Funded by the
Erasmus+ Programme
of the European Union

Prevencinės priemonės kovai su interneto sukčiais

dr. Renata Danielienė

doc. dr. Kęstutis Driaunys

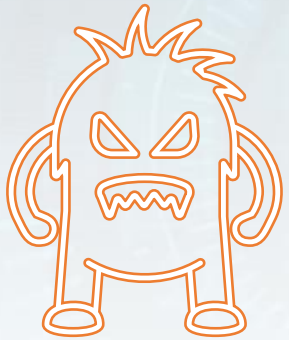
www.cyberphish.eu

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.

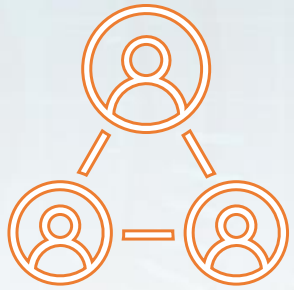
CyberPhish
Safeguarding your digital future

Socialinė inžinerija. Statistika

98 % kibernetinių atakų vyksta naudojant socialinę inžineriją



43% IT specialistai per pastaruosius metus tapo socialinės inžinerijos taikiniais



21% esamų ar buvusių darbuotojų naudoja socialinę inžineriją

2018 m. socialinės inžinerijos atakų išaugo daugiau nei 500 proc.

Šaltinis: https://purplesec.us/resources/cyber-security-statistics

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Socialinės inžinerijos atakos

„Shark Tank“ televizijos teisėja Barbara Corcoran 2020 m. buvo apgauta per beveik 400 000 JAV dolerių vertės sukčiavimo (phishing) apgaulės būdu.

Kibernetinis nusikaltėlis apsimetė jos padėjėju ir nusiuntė elektroninį laišką buhalteriui, prašydamas atnaujinti mokėjimą, susijusį su investicijomis į nekilnojamąjį turtą.

Jis naudojo el. pašto adresą, panašų į teisėtą. Sukčiavimas buvo aptiktas tik po to, kai buhalteris išsiuntė elektroninį laišką teisingu asistentės adresu, klausdamas apie sandorį.

Funded by the Erasmus+ Programme of the European Union

Kibernetinis saugumas: Europa

[Šaltinis: 2021 m. ENISA grėsmių aplinka]

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kibernetinis saugumas: Lietuva

Nr.	Kibernetinio incidento grupės	2021 m. kiekis	2020 m. kiekis	Pokytis vnt.
01	Kenkimo PĮ	1 890	1 966	↓ 76
02	Informacijos rinkimas (angl. *phishing*)	1 187	962	↑ 225
03	Nepageidaujamų laiškų, klaidinančios informacijos platinimas	399	739	↓ 340
04	Mėginimas įsilaužti	278	171	↑ 107
05	Neteisėta veikla, sukčiavimas	136	85	↑ 51
06	Sėkmingas įsilaužimas	125	61	↑ 64
07	Paslaugų trikdymas (angl. DDoS)	43	75	↓ 32
08	Kiti incidentai (atskiri, neatitinkantys nė vienos iš nurodytų grupių aprašymų)	22	271	↓ 241
	Iš viso:	4088	4330	↓ 242

Šaltinis: Nacionalinio kibernetinio saugumo būklės ataskaita 2021

Funded by the Erasmus+ Programme of the European Union

Žmogiškasis faktorius

- Žmonės dažnai yra silpniausia saugumo grandinės grandis ir yra dažniausiai jie yra atsakingi už įvairius apsaugos sistemų gedimus.

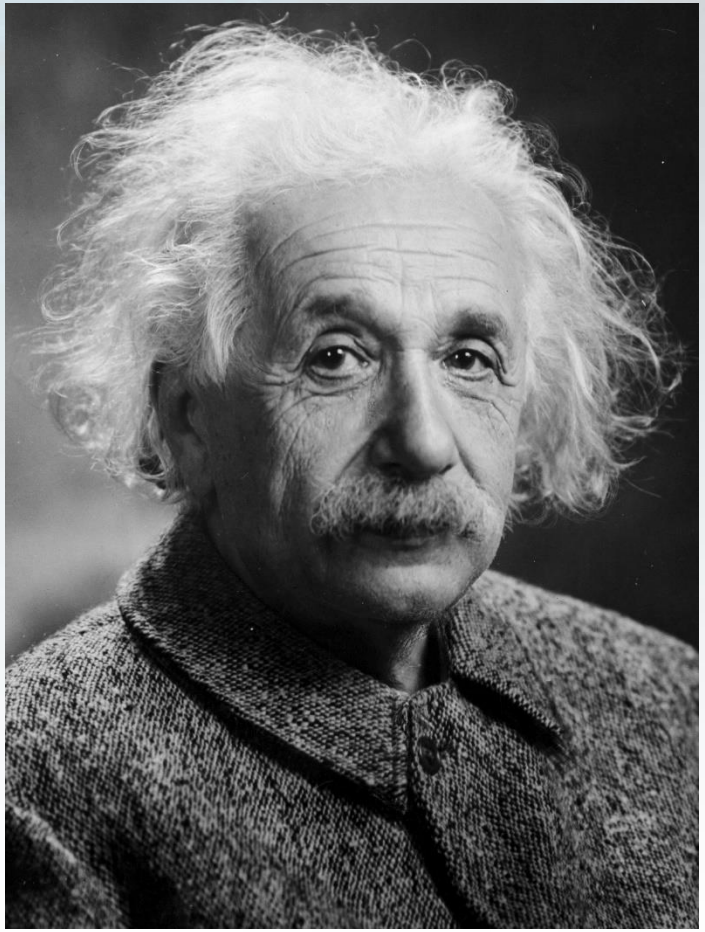
- Techninės saugumo priemonės nuolat tobulėja, tačiau žmonės nesikeičia, su savo silpnybėmis, stereotipais ir požiūriais jie yra lengvai pažeidžiami.

Funded by the
Erasmus+ Programme
of the European Union

Žmogiškasis faktorius

-Begaliniai yra tik du dalykai: Visata ir žmonių kvailumas. Bet dėl Visatos aš dar nesu tikras.

Albertas Ensteinas



Šaltinis: https://iheartintelligence.com/

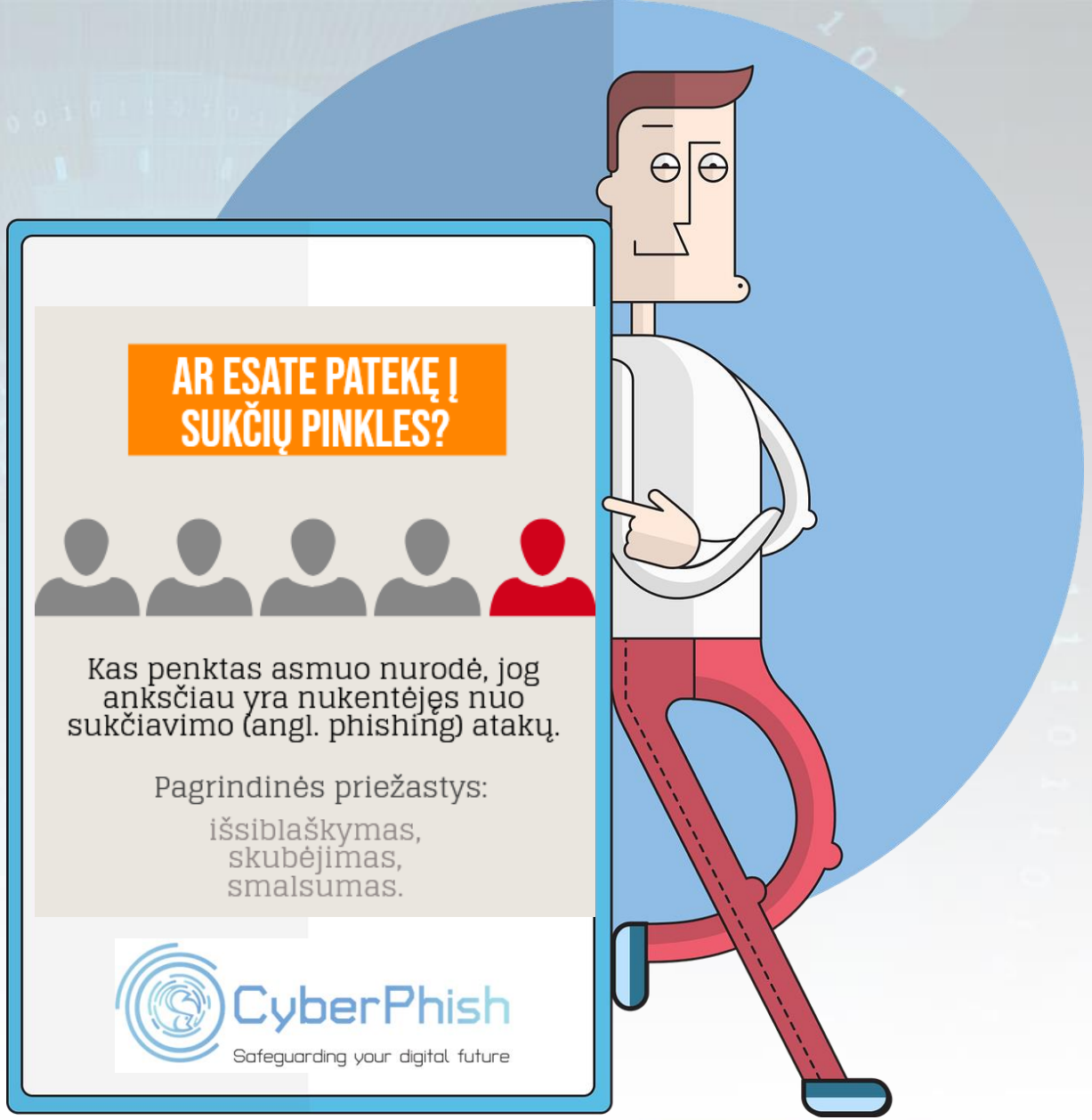
Kas yra socialinė inžinerija?

> Socialinė inžinerija – tai bet koks veiksmas, įtakojantis asmenį imtis veiksmų, kurie gali būti arba nebūti jo interesais

[Hadnagy, 2018]

Funded by the Erasmus+ Programme of the European Union

Kodėl žmonės pasiduoda manipuliacijoms?



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

[PAGRINDINĖS IŠVADOS]

KIBERNETINIO SAUGUMO MOKYMAI

- Respondetai (100%)
- Niekada nedalyvavo mokymuose (73.93%)
- Mokėsi savarankiškai (54.09%)

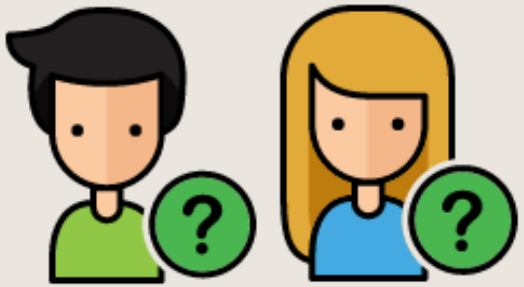
Kalbant apie mažiausiai tikėtiną pasekmę, apklaustieji teigia, jog intelektinės nuosavybės praradimo tikimybė yra nedidelė.

Trijų šalių apklaustieji iš Lietuvos, Estijos ir Maltos skeptiškai vertina galimybes patirti finansinių nuostolių iš verslo ir klientų sąskaitų po sėkmingai įvykdytos kibernetinės atakos.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

KODĖL SUKČIAMS SEKASI APGAUDINĖTI ŽMONES?



FIŠINGAS AR NE FIŠINGAS

Pavyzdys: Labiau tikėtina, kad respondentai paspaus el. laiške ar žinutėje esančią nuorodą ar priedą, jei jį atsiuntė viršininkas ar kolega, įmonė, kurios paslaugomis jie naudojasi, bankas ar valstybinė institucija.

ŠALTINIS: < CyberPhish projektas https://cyberphish.eu >

Tyrimas „Sukčiavimo atvejų ir įgūdžių spragų identifikavimas“:
https://cyberphish.eu/wp-content/uploads/2021/10/IO1_A1_LT_CYBERPHISH-REPORT.pdf

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kodėl socialinė inžinerija tokia efektyvi?

Iš prigimties esame socialūs

- Mūsų troškimas išsiskirti iš kitų

Kiti žmonės turi didelę įtaka mūsų priimamiems sprendimams

- Mūsų troškimas būti naudingais
- Mūsų polinkis pasitikėti nepažįstamais žmonėmis

Funded by the
Erasmus+ Programme
of the European Union

Kodėl socialinė inžinerija tokia efektyvi?

Esame „perkrauti“ informacija, neužtenka laiko ją visą išanalizuoti.

- Mūsų troškimas, kad viskas kas gera įvyktų greitai ir be pastangų
- Mūsų baimė patekti į bėdą

Saugumo žinių trūkumas.

Pernelyg didelis dalijimasis asmenine informacija socialiniuose tinkluose.

Funded by the Erasmus+ Programme of the European Union

Sustiprintos emocijos

[Montañez at al. 2020]

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.
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

Funded by the Erasmus+ Programme of the European Union

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.

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.

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

Kam: man

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

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

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

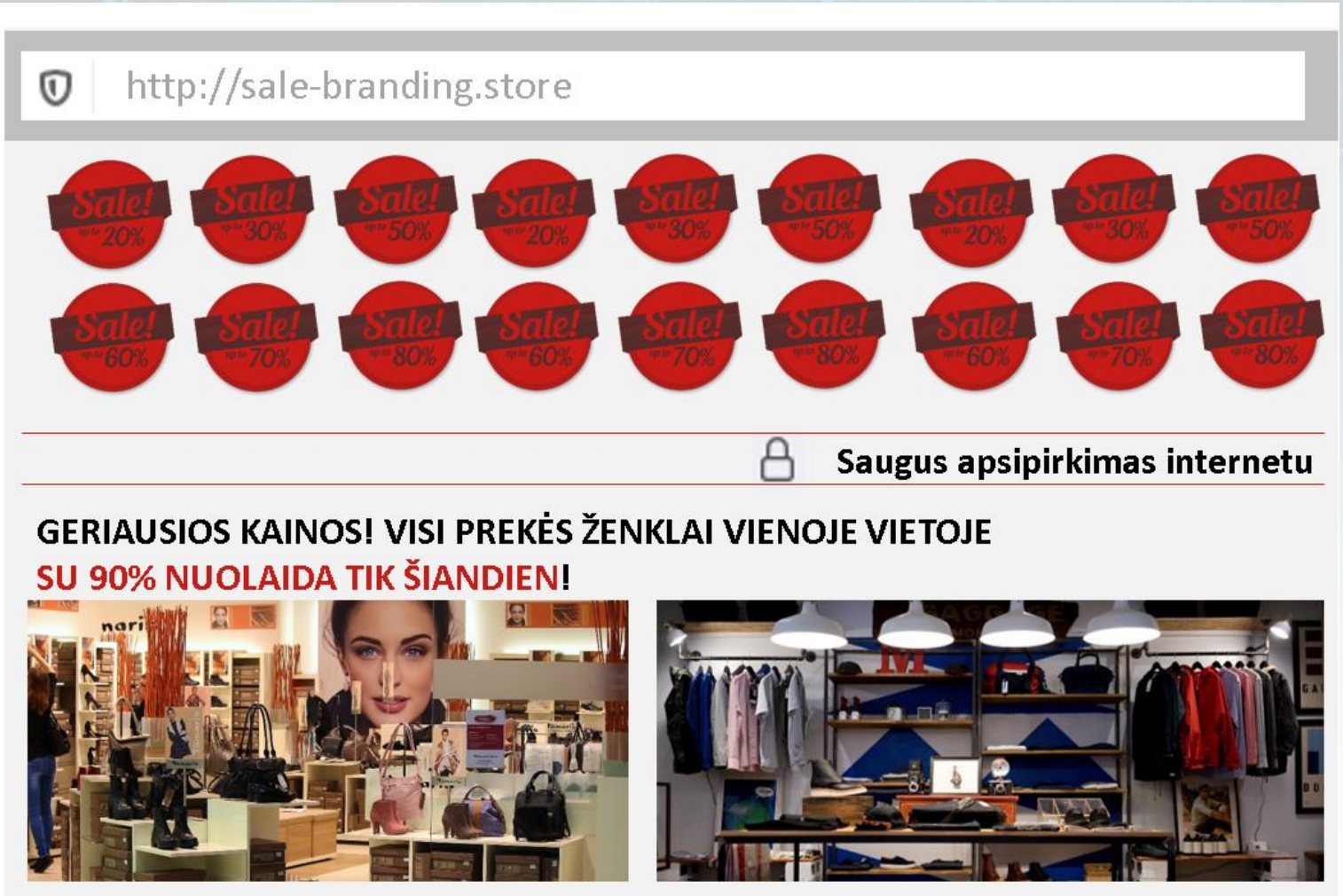
Fišingo nuorodos

Jei pateikiamos trumpos nuorodos, o laiškas atrodo įtartinas. Nuorodas galima patikrinti http://www.getlinkinfo.com/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

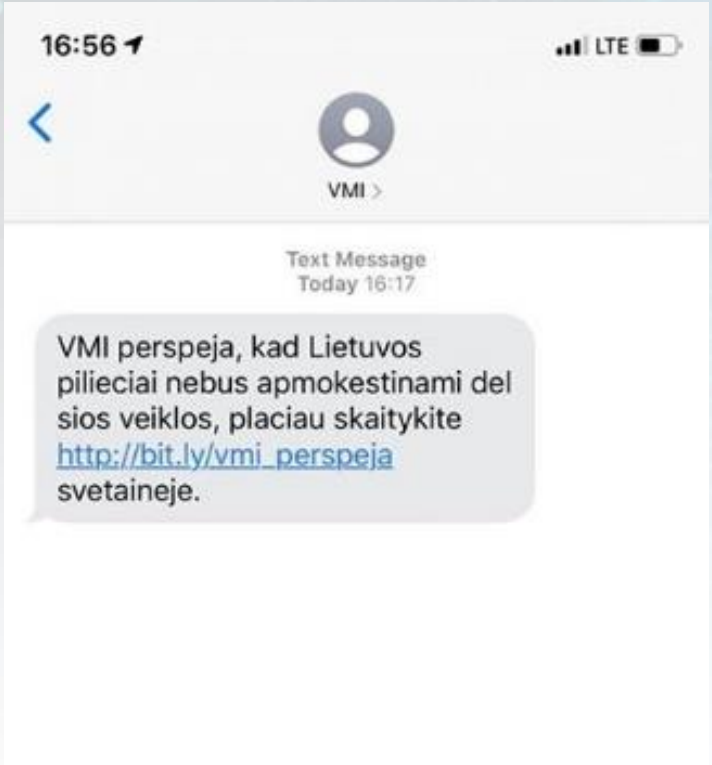
Fišingo svetainių pavyzdžiai

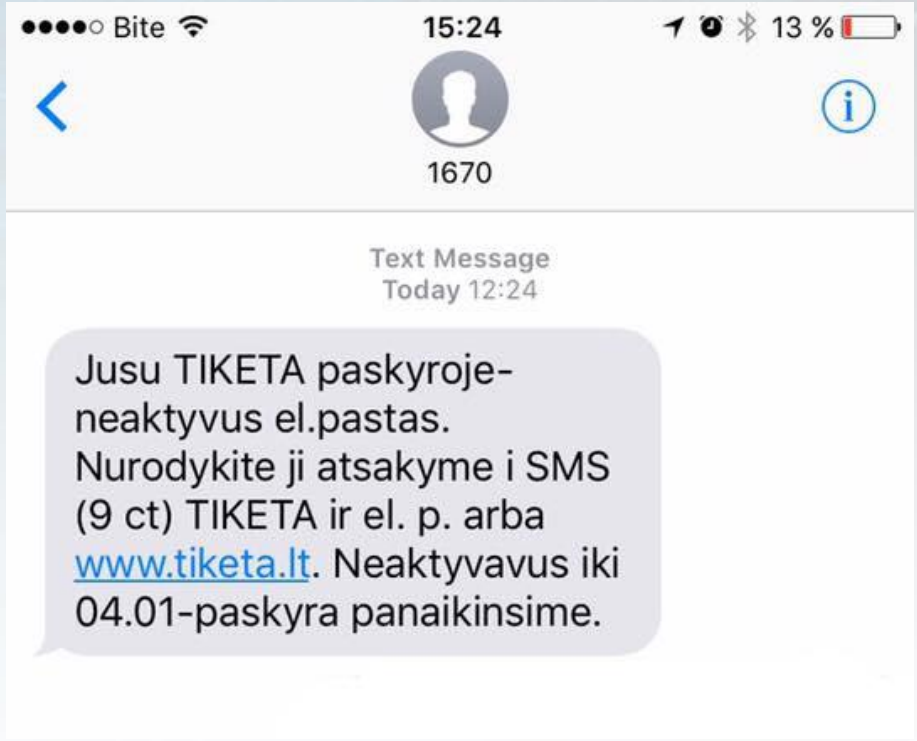


CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Fišingo sms pavyzdžiai

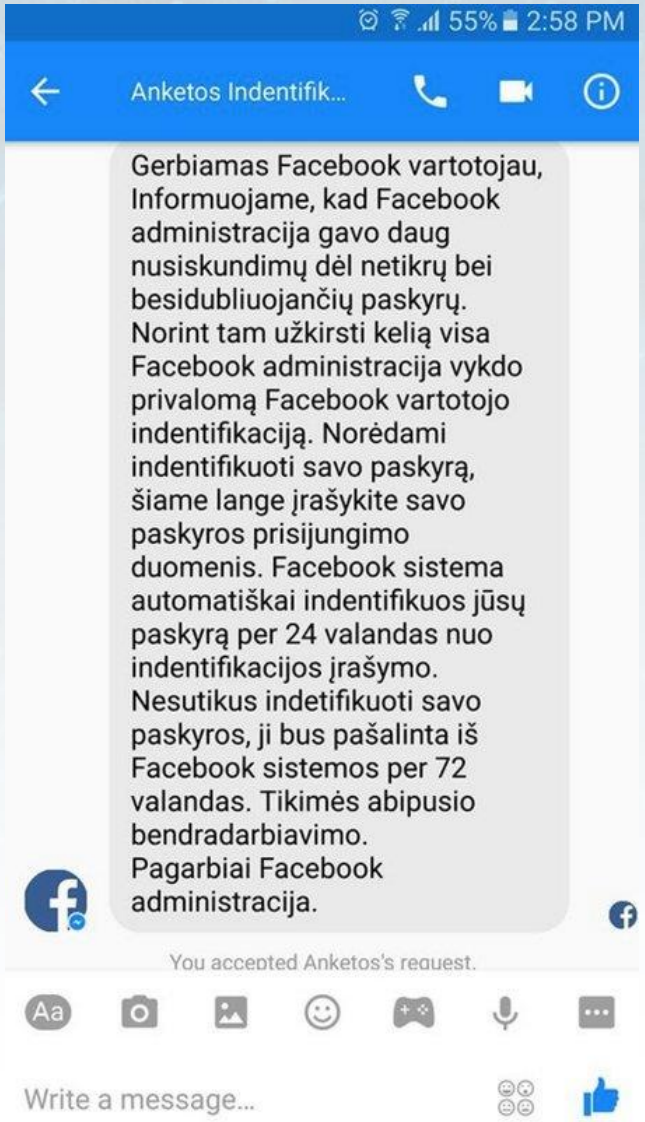




CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Fišingo soc. tinkluose pavyzdžiai



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Fišingo soc. tinkluose pavyzdžiai

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Veiksmai, kaip elgtis galimos atakos atveju

1 žingsnis: žinoti dažniausias kibernetinės grėsmes

2 žingsnis: pereiti į kibernetinio saugumo veiksmų režimą

3 žingsnis: įvertinti rizikos poveikį

4 žingsnis: sukurti apsaugos ir aptikimo priemones

5 žingsnis: parengti nenumatytų atvejų veiksmų planą

6 žingsnis: atstatymas

Funded by the
Erasmus+ Programme
of the European Union

Kibernetinių atakų vengimas

- Veiksmingiausias būdas kovoti su kibernetinėmis atakomis - naudoti tinkamas prevencines priemones.

- Norint išvengti atakos arba ją sušvelninti, reikia išsiugdyti tam tikrus įpročius, kurie dažnai vadinami **saugumo higiena** arba **kibernetine higiena**.

- Jei jūs ir jūsų darbuotojai laikysis saugumo higienos, **tikimybė** tapti kibernetinės atakos auka gali sumažėti **bent 90 procentų** !

Funded by the Erasmus+ Programme of the European Union

Sąmoningumo ugdymas

- Pirmasis ir vienas svarbiausių patarimų, kaip kovoti su kibernetinėmis atakomis, yra **sąmoningumo ugdymas**.
- Tai užtikrins, kad visi darbuotojai pagal savo pareigas arba piliečiai gebėtų atremti kibernetinį incidentą.

- Mokymas taip pat yra viena iš pagrindinių rizikos mažinimo priemonių.
- *Tai negali užtikrinti 100 proc. saugumo, tačiau gali sumažinti riziką.*

Funded by the
Erasmus+ Programme
of the European Union

Prevencinės priemonės kovai su fišingu 4-sios pramonės revoliucijos amžiuje

- Erasmus + strateginės partnerystės projektas 2020.11-2022.11
- Tikslas edukuoti aukštųjų mokyklų studentus, pedagogus, universiteto darbuotojus (bendruomenės narius), suaugusiųjų švietimo centrus ir verslo sektorius bei skatinti tikslinės grupės kritinį mąstymą kibernetinio saugumo srityje.
- Projekto koordinatorius Vilniaus universitetas ir penki partneriai:
  - Tartu universitetas (Estija)
  - Altacom (Latvija)
  - Informacinių technologijų institutas (Lietuva)
  - DOREA švietimo institutas (Educational Institute, Kipras)
  - MACDAC konsultacinė kompanija (Engineering Consultancy Bureau, Malta)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Projekto partneriai sukūrė

- mokymo programą (PDF, PPT),
- el. mokymosi medžiagą ir mokymosi aplinką,
- savitikros testus žinių įsivertinimui bei žinių patikrinimo testus (PPT),
- simuliacijų scenarijus studentams ir kitiems naudotojams (PPT),
- gaires mokymų vadovams / mentoriams bei rekomendacijas, kaip įsidiegti mokymo kursą, siekiant apsisaugoti nuo sukčiavimo atakų, įgyti kompetencijų, kurios padės atkreipti dėmesį į grėsmes ir imtis reikiamų prevencijos priemonių (PDF).
- Projekto rezultatai skelbiami https://cyberphish.eu/
- Mokymosi sistema pasiekiama adresu https://cyberphish.eu/learn/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

CyberPhish kursas:

https://cyberphish.vuknf.lt arba www.cyberphish.eu/learn

Mokymo medžiaga, testai ir simuliacijos

Plačiau apie projektą:

www.cyberphish.eu

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union