisaidi näide

CyberPhish

http://mobile-company.online/prizes

CONGRATULATIONS!
Our company celebrates its anniversary this year, therefore we share the joy with our customers and invite you to collect your prize absolutely free.

Win one of the following prizes:
Samsung Galaxy S21, Apple iPhone 13 Pro or Samsung Watch 4 LTE.

153 participants are already enjoying their prizes. The number of prizes is limited!

Time reserved for you: 1 min. 29 seconds.

I WANT TO RECEIVE MY PRIZE!

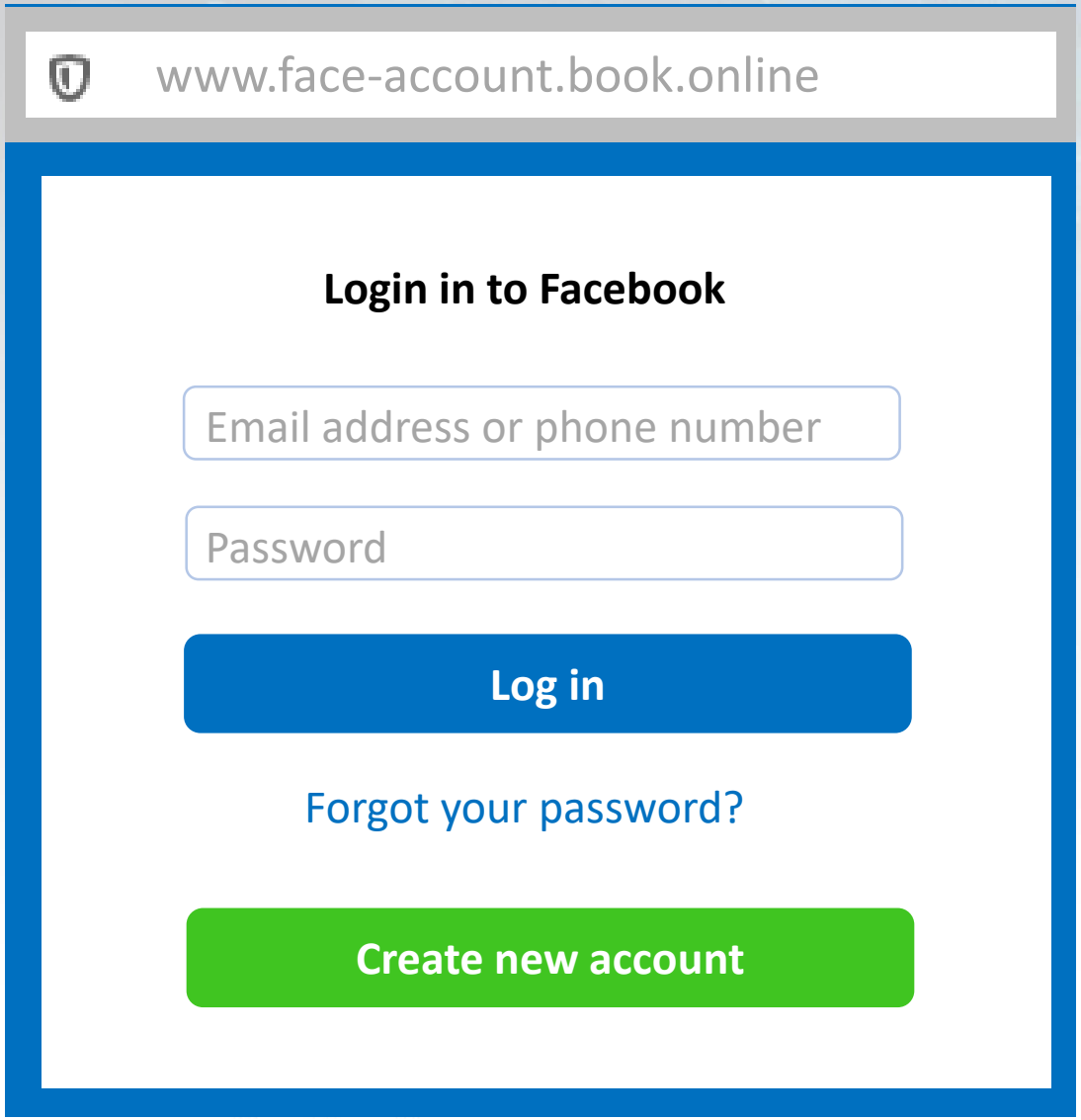
http://mobile-company.online/iwantget

Samsung Galaxy S21
Price: 780 Eur
Out of stock
Not available

Apple iPhone 13 Pro
Price: 920 Eur
Only 2 items available
Get now!

Samsung Watch 4 LTE
Price: 320 Eur
Out of stock
Not available

Veebisaidi õngitsemine: andmepüügiveebisaidi näide



Funded by the Erasmus+ Programme of the European Union

Teemad:

Sündmuspõhine rünnak	E-mail	Tekstisõnum	Veebisait
Loterii pettus	Telefonikõne	Näost näkku	Üle-õla vaatamine

Funded by the Erasmus+ Programme of the European Union

Loterii pettused - *Lotteries Scams*

- Loteriipetturid kasutavad oma ohvrite tabamiseks erinevaid vahendeid:
  - Meil
  - SMS või sõnumid kiirsuhtlusprogrammide kaudu
  - Sotsiaalmeedia postitus võlts- või häkitud kontolt
  - Helista telefoni teel
  - Veebilehed
- Ohvritele on mõeldud tohutu rahasumma, suur auhind, näiteks autod, digiseadmed või muud kallid kaubad
- Nad võivad tutvustada seadusliku loterii, agentide või abi vajava pärijana.

Funded by the Erasmus+ Programme of the European Union

Loterii pettused - *Lotteries Scams*

- Peamised märgid, mis viitavad loteriipettustele*
  - Peate esitama isiku- ja finantsteabe
  - Kui petturid nõuavad võiduvõimaluste suurendamiseks maksta teatud summa raha
  - Auhinna saamiseks peate maksma teatud tasu
- Loteriipetturid ootavad isiku- ja finantsteabe hankimist või nippi raha saatmiseks, nagu tasud, maksud, saatmislaadija, valuutade ebakõlad või raha muude kulude katteks, auhinna saamiseks kinkekaartidega maksmine jne.
- Nad võivad paluda sooritada teatud toiminguid ja mitte avaldada mõnda aega teavet võidu kohta, st hoida seda saladuses.

* www.consumer.ftc.gov/articles/fake-prize-sweepstakes-and-lottery-scams

Funded by the Erasmus+ Programme of the European Union

Loterii pettused - *Lotteries Scamming*

- **Miks seda tüüpi rünnak on edukas?** Võltsveebisaite on raske eristada päris veebisaitidest, kasutatakse muid andmepüügitegureid, et innustada kasutajaid veebisaite avama, teatud toiminguid tegema.
- **Sihtrühm:** kõik inimesed
- **Rünnaku meetod:** meilid, SMS-id, kiirsõnumid, sotsiaalmeedia postitused, kombineeritud meetodid.
- **Taktika:**
  - Meil või sõnum koos lingiga. Sõnumid paluvad uuendada kontot, muuta seadeid, avada dokumente või pilte, soovitada häid allahindlusi jne.
  - Võltsveebisaite leiavad kasutajad otsingumootori abil: tegemist võib olla heade allahindlustega veebipoe kaupadega
  - Petturid võivad helistada ohvritele ja kutsuda neid üles tegema edukaid investeeringuid

- **Tunnused:**
  - **Inspireeriv kiireloomulisuse tunne**
  - **Inspireeriv hirmutunne**
  - **Sisendab ahnust**
  - **Naiivsuse ärakasutamine**
- **Ohvrid:**
  - kodanikud, kellel on andmepüügist piiratud või puuduvad igasugused teadmised ja keda ei peeta andmepüügi sihtrühmaks
- **Tulemus:**
  - Nakatunud digiseadmed, identiteedivargus, volikirjade vargus, raha kaotamine

Funded by the Erasmus+ Programme of the European Union

Näide: Loterii pettused

Saatja: National lottery<jim-*Stanley*@info-winlottery.online>

Saaja: me
Pealkiri: Congratulations!

Dear user,

we would like inform that your email was selected to claim the sum of 150.000 EUR.

In order to get your money please follow attached instructions.

National lottery team
CEO Jim Stanley

Instructions-for-winners.pdf

Muud loterii näited on toodud järgmistel slaididel:

- Email section
- Instant messaging slide
- SMSishing slide
- Website phishing section

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Teemad:

Sündmuspõhine rünnak	E-mail	Tekstisõnum	Veebisait
Loterii pettus	Telefonikõne	Näost näkku	Üle-õla vaatamine

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Telefonikõned: telefonkalastus (*Vishing*)

- Vishingut võib seletada häälega andmepüügina
- Ründajad kasutavad läbitöötatud stsenaariume ja juhtnööre, et võita ohvrite enesekindlus
- Vishingut saab kombineerida teiste sotsiaalse ründe meetoditega
- Mõnikord võib ründaja enne ohvrile helistamist uurida tausta, et saada rohkem enesekindlust.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Telefoni kõned: Vishing

- **Miks seda tüüpi rünnak on edukas?** Võltskõnesid tegelikest kõnedest on raske eristada. Ründaja esindab end teise isikuna või juriidilise institutsiooni, näiteks politsei või panga esindajana, ja ei kasuta muid tehnilisi vahendeid peale telefoni, kasutab manipulatsioone, kasutab tundliku teabe saamiseks ära inimeste hirme, autoriteeti või soove.
- **Sihtrühm:** kõik inimesed
- **Rünnaku meetod:** kõned telefoni teel, kõned kiirsuhtlusprogrammide kaudu, nagu Viber. Ründajad võivad kombineerida muid tehnikaid, näiteks võltsitud veebisaite.
- **Telefonikalastuse taktikad:**
  - Juriidilise organisatsiooni töötajana esinev pettur helistab tavaliselt ohvrile ja pakub investeerimisvõimalusi; petturid võivad teeselda politsei esindajana, hirmutada ohvrit tema kontol olevate finantsmahhinatsioonidega, et pääseda ligi ohvri pangakontole.
- **Tunnused:**
  - **Inspireeriv kiireloomulisuse tunne**
  - **Inspireeriv hirmutunne**
  - **Sisendab ahnust**
  - **Naiivsuse ärakasutamine**
- **Ohvrid:**
  - kodanikud, kellel on piiratud või puuduvad teadmised vishingust
- **Tulemus:**
  - Raka kaotus, info leke

Funded by the Erasmus+ Programme of the European Union

Teemad:

Sündmuspõhine rünnak	E-mail	Tekstisõnum	Veebisait
Loterii pettus	Telefonikõne	Näost näkku	Üle-õla vaatamine

Funded by the Erasmus+ Programme of the European Union

Näost näkku: kannul sisenemine - Tailgating

- Kannul sisenemine, mida nimetatakse ka "piggybacking", kasutatakse siis, kui küberkurjategija kasutab ära ettevõtte töötajaid, et pääseda organisatsiooni piiratud ruumidesse. Juurdepääs piirangualale on lubatud ainult selleks volitatud töötajatel

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Näost näkku: kannul sisenemine - Tailgating

- **Miks seda tüüpi rünnak on edukas?** Suurtes organisatsioonides ei pruugi töötajad teisi kolleege tunda, inimesed usaldavad võõraid inimesi.
- **Sihtrühm:** organisatsioonide töötajad
- **Rünnaku meetod:** ründaja võib esineda uue töötajana, teenusepakkujana, kauba kohaletoimetamise assistendina jne.
- **Kannul sisenemise taktikad:**
  - Küberkurjategijad lihtsalt petavad ja lollitavad ühte volitatud töötajat, järgnedes talle sissepääsu saamiseks.
  - Ründaja võis teeselda, et ta on kohaletoimetaja, kelle käes on mitu kasti, toidu kohaletoimetaja ja palub personalil uks avada.
  - Teine näide sellest rünnakust võib olla ettevõtte töötajana esinemine ja vestluse alustamine avalikes ettevõtete piirkondades, näiteks suitsetamisalades. Pärast vaheaega võis teeskleja minna valitud töötajaga koos vestlusele, järgnedes talle keelualale.

- **Tunnused:**
  - **Inspireeriv kiireloomulisuse tunne**
  - **Usaldust äratav**
  - **Naiivsuse ärakasutamine**
- **Ohvrid:**
  - töötajad, kelle teadmised tagaluugi tagamise kohta on piiratud või puuduvad
- **Tulemused:**
  - Kõrvaliste isikute sattumine piirangualale võib tekitada tohutuid kahjusid.
  - Kui kõrvaline inimene satub piirangualasse, võib ta sooritada rünnaku, näiteks andmete varguse, andmerikkumise, pahavara rünnakute jms.

Funded by the Erasmus+ Programme of the European Union

Teemad:

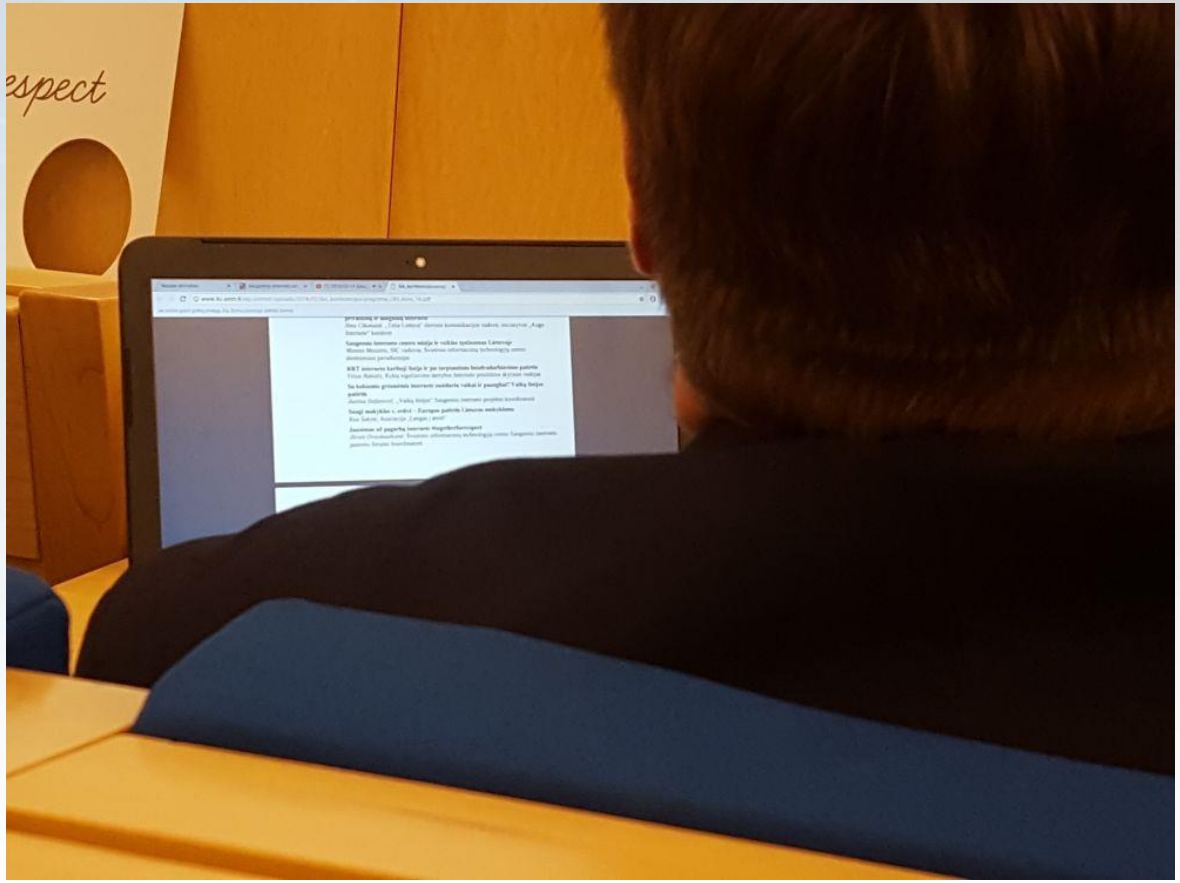
Sündmuspõhine rünnak	E-mail	Tekstisõnum	Veebisait
Loterii pettus	Telefonikõne	Näost näkku	Üle-õla vaatamine

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Üle õla vaatamine - Shoulder Surfing

- Õlas surfamine on tõhus viis kellegi arvuti, nutitelefoni või sularahaautomaadi ekraani jälgimiseks, et saada isiklikku sisselogimist süsteemiandmetesse, nagu sisselogimised ja paroolid, PIN-koodid või muu tundlik teave.
- Ründaja saab jälgida, seistes ekraani lähedal, kuulates suuliselt edastatud tundlikke andmeid või kasutada ka veebikaameraid vajalike andmete kogumiseks.



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Näost näkku: Üle õla vaatamine

- **Miks seda tüüpi rünnak on edukas?** Inimesed, kes tavaliselt töötavad sülearvutite ja nutiseadmetega avalikes kohtades, avalikel üritustel, ühistranspordis, ei mõtle sellele, et keegi võib tema ekraani vaadata, ega mõtle selle tagajärgedele.
- **Sihtrühm:** kõik inimesed
- **Rünnaku meetod ja taktika:** ründaja võib teeselda, et on tavaline inimene, kes istub või seisab ohvri kõrval, kuid tegelikult jälgib ta ohvri ekraani ja kogub tundlikke kasutajaandmeid. Kahtluste äratamise vältimiseks võivad petturid kasutada veebikaameraid.
- **Tunnused:**
  - **eesmärk on äratada usaldust**
- **Haavatavused:**
  - kodanikud, kellel on üle õla vaatamisega seotud teadmised on piiratud või üldse puuduvad
- **Tulemus:**
  - varastatud isiklik sisselogimine süsteemiandmetesse, nagu sisselogimised ja paroolid, PIN-koodid või muu tundlik teave.

Funded by the Erasmus+ Programme of the European Union

Kokkuvõte: Andmepüügiründed

Sündmusp õhine rünnak	E-mail	SMS	Tekstisõnum
Sotsiaal-võrgustik	Veebisait	Loterii pettus	Telefonikõne
	Näost näkku	Üle-õla vaatamine	

Petturid ja ründajad täiustavad pidevalt oma kasutatud tehnikaid või kasutavad tehnikate kombinatsiooni

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

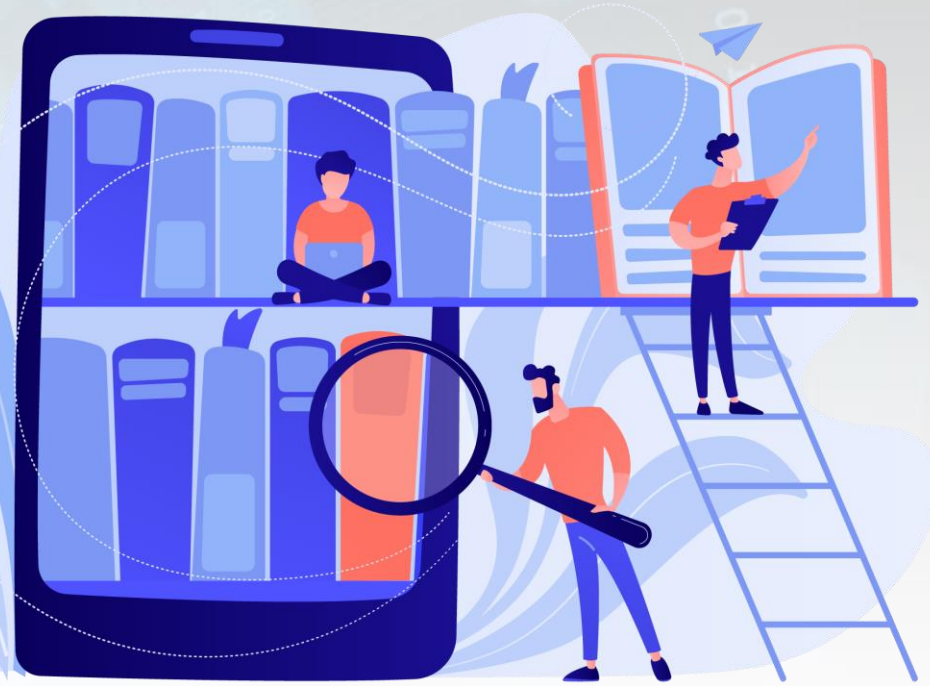
Ülesanded

- Arutage, millist tüüpi andmepüügirünnakuid teate
- Kas olete kunagi seisnud silmitsi andmepüügirünnakuga? Mis tüüpi see oli?
- Mis te arvate, milline andmepüügirünnak on kõige populaarsem?
- Millised võivad olla eduka andmepüügirünnaku tagajärjed?
- Loetlege vähemalt neli erinevat andmepüügi tunnust.

Funded by the Erasmus+ Programme of the European Union

Lisalugemine

- **Christopher Hadnagy** (2018). Social Engineering: The Science of Hu man Hacking 2nd Edition.
- **Erdal Ozkaya** (2018).Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert.
- **Martinez, Claudia**. Defending Against the $5B Cybersecurity Threat - Business Email Compromise. Cisco Blogs available at *https://blogs.cisco.com/security/defending-against-the-5b-cybersecurity-threat-business-email-compromise*
- **Tusan, Christina**. *Fake emails could cost you thousands*. US Federal Trade Commission available at *https://www.consumer.ftc.gov/blog/2017/05/fake-emails-could-cost-you-thousands*
- **US-CERT.** Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks. US Department of Homeland Security available at *https://www.us-cert.gov/ncas/tips/ST04-014*



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Lühivideod

- What is phishing? Learn how this attack works
  https://youtu.be/Y7zNlEMDml4
- What Is A Phishing Attack? And How To Avoid It
  https://youtu.be/j3nE8JQATXo
- Learn how to spot phishing and spam email
  https://youtu.be/AmPX4DdBz-k
- What is Spear Phishing | Difference from Phishing and Whaling
  https://youtu.be/JzoJeJBdhuI
- What is smishing? How phishing via text message works
  https://youtu.be/ZOZGQeG8avQ
- What is vishing? Understanding this high-tech phone scam
  https://youtu.be/DysFLnOf4Nw
- What Should I do if I Accidentally Click on a Phishing Link?
  https://youtu.be/d21-z8wsO7c

Thank you!

Resources of pictures used in the presentation from:

- www.pixabay.com
- Personal archives

Screenshots made from websites