Funded by the
Erasmus+ Programme
of the European Union

Kibernetinės atakos:
socialinė inžinerija ir sukčiavimas (angl. phishing)

Skirtingi sukčiavimo atakų tipai ir kategorijos

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

Mokymo tikslai

Supažindinti su skirtingais sukčiavimo atakų tipais ir išmokti atpažinti atakas.

Sukčiavimo atakos:

- atakos, vykdomos panaudojant realius ir aktualius įvykius,
- tiesioginio susirašinėjimo žinutės,
- socialiniai tinklai,
- svetainės,
- netikrų loterijų pranešimai (angl. lotteries scams),
- SMS žinutės,
- telefoniniai skambučiai,
- gyvai vykstantys susitikimai,
- duomenų vagystė paslapčia stebint asmenį, kuris duomenis veda į skaitmeninį įrenginį (angl. soulder surfing).

Funded by the Erasmus+ Programme of the European Union

Mokymo tikslai

Naudojamos technikos:

- „Spray and pray“ (el. laiškai siekiant pavogti konfidencialią informaciją),
- „Spear phishing“ (personalizuotas sukčiavimas (angl. phishing)),
- „Whaling“ (bandymas pavogti konfidencialią informaciją ir dažnai nukreiptas į aukščiausią vadovybę),
- „Vishing“ (telefoninis sukčiavimas), „Smishing“ (sukčiavimas SMS žinutėmis),
- „Angler Phishing“ (sukčiavimas socialiniuose tinkluose),
- „Clone Phishing“ (tikrų laiškų turinio panaudojimas sukčiavimui),
- „Malwertising“ (kenkėjiškas turinys reklamose).

Funded by the Erasmus+ Programme of the European Union

Studento darbo krūvis

Paskaitos	4 val.
Garso ir vaizdo medžiaga	2 val.
Panaudojimo atvejai	2 val.
Papildomi skaitiniai	2 val.
Pasiruošimas atsiskaitymui	2 val.

El. laiškais

Suklastotais laimėjimais

Žiūrėjimu per petį

Suklastotomis apklausomis

Suklastotomis SMS

Tiesioginio susirašinėjimo žinutėmis

Suklastotos svetainės

Socialiniai tinklais

Skambučiais

Sekant iš paskos

Viliojimais arba masalu

CyberPhish


Skambučiai telefonu
SMS
El. pašto laiškai
Patekimas į ribotos
prieigos patalpas
CyberPhish

Sėkmingos sukčiavimo atakos pasekmės

- Neskelbtinų duomenų praradimas
- Prisijungimo duomenų (vartotojo vardų ir slaptažodžių) praradimas
- Tapatybės vagystė
- Klientų informacijos vagystė
- Lėšų iš verslo ir klientų sąskaitų praradimas
- Prieiga prie IS būsimoms atakoms vykdyti
- Neteisėti sandoriai
- Intelektinės nuosavybės praradimas
- Duomenys, teikiami arba parduodami nusikaltėlėms trečiosioms šalims
- Organizacijos veiklos trikdymas
- Reagavimas į incidentus
- Padarinių likvidavimas ir atkūrimas
- Atkūrimui prarastos darbo valandos
- Žala reputacijai
- Prarastos pajamos
- Baudos, teisiniai mokesčiai...

Funded by the Erasmus+ Programme of the European Union

Turinys

Atakos, vykdomos panaudojant realius ir aktualius įvykius	El. pašto laiškai	Tekstinės žinutės	Svetainės
Netikrų loterijų pranešimai	Skambučiai telefonu	Gyvai vykstančios atakos	Stebėjimas per petį

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Atakos, vykdomos panaudojant realius ir aktualius įvykius

- Didelio masto įvykiai, karai, pandemijos, pavyzdžiui, COVID-19, verčia žmones elgtis impulsyviau nei įprastomis aplinkybėmis.

- Dažniausiai naudojami metodai: el. laiškai, personalizuotas sukčiavimas el. paštu, SMS, Pasinaudojimas kieno nors teise patekti į ribotos prieigos patalpas, apgaulingi skambučiai telefonu ir kt.

Funded by the Erasmus+ Programme of the European Union

Su BDAR susijusios atakos

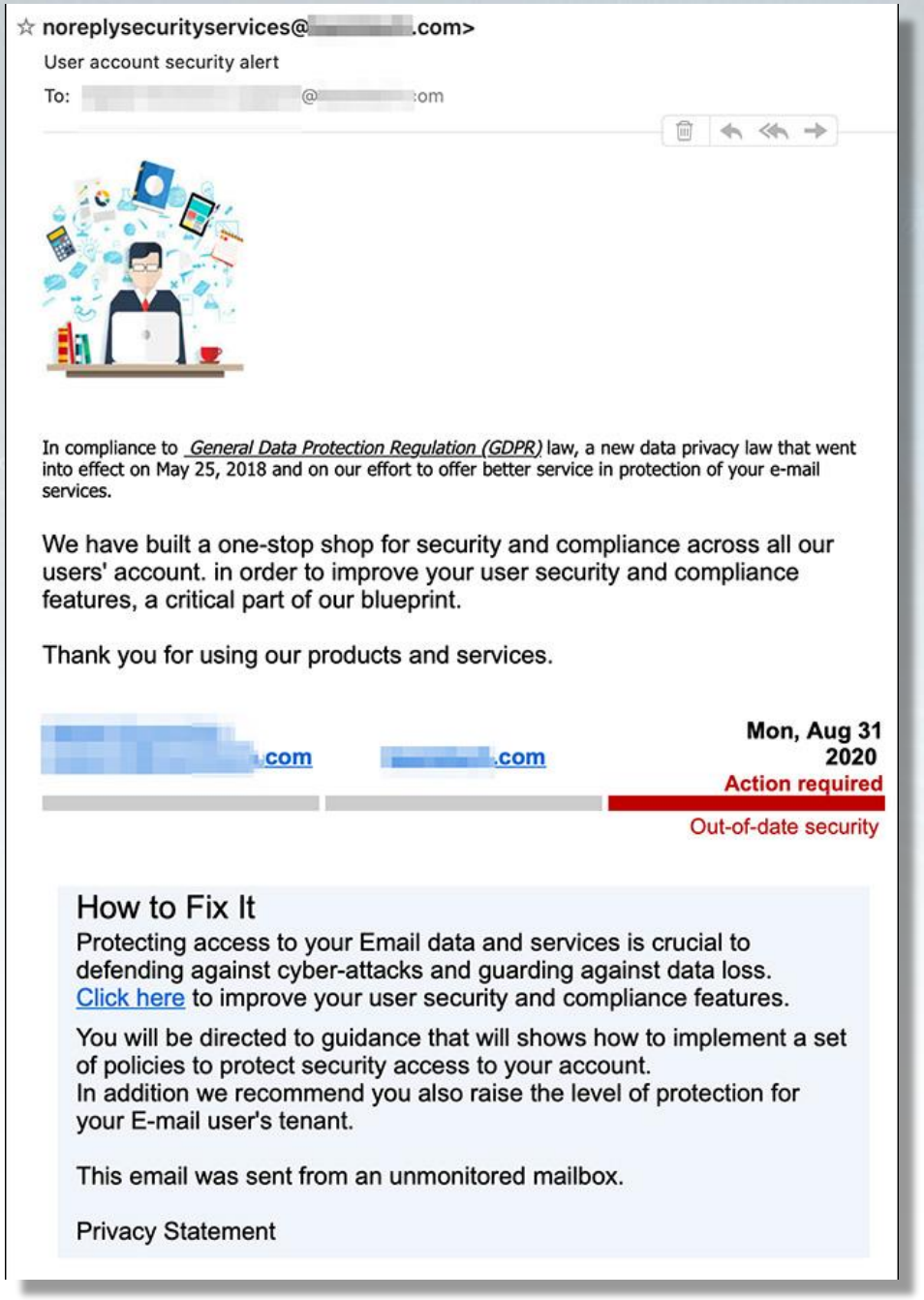
- **Bendrasis duomenų apsaugos reglamentas** (BDAR) – tai reglamentas (įsigaliojęs nuo 2018 m.) kontroliuoja, kaip įmonės ir organizacijos tvarko asmens duomenis.
- Įmonės, atliekančios automatizuotą arba iš dalies automatizuotą asmens duomenų tvarkymą, privalo vadovautis BDAR.
- Kadangi BDAR reglamentas įsigaliojo 2018 m., būtent tuo laikotarpiu padaugėjo su BDAR tema susijusių atakų, nes visos įmonės ir organizacijos privalėjo įsidiegti BDAR.

Su BDAR susijusios atakos, nukreiptos į organizacijas

- **Kodėl tokio tipo atakos būna sėkmingos?** Įmonės neturi pakankamai žinių apie BDAR.
- **Taikinys:** įmonės darbuotojai, dažniausiai:
  - tiems darbuotojams, kurių įmonės el. pašto adresai, yra viešai prieinami internete
  - tiesioginiams įmonių vadovams ar aukštesnio lygio vadovams (kurie, tikėtina, turi prieigą prie klientų duomenų arba yra atsakingi už BDAR laikymąsi)
- **Grėsmė:** el. laiškai iš „saugumo organizacijų“, teikiančių paslaugas, kuriomis siekiama pagerinti naudotojų duomenų saugumą ir atitiktį BDAR.
- **Atakos metodas:** el. paštas (personalizuotas sukčiavimas (angl. spear phishing)).
- **Sukčiavimo taktika:** el. laiškai yra suformatuoti taip, kad jie atrodo, kaip teisėtos organizacijos siųstas laiškas. Tokiu būdu sukčiai sudaro įspūdį, kad el. laiškai buvo išsiųsti iš teisėto šaltinio.
- **Sukčiavimo faktoriai:**
  - baimė dėl įstatymų pažeidimų
  - skubos jausmo sukėlimas: siekdami padidinti spaudimą gavėjui, užpuolikai naudojo atitikties BDAR reikalavimams įdiegimo organizacijoje terminų laiko juostą.
- **Pažeidžiamumai:**
  - Neapmokytas personalas (paspaudžia el. laiške esančią nuorodą ir pateikia duomenis).

Funded by the Erasmus+ Programme of the European Union

Su BDAR susijusi ataka: naudotojų saugumo ir atitikties BDAR reikalavimams gerinimas



- Paspaudus laiške pateiktą nuorodą, bus atidaryta sukčių sukurta svetainė.
- Svetainė gali būti suasmeninta pagal aukos el. pašto adresą
- Aukos gali būti paprašyta prisijungti (pateikiant prisijungimo duomenis) prie netikros svetainės, kuri atrodo kaip tikra svetainė
- **Rezultatas**:
  - Pavogti aukos el. pašto prisijungimo duomenys, kad būtų galima gauti prieigą prie el. pašto
  - Iš aukos el. pašto gali būti pavogti konfidencialūs duomenys arba pavogti kontaktai gali būti panaudoti tolesnėms kibernetinėms atakoms vykdyti

Source: https://www.helpnetsecurity.com/2020/09/24/phishers-targeting-employees-fake-gdpr-compliance-reminders/

Su BDAR susijusios atakos, nukreiptos į klientus

- **Kodėl tokio tipo atakos būna sėkmingos?** Įmonės siuntė klientams el. laiškus apie BDAR atnaujinimus, susijusius su klientų duomenų privatumo politika.
- **Taikinys:** įvairių organizacijų klientai, dažniausiai IT paslaugų teikėjai, finansinių organizacijų klientai.
- **Grėsmė:** el. laiškai iš „organizacijų“, kuriuose prašoma patvirtinti leidimą saugoti ir tvarkyti asmens duomenis.
- **Atakos metodas:** el. paštas.

- **Sukčiavimo taktika:**
  - el. laiškai yra suformatuoti taip, kad jie atrodo, kaip teisėtos organizacijos siųstas laiškas. Tokiu būdu sukčiai sudaro įspūdį, kad el. laiškai buvo išsiųsti iš teisėto šaltinio.
  - užpuolikai naudojasi prekių ženklais, kurie turi gerą reputaciją.
- **Sukčiavimo faktoriai:**
  - **Įsipareigojimas ir nuoseklumas**
  - **Lojalumas organizacijai**
- **Pažeidžiamumai:**
  - Klientai, turintys nepakankamai žinių apie sukčiavimą (paspaudžia el. laiške esančią nuorodą ir pateikia duomenis).

Funded by the Erasmus+ Programme of the European Union

Su BDAR susijusi ataka: patvirtinkite naują privatumo politiką

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

- Paspaudus laiške pateiktą nuorodą, bus atidaryta sukčių sukurta svetainė.
- Šioje svetainėje, kuri atrodo kaip realiai egzistuojančios organizacijos svetainė, aukos gali būti paprašyta pateikti savo asmeninę informaciją, įskaitant paskyros prisijungimo duomenis ir mokėjimo kortelės informaciją.
- **Rezultatas**:
  - Pavogti aukos el. pašto prisijungimo duomenys, siekiant gauti prieigą prie el. pašto.
  - Iš aukos el. pašto gali būti pavogti konfidencialūs duomenys arba pavogti kontaktai gali būti panaudoti tolesnėms kibernetinėms atakoms.
  - Pavogti finansiniai duomenys.
  - Užkrėsti įrenginiai (įdiegiant klaviatūros paspaudimų registratorių (angl. keylogger), išpirkos reikalaujanti programinė įranga (angl. ransomare) ir kt.)

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

Su COVID susijusios atakos

- COVID-19 pandemijos metu daug žmonių dirbo iš namų. Darbuotojai, dirbdami nuotoliniu būdu, naudojo savo asmeninius kompiuterius darbo užduotims, pagrindinis bendravimas vyko elektroniniais laiškais – tai reiškia, kad darbuotojai tapo labiau pažeidžiami kibernetinėms atakoms.
- COVID-19 metu pastebėta, kad padaugėjo su pandemija susijusių sukčiavimo atvejų, pavyzdžiui, suklastotų Ligų prevencijos ir kontrolės centro (CDC) ar sveikatos organizacijų el. laiškų, el. laiškų apie skiepijimo apimtis, kur galima gauti vakcinos, skiepų statistiką, darbuotojų skiepijimo būklę ir pan.

Funded by the Erasmus+ Programme of the European Union

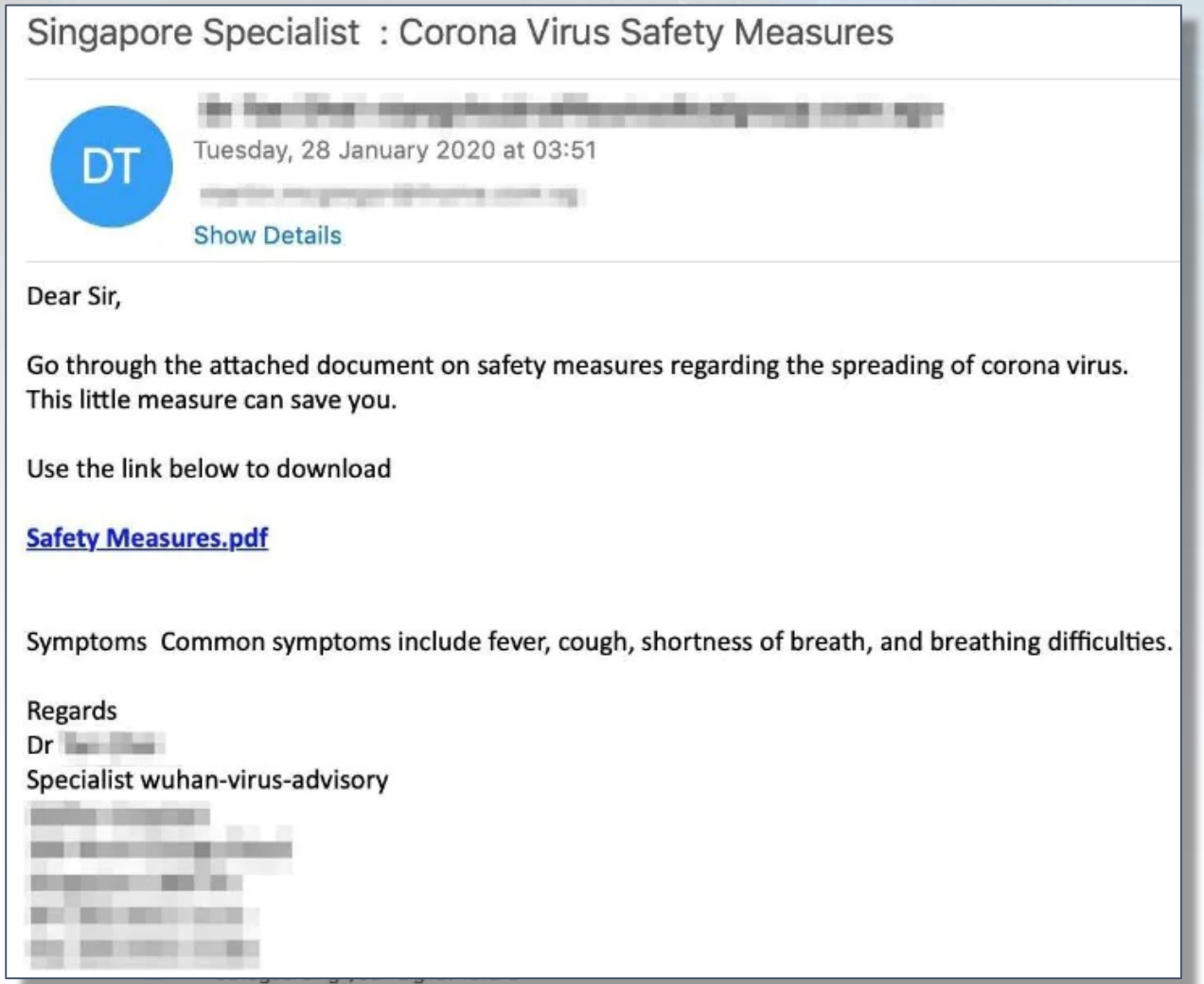
Su COVID susijusios atakos: el. paštas

- **Kodėl tokio tipo atakos būna sėkmingos?** COVID-19 sukėlė žmonėms nestabilumo ir netikrumo jausmą, dažnai keitėsi politikų sprendimai dėl karantino, vakcinacijos, skiepus patvirtinančių dokumentų ir kt.
- **Taikinys:** visi gyventojai
- **Grėsmė:**
  - el. laiškai, kuriuose prašoma pateikti konfidencialią informaciją suklastotoje svetainėje
  - el. laiškai, kuriuose prašoma spustelėti nuorodą
- **Atakos metodas:** el. pašto laiškai.

- **Sukčiavimo taktika:**
  - el. laiškai yra suformatuoti taip, kad jie atrodo, kaip teisėtos organizacijos siųstas laiškas.
  - užpuolikai paprastai siūlo atsisiųsti dokumentą, kuriame neva pateikiama COVID-19 statistika, atsisiųsti COVID formą, užpildyti internetinę formą arba užpildyti atsisiųstus dokumentus apie skiepijimo būklę ar įkelti neigiamą COVID testą ir t. t.
- **Sukčiavimo faktoriai:**
  - **Skubos jausmo sukėlimas**
  - **Baimės jausmo sukėlimas**
  - **Prašymas laikytis nestandartinio proceso (pvz., apeiti įstatymus)**
- **Pažeidžiamumai:**
  - asmenys, turintys nepakankamai žinių apie sukčiavimą (asmenys, kurie atlieka sukčiavimo el. laiškuose prašomus veiksmus).

Funded by the Erasmus+ Programme of the European Union

Su COVID susijusi ataka: Sveikatos patarimai el. laiške



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.

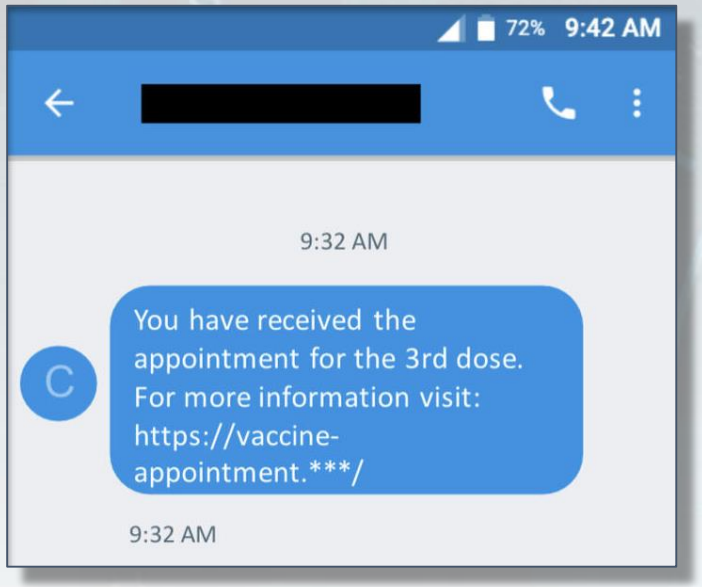
Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

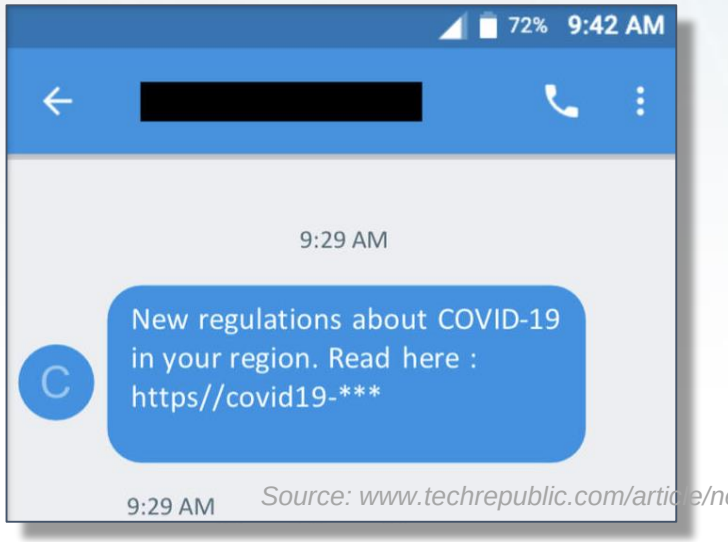
Source: https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

- Paspaudus nuorodą, kuri atrodo kaip nuoroda į PDF failą, atidaroma sukčių sukurta svetainė.
- Aukos gali būti paprašyta pateikti savo asmeninę informaciją, įskaitant paskyros prisijungimo duomenis ir mokėjimo kortelės informaciją, kad būtų galima „patvirtinti tapatybę“.
- **Rezultatas**:
  - Pavogti aukos el. pašto prisijungimo duomenys, norint gauti prieigą prie aukos el. pašto.
  - Pavogti finansiniai duomenys.
  - Užkrėsti įrenginiai (įdiegiant klaviatūros paspaudimų registratorių (angl. keylogger), išpirkos reikalaujanti programinė įranga (angl. ransomare) ir kt.)

Funded by the Erasmus+ Programme of the European Union

Su COVID susijusios atakos: Informacija apie vakcinas SMS žinutėmis





- **Kodėl tokio tipo atakos būna sėkmingos?** Įstaigos gyventojams siunčia SMS žinutes apie skiepijimą ir kitą su COVID aktualią informaciją.
- **Taikinys:** visi gyventojai
- **Grėsmė:**
  - SMS žinutės, kuriose prašoma paspausti nuorodą
- **Atakos metodas:** SMS.
- **Sukčiavimo taktika:**
  - SMS žinutės dažniausiai yra trumpos: vienas arba du sakiniai. Žinutėje dažnai pateikiama nuoroda į suklastotą svetainę
- **Sukčiavimo faktoriai:**
  - nestabilumo ir netikrumo jausmo sukėlimas
- **Pažeidžiamumai:**
  - asmenys, turintys nepakankamai žinių apie sukčiavimą (asmenys, kurie atlieka sukčiavimo el. laiškuose prašomus veiksmus).

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

Funded by the Erasmus+ Programme of the European Union

Turinys

Atakos, vykdomos panaudojant realius ir aktualius įvykius	El. pašto laiškai	Tekstinės žinutės	Svetainės
Netikrų loterijų pranešimai	Skambučiai telefonu	Gyvai vykstančios atakos	Stebėjimas per petį

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo el. laiškai

- Vienas iš labiausiai žinomų sukčiavimo būdų.
- Sukčiavimo el. laiškuose sukčiai naudoja tokią taktiką:
  - Prašymai el. paštu atsiųsti konfidencialią informaciją
  - Prašymas spustelėti el. laiške pateiktą nuorodą
  - Prašymas atidaryti priedą, paprastai tai būna PDF arba DOC formato dokumentas
- Įprastos sukčiavimo el. laiškų temos:
  - Paskyros problemos
  - Techninės pagalbos klausimai
  - Romantiniai santykiai
  - Norint susigrąžinti, grąžinti pinigus arba gauti finansinę paramą iš institucijos
- Vykdomiesiems direktoriams ir vadovams gali būti siunčiami personalizuoti sukčiavimo el. laiškai

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo el. laiškai

Dažnai sutinkami šie sukčiavimo (angl. phishing) tipai:

- **Spray and pray** – kenkėjiški el. laiškai, siunčiami bet kuriuo ir visais el. pašto adresais, bandant pavogti konfidencialią informaciją;
- **Advanced fee scam** – dažnas sukčiavimas, susijęs su Nigerijos piliečiais, pvz., prašymas padėti pervesti didelę pinigų sumą;
- **Personalizuotas sukčiavimas (angl. spear phishing)** – kenkėjiški el. laiškai, specialiai sukurti ir siunčiami konkrečiam asmeniui ar organizacijai, siekiant pavogti konfidencialią informaciją;
- **Whaling** – bandymas pavogti konfidencialią informaciją ir dažnai nukreiptas į aukščiausią vadovybę;
- **Angler Phishing** – santykinai naujas atakų tipas socialiniuose tinkluose, kai naudojamos netikros internetinės nuorodos, klonuotos svetainės, pranešimai, tviterio žinutės ar tiesioginio susirašinėjimo žinutės;
- **Clone Phishing** – sukčiavimo tipas, kai tikras anksčiau išsiųstas el. laiškas panaudojamas identiško el. laiško sukūrimui su kenkėjišku turiniu;
- **Malvertising** – šis sukčiavimo tipas naudoja internetines reklamas ar iššokančius langus (angl. pop-ups), kad priverstų žmones paspausti ant įtarimo nekeliančios nuorodos, siekiant įdiegti kenkėjišką programą kompiuteryje.

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo el. laiškai: Prašymai siųsti konfidencialią informaciją el. paštu

- **Kodėl tokio tipo atakos būna sėkmingos?** Sukčiavimo atakos atrodo įtikinamai: sudaromas įspūdis, kad siuntėjas yra patikimas šaltinis. Organizacijos nepakankamai kruopščiai tikrina el. laiškus, ir tokie laiškai patenka darbuotojams. Užpuolikai naudoja sudėtingesnes sukčiavimo atakas, kurias sunku aptikti ir pan.
- **Taikinys:** visi gyventojai
- **Grėsmė:**
  - el. laiškai, kuriuose prašoma atsiųsti atsakymą.
  - el. laiškai, kuriuose prašoma el. paštu pateikti neskelbtiną informaciją.
- **Sukčiavimo taktika:**
  - ieško partnerių, turi gerų naujienų aukai, siūlo pinigų, praneša apie laimėjimą, apsimeta draugu ir prašo paskolinti pinigų dėl netikėtos nelaimės, siūlo pinigų, praneša apie konkurso laimėtoją ir pan.
- **Sukčiavimo faktoriai:**
  - **Sudaro įspūdį aukai, kad siuntėjas yra naudingas**
  - **Sukelia godumo jausmą**
- **Pažeidžiamumai:**
  - asmenys, turintys nepakankamai žinių apie sukčiavimą (asmenys, kurie atsako arba atlieka veiksmus, kurių prašoma sukčiavimo el. laiškuose).
- **Rezultatas:**
  - Tapatybės vagystė, pinigų praradimas.

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo el. laiško pavyzdys: Prašymas siųsti konfidencialią informaciją el. paštu

Siuntėjas: eduardorodriguez <andreasjohnson874@gmail.com>

Kam: andreasjohnson847@gmail.com

Tema:

Sveikas, mano drauge

Aš esu ANTONI FELIKS iš Lenkijos ir turiu jums gerų naujienų. SVEIKINU!!!
Susisiekite su manimi: homebankpln@gmail.com arba homebankpln@polandmail.com ir aš atsiųsiu daugiau informacijos apie gerą naujieną.

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

Kam:

Tema: Sveikinimai!!!

Džiaugiamės galėdami pranešti, kad jūsų el. pašto adresas buvo įtrauktas į internetinę loteriją ir jūs laimėjote $ 7,500. Norėdami gauti šį apdovanojimą, turite pateikti tokią informaciją:
Gavėjo vardas ir pavardė:_____
Gavėjo adresas:_____
Gavėjo šalis: _____
Gavėjo kredito kortelės numeris: _____
Gavėjo kredito kortelės CVC2: _____

PASTABA: laimėjimo informaciją laikykite konfidencialia.

Pasirašyta
Generalinis direktorius: Luis Andres Jonson

Siuntėjas: Ava Williams <avawilliamsj@gmail.com>

Kam: avawilliamsj@gmail.com

Tema: Labas…

Sveiki

Žinau, kad nustebote gavę šią žinutę iš manęs, nes mes dar nebuvome susitikę. Jūsų el. laišką gavau atlikęs Google paiešką. Rašau jums iš ligoninės, kurioje esu gydomas: man nustatytas vėžys.

Susisiekiau su jumis šiandien, nes man reikia jūsų pagalbos investuoti lėšas, kurias paveldėjau iš savo mirusio vyro.
Jei sutiksite man padėti, atsilyginsiu jums skirdama jums 30 proc. nuo paveldėtos sumos.

Daugiau apie save ir savo planus galėčiau papasakoti, kai iš jūsų sulauksiu atsakymo.

Su pagarba
Ava Williams

Siuntėjas: manyrib7@gmail.com

Kam:

Tema: Labas…

Mano vardas yra Rihab Manyang. Ieškau verslo partnerio ar draugo, kuris padėtų man investuoti savo lėšas jūsų šalyje.

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo el. laiškai: Prašo spustelėti el. laiške pateiktą nuorodą

- **Kodėl tokio tipo atakos būna sėkmingos?** Sukčiavimo atakos atrodo įtikinamai: sudaromas įspūdis, kad tai patikimas šaltinis. Organizacijos nepakankamai kruopščiai tikrina el. laiškus. Užpuolikai naudoja sudėtingesnes sukčiavimo atakas, kurias sunku aptikti: jie gali naudoti turinio, konteksto ir emocinių motyvatorių derinį, kuris lemia sukčiavimo atakos sėkmę ir pan.
- **Taikinys:** visi gyventojai
- **Grėsmė:**
  - vykdant sukčiavimo atakas kopijuojamos esamos darbų sekos.
  - sukčiai prašo paspausti el. laiške pateiktą nuorodą
- **Sukčiavimo taktika:**
  - Elektroniniai laiškai apie „nutekintus“ el. pašto adresus ar slaptažodžius
  - Elektroniniai laiškai, kuriais siunčiami bendrinami dokumentai, kurie skirti bendradarbiavimui
  - Elektroniniai laiškai, informuojantys apie technines problemas

- **Sukčiavimo faktoriai:**
  - **Skubos jausmo sukėlimas**
  - **Baimės jausmo sukėlimas**
  - **Užpuolikai naudojasi aukos emocijomis ir instinktais**
- **Pažeidžiamumai:**
  - gyventojai, turintys nepakankamai žinių apie sukčiavimą (kurie atsako į laiškus arba atlieka veiksmus, kurių prašoma sukčiavimo el. laiškuose).
- **Rezultatas:**
  - Tapatybės vagystė, pinigų praradimas

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo el. laiškų pagrindiniai bruožai

- Naudoja geros reputacijos organizacijų ar asmenų vardus.
- Naudoja patikimų šaltinių duomenis
- Prašo pateikti neskelbtiną informaciją
- Elektroniniuose laiškuose gali būti priedų
- Paprastai gavėjas yra nežinomas
- Nuorodos į svetaines (nuorodos gali būti sutrumpintos)
- Pateikiamos nuorodos į kenkėjiškas svetaines
- Pasitelkiama baimė arba sukeliamas skubos jausmas
- Neįtikinama dingstis (loterija, nuolaidos, paveldėjimas,...)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo el. laiškuose naudojamos nuorodos

- Sukčiai sukčiavimo el. laiškuose paprastai naudoja nuorodas į suklastotas svetaines:
  - Sukčiai gali užregistruoti suklastotą domeną. URL pavadinimas gali būti panašus į tikros organizacijos pavadinimą, jie tik pakeičia vieną ar kelias domeno vardo raides, pavyzdžiui, vietoj raidės "l" gali naudoti raidę "i", vietoj "m" - "rn" ir t. t. Pavyzdžiui, jie gali užregistruoti tokį netikrą domeno vardą ***www.exarnple.com*** (tikrasis URL ***www.example.com***).
  - Sukčiai gali užregistruoti domeną, naudodami tikrąjį organizacijos pavadinimą, pavyzdžiui, ***www.sales-organization.com*** (tikrasis URL ***www.organization.com***).
  - Sukčiai gali naudoti sutrumpintas nuorodas, pvz., ***Bitly***, ***TinyURL***, ***Short.io*** (daugiau apie tai sekcijoje ***nuorodų trumpinimas***)
  - Sukčiai gali naudoti nuorodą svetainės, į kurią buvo įsilaužta (naudojamas tikros organizacijos domeno vardas, tačiau likusią URL dalį sukuria įsilaužėliai).
  - Sukčiai į teisėtą tinklalapį įterpia kenkėjišką kodą (angl. Injection attack). Kai auka atidaro šią svetainę, vykdomas kenkėjiškas scenarijus. Tokio tipo atakos rezultatas būtų duomenų vagystė, klaviatūros paspaudimų registratoriaus įdiegimas, slapukų vagystė ir pan.

Siuntėjas: NB Sukčiavimo internete prevencija <info@nat1onalbank.com>

Kam: nenurodyti gavėjai

Tema: Prieiga prie Jūsų sąskaitos Nacionaliniame banke buvo sustabdyta

CyberPhish

National Bank

Gerbiamas kliente,

Neseniai pastebėjome, kad prie Nacionalinio banko Jūsų sąskaitos bandė prisijungti skirtingi įrenginiai iš skirtingų vietų. Pateikiame IP adresų, iš kurių neseniai bandyta prisijungti prie jūsų paskyros, sąrašą:
12.55.155.6:8080
32.44.789.99:3128
54.22.124.44:8080
78.44.457.14:80

Šiuo metu prieiga prie Jūsų sąskaitos Nacionaliniame banke buvo sustabdyta. Turite ją aktyvuoti per 7 dienas, kitaip paskyra bus užblokuota..

Norėdami patvirtinti, kad esate sąskaitos naudotojas, ir aktyvuoti paskyrą, spustelėkite
HTTP://WWW.NAT1ONALBANK.COM?PROFILE
Daugiau informacijos čia.

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

Pagarbiai,
Nacionalinio banko sukčiavimo internete prevencijos vadybininkas
JohnBank@gmail.com

ZIP **Bandymu-prisijungti-sarasas.zip**

Sukčiavimo el. laiškai su priedais

- **Kodėl tokio tipo atakos būna sėkmingos?** Sukčiavimo atakos atrodo įtikinamai, kai sudaromas įspūdis, kad tai patikimas šaltinis. Užpuolikai naudoja sudėtingesnes sukčiavimo atakas, kurias sunku aptikti.
- **Taikinys:** visi gyventojai
- **Grėsmė:**
  - Sukčiavimo atakos kopijuoja mūsų esamas darbo sekas.
  - Sukčiai prašo atidaryti prisegtas nuotraukas, muzikos failus, filmus, dokumentus (pvz., PDF, DOC, ZIP), kuriuose yra įdiegta kenkėjiška programinė įranga.
  - Sukčiai prideda HTML failus: juose yra visi sukčiavimui reikalingi elementai, užpuolikams nereikia skelbti HTML failų internete
- **Pažeidžiamumai:**
  - gyventojai, turintys nepakankamai žinių apie sukčiavimo atakas (kurie atidaro priedus)
- **Sukčiavimo taktika:**
  - Elektroniniai laiškai su priedais: failas su verslo ar individualiu pasiūlymu, failas su „konfidencialia“ ar „labai svarbia“ informacija, pardavimo ar finansinė informacija (neapmokėtos sąskaitos faktūros, pirkimo užsakymas), skubus balso pranešimas, atnaujinta organizacijos politika, failai su techninėmis problemomis, konkretaus laikotarpio informacija, pvz., pandemija ir pan.
  - Elektroniniai laiškai, kuriuose prašoma užpildyti pridedamą dokumentą, skirtą svarbiems darbo procesams
- **Sukčiavimo faktoriai:**
  - **Skubos jausmo sukėlimas**
  - **Užpuolikai naudojasi aukos emocijomis ir instinktais**
- **Rezultatas:**
  - užkrėsti kompiuteriai, tapatybės vagystė, pinigų praradimas

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo el. laiško pavyzdžiai:
Sukčiavimo el. laiškai su priedais

Nespauskite el. laiške esančių nuorodų, neatidarykite priedų, net jei juos siunčia patikimas asmuo.

Siuntėjas: Jonas Vidliauskas <cdg446@comcast.net>

Kam: Lina Singaitė <lina.singaite@*organizacijospav.com*>

Tema: labas Lina

Jums reikia skubiai atlikti sąskaitos faktūros apmokėjimą.
Maloniai prašau pranešti man, ar galite kuo greičiau apmokėti.

Pagarbiai
Jonas Vidliauskas

Sent from my iPhone

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

Kam:

Tema: ABC banko sąskaitų priežiūros departamentas

Gerbiamas ABC banko naudotojau,

pastebėjome neįprastą veiklą jūsų kredito/debetinėje sąskaitoje. Dėl to turime apriboti prieigą prie jūsų banko sąskaitos. Jūsų ribota prieiga išliks tol, kol problema bus išspręsta.

Mes stengiamės užtikrinti Jūsų sąskaitos saugumą, todėl dėkojame už Jūsų supratimą.

Siekdami užtikrinti jūsų sąskaitos saugumą, pridedame dokumentą, kurį turite atidaryti interneto naršyklėje. Atlikite atidarytame tinklalapyje pateiktus veiksmus, norėdami atkurti savo paskyrą.

Su pagarba
ABC banko sąskaitų priežiūros departamentas

Sukčiavimo el. laiškų pavyzdžiai:
Sukčiavimo el. laiškai su nuoroda / priedu

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

Kam: man

Tema: info@wetransfering-files.net **siunčia atnaujintą organizacijos politiką**

we

info@wetransfering-files.net per WeTransfer siunčia atnaujintą organizacijos politiką

1 dokumentas, 25.6 KB · dokumentas saugomas 2 dienas

Svarbi informacija darbuotojams!

Siunčiamas konfidencialus dokumentas - atnaujinta organizacijos politika. Atsisiųskite jį ir atidžiai perskaitykite, kitaip negalėsite naudotis savo darbo vietos patalpomis ar informacinėmis sistemomis. Sistemos saugumo grupė

Atsisiųsti dokumentą

Atsisiuntimo nuoroda https://bit.ly/2YI6BY6

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

Kam:

Tema: Svarbu: įspėjimas apie duomenų saugumą

Microsoft

Gerbiamas Microsoft naudotojau,

Rūpindamiesi jūsų saugumu internete, siunčiame jums saugos pranešimą. Pastebėjome, kad jūsų dokumentas su slaptais duomenimis yra laisvai prieinamas internete.

Primename, kad dalydamiesi kitų asmenų neskelbtina informacija pažeidžiate BDAR. Už tai gali tekti sumokėti didelę baudą.

Atsisiųskite dokumentą ir pakeiskite bendrinimo parinktis.

Atsisiųsti dokumentą.

Microsoft saugumo komanda

Personalizuotas sukčiavimas el. paštu (angl. Spear Phishing)

- **Kodėl tokio tipo atakos būna sėkmingos?** Personalizuoto sukčiavimo el. paštu pranešimai skirti konkrečiai aukai, tokiai atakai ruošiamasi ilgą laiką. Tokios atakos sėkmingos, kai įmonės neturi IT naudojimo politikos arba jos neįgyvendina. Kiekvienas „spear phishing“ el. laiškas atrodo autentiškas. Kai auka vykdo nurodytą prašymą ir t. t.
- **Taikinys.** Darbuotojai: personalo vadovai, buhalterių komanda, žmogiškųjų išteklių komanda ir t. t.
- **Grėsmė:**
  - sukčiai kopijuoja eilinius darbo procesus.
- **Sukčiavimo taktika:**
  - Naudojami el. laiškai su priedais: failas su verslo ar individualiu pasiūlymu, failas su „konfidencialia“ ar „labai svarbia“ informacija, pardavimo ar finansinė (neapmokėtos sąskaitos faktūros, pirkimo užsakymas) informacija, skubus balso pranešimas ir pan.
  - Elektroniniai laiškai su nuorodomis į netikras svetaines
- **Sukčiavimo faktoriai:**
  - **Skubos jausmo sukėlimas**
  - **Užpuolikai naudojasi aukos emocijomis ir instinktais**
- **Pažeidžiamumai:**
  - darbuotojų, turinčių ribotas žinias apie sukčiavimą arba neturinčių jokių žinių apie sukčiavimą.
- **Rezultatas:**
  - Konfidencialios informacijos praradimas, intelektinės nuosavybės praradimas, verslo paslapčių praradimas, užkrėsti skaitmeniniai įrenginiai ir pan.

Funded by the Erasmus+ Programme of the European Union

Personalizuotas sukčiavimas el. paštu (vadovas): Sukčiavimo el. laiškai su prašymu / priedu

CyberPhish

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

Kam: man

Tema: Skubiai apmokėti sąskaitą

Labas Diana,
šiuo metu esu susitikime ir jame užtruksiu kelias valandas.
Kadangi vyks intensyvios diskusijos, turėsiu ribotą prieigą prie darbinio el. pašto ir negalėsiu atsiliepti mobiliuoju telefonu.
Ką tik gavau žinutę, kurioje pranešama, kad vėluojame apmokėti sąskaitą mūsų išskirtiniam partneriui.
Tam, kad prekes gautume laiku, **prašau šiandien skubiai atlikti mokėjimą tiesiogiai partnerio tiekėjui**.

Banko duomenys: AA 00 0000 0000 0000 0000 0000 0000.
Mokėjimo paskirtis: už prekes

Pasitikiu Tavimi, Diana, kad laiku atliksi pavedimą.
Bill Jonson

Siuntėjas: Vadovė <eliza.strieliute53@yahoo.com>

Kam: man

Tema: Einamojo mėnesio atlyginimai

Sveiki, Tomai,

Šiandien dirbu namuose, todėl rašau iš savo asmeninio el. pašto.

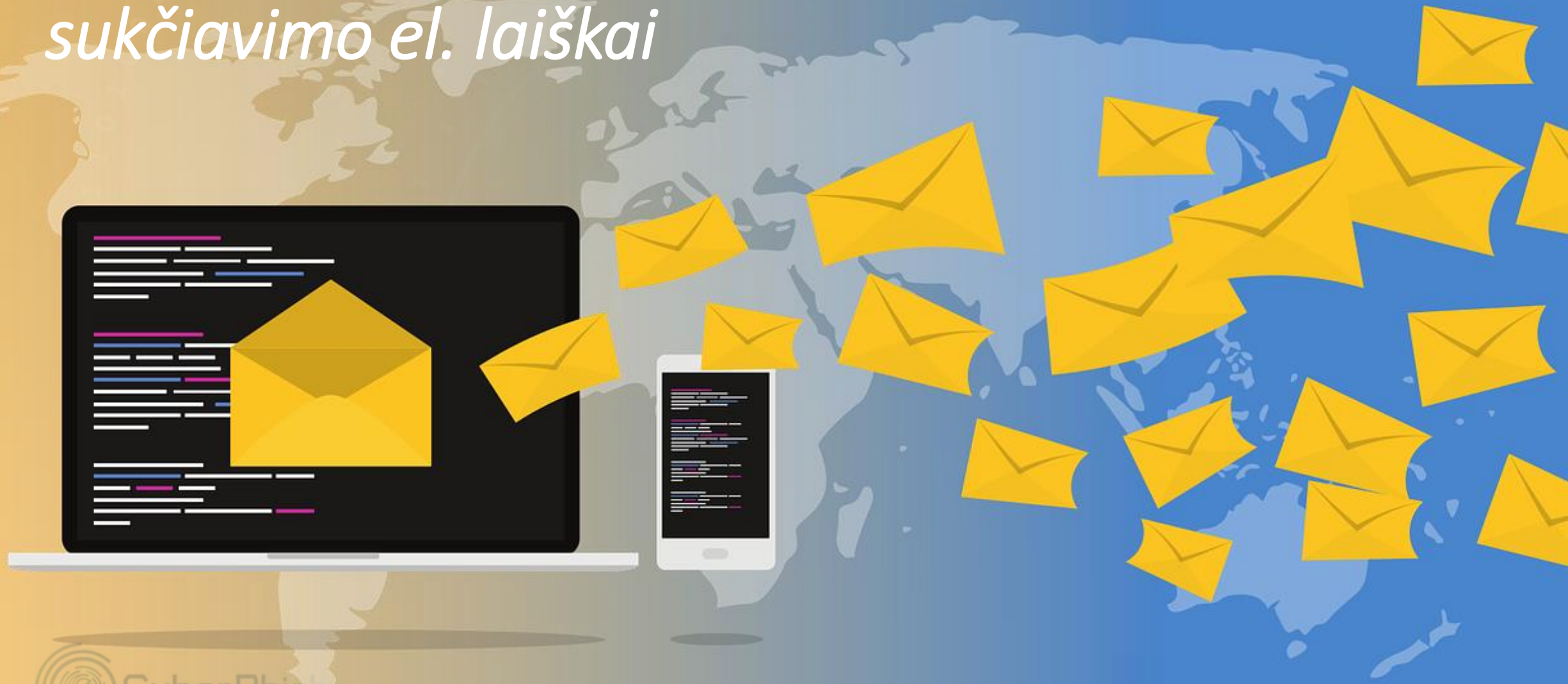
Atnaujinau einamojo mėnesio atlyginimus ir padariau keletą pakeitimų. Atsiprašau už šį nesusipratimą, tikiuosi, kad galėsite atlikti pakeitimus ir visi darbuotojai gaus atlyginimus laiku.

Susisiekite su manimi, jei turite klausimų.

Pagarbiai
Eliza Strieliūtė, Vadovė

Atnaujinti-atlyginimai.xls

Techninės pagalbos sukčiavimo el. laiškai



CyberPhish
Safeguarding your digital future

Sukčiavimas: Techninė pagalba

- **Kodėl tokio tipo atakos būna sėkmingos?** Naudodamiesi skaitmeniniais prietaisais naudotojai paprastai gauna įvairių klaidų arba įspėjimų. Todėl sukčiai gali teigti, kad jie teikia techninę pagalbą ir siūlo padėti išspręsti saugumo pažeidimus naudojant nuotolinės prieigos programinę įrangą arba spustelėjus el. laiške esančią nuorodą.
- **Taikinys:** visi gyventojai, ypač skaitmeninių įgūdžių neturintys žmonės, vyresnio amžiaus žmonės.
- **Grėsmė:**
  - sukčiai kopijuoja eilinius darbo procesus.
  - užpuolikai prašo paspausti el. laiške pateiktą nuorodą arba paskambinti nurodytu telefono numeriu
- **Sukčiavimo taktika:**
  - El. laiškai apie pažeistus el. pašto adresus ar slaptažodžius
  - El. laiškai apie dokumentus, skirtus bendradarbiavimui
  - El. laiškai, informuojantys apie technines problemas
- **Sukčiavimo faktoriai:**
  - Skubos jausmo sukėlimas
  - Baimės jausmo sukėlimas
  - Užpuolikai naudojasi aukos emocijomis ir instinktais
- **Pažeidžiamumai:**
  - gyventojai, turintys nedaug žinių apie sukčiavimą arba neturintys jokių žinių apie jį.
- **Rezultatas:**
  - Išpirkos reikalaujanti programinė įranga gali užkrėsti skaitmeninį įrenginį, sukčiai gali gauti prieigą prie skaitmeninio įrenginio; įgiję prieigą prie įrenginio sukčiai gali jį panaudoti vėlesnėms atakoms, pakeisti įrenginio nustatymus, pavogti slaptus duomenis. Vartotojas gali prarasti pinigus ir t. t.

Sukčiai taip pat gali naudoti kito tipo atakas:
Iškylančių langų pranešimai
Suklastotos svetainės (plačiau *Sukčiavimas naudojant svetaines*)
Netikėti skambučiai (plačiau *Telefoninis sukčiavimas*)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Techninės pagalbos el. pašto sukčiavimo pavyzdys

Siuntėjas: El. pašto pagalba<tech-support.954mail-delivery352477@cloud.website.com>

Kam: Lucy Bradson

Tema: El. laiško pristatymo klaida

Labas lucy.bradson

El. pašto serveriui kyla problemų tikrinant jūsų el. paštą.

Naujų laiškų negalėsite gauti, kol nepatvirtinsite šios pašto dėžutės.

Automatiškai patikrinkite savo pašto dėžutę dabar naudodamiesi toliau pateikta instrukcija.

JUNGTIS PRIE SAVO PASKYROS

Jūsų el. pašto paskyra bus IŠJUNGTA po 24 valandų, jei nebus imtasi reikiamų veiksmų.

El. pašto administratorius

Techninės pagalbos sukčiavimas telefoniniais skambučiais

Techninės pagalbos sukčiavimas: pavyzdys

Microsoft Saugumo Pranešimas X

Jūsų kompiuteryje aptiktas pavojingas virusas.

Prašome nedelsiant skambinti
1 877 00 11 00 145.

Jūsų IP adresas:
147.254.114.741

Data:
2022 m. sausio 10 d.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo laiškai: Romantiniai santykiai (angl. Cat Phishing)

- **Kodėl tokio tipo atakos būna sėkmingos?** Yra žmonių, kurie yra vieniši, išsiskyrę. Jie gali gauti sukčių apgaulingus el. laiškus arba socialinės žiniasklaidos pranešimus arba sukčiai gali būti užsiregistravę pažinčių svetainėse.
- **Taikinys:** vieniši, išsiskyrę žmonės, žmonės, ieškantys naujų santykių, socialinės žiniasklaidos vartotojai
- **Grėsmė:**
  - Sukčiai, turintys suklastotą tapatybę, greitai užmezga santykius ir įgyja aukos pasitikėjimą. Po to sukčiai prašo pinigų ir gavę juos dingsta.
- **Sukčiavimo taktika:**
  - Nežinomo asmens el. laiškai
  - Tekstinė žinutė per socialinius tinklus, tiesioginio susirašinėjimo programas
- **Sukčiavimo faktoriai:**
  - **Greitai užmezga santykius**
  - **Skuba įgyti aukos pasitikėjimą**
- **Pažeidžiamumai:**
  - emociškai pažeidžiami asmenys
- **Rezultatas:**
  - finansiniai nuostoliai.

Funded by the Erasmus+ Programme of the European Union

Pavyzdys: Romantiniai santykiai (angl. Cat Phishing)

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

Kam: man

Tema: mano meilei

Mano meile,

esu labai laimingas turėdamas galimybę surasti tave, nes tik tu visame pasaulyje gali mane suprasti. Jaučiu, kad esi mano antroji puselė. Tikiu, kad tūkstantis kilometrų nepaveiks mūsų artimų santykių. Padarysiu viską, ką galiu, kad atvykčiau į Tavo šalį, pakeisiu savo darbą ir likusį gyvenimą praleisčiau didelėje laimėje su Tavimi.

Laukiu tavo žinutės.
Su meile, Džonas

Illustration by Freepik Storyset

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

Kam: man

Tema: mano meilei

labas, mano meile,

tu nepatikėsi, bet norėjau padaryti tau staigmeną ir pamatyti tave tavo mieste. Kai nusileidau Frankfurte, turėjau 18 valandų laukti kito lėktuvo. Todėl nuvykau į miesto viešbutį, o čia pavogė mano krepšį. Ar galėtumėte man padėti, prašau. Apsistojau viešbutyje ir rytoj turiu apmokėti viešbučio sąskaitą. Ar galėtumėte padengti mano viešnagės išlaidas?

Laukiu tavo žinutės kuo greičiau, brangioji.
Su meile, Džonas

Viliojimas arba masalas

Viliojimas arba masalas

- **Kodėl tokio tipo atakos būna sėkmingos?** Žmonės yra linkę pasitikėti ir tiki, kad gali ką nors gauti nemokamai, nusipirkti su nuolaida, gauti pinigų ar prizų.
- **Taikinys:** visi piliečiai, įskaitant darbuotojus.
- **Grėsmė:**
  - sukčiai siūlo ką nors labai patrauklaus, pvz., atsisiųsti muzikos, filmų, siūlo netikėtus laimėjimus ar apdovanojimus, didžiules nuolaidas ir pan.
- **Sukčiavimo taktika:**
  - El. laiškai, iššokantys langai, tekstinės žinutės, pranešimai socialiniuose tinkluose su labai patraukliu pasiūlymu
  - Netoli biuro patalpų pamestos USB laikmenos

- **Sukčiavimo faktoriai:**
  - **Melagingas pažadas**
  - **Godumo jausmo sukėlimas**
  - **Smalsumo jausmo sukėlimas**
- **Pažeidžiamumai:**
  - godūs ar smalsūs asmenys, nerūpestingi darbuotojai
- **Rezultatas:**
  - gauta slapta informacija, tapatybės vagystė, intelektinės nuosavybės vagystė, sabotažas, pinigų praradimas, įdiegta kenkėjiška programinė įranga.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Viliojimas arba masalas.
Pavyzdys: el. paštu siūloma nuolaida

Siuntėjas: Juodojo penktadienio pasiūlymas <Black-Friday-Proposal@trust-fridays.com>

Kam: man

Tema: Sveikiname! Jūs gavote slaptą pasiūlymą

www.trust-fridays.com/discounts/sdtuyx5D7rtkh6

Neįtikėtinai didelės nuolaidos arba mažos labai gerai žinomų prekių ženklų ir produktų kainos

Viliojimas arba masalas.
Pavyzdys: el. paštu siūloma susigrąžinti mokesčius

Siuntėjas: sPaslaugų vartai<do-not-reply@online-gateway.com>
Kam: man
Tema: Vyriausybės išmoka dėl COVID-19

Tiems, kam tai gali būti aktualu:

Vyriausybė ėmėsi veiksmų, padedančių nuo Covid-19 nukentėjusiems piliečiams ir organizacijoms.

Informuojame, kad turite teisę gauti vienkartinę 2 500 EUR kompensaciją.
Norėdami gauti šią kompensaciją, turite užpildyti šią formą.

Šį pranešimą automatiškai sugeneravo ePaslaugų vartų portalas

Sukčiai gali sekti realaus gyvenimo įvykius ir panaudoti juos išpuoliams, taip pat gali siūlyti paklausius produktus arba susigrąžinti mokesčius, kaip šiame pavyzdyje.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Viliojimas arba masalas.
Pavyzdys: el. paštu siunčiamas laimėjimas, apdovanojimai

Siuntėjas: Ade Goodchild <admin>

Kam: man

Tema: laba diena

Laba diena,

Jūsų el. paštą atsitiktine tvarka pasirinko mano fondas, jums skiriamas 1 000 000,00 Eur (vienas milijonas Eurų), iš kurių bent 20 % turite panaudoti nepasiturintiems asmenis sušelpti, likusią sumą galėsite panaudoti laimėjimo administravimui ir nereikės pateikti išlaidų pagrindimo dokumentų.

Daugiau informacijos apie tai, kaip tapau milijonieriumi, skaitykite https://www.bbc.cominews/uk-england-hereford-worcester-47637306

Maloniai prašome patvirtinti savo elektroninio pašto nuosavybę, nedelsdami atsiųsdami atsakymą man, ir aš išsamiai paaiškinsiu, ka iums reikia žinoti.

Nuoširdžiai,
Ade Goodchild Goodchild fondas

Masalo sukčiai gali siųsti el. laiškus, kuriuose informuoja aukas apie laimėjimus, apdovanojimus ir lengvus pinigus.

Turinys

Atakos, vykdomos panaudojant realius ir aktualius įvykius

El. pašto laiškai

Tekstinės žinutės

Svetainės

Netikrų loterijų pranešimai

Skambučiai telefonu

Gyvai vykstančios atakos

Stebėjimas per petį

Tekstinės žinutės

- Trumposios žinutės, siunčiamos telefonais, programėlėmis ar socialinės žiniasklaidos platformomis.
- Užpuolikai gali naudoti tokią taktiką:
  - prašyti atsiųsti konfidencialią ar asmeninę informaciją teksto žinute
  - prašyti spustelėti pateiktą nuorodą teksto žinutėje
  - Prašo atidaryti priedą
  - skambinti nurodytu telefono numeriu
- Įprastos sukčiavimo tekstinių žinučių temos:
  - Atnaujinti asmeninę arba prekių pristatymo informaciją
  - Gauti didelę nuolaidą arba dalyvauti konkurse dėl prizo
  - Sąskaitos problemos
  - Romantiniai santykiai
  - Teikti finansinę paramą

Tekstinės žinutės

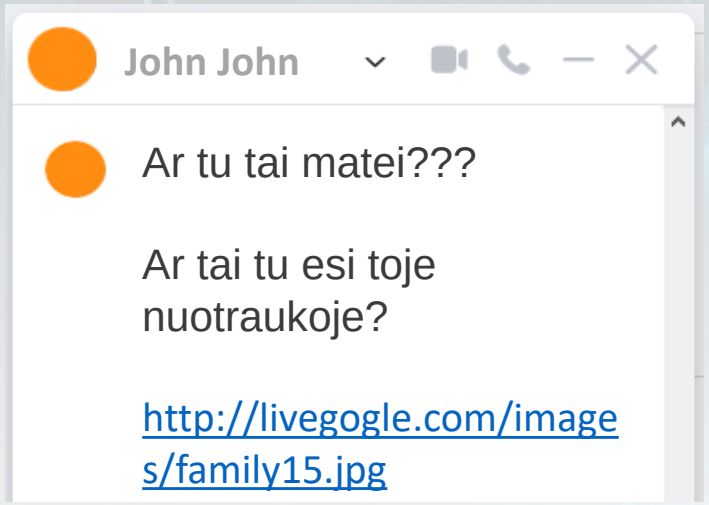
- Tekstiniai pranešimai atrodo kaip iš patikimų šaltinių.
- Apgaulingos tekstinės žinutės gali būti siunčiamos per įvairias platformas:
  - Tiesioginio susirašinėjimo žinutės: Hangouts, Skype ir kt.
  - Socialinių tinklų platformos: „Instagram“, „Facebook“, „LinkedIn“, „Snapchat“, „Twitter“ ir kt.
  - Sukčiavimas SMS žinutėmis (angl. smishing): įskaitant „WhatsApp“, „Telegram“, „Viber“)
- Apgaulingose tekstinėse žinutėse dažnai naudojamos sutrumpintos nuorodos

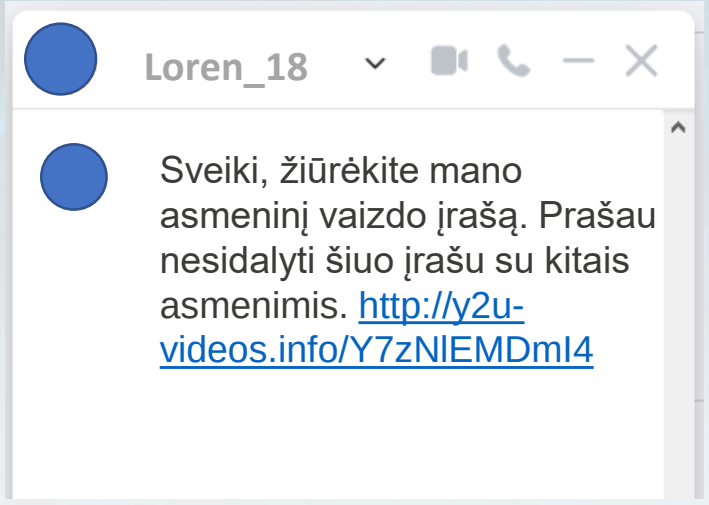
Funded by the Erasmus+ Programme of the European Union

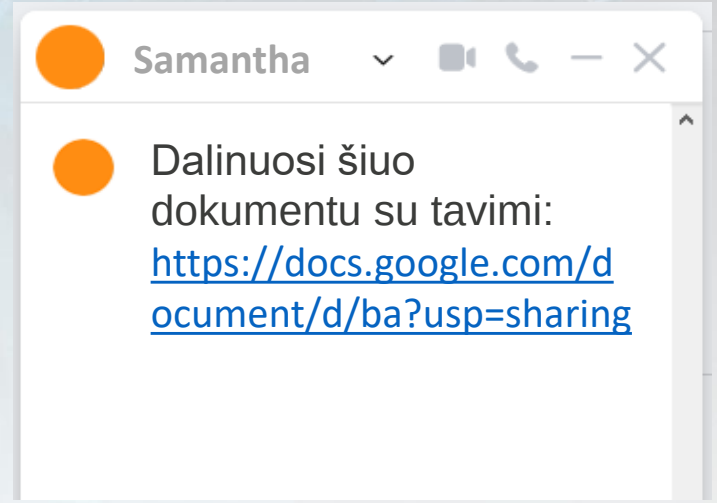
Tekstinės žinutės socialiniai tinklai ir tiesioginio susirašinėjimo programos

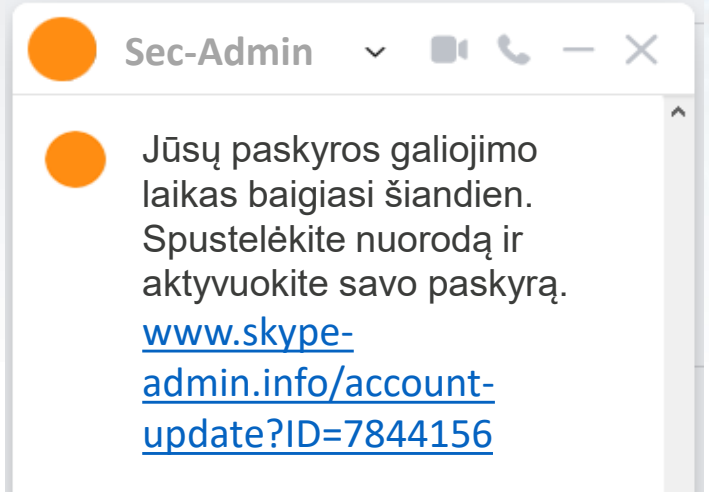
- **Kodėl tokio tipo atakos būna sėkmingos?** Tokias žinutes sudėtinga atskirti nuo tikrų pranešimų (dažniausiai sukčiai naudoja tiesioginio susirašinėjimo programų kirminą, kuris užkrečia įrenginius paspaudus nuorodą arba atidarius priedą) ir pan.
- **Taikinys:** visi gyventojai
- **Grėsmė:**
  - žinutės su priedais, su nuorodomis, žinutės, kuriose prašoma finansinės paramos, romantiškų sukčių žinutės ir pan.
- **Atakos metodas:** tekstinės žinutės per tiesioginių susirašinėjimo programas ar žinutės socialiniais tinklais iš esamų ar nežinomų kontaktų.
- **Sukčiavimo faktoriai:**
  - **Skubos jausmo sukėlimas**
  - **Baimės jausmo sukėlimas**
  - **Pasinaudojimas naivumu**
- **Sukčiavimo taktika:**
  - Trumpa žinutė (paprastai vienas ar du sakiniai) su nuoroda.
  - Žinutėse prašoma atnaujinti paskyrą, pakeisti nustatymus, atidaryti dokumentus ar nuotraukas, siūlo gerų nuolaidų ir pan.
  - Trumpa žinutė (paprastai vienas ar du sakiniai) su priedu.
  - Trumposios žinutės, kuriose prašoma finansinės paramos
- **Pažeidžiamumai:**
  - gyventojai, turintys nedaug žinių apie sukčiavimą arba neturintys jokių žinių apie sukčiavimą ir nesitikintys būti apgauti trumposiomis žinutėmis.
- **Rezultatas:**
  - Užkrėsti skaitmeniniai įrenginiai, tapatybės vagystė, prisijungimų prie sistemų vagystė, pinigų praradimas

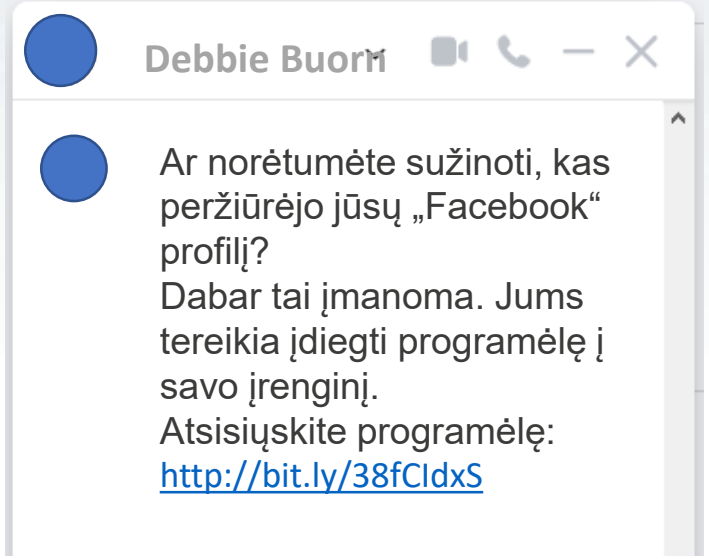
Tekstinės žinutės
Tiesioginio susirašinėjimo žinučių sukčių pavyzdžiai

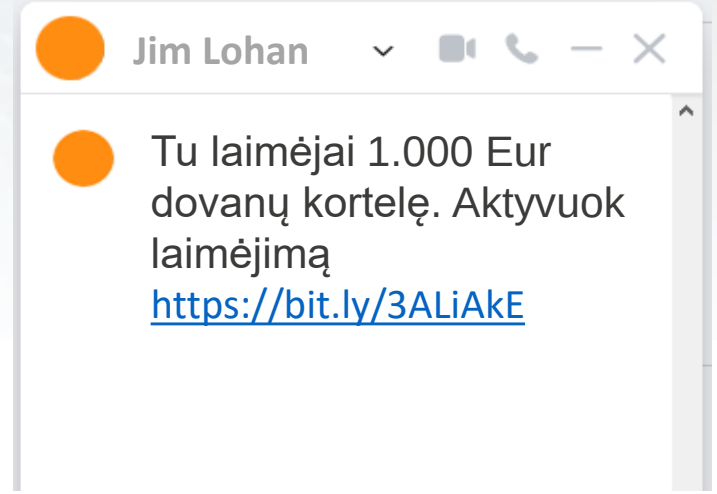












Tekstinės žinutės
Socialinių tinklų sukčių žinučių pavyzdžiai

Instagram

Sveiki, kažkas kelis kartus nesėkmingai bandė prisijungti prie jūsų paskyros. Dėl saugumo priežasčių jūsų paskyra užblokuota. Norėdami atrakinti, prisijunkite čia ir pateikite šį kodą:
753147

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

Instagram

Nustatėme, kad paskelbėte turinį, kuris pažeidžia autorių teisės. Jūsų paskyra buvo užblokuota.

Spauskite čia norėdami aktyvuoti savo paskyrą.

© 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

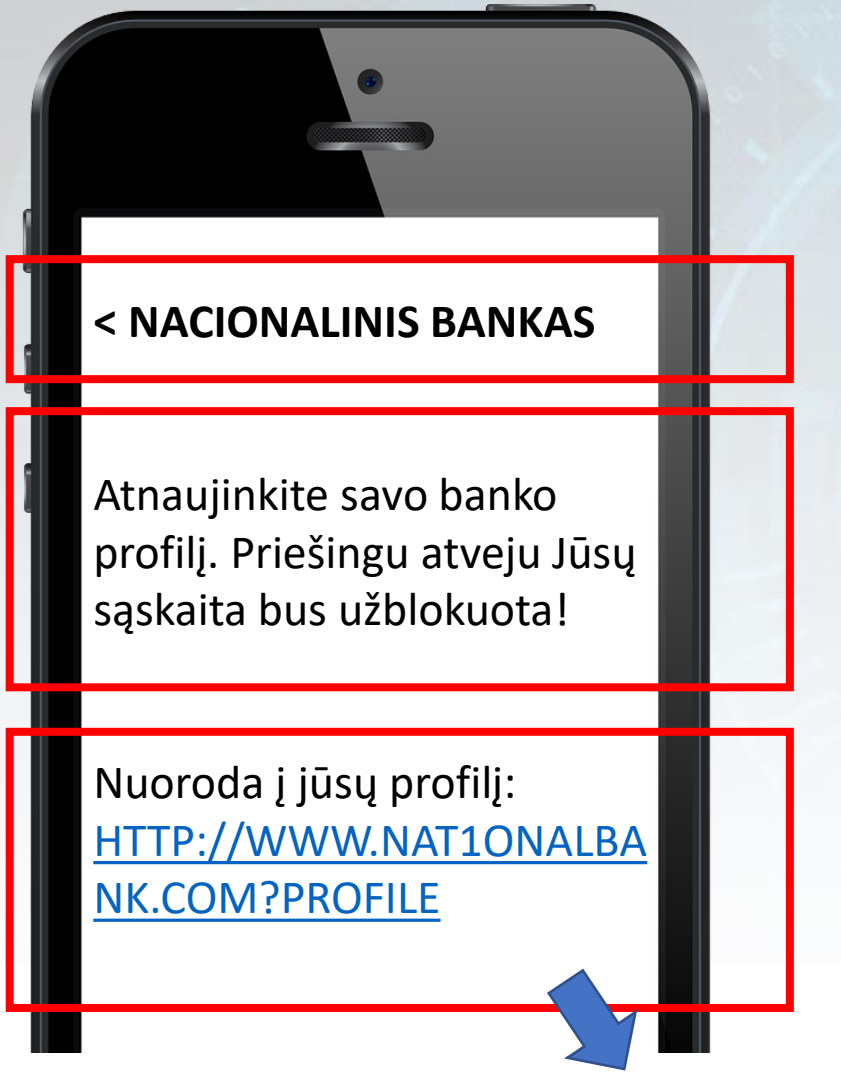
Sukčiavimas SMS žinutėmis (angl. Smishing)

CyberPhish

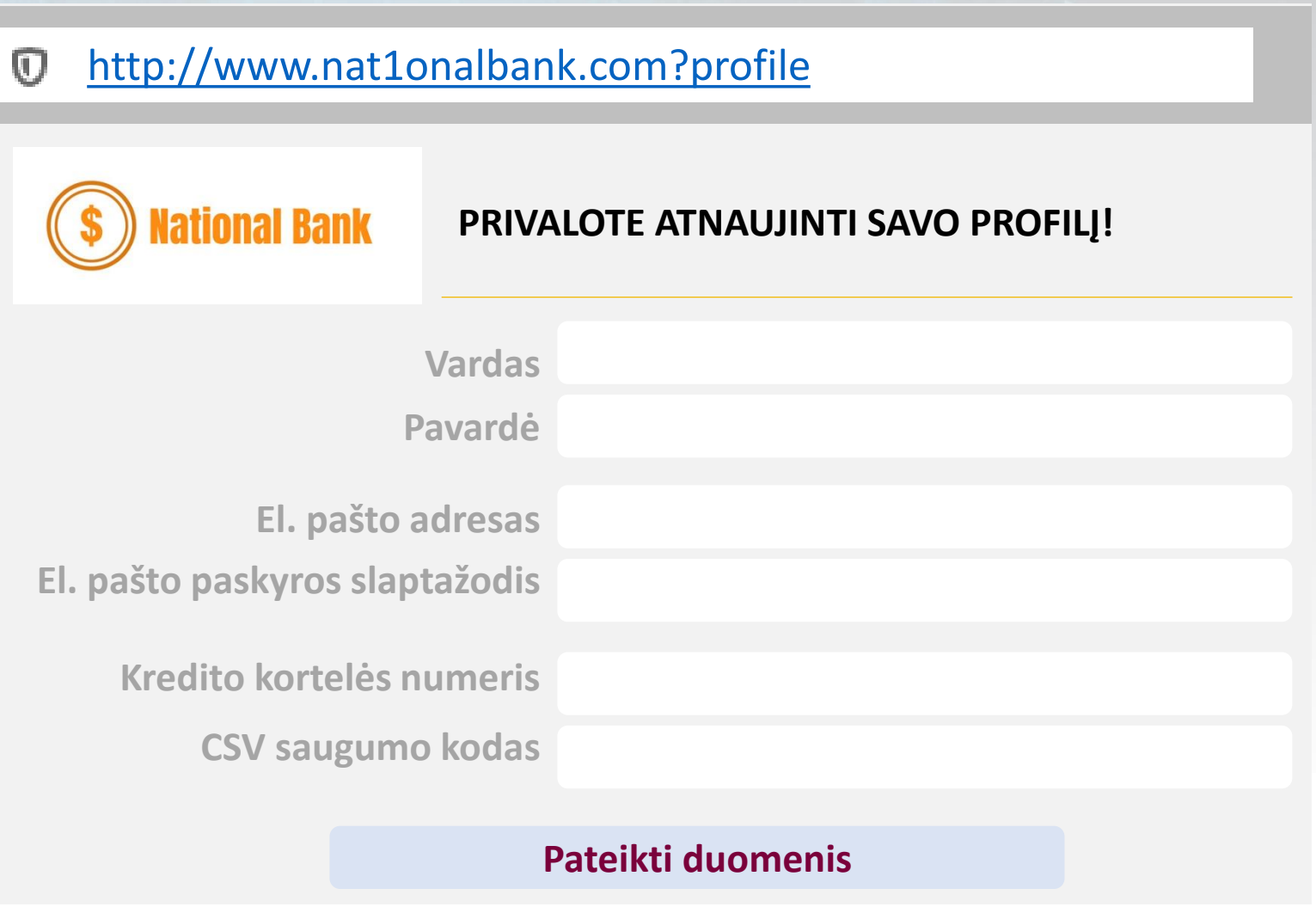
Tekstinės žinutės: SMS (angl. Smishing)

- **Kodėl tokio tipo atakos būna sėkmingos?** Sudėtinga atskirti nuo tikrų žinučių (paprastai sukčiai naudoja tikrus įstaigų pavadinimus).
- **Taikinys:** visi gyventojai
- **Grėsmė:**
  - žinutės su nuorodomis, žinutės, kuriose prašoma suteikti finansinę paramą, prašoma atsakyti arba paskambinti.
- **Atakos metodas:** SMS tekstinės žinutės.
- **Sukčiavimo taktika:**
  - Trumpa žinutė (paprastai vienas ar du sakiniai) su nuoroda. Žinutėse prašoma pakeisti nustatymus, atnaujinti paskyrą, pakeisti siuntos duomenis ir pan.
- **Sukčiavimo faktoriai:**
  - **Skubos jausmo sukėlimas**
  - **Baimės jausmo sukėlimas**
  - **Pasinaudojimas naivumu**
- **Pažeidžiamumai:**
  - gyventojai, turintys ribotas žinias apie sukčiavimą arba neturintys jokių žinių apie sukčiavimą ir nesitikintys, kad bus apgaudinėjami SMS žinutėmis.
- **Rezultatas:**
  - Užkrėsti skaitmeniniai įrenginiai, tapatybės vagystė, prisijungimo duomenų vagystė, pinigų praradimas

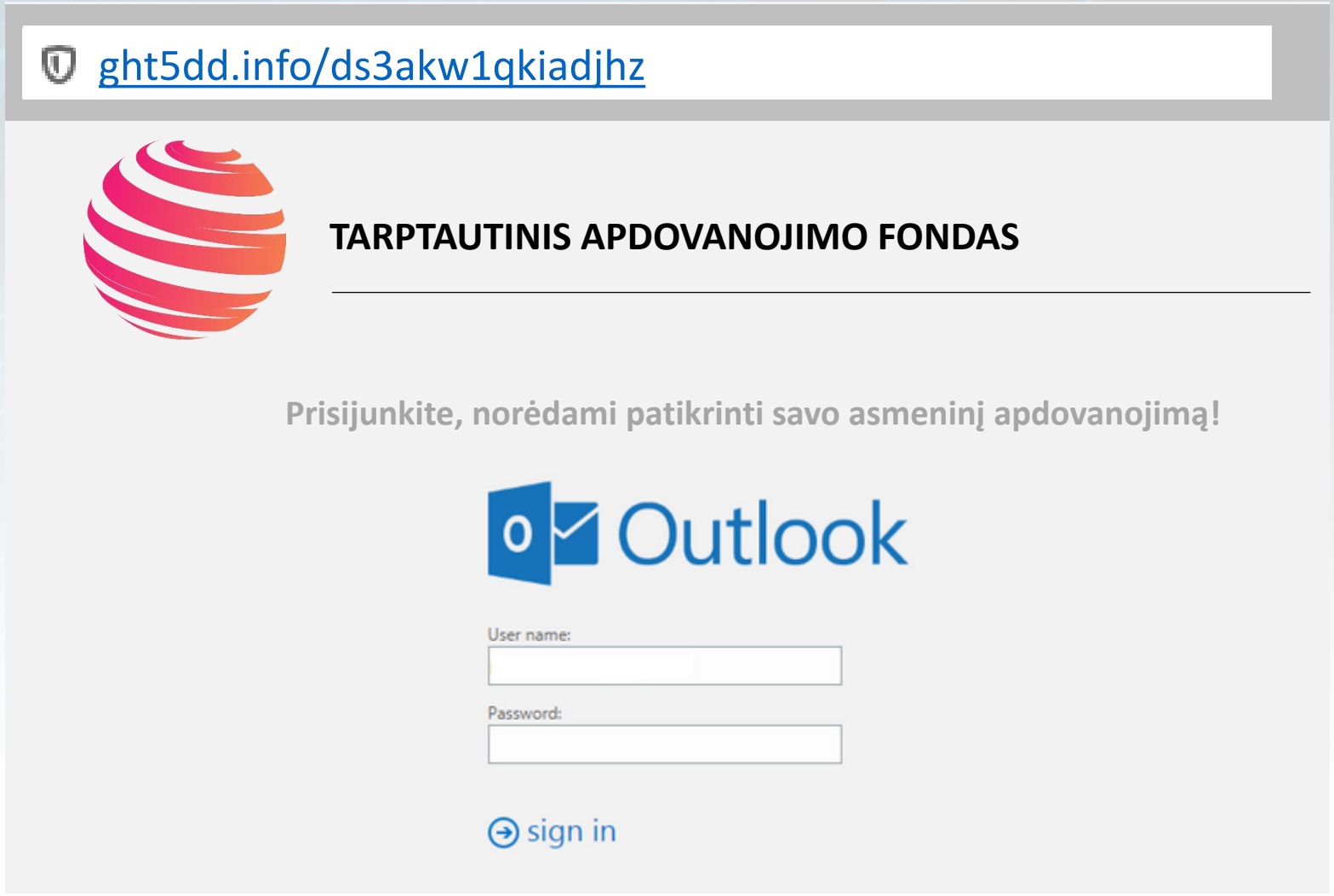
Tekstinės žinutės: sukčiavimo SMS žinutėmis pavyzdys



http://www.nat1onalbank.com?profile

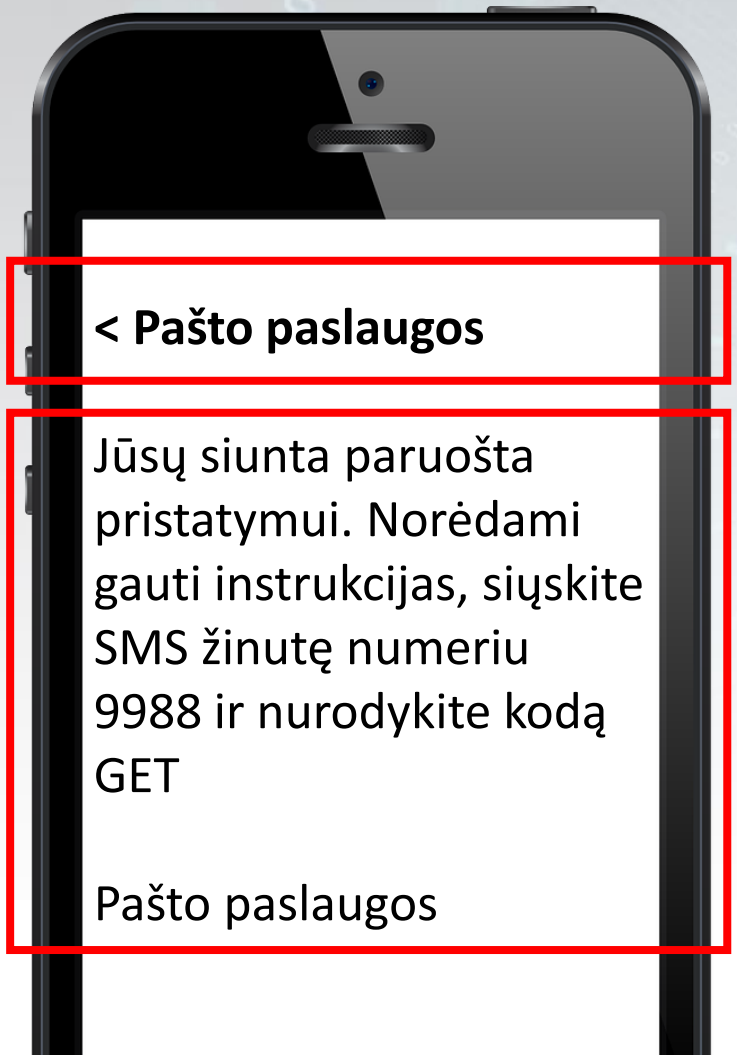


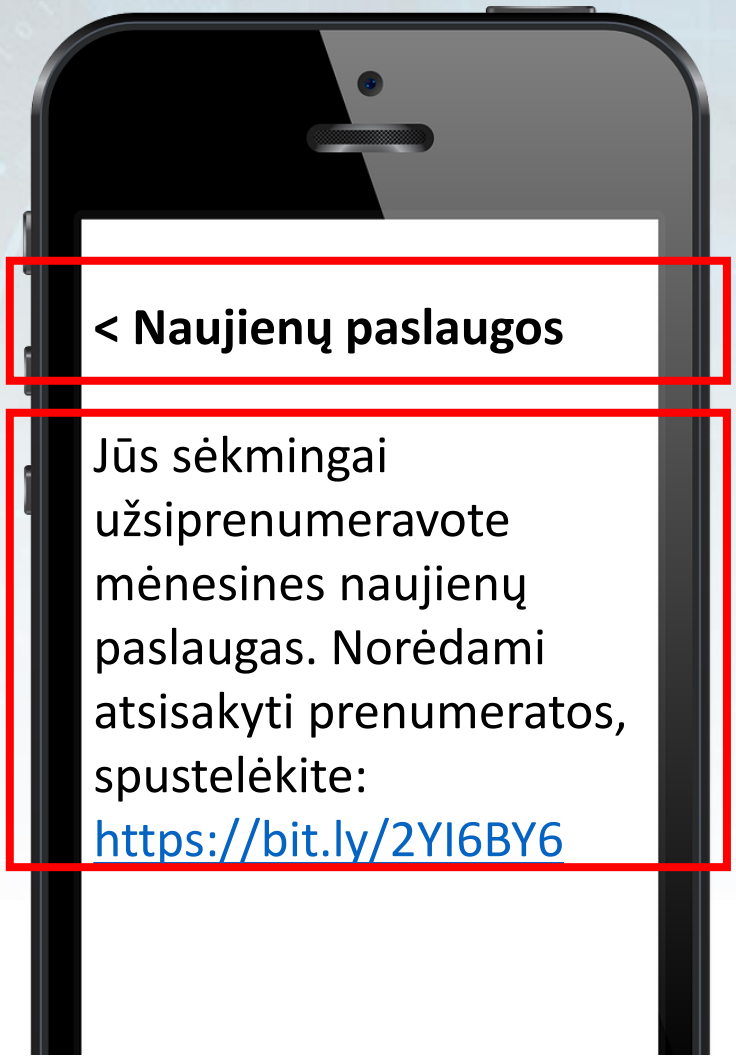
Tekstinės žinutės: sukčiavimo SMS žinutėmis pavyzdys



Tekstinės žinutės: sukčiavimo SMS žinutėmis pavyzdys

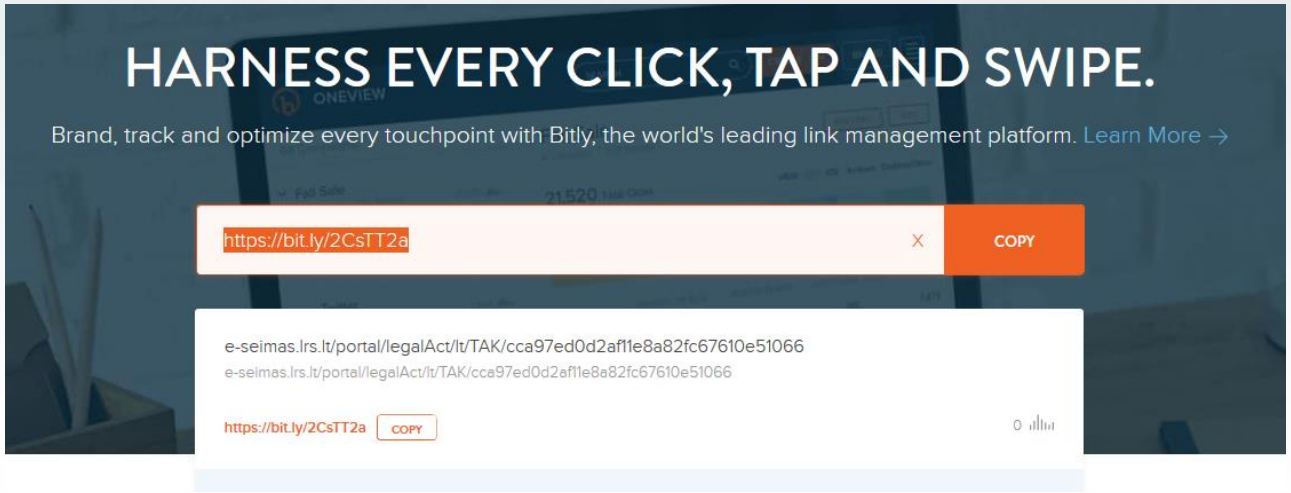
Tekstinės žinutės: sukčiavimo SMS žinutėmis pavyzdžiai





Nuorodų trumpinimas

- Sutrumpintos nuorodos dažnai naudojamos el. laiškuose, žinutėse, kadangi ilga nuoroda yra sutrumpinama.
- Nuorodų trumpinimo paslaugų tiekėjų pavyzdžiai:
  - 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

Nuorodų trumpinimo paslaugų naudojimo tikslai

- Sudėtinga įsiminti ilgą URL adresą
- Patogus naudojimas svetainėse, socialinėje žiniasklaidoje, spausdintuose leidiniuose
- Trumpą nuorodą patogu naudoti siunčiant SMS, trumpąsias žinutes
- Yra nuorodų trumpinimo paslaugų teikėjų, kurie gali sukurti žmogui suprantamus URL adresus, o ne simbolių „kratinį“

Funded by the Erasmus+ Programme of the European Union

Bit.ly santrumpos „išskleidimas“: adreso pabaigoje įrašant +

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Kas slepiasi po santrumpa?

CyberPhish

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

Informacijos apie svetainė patikrinimas

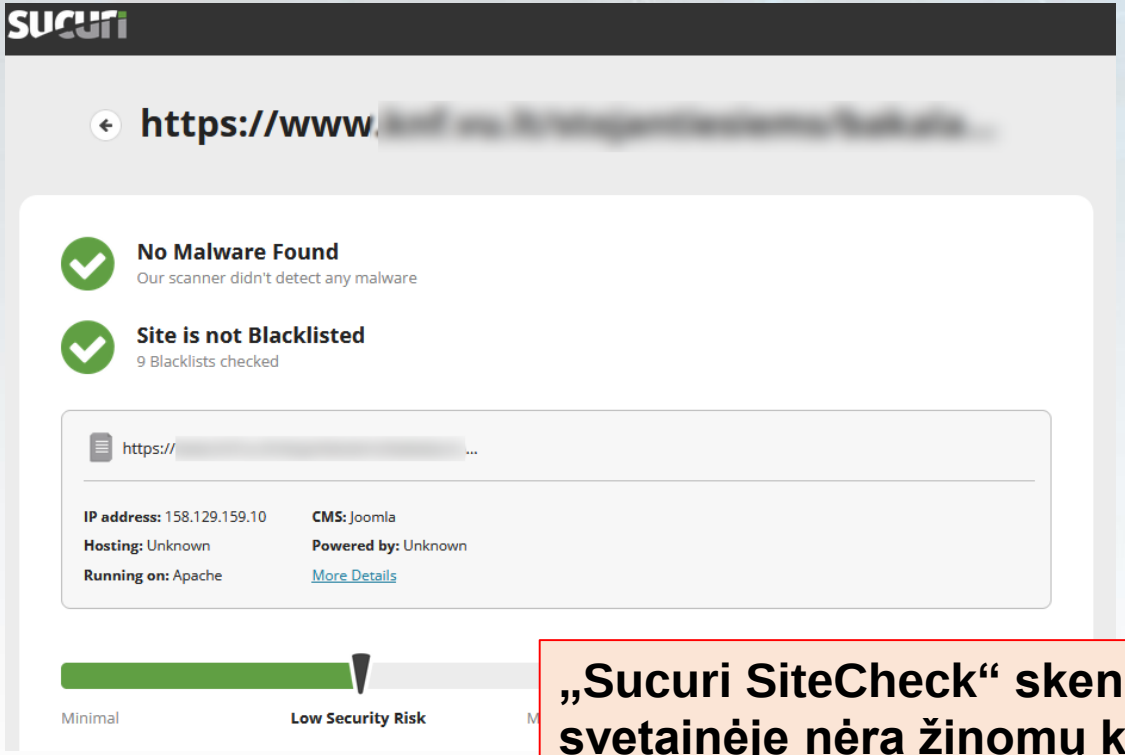
- http://www.getlinkinfo.com: patikrinkite, ar svetainėje yra kenkėjiškos programinės įrangos, ar tai yra sukčiavimo svetainė.

Funded by the Erasmus+ Programme of the European Union

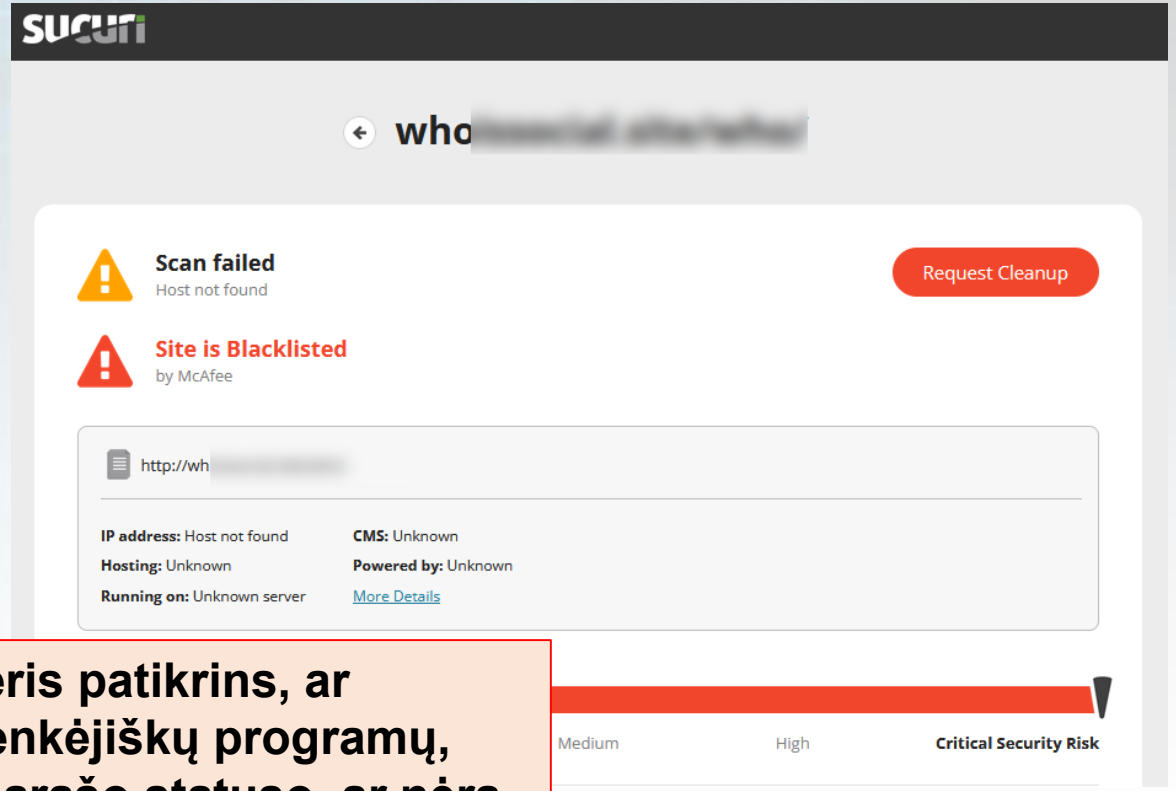
Informacijos apie svetainė patikrinimas

https://sitecheck.sucuri.net

Saugi svetainė



Nesaugi svetainė



„Sucuri SiteCheck“ skeneris patikrins, ar svetainėje nėra žinomų kenkėjiškų programų, virusų, ar neturi juodojo sąrašo statuso, ar nėra svetainės klaidų, pasenusios programinės įrangos ir kenkėjiško kodo.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Turinys

Atakos, vykdomos panaudojant realius ir aktualius įvykius	El. pašto laiškai	Tekstinės žinutės	Svetainės
Netikrų loterijų pranešimai	Skambučiai telefonu	Gyvai vykstančios atakos	Stebėjimas per petį

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Sukčiavimas naudojant svetaines

- Pasitelkiant interneto svetaines gali būti atliekami sukčiavimo veiksmai, apsimetant kuo nors kitu ar kitos teisėtos organizacijos svetaine
- Sukčiavimas interneto svetainėse gali būti naudojamas tokiais būdais:
  - **Suklastotos svetainės su suklastotu domeno adresu** – sukčiai sukuria labai gerai žinomų įstaigų ar organizacijų svetainių, kuriomis naudotojai pasitiki, suklastotos kopijos*
  - **Sukčių sukurtos svetainės, skirtos sukčiavimui** – sukčiai sukuria savo svetaines, pavyzdžiui, netikras internetines parduotuves, investicinius portalus*.
  - Sukčių puslapiai gali būti sukurti portaluose, kurie siūlo nemokamos svetainių kūrimo paslaugas
  - **Iššokantys langai** interneto svetainėse
  - Portaluose **naudojami reklamos blokai**, būna net ir patikimose svetainėse
- Netikrų svetainių nuorodos naudojamos sukčiavimo el. laiškuose, SMS, tiesioginio susirašinėjimo žinutėse, socialiniuose tinkluose ir pan.
- Paieškos portaluose atlikus paiešką, taip pat gali būti pateikiamos nuorodas į sukčių svetaines

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

Sukčiavimas naudojant svetaines

- Pagrindinis netikrų svetainių tikslas:
  - gauti prisijungimo prie informacinių sistemų duomenis,
  - gauti finansinę informaciją, pavyzdžiui, banko kortelių duomenis ir saugumo kodus
  - užkrėsti naudotojų įrenginius, nes tokiose svetainėse gali būti kenkėjiško kodo
- Sukčiai gali naudoti panašius į teisėtų tinklalapių domenų pavadinimus, paprastai pakeičiant vieną ar kelias domeno vardo raides, pavyzdžiui, vietoj „i“ naudoja raidę „l“; pvz.:
  - originalios svetainės adresas www.website.eu
  - suklastotos svetainės adresas www.webslte.eu

Funded by the Erasmus+ Programme of the European Union

Sukčiavimas naudojant svetaines

- Suklastotose svetainėse naudojamas toks pat dizainas, logotipai ir spalvos kaip ir teisėtose svetainėse, todėl jas sunku atpažinti. Todėl reikėtų patikrinti ir kitus požymius, pvz.:
  - URL adresas
  - Kontaktinė informacija
- Būkite atsargūs pateikdami prisijungimo duomenis arba finansinius duomenis, kai atidarote svetainę spustelėję nuorodą iš el. pašto laiško

Funded by the Erasmus+ Programme of the European Union

Suklastotos svetainės adresas

- Suklastotų svetainių URL paprastai prasideda HTTP
- Suklastotos svetainės taip pat gali prasidėti HTTPS
- HTTPS naudojama SSL sertifikatą, kuriuo patvirtinama svetainės nuosavybė ir užtikrinamas naudotojo duomenų saugumas: užtikrinamas saugus duomenų perdavimas tarp kliento ir serverio, tačiau HTTPS neįrodo, kad svetainė nėra sukurta sukčių.

Plačiau apie 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

Sukčiavimas naudojant svetaines

- **Kodėl tokio tipo atakos būna sėkmingos?** Sudėtinga atskirti suklastotas svetaines nuo tikrų svetainių. Naudojami kiti sukčiavimo veiksniai, siekiant paraginti naudotojus atidaryti svetaines, atlikti tam tikrus veiksmus.
- **Taikinys:** visi gyventojai
- **Atakos metodas:** suklastotų svetainių nuorodos gali būti naudojamos sukčių el. laiškuose, SMS žinutėse, tiesioginio susirašinėjimo programų socialinių tinklų žinutėse, gali būti naudojami kombinuoti metodai.
- **Sukčiavimo taktika:**
  - El. laiškai ar žinutės su nuoroda.
  - Žinutėse prašoma atnaujinti paskyrą, pakeisti nustatymus, atidaryti dokumentus ar nuotraukas, siūlo gerų nuolaidų ir pan.
  - Vartotojai, naudodami paieškos sistemą, gali rasti suklastotų ar sukčių svetainių: tai gali būti internetinės parduotuvės su geromis nuolaidomis
  - Sukčiai gali skambinti aukoms ir kviesti jas sėkmingai investuoti

- **Sukčiavimo faktoriai:**
  - **Skubos jausmo sukėlimas**
  - **Baimės jausmo sukėlimas**
  - **Godumo sukėlimas**
  - **Pasinaudojimas naivumu**
- **Pažeidžiamumai:**
  - asmenys, turintys nedaug žinių apie sukčiavimą arba neturintys jokių žinių apie sukčiavimą ir nesitikintys būti apgauti.
- **Rezultatas:**
  - Užkrėsti skaitmeniniai įrenginiai, tapatybės vagystė, prisijungimo duomenų vagystė, pinigų praradimas

Funded by the Erasmus+ Programme of the European Union

Sukčiavimas naudojant svetaines: suklastotos svetainės pavyzdys

http://sale-branding.store

Saugus apsipirkimas internetu

GERIAUSIOS KAINOS! VISI PREKĖS ŽENKLAI VIENOJE VIETOJE

SU 90% NUOLAIDA TIK ŠIANDIEN!

Funded by the Erasmus+ Programme of the European Union

Sukčiavimas naudojant svetaines: suklastotų svetainių pavyzdžiai

CyberPhish

http://mobile-company.online/prizes

SVEIKINIMAI!
Mūsų įmonė šiemet švenčia jubiliejų, todėl dalijamės džiaugsmu su savo klientais ir kviečiame jus atsiimti prizą visiškai nemokamai.

Laimėk vieną iš šių prizų:
Samsung Galaxy S21, Apple iPhone 13 Pro arba Samsung Watch 4 LTE.

153 dalyviai jau džiaugiasi prizais. Prizų skaičius ribotas!

Tau rezervuotas laikas: 1 min. 29 sek.

NORIU GAUTI SAVO PRIZĄ!

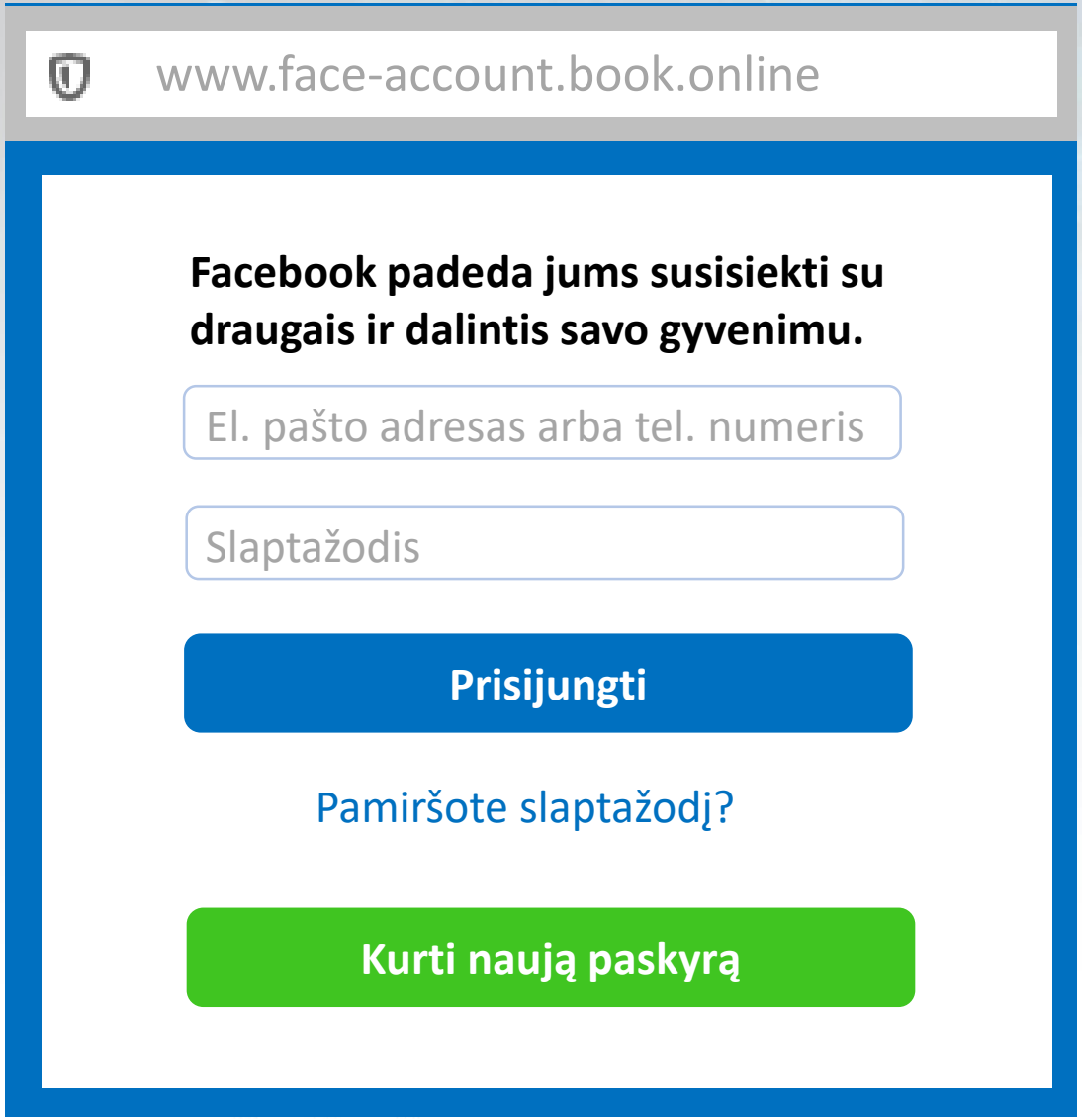
http://mobile-company.online/iwantget

Samsung Galaxy S21
Kaina: 780 Eur
Nėra sandėlyje
Nebeliko

Apple iPhone 13 Pro
Kaina: 920 Eur
Liko tik 2 vienetai
Gauti dabar!

Samsung Watch 4 LTE
Kaina: 320 Eur
Nėra sandėlyje
Nebeliko

Sukčiavimas naudojant svetaines: suklastotos svetainės pavyzdys



Funded by the Erasmus+ Programme of the European Union

Turinys

Atakos, vykdomos panaudojant realius ir aktualius įvykius	El. pašto laiškai	Tekstinės žinutės	Svetainės
Netikrų loterijų pranešimai	Skambučiai telefonu	Gyvai vykstančios atakos	Stebėjimas per petį

Funded by the Erasmus+ Programme of the European Union

Loterijų sukčiai

- Loterijų sukčiai naudoja įvairias priemones, kad sugautų savo aukas:
  - El. laiškus
  - SMS žinutes arba tiesioginio susirašinėjimo žinutes
  - Pranešimų žinutės socialiniuose tinkluose iš suklastotų paskyrų arba paskyrų, į kurias buvo įsilaužta
  - Skambinant telefonu
  - Interneto puslapiuose
- Aukoms ketinama perduoti didelę pinigų sumą, didelį prizą, pavyzdžiui, automobilį, skaitmeninius prietaisus ar kitas brangias prekes
- Jie gali prisistatyti apsimesdami teisėtos loterijos agentu arba kaip paveldėtojas, kuriam reikia pagalbos

Loterijų sukčiai

- Pagrindiniai požymiai, rodantys apie loterijų sukčiavimą*
  - Jei prašo pateikti asmeninę ir finansinę informaciją
  - Jei prašo sumokėti tam tikrą pinigų sumą, kad padidintumėte laimėjimo tikimybę
  - Jei prašo sumokėti tam tikrus mokesčius, kad gautumėte prizą
- Loterijų sukčiai tikisi išgauti asmeninę ir finansinę informaciją arba apgaulės būdu siųsti jiems pinigus, pavyzdžiui, mokesčius, rinkliavas, siuntimo mokestį, valiutų neatitikimus arba pinigus kitoms išlaidoms padengti, mokėti dovanų kortelėmis, kad gautumėte prizą ir pan.
- Jie gali prašyti atlikti tam tikrus veiksmus ir kurį laiką neatskleisti informacijos apie laimėjimą, t. y. laikyti jį paslaptyje.

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

Funded by the Erasmus+ Programme of the European Union

Loterijų sukčiai

- **Kodėl tokio tipo atakos būna sėkmingos?** Žmonės masinami įvairiais laimėjimais, pinigais, prizais ir pan. Naudojami kiti sukčiavimo veiksniai, siekiant įkvėpti naudotojus atlikti tam tikrus veiksmus..
- **Taikinys:** visi gyventojai
- **Atakos metodas:** sukčiai naudoja el. laiškus, SMS žinutes, tiesioginio susirašinėjimo žinutes, pranešimus socialiniuose tinkluose, kombinuotus metodus.
- **Sukčiavimo taktika:**
  - Žinutėse siūlomi įvairūs laimėjimai, geros nuolaidos, pinigai ir pan.
  - Vartotojai, naudodamiesi paieškos sistema, gali rasti netikrų svetainių, kuriose siūlomi laimėjimai
  - Tikrose svetainėse gali būti naudojami reklaminiai skydeliai, viliojantys aukas paspausti skydelį
  - Gali būti įsilaužiama į tikras svetaines ir jose sukuriami puslapiai, kuriuose rodomos įvairūs pasiūlymai, laimėjimai ir pan.
- **Sukčiavimo faktoriai:**
  - **Skubos jausmo sukėlimas**
  - **Baimės jausmo sukėlimas**
  - **Sukeliamas godumo jausmas**
  - **Naudojamasi naivumu**
- **Pažeidžiamumai:**
  - asmenys, turintys nedaug žinių apie sukčiavimą arba neturintys jokių žinių apie sukčiavimą ir nesitikintys būti apgauti.
- **Rezultatas:**
  - Užkrėsti skaitmeniniai įrenginiai, tapatybės vagystė, įgaliojimų vagystė, pinigų praradimas

Funded by the Erasmus+ Programme of the European Union

Pavyzdys: Loterijų sukčiai

Siuntėjas: Nacionalinė loterija<jim-*Stanley*@info-winlottery.online>

Kam: man

Tema: Sveikinimai!

Gerbiamasis,

norėtume pranešti, kad Jūsų el. paštas buvo atrinktas pretenduoti į 150 000 EUR apdovanojimą.

Norėdami gauti pinigus, vadovaukitės pridedamais nurodymais.

Nacionalinės loterijos komanda
Generalinis direktorius Džimas Stenlis

Instrukcijos-laimėtojui.pdf

Kiti loterijų pavyzdžiai pateikti šiose skaidrėse:

- El. pašto laiškai
- Tiesioginio susirašinėjimo žinutės
- Sukčiavimas SMS skaidrėje
- Sukčiavimas svetainėse

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Turinys

Atakos, vykdomos panaudojant realius ir aktualius įvykius	El. pašto laiškai	Tekstinės žinutės	Svetainės
Netikrų loterijų pranešimai	Skambučiai telefonu	Gyvai vykstančios atakos	Stebėjimas per petį

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Skambučiai telefonu: telefoninis sukčiavimas (angl. vishing)

- Telefoninis sukčiavimas gali būti paaiškinamas kaip sukčiavimas balsu
- Siekdami įgyti aukų pasitikėjimą, sukčiai naudoja išgalvotus scenarijus ir išgalvotas situacijas
- Telefoninis sukčiavimas gali būti derinamas su kitais socialinės inžinerijos metodais
- Kartais prieš skambindamas aukai užpuolikas gali atlikti tyrimą, kad įgytų didesnį pasitikėjimą

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Skambučiai telefonu: telefoninis sukčiavimas (angl. vishing)

- **Kodėl tokio tipo atakos būna sėkmingos?** Sudėtinga atskirti netikrus skambučius nuo tikrų skambučių. Užpuolikas prisistato kitu asmeniu arba teisinės institucijos, pavyzdžiui, policijos ar banko, atstovu ir, nenaudodamas jokių kitų techninių priemonių, išskyrus telefoną, manipuliuoja, naudojasi žmogaus baimėmis, autoritetu ar troškimais, kad gautų slaptos informacijos ar „priverstų“ atlikti tam tikrus veiksmus.
- **Taikinys:** visi gyventojai
- **Atakos metodas:** skambučiai telefonu, skambučiai per tiesioginio susirašinėjimo programas, pavyzdžiui, „Viber“. Sukčiai gali kartu naudoti kitus metodus, pvz. suklastotos svetainės.
- **Pažeidžiamumai:**
  - gyventojai, turintys ribotas žinias arba neturintys jokių žinių apie telefoninį sukčiavimą.
- **Sukčiavimo taktika:**
  - Teisinės organizacijos darbuotoju apsimetantis sukčius paprastai skambina aukai ir siūlo investavimo galimybes; sukčiai gali apsimesti policijos atstovais, gąsdinti auką, kad atliekamos finansinės machinacijos jos sąskaitoje, kad gautų prieigą prie aukos banko sąskaitos.
- **Sukčiavimo faktoriai:**
  - **Skubos jausmo sukėlimas**
  - **Baimės jausmo sukėlimas**
  - **Sukeliamas godumo jausmas**
  - **Naudojamasi naivumu**
- **Rezultatas:**
  - Pinigų praradimas

Funded by the Erasmus+ Programme of the European Union

Turinys

Atakos, vykdomos panaudojant realius ir aktualius įvykius

El. pašto laiškai

Tekstinės žinutės

Svetainės

Netikrų loterijų pranešimai

Skambučiai telefonu

Gyvai vykstančios atakos

Stebėjimas per petį

Gyvai vykstančios atakos: pasinaudojimas kieno nors teise patekti į ribotos prieigos patalpas (angl. tailgating)

- Tokio tipo atakos angliškai vadinamos „Tailgating“, „piggybacking“, vykdomos, kai kibernetiniai nusikaltėliai pasinaudoja įmonės darbuotojais, kad patektų į riboto naudojimo organizacijos patalpas.
- Į riboto naudojimo patalpas gali patekti tik įgalioti darbuotojai

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Gyvai vykstančios atakos: pasinaudojimas kieno nors teise patekti į ribotos prieigos patalpas (angl. tailgating)

- **Kodėl tokio tipo atakos būna sėkmingos?** Didžiulėse organizacijose darbuotojai gali nepažinti kitų kolegų, žmonės linkę pasitikėti nepažįstamais žmonėmis.
- **Taikinys:** darbuotojai organizacijose.
- **Atakos metodas:** sukčius gali apsimesti nauju darbuotoju, paslaugų teikėju, prekių pristatymo asistentu ir t. t..
- **Sukčiavimo taktika:**
  - Kibernetiniai nusikaltėliai paprasčiausiai apgauna ir suklaidina vieną iš darbuotojų, sekdami jam iš paskos, kad galėtų patekti į ribotos prieigos patalpas.
  - Sukčius gali apsimesti, kad yra siuntų pristatymo agentas su keliomis dėžėmis, maisto išvežiotojas, ir paprašyti darbuotojų atidaryti duris.
  - Kitas šios atakos pavyzdys galėtų būti apsimetinėjimas įmonių darbuotoju ir pokalbio užmezgimas viešose įmonės patalpose, pavyzdžiui, rūkymo vietose. Po pertraukos apsimetėlis galėtų eiti kartu su pasirinktu darbuotoju, kuris įsitraukęs į pokalbį seka jį į ribotos prieigos patalpas.
- **Sukčiavimo faktoriai:**
  - **Skubos jausmo sukėlimas**
  - **Pasitikėjimo jausmo sukėlimas**
  - **Naudojamasi naivumu**
- **Pažeidžiamumai:**
  - darbuotojai, turintys ribotas žinias arba neturintys jokių žinių apie tokio pobūdžio atakas.
- **Rezultatas:**
  - Neįgaliotam asmeniui patekus į ribotos prieigos patalpą, gali būti padaryta didžiulė žala.
  - Kai pašalinis asmuo patenka į ribotos prieigos patalpas, jis gali įvykdyti ataką, pavyzdžiui, duomenų vagystę, duomenų saugumo pažeidimą, kenkėjiškų programų atakas ir pan.

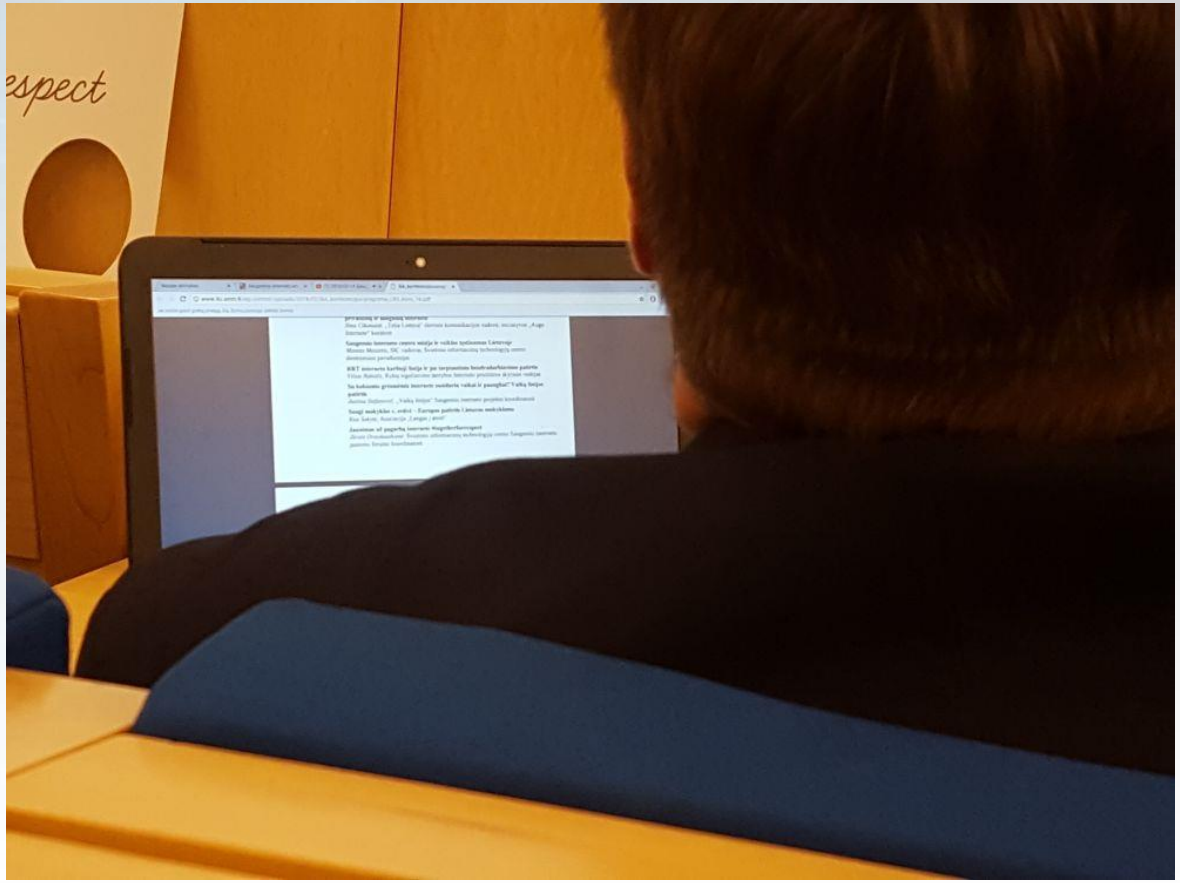
Turinys

Atakos, vykdomos panaudojant realius ir aktualius įvykius	El. pašto laiškai	Tekstinės žinutės	Svetainės
Netikrų loterijų pranešimai	Skambučiai telefonu	Gyvai vykstančios atakos	Stebėjimas per petį

Funded by the Erasmus+ Programme of the European Union

Stebėjimas per petį

- Stebėjimas per petį – tai veiksmingas būdas stebėti kieno nors kompiuterio, išmaniojo telefono ar bankomato ekraną, siekiant gauti asmeninius prisijungimo prie sistemų duomenis, pvz., prisijungimo vardus ir slaptažodžius, PIN kodus ar kitą slaptą informaciją.
- Sukčius gali stebėti stovėdamas šalia ekrano, klausydamasis žodžiu pateikiamų slaptų duomenų arba taip pat užpuolikas gali naudoti slaptas kameras, kad surinktų reikiamus duomenis.



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Stebėjimas per petį

- **Kodėl tokio tipo atakos būna sėkmingos?** Žmonės, kurie paprastai dirba su nešiojamaisiais kompiuteriais ir išmaniaisiais įrenginiais viešose vietose, viešuose renginiuose, viešajame transporte, nepagalvoja apie tai, kad kažkas gali žiūrėti į jų ekraną, ir nesusimąsto apie pasekmes.
- **Taikinys:** visi gyventojai
- **Atakos metodas ir taktika:** užpuolikas gali stebėti šalia sėdinčio ar stovinčio asmens ekraną ir renka slaptus naudotojo duomenis. Kad nesukeltų įtarimų, sukčiai gali naudoti slaptas kameras.
- **Sukčiavimo faktorius:**
  - **siekiama įgyti pasitikėjimą.**
- **Pažeidžiamumai:**
  - asmenys, turintys mažai žinių arba neturintys jokių žinių apie stebėjimą per petį.
- **Rezultatas:**
  - pavogti asmeniniai prisijungimo prie sistemų duomenys, pavyzdžiui, prisijungimo vardai ir slaptažodžiai, PIN kodai ar kita slapta informacija.

Funded by the Erasmus+ Programme of the European Union

Santrauka: sukčiavimo atakos

Atakos, vykdomos panaudojant realius ir aktualius įvykius	El. pašto laiškai	Tiesioginio susirašinėjimo programos	Socialiniai tinklai
Suklastotos svetainės	Loterijų sukčiai	SMS	Skambučiai telefonu
	Gyvai vykstančios atakos	Stebėjimas per petį	

Sukčiai ir kibernetiniai nusikaltėliai sąmoningai tobulina savo naudojamus metodus arba naudoja jų derinius.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

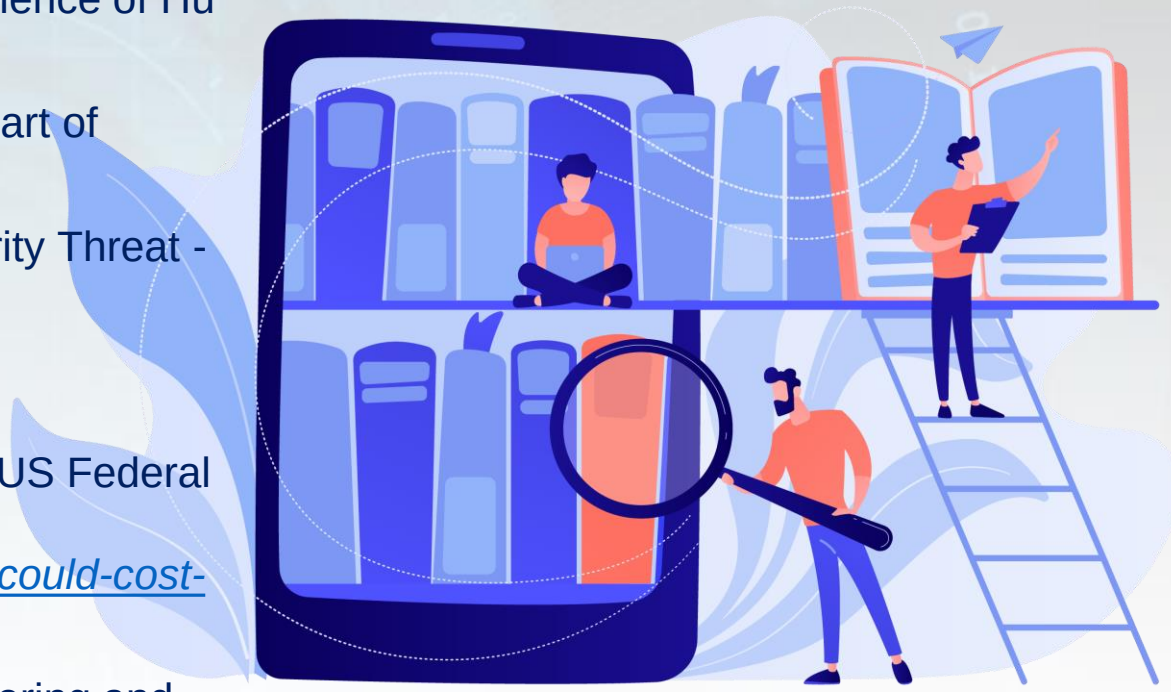
Užduotys

- Diskutuokite, kokių tipų sukčiavimo atakas žinote.
- Ar kada nors esate susidūrę su sukčiavimo ataka, galbūt neseniai girdėjote apie kibernetinę ataką? Kokio pobūdžio ataka buvo?
- Kaip manote, kokio tipo sukčiavimo atakos yra populiariausios?
- Kokie gali būti sėkmingai įvykdytos atakos rezultatai?
- Išvardykite bent keturis skirtingus sukčiavimo faktorius.

Funded by the Erasmus+ Programme of the European Union

Papildomi skaitiniai

- **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

Trumpi vaizdo įrašai

- Kas yra sukčiavimas? Sužinokite, kaip veikia ši ataka (EN).
  https://youtu.be/Y7zNlEMDmI4
- Kas yra sukčiavimo ataka? Ir kaip jos išvengti (EN).
  https://youtu.be/j3nE8JQATXo
- Sužinokite, kaip atpažinti apgaulingus ir nepageidaujamus el. laiškus (EN).
  https://youtu.be/AmPX4DdBz-k
- Kas yra personalizuotas sukčiavimas | „Phishing“ ir „Whaling“ skirtumai (EN).
  https://youtu.be/JzoJeJBdhuI
- Kas yra „smishing“? Kaip veikia sukčiavimas SMS žinutėmis? (EN)
  https://youtu.be/ZOZGQeG8avQ
- Kas yra „vishing“? Kaip suprasti šį sukčiavimo būdą? (EN)
  https://youtu.be/DysFLnOf4Nw
- Ką daryti, jei netyčia spustelėjau sukčiavimo nuorodą? (EN)
  https://youtu.be/d21-z8wsO7c

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Dėkojame!

Pateiktyje naudojamų nuotraukų šaltiniai:

- www.pixabay.com
- asmeninis archyvas
- svetainių ekrano nuotraukos