Funded by the
Erasmus+ Programme
of the European Union

Kibernetinės atakos: Socialinė inžinerija ir sukčiavimas

Atvejų analizė

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

Mokymosi tikslai

Paaiškinti skirtingus sukčiavimo atakų metodus ir išmokti juos atpažinti

Studento darbo krūvis

Paskaita	1,5 val.
Garso ir vaizdo medžiaga	0,5 val.
Panaudojimo atvejai	4,5 val.
Papildomi skaitiniai	0,5 val.
Pasiruošimas atsiskaitymui	2 val.

Turinys

- Valetos bankas
- Kipro paštas
- Smart-ID
- Asmens duomenų nutekėjimas
- Emotet kenkėjiškas programinis kodas
- Sukčiavimo (angl. phishing) atakos simuliacija

Funded by the
Erasmus+ Programme
of the European Union

Turinys

- **Valetos bankas**
- Kipro paštas
- Smart-ID
- Asmens duomenų nutekėjimas
- Emotet kenkėjiškas programinis kodas
- Sukčiavimo (angl. phishing) atakos

Aptarkite, kaip saugumo rizika gali pakenkti infrastruktūrai ir paveikti žmonių gyvenimą

Funded by the Erasmus+ Programme of the European Union

Valetos bankas

Atvejo aprašymas

Programišiai įsilaužę į Valetos banką pervedė į užsienio sąskaitas 13 mln. eurų. Siekdamas sustabdyti ataką bankas nutraukė bankomatų, pranešimų sistemų, mobiliosios bankininkystės paslaugas ir savo filialų darbą. Daug banko klientų kelioms valandoms ar net kelioms dienoms prarado prieigą prie savo sąskaitų. Žmonės liko be pinigų ir negalėjo nusipirkti net ir kasdienių prekių.

Valetos bankas

Atvejo aprašymas

- Į užsienio sąskaitas buvo pervėsti pinigai
- Bankas susekė apgaulingas operacijas ir jas atšaukė
- Ataka buvo surengta užsienyje
- Siekdamas užkardyti išpuolį bankas glaudžiai bendradarbiavo su tarptautine policija
- HSBC teigė, kad jų paslaugos veikė sklandžiai
- Buvo užblokuoti mokėjimai į keturias šalis
- Įsilaužėliai bandė siųsti lėšas į Jungtinę Karalystę, JAV, Čekiją ir Honkongą, bankas įspėjo ministrą pirmininką ir pradėjo atvirkštines operacijas
- Maltos finansinių paslaugų institucija (MFSA) atidžiai sekė situaciją
- Parduotuvės negalėjo aptarnauti klientų

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

Funded by the Erasmus+ Programme of the European Union

Klausimai diskusijoms

- Ko galima pasimokyti iš šios atakos?

  Kalbant apie

  - *saugomą turtą*
  - *riziką*
  - *rizikos poveikį*

- Kaip būtumėte pasielgė būdami?
  - *Banko klientu*
  - *Banko vadybininku*
  - *Sistemų administratoriumi*

Klausimai diskusijoms

- Kaip būtų galima išvengti šių situacijų?
  - *Įsilaužimo į banką*
  - *Krizės po incidento*
- Jei būtumėte banko vadovas:
  - *Kaip būtumėte suvaldęs/nuraminęs situaciją?*
  - *Kaip atgautumėte prarastus pinigus ir banko reputaciją?*

Funded by the Erasmus+ Programme of the European Union

Turinys

- Valetos bankas
- **Kipro paštas**
- Smart-ID
- Asmens duomenų nutekėjimas
- Emotet kenkėjiškas programinis kodas
- Sukčiavimo (angl. phishing) atakos

Aptarkite įtikinėjimo principus ir galimus veiksmus, kuriuos reiktų atlikti, siekiant sumažinti sukčiavimo atakų poveikį

Funded by the Erasmus+ Programme of the European Union

Atvejo aprašymas

- Kipro paštas yra strateginė, tiesiogiai Kipro vyriausybei pavaldi organizacija. Dauguma Kipro gyventojų naudojasi pašto paslaugomis, ypač siuntinių pristatymu (apsipirkimas internetu), kurių labai padaugėjo prasidėjus COVID-19 pandemijai.
- Tai jau ne pirmas kartas, kai sukčiai savo sukčiavimo objektu pasirenka Kipro paštą. Prieš tai, 2018 m., sukčiai pasinaudodami įvairiais medijos kanalais įskaitant Facebook, siuntė tekstines žinutes, teigdami, kad Kipro paštas atrinko žinutės gavėją ir jis turi galimybę laimėti prabangų mobilųjį telefoną. Žinutės įvairiais būdais klaidino gavėjus siekiant gauti prieigą prie asmeninių elektroninių paslaugų paskyrų ar teikiamų paslaugų, taip pat bandė pavogti ir kitokią asmeninę informaciją.

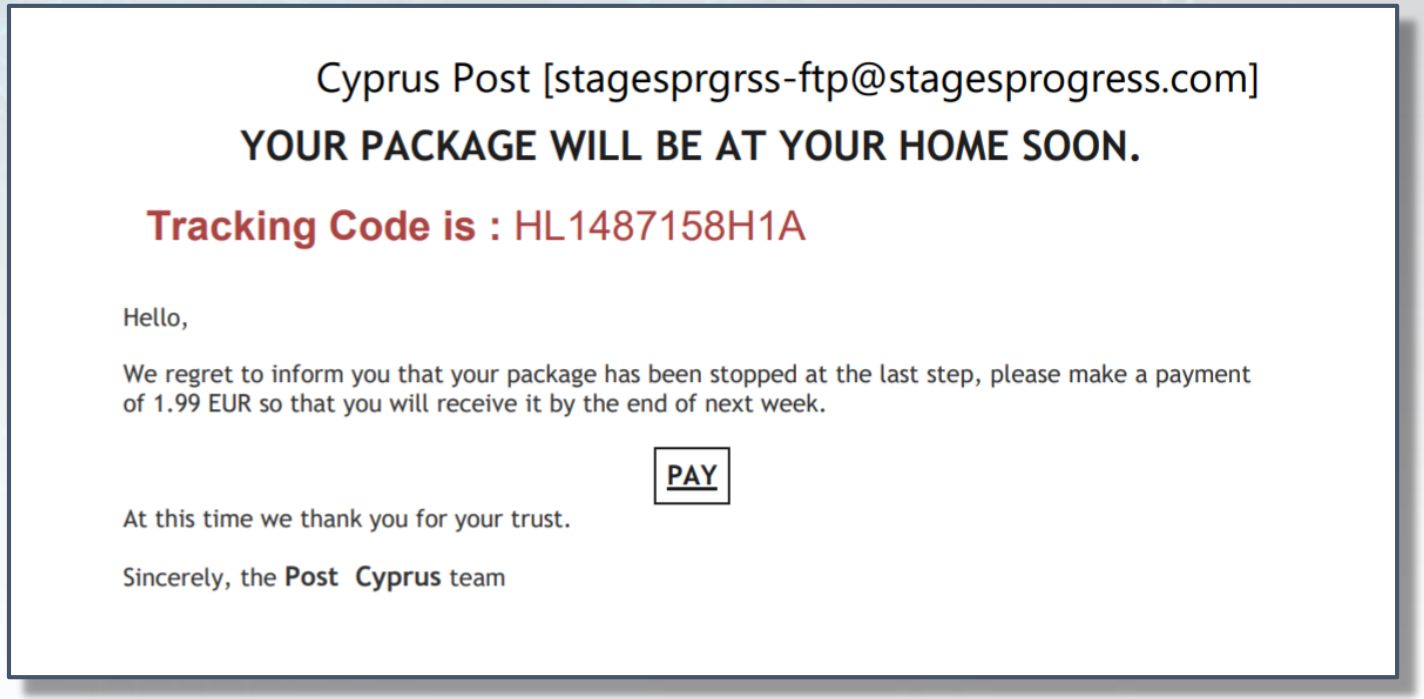
Funded by the Erasmus+ Programme of the European Union

Kipro paštas

Atvejo aprašymas

2018 m. sukčiavimo žinutė:

2021 m. sukčiavimo žinutė:



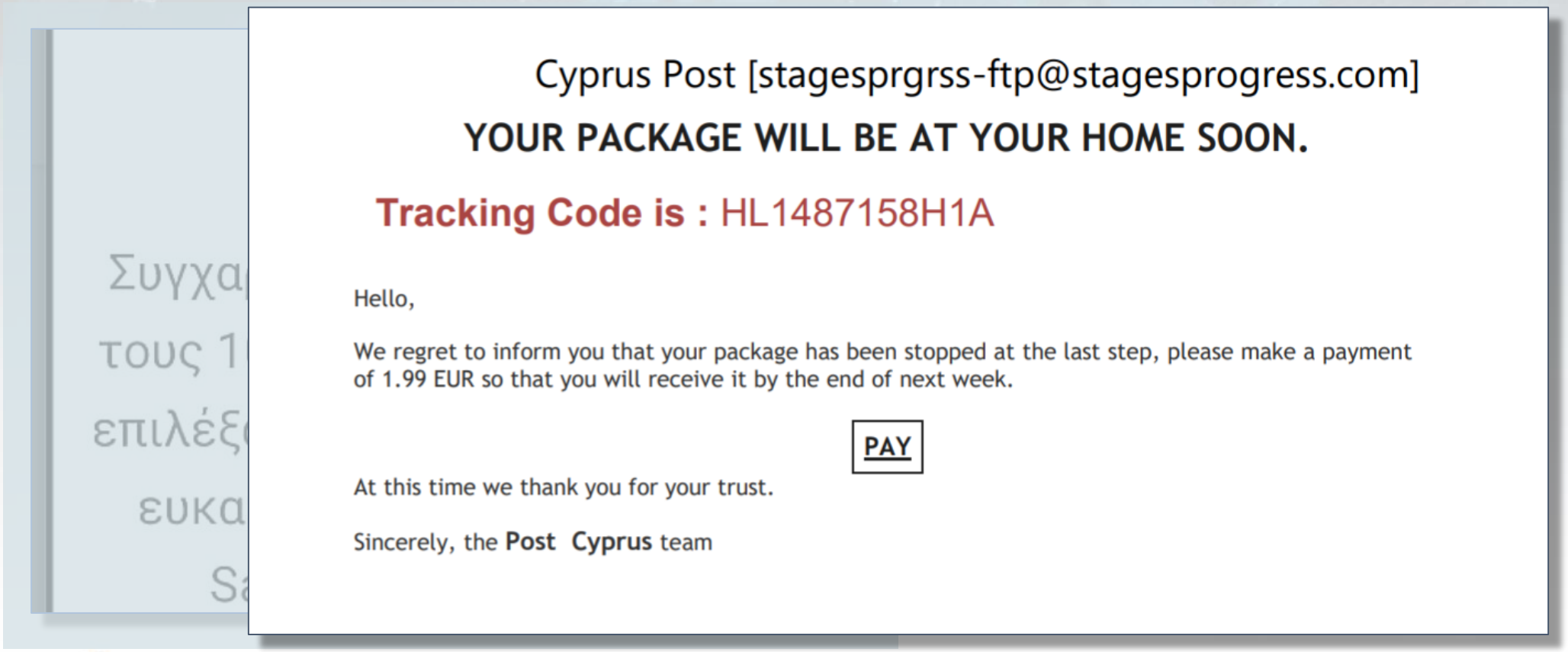
Kipro paštas įspėjo visuomenę, kad jo vardu elektroniniu paštu išplatintas suklastotas pranešimas prašanti susimokėti muito mokestį už gautą siuntinį.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kipro paštas

Atvejo aprašymas



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

Funded by the Erasmus+ Programme of the European Union

Klausimai diskusijoms

- Kokius įtikinėjimo principus galima pastebėti Kipro pašto atakose?
- Kodėl Kipro pašto atvejis turėtų būti laikomas sukčiavimo ataka?
- Kodėl sukčiai apsimeta esantys iš "žinomų" valdžios institucijų ir (arba) organizacijų?
- Kaip "žinomos" valdžios institucijos ir (arba) organizacijos pačios turėtų reaguoti į sukčiavimo atvejus?

Funded by the Erasmus+ Programme of the European Union

Turinys

- Valetos bankas
- Kipro paštas
- **Smart-ID**
- Asmens duomenų nutekėjimas
- Emotet kenkėjiškas programinis kodas
- Sukčiavimo (angl. phishing) atakos

Aptarkite, kaip grėsmės agentai naudoja šiuolaikinius autentifikavimo metodus, kad pakenktų saugomam turtui

Funded by the Erasmus+ Programme of the European Union

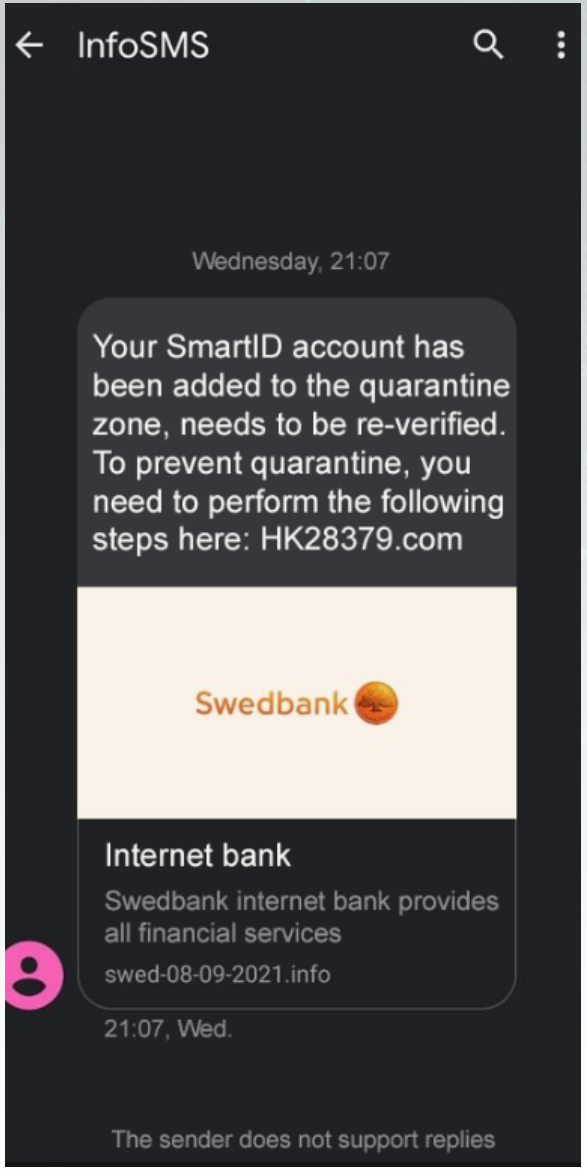
Atvejo aprašymas

Smart-ID yra lengviausias, saugiausias ir greičiausias būdas patvirtinti tapatybę internete, užsiregistruoti e. paslaugoms ir pasirašyti dokumentus. Smart-ID leidžia asmeniui saugiai ir patogiai prisijungti prie interneto ar mobiliojo banko ir kitų e. paslaugų naudojantis pageidaujamu išmaniuoju įrenginiu. Smart-ID nesusijęs su SIM kortelėmis ar mobiliojo ryšio operatoriais; reikia tik prieigos prie interneto.

https://www.smart-id.com

Funded by the Erasmus+ Programme of the European Union

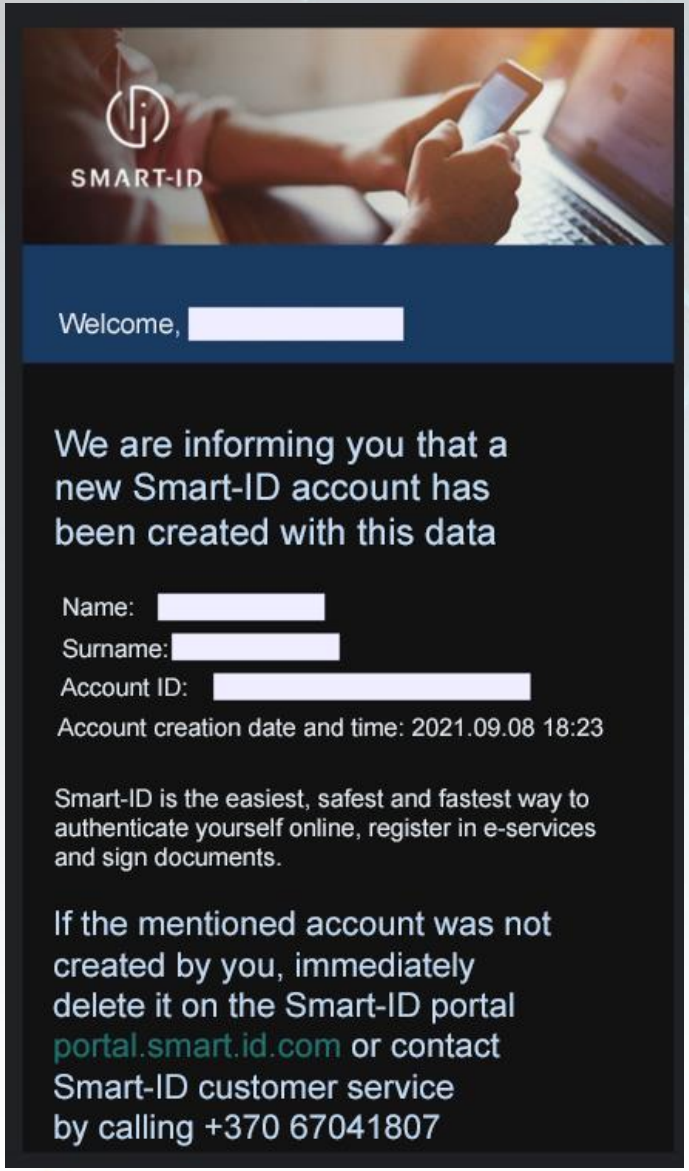
Atvejo aprašymas



2021 m. rugsėjį sukčiai Lietuvos piliečiams siuntė įvairaus turinio žinutes, kurių tikslas - atkreipti vartotojų dėmesį į tariamą jų asmeninių lėšų, "Smart-ID" ar internetinės bankininkystės paskyrų saugumą. Žinutėse prašoma spustelėti aktyvią interneto nuorodą ir pateikti asmeninius prisijungimo duomenis, kad būtų neutralizuota rizika.

Funded by the Erasmus+ Programme of the European Union

Atvejo aprašymas



Jei auka paspaudžia nuorodą, atidaroma suklastota svetainė, kurioje vartotojas turi pateikti asmeninę informaciją arba "aktyvuoti" paskyrą.

Klausimai diskusijoms

- Ar galima ir kaip saugius autentifikacijos įrankius panaudoti vagiant vartotojų pinigus?
- Kokių veiksmų reikėtų imtis gavus tokią žinutę?
- Įvardinkite požymius parodančius, kad tai sukčiavimo žinutė?
- Kokių veiksmų turėtume imtis, jei į mūsų paskyrą buvo įsilaužta?
- Ar įmanoma atgauti prarastus pinigus?
- Ko galima pasimokyti iš šios situacijos?

Funded by the Erasmus+ Programme of the European Union

Turinys

- Valetos bankas
- Kipro paštas
- Smart-ID
- **Asmens duomenų nutekėjimas**
- Emotet kenkėjiškas programinis kodas
- Sukčiavimo (angl. phishing) atakos

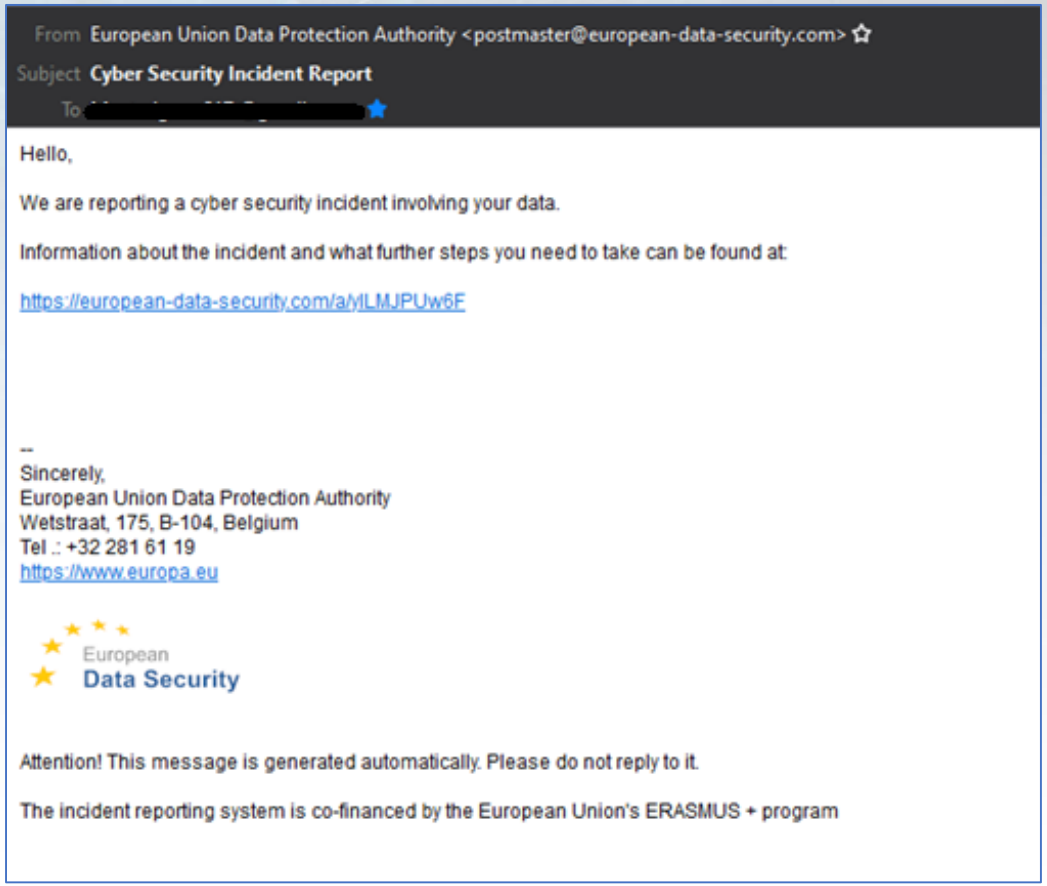
Aptarkite, kaip atpažinti suklastotus el. laiškus, kuriuose siūlomos įvairios paslaugos iš nepatikimų organizacijų

Funded by the Erasmus+ Programme of the European Union

Asmens duomenų nutekėjimas

Atvejo aprašymas

Per tris 2021 m. pavasario savaites Lietuvoje buvo paviešintos mažiausiai keturios didelės asmens duomenų vagystės. Šie įvykiai sukėlė didžiulį žiniasklaidos dėmesį ir daug diskusijų. Sukčiai pasinaudojo situacija ir išsiuntė suklastotus laiškus. Šiuose laiškuose gavėjai buvo raginami prisijungti prie neegzistuojančios organizacijos tinklalapio ir patikrinti, ar jų asmens duomenys nebuvo



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

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

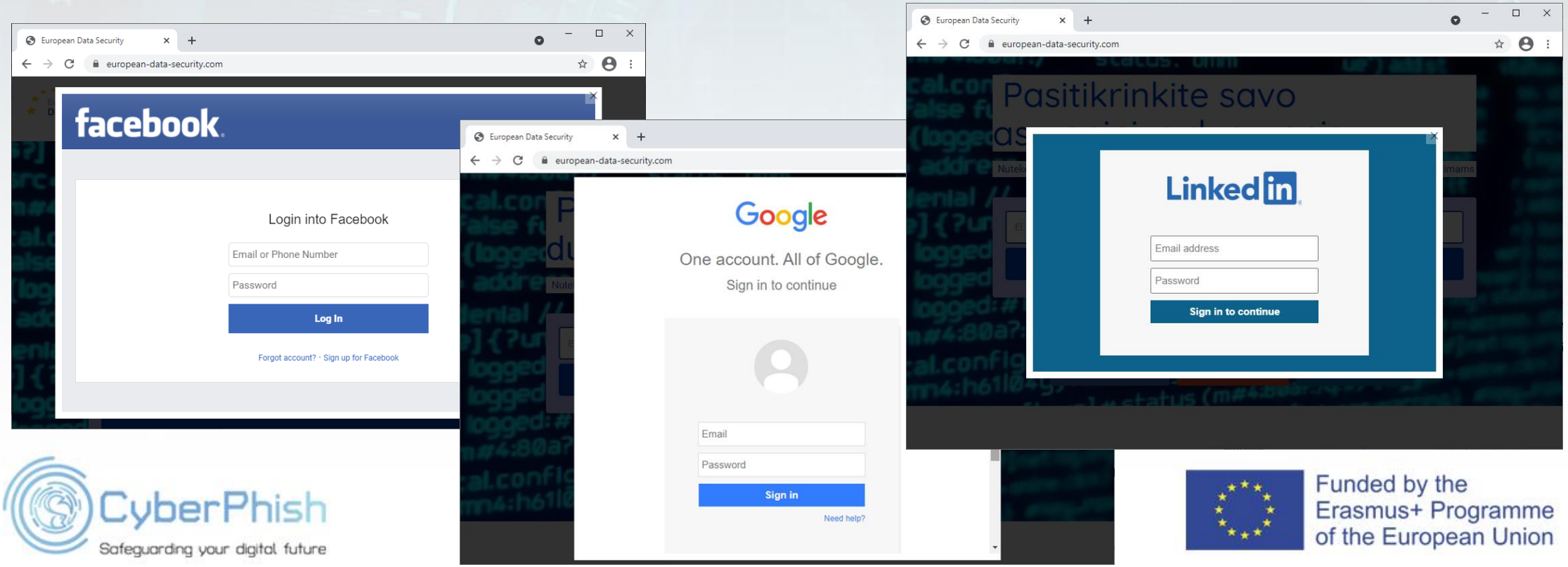
Asmens duomenų nutekėjimas

Atvejo aprašymas

Paspaudus nuorodą, auka būdavo nukreipiama į neegzistuojančios organizacijos tinklalapį. Šiame puslapyje aukos buvo prašoma prisijungti prie vieno iš socialinių tinklų

Atvejo aprašymas

Kai auka pasirinkdavo vieną iš paskyrų, atsidarydavo suklastoti prisijungimo langai. Šiuose languose įvesta informacija (pvz., prisijungimo duomenys - prisijungimo vardas ir slaptažodis) buvo pavagiami.



Klausimai diskusijoms

- Kaip elgtis, jei nutekėjo jūsų paskyros prisijungimo duomenys?
- Kaip elgtis gavus tokį el. laišką?
- Kokie požymiai išduoda suklastotą el. laišką, suklastotas prisijungimo formas?
- Ko išmokote išanalizavę šį atvejį?

Funded by the Erasmus+ Programme of the European Union

Turinys

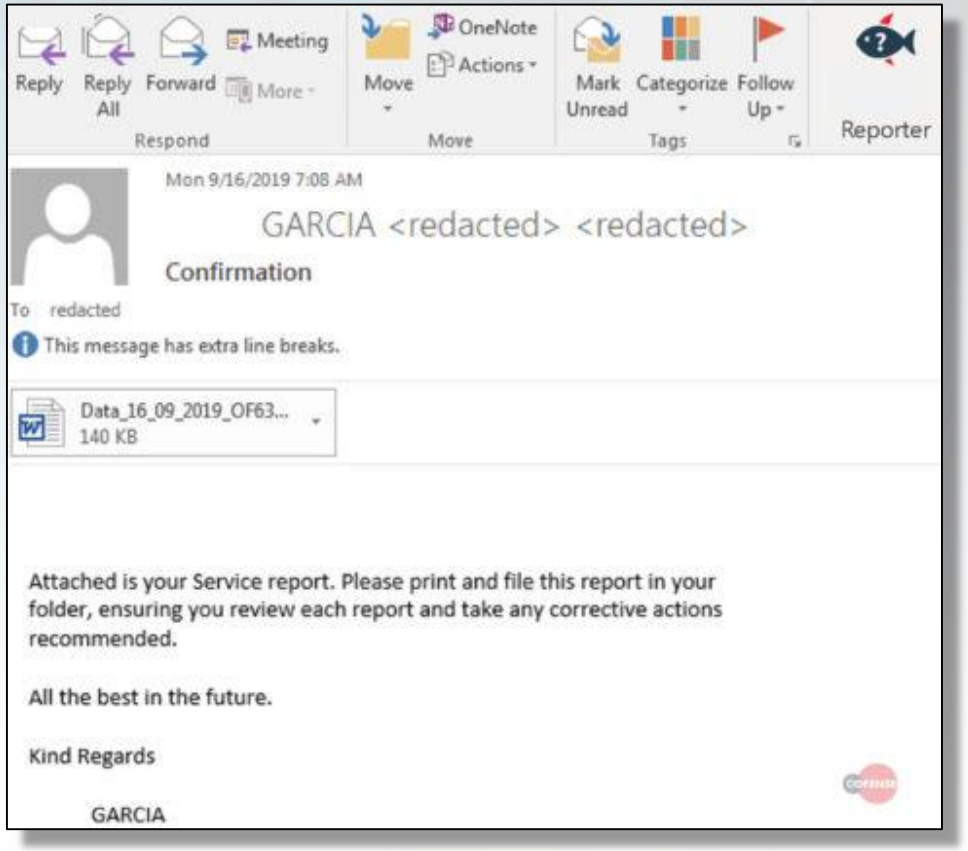
- Valetos bankas
- Kipro paštas
- Smart-ID
- Asmens duomenų nutekėjimas
- **Emotet kenkėjiškas programinis kodas (KPK)**
- Sukčiavimo (angl. phishing) atakos

Aptarkite galimai kenkėjiškų el. laiškų, gautų iš patikimų siuntėjų, poveikį

Funded by the Erasmus+ Programme of the European Union

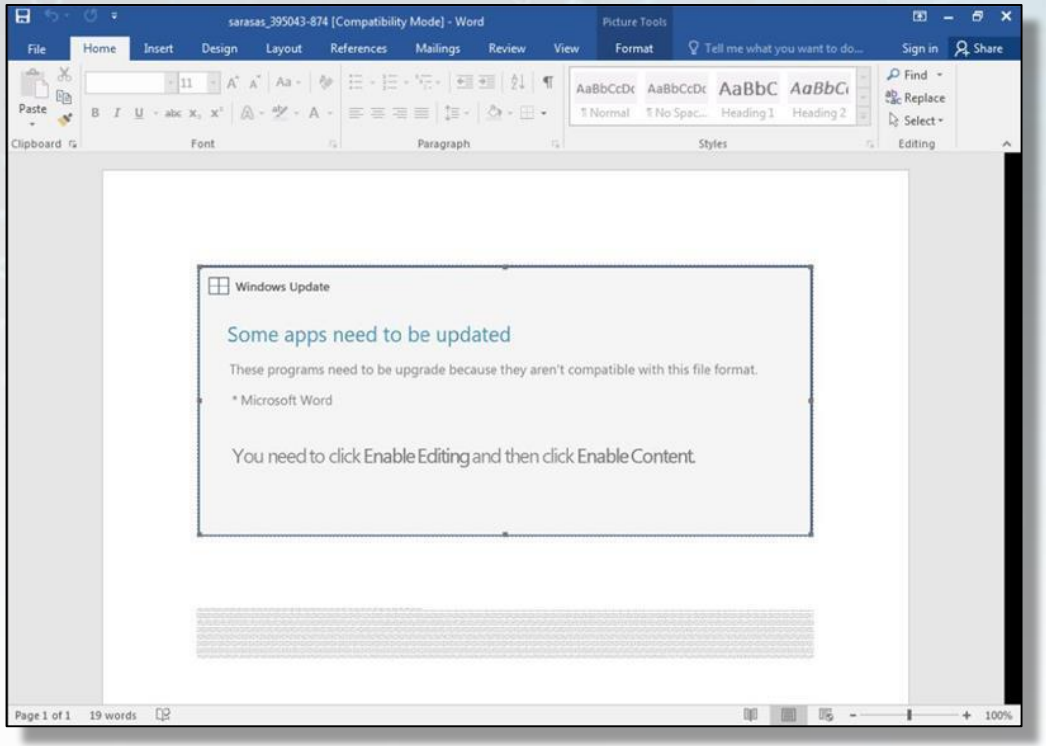
Atvejo aprašymas

- Kenkėjiškos nepageidaujamos žinutės (malspam), tokios kaip "Emotet" yra viena iš labiausiai paplitusių su el. paštu susijusių grėsmių. Jis naudoja "thread hijacking" metodą, kurio esmė sukčiavimui panaudoti tikrus iš aukos el. pašto pavogtus laiškus. Laiško siuntėjams parengiamas atsakymas prie laiško prisegant kenkėjišku kodu užkrėstus dokumentus ir išsiunčiamas kaip atsakymas



Funded by the Erasmus+ Programme of the European Union

Atvejo aprašymas



Šis metodas veiksmingesnis nei paprastesni metodai, kuriuos nemažai žmonių jau išmoko atpažinti. Šiuo metodu sėkmingiau pavyksta įtikinti potencialias aukas spustelėti prisegtą failą arba spustelėti nuorodą ir atsisiųsti kenkėjišką "Word" dokumentą su makrokomandomis, skirtomis užkrėsti naudotoją "Emotet

Klausimai diskusijoms

- Kaip gavėjas galėtų papildomai pasitikrinti, ar el. laiškas gautas iš teisėto šaltinio, net jei jis atrodo kaip atsakymas į pokalbį?
- Ar žmogus turėtų gauti tokius failus dirbdamas kasdienį darbą?
- Ar asmeniniame kompiuteryje ar darbo vietoje reikalinga antivirusinė programinė įranga net ir tuo atveju jei vartotojas niekada nelanko įtartino turinio tinklapių ar įrenginį naudoja griežtai tik darbo veikloms?

- Kaip elgtis darbuotojui gavus svarbų darbinį el. laišką su svarbiu prisegtu dokumentu? Ar galima jį atidaryti jie prisegtas dokumentas jam atrodo įtartinas?

Funded by the Erasmus+ Programme of the European Union

Turinys

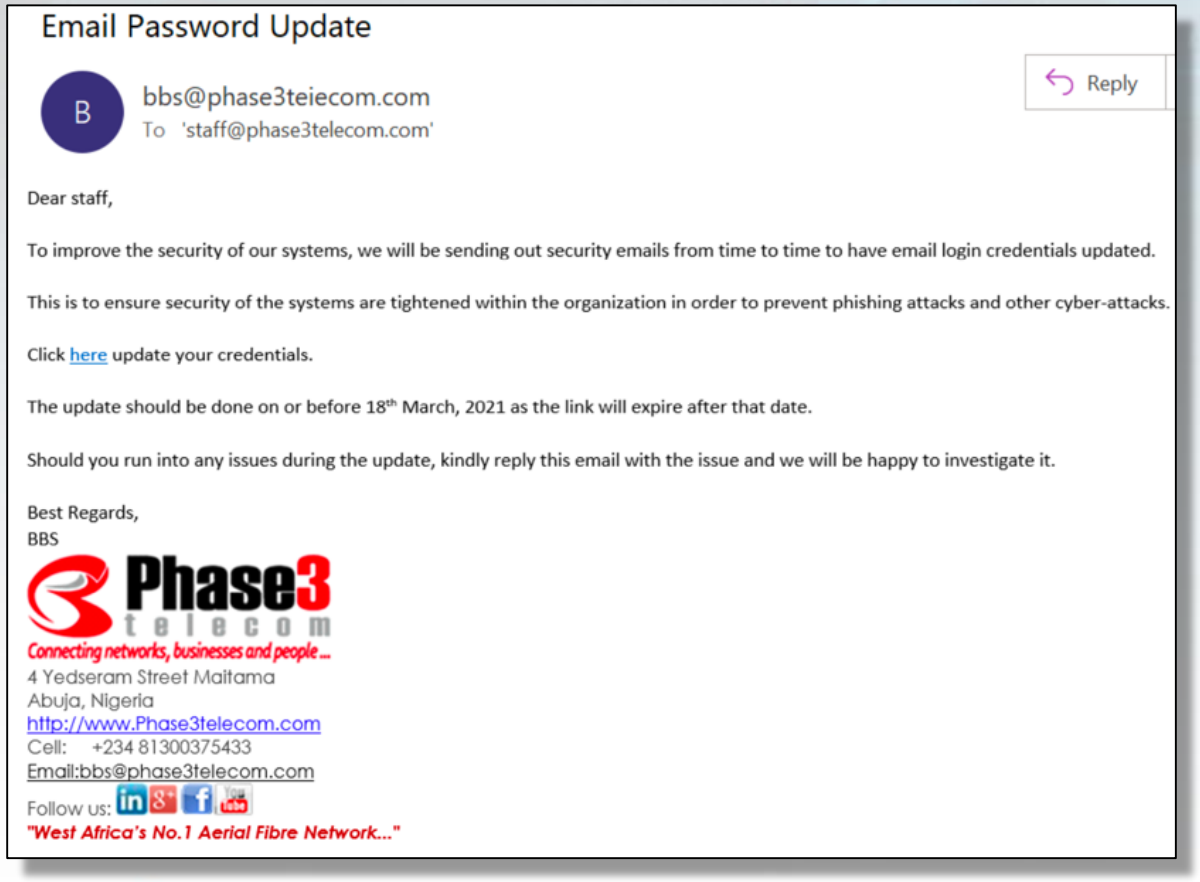
- Valetos bankas
- Kipro paštas
- Smart-ID
- Asmens duomenų nutekėjimas
- Emotet kenkėjiškas programinis kodas
- **Sukčiavimo (angl. phishing) atako[illegible]**

Aptarkite sukčiavimo atakų poveikį organizacijai

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo (angl. phishing) atakos simuliacija

Atvejo aprašymas



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..."

Telekomunikacijų bendrovė atliko kontroliuojamą sukčiavimo simuliaciją, siekdama ištirti, kaip jos darbuotojai elgiasi sukčiavimo atakos metu. Apgaulingas el. laiškas buvo išsiųstas 2021 m. kovo 17 d. 8.26 val. Ankstyvas laikas pasirinktas tam, kad darbuotojai būtų užklupti nepasiruošę, ir tai būtų vienas pirmųjų tą dieną gautų el. laiškų. Apgaulingo el. laiško turinyje buvo reikalaujama įdiegti saugumo atnaujinimą, ir pateikiama nuorodą į jį. Paspaudus nuorodą, vartotojas nukreipiamas į suklastotą svetainę.

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

Atvejo aprašymas

Simuliacijos rezultatai

- Simuliacijoje dalyvavo apie **250** darbuotojų.
- Suklastota nuoroda buvo paspausta **179** kartus daugiau nei 40 paspaudimų buvo atlikta ne iš vidinio organizacijos tinklo.
- Apie sukčiavimo ataką pranešė tik 3 darbuotojai dar 4 darbuotojai paskambino norėdami gauti patvirtinimą, kad el. laiškas yra teisėtas. 2 darbuotojai paskambino skųstis dėl neveikiančios nuorodos.

Diena	**Paspaudimai iš vidinio tinklo**	**Paspaudimai iš išorinio tinklo**
1	161	>30
2	18	>10
Iš viso	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

Atvejo aprašymas

Aukų profiliai

- **Finansų skyriaus darbuotojas**
  - *Paspausta praėjus keltui minučių po laiško išsiuntimo.*
  - *Turi prieigą klientų duomenų, mokėjimo procesų / duomenų, apskaitos duomenų*
- **Padalinio vadovas**
  - *Prieiga prie skirtingų duomenų tipų*
  - *Potenciali žala organizacijos reputacijai*
- **Ne inžinierių komandos narys**
  - *Prieiga prie padalinio kolegų duomenų*
  - *Sukuria galimybę tolimesnėms atakoms*
- **Regiono inžinierių komandos narys**
  - *Prieiga prie regioninio padalinio duomenų*
  - *Galima žala paslaugoms regione*
- **Inžinierių komandos narys**
  - *Turi prieigą prie organizacijos Intraneto*

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

Klausimai diskusijoms

- Apibrėžkite sukčiavimo ataką:
  - *Sukčiaus profilis?*
  - *Sukčiavimo atakos metodai ?*
  - *Pažeidžiamumas?*
  - *Poveikis?*
- Kokie el. laiško požymiai leidžia atpažinti sukčiavimo ataką?
- Kokią įtaką ši ataka daro nagrinėjamai telekomunikacijų bendrovei?
- Kaip nagrinėjamoje bendrovėje pagerinti sukčiavimo atakų atpažinimą?

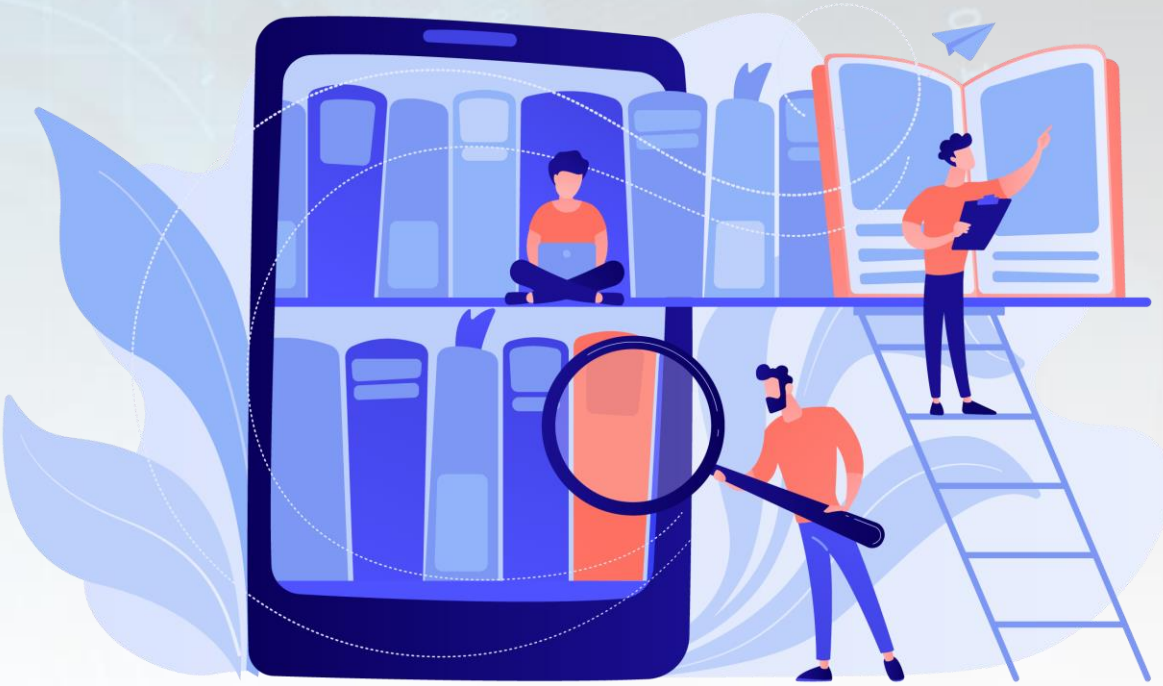
Funded by the Erasmus+ Programme of the European Union

Apibendrinimas

- Kaip saugumo rizika kenkia infrastruktūrai ir daro poveikį žmonių gyvenimui?
- Kokie veiksmai ir įtikinėjimo principai siekiant sumažinti sukčiavimo atakų poveikį?
- Kaip grėsmių agentai naudoja šiuolaikinius autentifikavimo metodus, siekdami pažeisti saugomus resursus?
- Kaip atpažinti suklastotus el. laiškus, kuriuose siūlomos įvairios nepatikimų organizacijų paslaugos?
- Kenkėjiškų el. laiškų, gautų iš patikimų siuntėjų, poveikis?
- Sukčiavimo atakų poveikis organizacijai

Papildomi skaitiniai

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



Trumpi vaizdo įrašai

- Banko saugumo pažeidimas
  https://youtu.be/kkc3nkCXUk0
- Kibernetinė ataka prieš bankus ir paštą
  https://youtu.be/yB3N9U6V3c4
- Smart-ID registracija su ID kortele
  https://youtu.be/m9t4PY0DROM
- Emotet - kenkėjiškų programų evoliucija
  https://youtu.be/CkwKTBifXJg
- Sukčiavimo atakų simuliatorius
  https://youtu.be/hh25C0cdop0

Dėkojame!