Projekto Nr. 2020-1-LT01-KA203-078070

IO1 A1: Sukčiavimo atvejų ir įgūdžių spragų identifikavimas

ATASKAITA

2021

Partneriai

Vilnius University, Lithuania

Website: http://www.vu.lt

University of Tartu

Website: https://www.ut.ee/et

MECB - Macdac Engineering Consultancy Bureau LTD , Malta

Website: http://www.mecb.com.mt/eu

Altacom SIA, Latvia

Website: https://www.altacom.eu/

DOREA Educational Institute, Cyprus

Website: https://dorea.org/

ECDL- Information Technologies Institute, Lithuania

Website: http://www.ecdl.lt/

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Turinys

Lentelių sąrašas

Paveikslėlių sąrašas

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Santrumpų sąrašas

BEC	Verslo elektroninio pašto atakos (angl. Business Email Compromise. BSC)
CEO	Įmonės vadovas (angl. Chief executive officer)
ENISA	Europos Sąjungos kibernetinio saugumo agentūra (angl. European Union Agency for Cybersecurity)
EU	Europos Sąjunga
EUROPOL	The European Union Agency for Law Enforcement Cooperation

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

1. Įvadas

1.1. Kibernetinis saugumas Europos sąjungoje: realybė ir poreikiai

Europos Komisija 2019 m. parengė ir atliko specialų „Eurobarometro“ tyrimą1, kurio tikslas buvo suprasti ES piliečių sąmoningumą, patirtį ir suvokimą apie kibernetinį saugumą.
Nenuostabu, kad rezultatai parodė, kad interneto naudojimas Europoje vis didėja, ypač naudojant išmaniuosius telefonus. Rezultatai taip pat parodė, kad ES piliečiai geriau žino apie galimus internetinio naudojimo pavojus, o 52 % respondentų teigė, kad yra pakankamai gerai arba labai gerai informuoti apie elektroninius nusikaltimus, palyginti su 46 % 2017 metais. Remiantis tyrimo išvadomis, susirūpinimas dėl privatumo ir saugumo internete paskatino daugiau nei 9 iš 10 interneto vartotojų pakeisti savo elgesį internete – dažniausiai neatidaryti nežinomų žmonių el. laiškų, įsidiegti antivirusinę programinę įrangą, lankytis tik žinomose ir patikimose svetainėse ir jungtis tik prie savo kompiuterių.

Nors šie rezultatai yra gana džiuginantys, daugelis interneto vartotojų vis dar patenka į internetinio sukčiavimo ir elektroninio pašto sukčiavimo (angl. phishing) pinkles. Remiantis Eurostato duomenimis, 2019 m. maždaug kas trečias 16–74 metų ES pilietis pranešė apie su saugumu susijusius incidentus, kai naudojosi internetu privačiais tikslais per pastaruosius 12 mėnesių.

Per šį laikotarpį – sukčiavimas buvo dažniausias saugumo incidentas, apie kurį pranešta 2019 metais[2]. 25 % respondentų pranešė, kad gavo apgaulingus pranešimus, žinomus kaip sukčiavimas (angl. *phishing*), o 12 % respondentų teigė, kad jie buvo nukreipti į suklastotas svetaines, prašančias pateikti asmeninę informaciją (angl. *Pharming*). Žmonių, kurie patyrė su saugumu susijusių problemų naudodamiesi internetu privačiais tikslais, dalis ES valstybėse narėse buvo skirtinga. Didžiausias rodikliai pastebėti Danijoje (50 %), po to sekė Prancūzija (46 %), Švedija (45 %), Malta ir Nyderlandai (abi po 42 %), Suomija (41 %) ir Vokietija (40 %). Priešingai, mažiausia dalis užfiksuota Lietuvoje (7 proc.), Lenkijoje (9 %), Latvijoje (10 %), Bulgarijoje (13 %) ir Graikijoje (13 %). Žmonių, patiriančių su saugumu susijusių problemų, dalis Estijoje ir Kipre buvo atitinkamai 32 % ir 21 %.

Tai galima paaiškinti skirtingu ES šalių sąmoningumo apie kibernetinius nusikaltimus lygiu, apskritai mažėjančiu ES piliečių pasitikėjimu, kad jie gali apsisaugoti nuo kibernetinių atakų, taip pat sudėtingesnėmis kibernetinėmis atakomis, kurias sunkiau aptikti ir išvengti, naujais naudojamais metodais ir naujomis platformomis tokioms atakoms vykdyti.

Kibernetinio saugumo problemos paliečia ir Europos verslo sektorių. Europos šalys ir įmonės vis dažniau tampa kibernetinių atakų taikiniais. Remiantis 2017 m. pasaulinės informacijos saugumo būklės tyrimo duomenimis, apie 80 % Europos įmonių tais metais patyrė bent vieną kibernetinio saugumo incidentą, o darbuotojai yra atsakingi už 27 % visų kibernetinio saugumo incidentų.

Remiantis naujausiais duomenimis, 2019 m. pirmąjį ketvirtį įmonės visame pasaulyje buvo taikiniais 120 proc. dažniau nei metais anksčiau, todėl nuostoliai siekė net 22,2 mlrd. eurų.

1 EU Commission (2020): Special Eurobarometer 499: Europeans' attitudes towards cyber security, URL https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG (žiūrėta 11.02.2021)

2 EUROSTAT (2020): Is internet use safer today?, URL https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb/default/table?lang=en (žiūrėta 11.02.2021)

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Daugiau nei 99% el. laiškų, kurie platina kenkėjišką programinę įrangą, reikalingas žmogaus įsikišimas t. y. atverti nuorodas, atidaryti dokumentus, patvirtinti saugos įspėjimus ir kitą elgesį.3

Taigi, žmonės, tiek darbe, tiek namuose, žinantys įspėjamuosius ženklus ir išmanantys tinkamus metodus, yra pagrindiniai elementai, padedantys sulėtinti kibernetines atakas arba užkirsti joms kelią. Todėl reikalinga atnaujinti esamas kibernetinio saugumo programas arba sukurti naujas, kad būtų stiprinami ES piliečių įgūdžiai, švietimas ir sąmoningumo didinimas apie naujausius kylančius kibernetinio saugumo klausimus ir grėsmes.

Be to, reikalinga siūlyti tokias programas visiems studentams, atsižvelgiant į tai, kad, ENISA duomenimis, universitetuose su kibernetiniu saugumu susiję dalykai yra nepakankamai pristatomi netechninėse studijų programose.

1.2. Projektas „Prevencinės priemonės kovai su fišingu 4-sios pramonės revoliucijos amžiuje“

Kibernetnis saugumas tampa vienu iš didžiausių iššūkių skaitmeniniame amžiuje[4], nes informacija tampa brangiu turtu, susijusiu su didžiuliais duomenų kiekiais, gerėjančiu ryšiu su skaitmenine aplinka. Skaitmeniniai įrenginiai ir informacinės sistemos vis labiau tampa patrauklūs kibernetinėms atakoms.

Viena didžiausių problemų yra sukčiavimas (angl. phishing), nes kibernetiniai nusikaltėliai sukčiavimo kampanijoms vykdyti naudoja greitesnes ir naujoviškas technologines priemones. Todėl turėtų būti sukurta ir plačiai auditorijai laisvai prieinama žmogaus valdomos apsaugos nuo sukčiavimo (angl. phishing) sistema, kurioje aptikimui naudojamas žmogaus instinktas, o atsako masto didinimui – technologijos. Norint sukurti žmogaus valdomą apsaugos nuo sukčiavimo sistemą, reikia šviesti naudotojus, kad jie galėtų atpažinti sukčiavimo atakas ir tinkamai į jas reaguoti.

Vilniaus universiteto Kauno fakulteto ir partnerių inicijuotas tarptautinis projektas „Prevencinės priemonės kovai su fišingu 4-sios pramonės revoliucijos amžiuje“ (CyberPhish) prasidėjo 2020 m. lapkričio pradžioje ir truks dvejus metus.

Projekto tikslas – šviesti aukštųjų mokyklų studentus, dėstytojus, universitetų darbuotojus (bendruomenės narius), švietimo centrus, verslo sektorių (darbdavius ir darbuotojus) ir skatinti tikslinės grupės kritinį mąstymą kibernetinio saugumo srityje.

Projekto partneriai sukurs mokymo programą, el. mokymosi medžiagą, mišrią mokymosi aplinką, žinių ir įgūdžių įsivertinimo bei patikrinimo testus studentams ir kitiems naudotojams, siekiant apsisaugoti nuo fišingo atakų, įgyti kompetencijų, kurios padės atkreipti dėmesį į grėsmes ir imtis reikiamų prevencijos priemonių.

Projekto konsorciumą sudaro šios organizacijos:

1. Vilniaus universitetas, Lietuva (Koordinatorius)
2. Informacinių Technologijų Institutas, Lietuva
3. DOREA Edukacinis Institutas, Kipras
4. Tartu universitetas, Estija
5. Altacom SIA, Latvija

3 Proofpoint (2019): Human Factor Report 2019, URL https://www.proofpoint.com/us/resources/threat-reports/human-factor (žiūrėta 12.02.2021)

4 European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

6. Macdac Engineering Consultancy Bureau Ltd (MECB), Malta

Daugiau informacijos apie projektą ir projekto veiklas pateikiama projekto puslapyje: https://cyberphish.eu/ .
Naujienos apie projektą ir apie kibernetinį saugumą publikuojamos Facebook puslapyje: https://www.facebook.com/eucyberphish.

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

2. Sukčiavimas (angl. phishing)

2.1. Kas yra sukčiavimas (angl. phishing)?

Sukčiavimas (angl. phishing) – tai yra neteisėtas bandymas pasisavinti vartotojo duomenis, tokius kaip prisijungimo duomenys, kreditinės kortelės informacija, ar netgi pinigus, panaudojant socialinės inžinerijos technikas. Šis atakos tipas paprastai atliekamas el. pašto žinučių, kurios atrodo lyg būtų siunčiamos iš patikimo šaltinio, pagalba. Šių žinučių tikslas yra įtikinti vartotoją atverti kenkėjišką priedą ar paspausti suklastotą internetinę nuorodą.5
Sukčiavimas (angl. phishing) taip pat yra vienas iš seniausių kibernetinių atakų tipų, pasirodęs 1990 metais. Nepaisant to, kad egzistuoja jau keletą dešimtmečių, tai vis dar yra viena iš labiausiai paplitusių ir daugiausiai žalos sukeliančių kibernetinių atakų.6

Labiausiai paplitę iš daugelio skirtingų sukčiavimo (angl. phishing) tipų yra šie:

1) *Spray and pray* – kenkėjiški el. laiškai, siunčiami bet kuriuo ir visais el. pašto adresais, bandant pavogti konfidencialią informaciją;
2) *Cat phishing* – kieno nors įviliojimas į santykius su išgalvota internetine asmenybe;
3) *Advanced fee scam* – dažnas sukčiavimas, susijęs su Nigerijos piliečiais, pvz., prašymas padėti pervesti didelę pinigų sumą;
4) *Spear fishing* – kenkėjiški el. laiškai, specialiai sukurti ir siunčiami konkrečiam asmeniui ar organizacijai, siekiant pavogti konfidencialią informaciją;
5) *Whaling* – bandymas pavogti konfidencialią informaciją ir dažnai nukreiptas į aukščiausią vadovybę;
6) *Vishing* – sukčiavimas, kuris vyksta telefonu;
7) *Smishing* – sukčiavimas, siunčiant asmeniui SMS žinutes;
8) *Angler Phishing* – santykinai naujas atakų tipas socialiniuose tinkluose, kai naudojamos netikros internetinės nuorodos, klonuotos svetainės, pranešimai, tviterio žinutės ar tiesioginio susirašinėjimo žinutės;
9) *Clone Phishing* – sukčiavimo tipas, kai tikras anksčiau išsiųstas el. laiškas panaudojamas identiško el. laiško sukūrimui su kenkėjišku turiniu;
10) *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.

Pastaruosius kelerius metus pastebėta, kad sukčiavimas (angl. phishing) tampa vis sudėtingesnis, kuomet sukčiavimo atakas tampa sudėtinga atpažinti, nes daugelis sukčiavimo el. laiškų ir suklastotų svetainių atrodo beveik identiški tikriems. Tuo pačiu metu sukčiavimo kampanijos tapo greitesnės ir labiau automatizuotos, verčiančios atakuojamuosius reaguoti greičiau, negu prieš tai. Kai kuriais atvejais tereikia vienos dienos nuo prisijungimo duomenų nutekėjimo iki atakos įvykdymo.

Remiantis Europol tyrimu, kibernetiniai nusikaltėliai pasitelkia holistinę sukčiavimo (angl. phishing) strategiją, parodydami aukštą kompetencijos lygį naudojantis įrankiais, sistemomis ir

5 European Union Agency for Cybersecurity (2020): Phishing - ENISA threat landscape 2019-2020

6 Deloitte (2019): Understanding Phishing Techniques URL

https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf (žiūrėta 112.02.2021)

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

pažeidžiamumais, kuriuos jie išnaudoja, pasitelkiant netikras tapatybes ir glaudžiai bendradarbiaujant su kitais kibernetiniais nusikaltėliais.7

Prognozuojama, kad ateityje el. paštas ir toliau bus pagrindinis sukčiavimo (angl. phishing) mechanizmas, tačiau tai truks neilgai. Ekspertai stebi didėjantį atakų skaičių pasitelkiant socialinių tinklų, tokių kaip WhatsApp ir kiti, žinutes. Pagal ENISA, labiausiai tikėtina, kad keisis žinučių siuntimui naudojami metodai – jie taps sudėtingesni, priešiškiems tikslams pritaikant dirbtinį intelektą (Artificial Intelligence, AI), kurio pagalba bus paruošiamos ir siunčiamos žinutės.

2.2. Socialinė inžinerija ir sukčiavimas (ang. phishing)

Informacijos saugos kontekste socialinė inžinerija yra apibrėžiama kaip psichologinė manipuliacija žmonėmis, siekiant, kad jie atliktų tam tikrus veiksmus ar atskleistų konfidencialią informaciją. Socialinė inžinerija išlieka pagrindine grėsme, padedančia vykdyti kitų tipų kibernetinius nusikaltimus, kadangi 84 % visų kibernetinių atakų remiasi socialine inžinerija (ENISA). Sukčiavimo aukų skaičius toliau didėja, nes jis išnaudoja žmogų kaip silpniausią grandį.

Taikymasis į žmonių silpnybes naudojant socialinę inžineriją daro didelę įtaką visuomenei ir leidžia atlikti daugumą kibernetinių nusikaltimų pradedant apgaulingomis žinutėmis (angl. scams) ir baigiant konfidencialios informacijos išgavimu bei sudėtingomis kenkėjiškų programų atakomis. Kibernetiniai nusikaltėliai paprastai naudoja socialinę inžineriją, kad įtikintų vartotojus dalyvauti apgaulingose schemose patiems to nežinant, o sukčiavimą (angl. phishing) jie naudoja norėdami gauti prisijungimo duomenis ir prieigą prie konfidencialių paskyrų ar sistemų (EUROPOL).

Kibernetiniai nusikaltėliai išmoko socialinės inžinerijos ir tapo jos ekspertais išnaudodami žmogaus prigimtį apgaulei. Patys dažniausi jų manipuliacijos metodai paprastai remiasi baime, gąsdinimu, skubos pojūčiu, gobšumu, smalsumu, pasitikėjimu ir empatija. Kibernetiniai nusikaltėliai žino, kad kruopščiai paruoštas ir personalizuotas el. laiškas, balso žinutė ar skambutis, arba tekstinė žinutė gali suklaidinti žmones taip, kad jie atskleistų konfidencialią informaciją, pervestų pinigus ar į kompanijos tinklą parsisiųstų failą, turintį kenkėjišką programą.

Kad geriau suprastume socialinės inžinerijos koncepciją, pažvelkime į 6 įtikinėjimo principus, kuriuos dr. Robert B. Cialdini paaiškino savo knygoje „Influence: The Psychology of Persuasion“8. Nors iš pradžių šie principai buvo naudojami rinkodaroje, jie buvo lengvai pritaikyti ir panaudoti socialinėje inžinerijoje, bei sukčiaujant (angl. phishing)9:

1) *Apsikeitimas (angl. Reciprocation)* – „duok ir imk“. El. laiškas, siūlantis nuolaidą ar kuponą kokiems nors pirkiniams mainais į pasidalinimą informacija arba paskyros sukūrimą; el. laiškas, žadantis prieigą prie konfidencialios informacijos, jeigu parsisiųsite tam tikrą priedą yra klasikiniai pavyzdžiai.
2) *Stygius (angl. Scarcity)* – norėti to, ką sunku gauti – yra žmogaus būdas. Sukčiavimo el. laiškai, kurie pabrėžia, jog kokia nors nauda yra galima tik tuo atveju, jeigu veiksmas bus priimtas nedelsiant, per tam tikrą trumpą laiką. „Paskyra bus deaktyvuota per 24 valandas,

7 EUROPOL (2020): Internet Organised Crime Threat Assessment 2020

8 Dr Robert B. Cialdini is a Psychology and Marketing professor in the Arizona State University in USA

9 NCC group (2020) :Psychology of the Phish: Leveraging the Seven Principles of Influence, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433 (žiūrėta 12.02.2021)

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

jeigu nepaspausite nuorodos tam, kad būtų išspręsta problema“ – tai yra šio principo panaudojimo pavyzdys.

3) *Autoritetas (angl. Authority)* – paprastai žmonės linkę sekti autoritetu ir patikimais ekspertais. Todėl daugelyje sukčiavimo el. laiškų stengiasi apsimesti, įkūnyti vietinius lyderius, vadovus, vyr. pareigūnus, žmogiškųjų resursų vadybininkus ir pan. Laiškas nuo tariamo vadovo, prašantis finansų departamentą tuojau pat pervesti tam tikrą pinigų sumą į departamentui nežinomą sąskaitą yra daugelį kartų pasikartojęs pavyzdys.
4) *Nuoseklumas (angl. Consistency)* – žmonės iš principo yra įpročio įkaitai. Sukčiavimo el. laiškai, atrodantys kaip oficiali komunikacija, išnaudoja šį faktą, tikėdamiesi, kad gavėjas nepastebės neįprasto prašymo. Pavyzdžiui, el. laiškas su „Amazon“ logotipu, pranešantis, kad siunta yra sulaikyta, ir prašantis gavėjo patvirtinti namų adresą gali ir nesukelti įtarimo, netgi jei nelaukiama jokio pristatymo – tokia yra plačiai pripažinto prekės ženklo galia.
5) *Sutarimas, konsensusas (angl. Consensus)* – žmonės yra linkę sekti kitais žmonėmis, ypač, jeigu jie nėra kuo nors įsitikinę. Sukčiavimo el. laiškas, teigiantis kažką panašaus į „544 iš 800 darbuotojų jau atnaujino savo programinę įrangą; paspauskite šią nuorodą norėdami atsisiųsti atnaujinimus“ išnaudoja šį polinkį.
6) *Mėgstamumas (angl. Liking)* – tai gana paprastas principas – jeigu žmonės mėgsta jus, arba patys nori būti mėgiami, labiausiai tikėtina, kad jie pasakys „taip“. El. laiškas, tariamai siųstas iš IT departamento ir prašantis naujo darbuotojo jo asmeninių duomenų ar slaptažodžio su tikslu atnaujinti saugumo sistemą, yra vienas iš pavyzdžių.
7) *Vienybė (angl. Unity)* – šis principas buvo pridėtas vėliau. Mintis yra tokia, kad kuo labiau mes susitapatiname su kitais, tuo labiau mes esame jų įtakojami. Sukčiavimo el. laiškas tariamai siųstas kieno nors, kas dalijasi bendrais su gavėju pomėgiais, tai yra informacija, kuri gali būti lengvai sužinoma iš socialinių tinklų, turi didelę sėkmės tikimybę. Pavyzdžiui, jeigu asmuo myli šunis, laiškas nuo kito tariamo šunų mylėtojo su priedu, kuriame tariamai yra mieli šuniukų paveikslėliai turi didelę tikimybę būti atvertas.

Šios technikos gali sąlygoti sėkmingas sukčiavimo (angl. phishing) atakas, joms panaudojant kenkėjiškas nuorodas ar kenkėjiškas programas. Todėl žmonėms ypač svarbu atpažinti šiuos principus ir strategijas tam, kad galėtų apsisaugoti. Tiesa, tai yra ganėtinai sunku, kadangi viskas remiasi pačia žmogaus esme – mūsų mąstymo ir elgesio būdu.

2.3. Sukčiavimas (angl. phishing) COVID-19 metu

Krizių ir nelaimių metu mes linkę pasitikėti kompiuteriais, mobiliaisiais įrenginiais ir internetu, kad galėtume dirbti, susisiekti su kitais žmonėmis, surasti, dalintis ir gauti informaciją, apsipirkti ir t.t.[10]

COVID-19 pandemija išryškino mūsų pažeidžiamumą ir pademonstravo kibernetinių nusikaltimų poveikio mūsų kasdieniniam gyvenimui potencialą visame pasaulyje. Tuo metu, kai suvaržymai tapo norma, o vis daugiau žmonių pasiliko ir dirbo namuose, kibernetiniai nusikaltimai paplito labiau nei anksčiau.

10 Council of Europe (2020): Cybercrime and COVID-19, URL https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (žiūrėta 12.02.2021)

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Vien tik per pirmąjį mėnesį nuo pandemijos pradžios 2020 metais Barracuda11 mokslininkai užfiksavo 667 % sukčiavimo atvejų padidėjimą.

Yra įrodymų, kad kibernetiniai nusikaltėliai toliau išnaudoja pažeidžiamumus savo naudai. Jie pritaikė jau esančias kibernetinių nusikaltimų formas pandemijos temai, pasinaudojo situacijos neapibrėžtumu ir visuomenės poreikiu patikimai informacijai. Nusikaltėliai pasinaudojo COVID-19 krize socialinės inžinerijos atakų vykdymui – tai yra masiškai siųsdami sukčiavimo (angl. phishing) laiškus, taip pat vykdydami tiksliau nukreiptas atakas, pavyzdžiui, verslo elektroninio pašto atakas (angl. business email compromise, BEC)12:

- Sukčiavimo (angl. phishing) kampanijos ir kenkėjiškų programų platinimas naudojant iš pirmo žvilgsnio tikras interneto svetaines (suklastotas), arba dokumentai, kuriuose pateikiama informacija arba patarimai dėl COVID-19, yra naudojami kompiuterių užkrėtimui ir vartotojų prisijungimo duomenų išgavimui.
- Pažeidėjai įgauna prieigą prie kompanijų ar kitų organizacijų sistemų taikydamiesi į darbuotojus, kuriuo dirba nuotoliniu būdu.

Remiantis EUROPOL, kibernetinių atakų skaičius yra labai didelis ir tikėtinai toliau didės. Kibernetinių nusikaltėlių išradingumas augs, ypač pasitelkiant įvairias kenkėjiškas programas ir išpirkos reikalaujančias programas už duomenų ar kompiuterio veiklumo atgavimą (angl. ransomware), susietus su COVID-19 pandemijos ir vakcinų tematika.

Tikėtina, kad kibernetiniai nusikaltėliai sieks išnaudoti vis didesnį skaičių atakų technikų tuo metu, kai darbdaviai naudos ir tęs prisitaikymą prie nuotolinio darbo bei leis prisijungti prie savo organizacijų sistemų.13

11 Barracuda Networks is the worldwide leader in Security, Application Delivery and Data Protection Solutions

12 Council of Europe (2020): Cybercrime and Covid, URL: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (žiūrėta 12.02.2021)

13 EUROPOL (2020): Pandemic profiteering - how criminals exploit the COVID-19 crisis

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project №.: 2020-1-LT01-KA203-078070)

3. STUDENTŲ, DARBUOTOJŲ IR AUKŠTO LYGIO VADOVŲ APKLAUSOS

3.1. Duomenų rinkimo metodai (metodologija)

Atlikdami tyrimą, projekto „CyberPhish“ konsorciumo partneriai parengė ir paskelbė apklausą, skirtą Lietuvos, Latvijos, Estijos, Maltos, Kipro ir Kipro studentams, verslo atstovams ir įmonių vadovams. Partneriai siekė, kad kiekvienoje šalyje partnerėje apklausoje dalyvautų ne mažiau kaip 70 dalyvių (įskaitant 20 verslo atstovų ir 10 generalinių direktorių).

Remiantis pirmine situacijos analize ir tyrimu bei visų partnerių atsiliepimais, buvo parengta angliška klausimyno versija, kuri vėliau buvo lokalizuota ir patalpinta internete anglų, lietuvių ir latvių kalbomis. Apklausa buvo pradėta 2020 m. gruodžio viduryje ir baigta rengti 2021 m. sausio pabaigoje.

Pagrindiniai apklausos tikslai buvo šie:

- nustatyti žmonių sąmoningumą apie sukčiavimą (angl. phishing) ir įvairias sukčiavimo rūšis;
- nustatyti, kaip žmonės atpažįsta sukčiavimo atakas;
- nustatyti įgūdžių spragas.

Klausimyne buvo apjungti klausimai, susiję su psichologinėmis ir IT žiniomis, kritinio mąstymo metodu, taip pat pateikti sukčiavimo (angl. phishing) pavyzdžiai, kad respondentai galėtų įvertinti savo žinias t.y. atskirti, kurie yra sukčiavimo atvejai. Kiekvienas sukčiavimo pavyzdys buvo pagrįstas šešiais įtikinėjimo principais, kuriuos sukūrė daktaras Robertas B. Cialdini. Klausimynas buvo padalintas į kelias dalis ir jame buvo renkami duomenys, susiję su:

- - asmenine informacija, įskaitant lytį, išsilavinimo lygį ir užimtumo statusą;
- - bendromis žiniomis ir elgsena sukčiavimo srityje;
- - asmenine patirtimi, susijusia su sukčiavimu;
- - sukčiavimo atakų atpažinimu – nurodant pagrindinius požymius (angl. red flags);
- - praktiniais sukčiavimo pavyzdžiais;
- - kritinio mąstymo įgūdžių įsivertinimu;
- - sukčiavimo atakų vengimu – kodėl sukčiavimo atakos yra sėkmingos, socialinė inžinerija (žmonių emocijos, kuriomis naudojasi užpuolikai), veiksmai, kurių reikia imtis;
- - įgūdžių, reikalingų siekiant išvengti sukčiavimo atakų, naudojimu.

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Surinkti duomenys naudojami nustatant įgūdžių spragas ir rengiant rekomendacijas naujai mokymo programai, skirtai stiprinti interneto vartotojų įgūdžius, švietimą ir sąmoningumą apie naujausias iškilusias kibernetinio saugumo problemas ir grėsmes, ypač sukčiavimą (angl. phishing).

Remdamasis šios apklausos rezultatais ir esamų kibernetinio saugumo studijų programų tyrimu, partnerių konsorciumas parengs mokymo medžiagą, žinių įsivertinimo ir žinių vertinimo testus bei simuliacijų scenarijus mokymui.

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

3.2. Rezultatų rinkimas

Klausimyno rezultatai buvo perkelti į nacionalinę rezultatų lentelę (sudaryta pagal šalis – Lietuva, Latvija, Estija, Malta ir Kipras). Į šią lentelę partneriai įtraukė svarbiausius surinktus rezultatus ir pateikdami informaciją apie:

- tyrime dalyvavusias tikslines grupes;
- apklausų rezultatų analizę, naudojant grafikus ir tekstą;
- pagrindines respondentų išvadas ir pasiūlymus;
- partnerių padarytas išvadas ir rekomendacijas, skirtas padėti partneriams apibrėžti ir parengti kitus rezultatus.
- lentelėse apžvelgtos respondentų žinios ir elgsena kibernetinio saugumo, ypač sukčiavimo (angl. phishing), tema. Šių lentelių rezultatai leido konsorciumui atlikti šalių palyginimą, nustatyti įgūdžių spragas ir poreikius.

3.3. Apklausų rezultatai ir analizė

3.3.1. Respondentų apžvalga

Nepaisant trumpo anketos platinimo laikotarpio, visos partneriai apklausė mažiausiai 70 respondentų. Iš viso buvo surinkta 514 atsakymų iš Kipro, Estijos, Latvijos, Lietuvos ir Maltos.

	Lietuva	Latvija	Estija	Malta	Kipras
Respondentai pagal šalis	93	76	165	104	76

1 lentelė. Respondentų skaičius pagal šalis

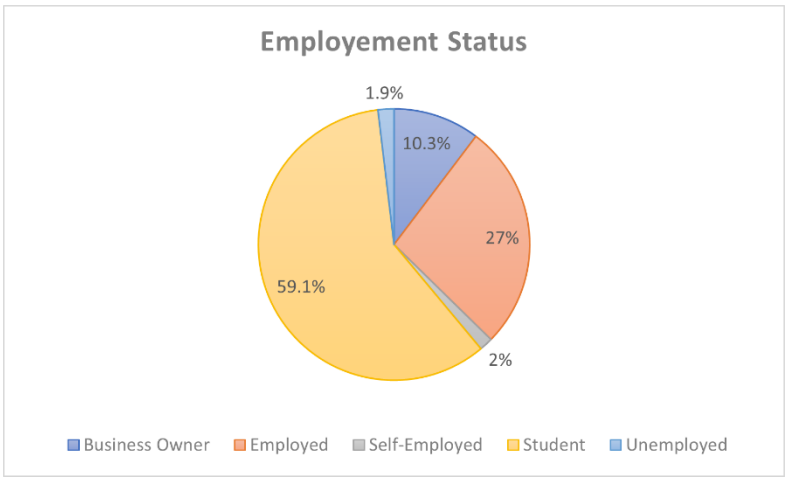
Iš 514 respondentų 259 buvo moterys, 248 vyrai, 7 respondentai nenorėjo nurodyti savo lyties. Visose šalyse partnerėse, išskyrus Estiją, moterų respondenčių skaičius buvo didesnis nei vyrų respondentų.

	Lietuva	Latvija	Estija	Malta	Kipras
Moterys	63,4%	57,9 %	34,6%	54,8%	55,3%
Vyrai	36,6%	40,8%	63%	45,2%	42,1%
Nenurodė	-	1,3 %	2,4%	-	2,6%

2 lentelė. Respondentai pagal lytį

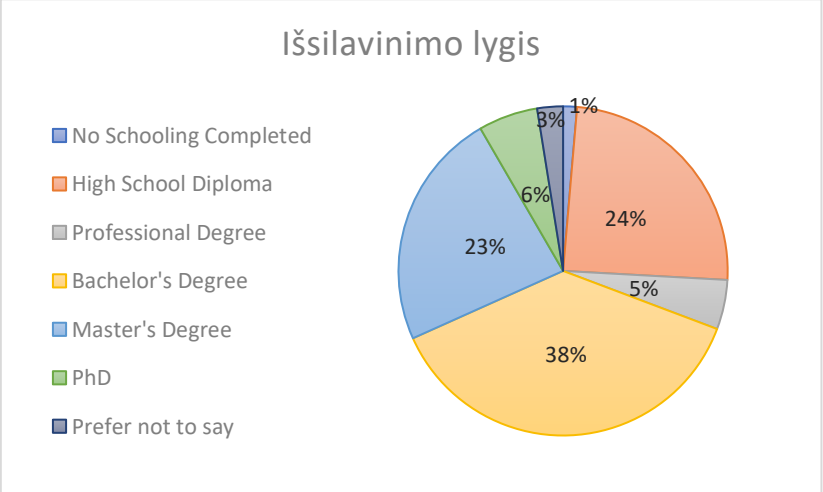
Dauguma respondentų yra studentai (59 %), po jų seka dirbantieji (27 %), verslo savininkai (10 %), bedarbiai (2 %) ir savarankiškai dirbantys asmenys (2 %).

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)



1 pav. Respondentų užimtumo statusas

Apklausos respondentai yra gerai išsilavinę: dauguma respondentų (38 %) turi bakalauro laipsnį, po to seka turintieji magistro laipsnį (23 %) ir daktaro laipsnį (6 %).



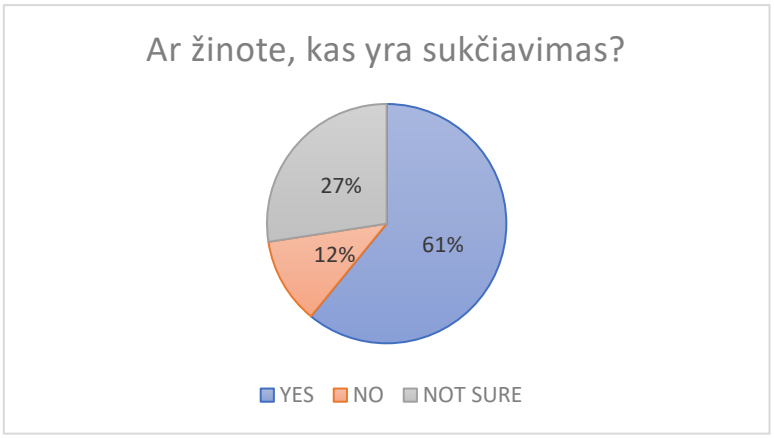
2 pav. Respondentų išsilavinimo lygis

3.3.2. Bendros žinios ir elgesys

Nors dauguma respondentų (74 %) nurodė, kad jie niekada nedalyvavo jokiuose formaliuose kibernetinio saugumo ar sukčiavimo mokymuose, seminaruose ar studijose, daugiau nei pusė respondentų (56 %) patys savarankiškai tyrinėjo šį dalyką. Šie rezultatai gali parodyti, kad kibernetinio saugumo ir sukčiavimo temos yra aktualios visose apklaustose šalyse, ir nors respondentai nebūtinai turi galimybę studijuoti temą formaliuoju būdu, jie linkę skirti laiko savarankiškam šios temos tyrimui, siekiant pagerinti savo žinias ir įgūdžius.

61 % respondentų atsakė, kad turi žinių apie sukčiavimą, 27 % nėra tikri ir 12 % nežino, kas yra sukčiavimas. Paprašius pasirinkti teisingą sukčiavimo apibrėžimą, 72 % apklaustų žmonių jį pasirinko teisingai. Maltoje ir Estijoje respondentų, teigiančių, kad žino, kas yra sukčiavimas, skaičius yra vienodas. Lietuvoje, Kipre ir Latvijoje teisingą atsakymą pasirinko daugiau žmonių nei tie, kurie nurodė žinantys, kas yra sukčiavimas. Šie rezultatai gali reikšti, kad daugiau respondentų iš šių šalių žino apie sukčiavimą, tačiau jie nepasitiki savo žiniomis.

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)



3 pav. Respondentų supratimas apie sukčiavimą

Beveik pusė respondentų (46 %) nurodė, kad dažnai bijo atidaryti nuorodą ar priedą el. laiške, manydami, kad tai gali būti netikra, kai tuo tarpu 13 % visuomet bijo. Tik 3 % respondentų niekada nebijo atidaryti nuorodų ar priedų, o 8 % – labai retai bijo.

Beveik trečdalis respondentų (32 %) dažnai bijo tapti sukčiavimo atakų taikiniais, o 19 % visuomet bijo. Tik 5 % respondentų nurodė, kad jie niekada nebijo tapti sukčiavimo atakos taikiniu, o 17 % retai bijo.
Aukščiau pateikti rezultatai rodo, kad dauguma respondentų žino apie kibernetinių atakų galimybę ir pagrindinius įsilaužėlių naudojamas priemones (suklastotas nuorodas ir priedus). Be to, nors 39 % respondentų nurodė, kad nežino ar nėra tikri, kas yra sukčiavimas, vis tiek 51% respondentų dažnai arba visada bijo tapti sukčiavimo atakų taikiniais. Šie rezultatai gali reikšti, kad net tie respondentai, kurie nurodė kad žino, kas yra sukčiavimas, nebūtinai turi reikiamų žinių, kad apsisaugotų, arba pasitikėtų savo įgūdžiais.

Paklausti kokius skirtingus sukčiavimo tipus jie žino, visų apklaustų šalių respondentai nurodė, kad jie geriausiai žino šiuos sukčiavimo tipus:

- „**Spray and Pray**“ (*el. laiškai siekiant pavogti konfidencialią informaciją*),
- „**Cat phishing**“ (*įviliojimas į santykius*) ir
- „**Malvertising**“ (*internetinės reklamos ar iššokantys (angl. pop-up) langai*).

Visų apklaustų šalių, išskyrus Lietuvą, respondentai taip pat geriausiai žino sukčiavimo tipą „**Advanced fee scam**“ (*dažnas sukčiavimas, susijęs su Nigerijos piliečiais, pvz., prašymas padėti pervesti didelę pinigų sumą*).

4 pav. Sukčiavimo tipai, kuriuos respondentai geriausiai žino

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

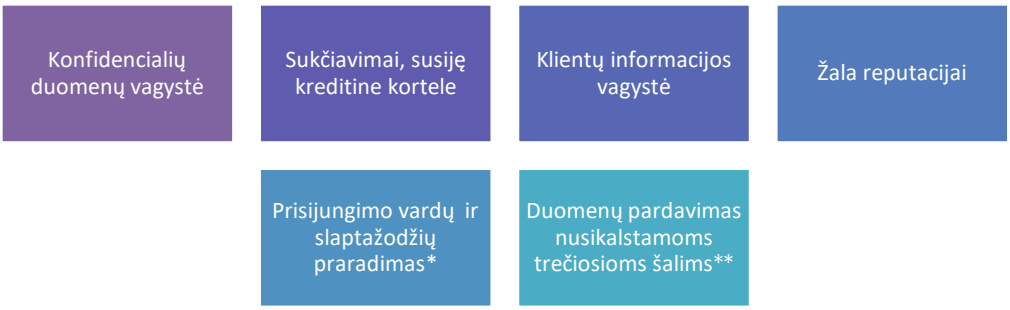
Kita vertus, respondentai mažiausiai žino šiuos sukčiavimo tipus:

- „**Whaling**“ (*bandymas pavogti konfidencialią informaciją ir dažnai nukreiptas į aukščiausią vadovybę*),
- „**Clone phishing**“ (*sukčiavimo tipas, kai teisėtas/tikras ir anksčiau/seniau gautas el. laiškas panaudojamas identiško el. laiško sukūrimui su kenkėjišku turiniu*) ir, išskyrus respondentus iš Kipro,
- “**Smishing**” (*sukčiavimas, siunčiant asmeniui SMS žinutes*)14.

Respondentai iš Maltos, Kipro, Lietuvos ir Latvijos taip pat mažiausiai žino apie „**Content injection**“ (*sukčiavimo tipas kai kibernetiniai nusikaltėliai įsilaužia į atpažįstamą svetainę ir patalpina suklastotą svetainės prisijungimo puslapį arba iššokantį langą, nukreipiantį svetainės lankytojus į suklastotą svetainę*), tuo tarpu Estijos respondentai nurodė, kad labiausiai žino apie šį sukčiavimo tipą.

5 pav. Sukčiavimo tipai, apie kuriuos respondentai mažiausiai žino

Paklausus, kokių pasekmių labiausiai tikėtina ar tikrai kils po sėkmingos sukčiavimo atakos asmeniui ar įmonei, dauguma respondentų iš visų apklaustų šalių įvardijo šias pasekmes – „konfidencialių duomenų vagystė“, „sukčiavimai, susiję kreditine kortele“, „klientų informacijos vagystė“, „žala reputacijai“ ir „prisijungimo vardų (angl. username) ir slaptažodžių praradimas“ (išskyrus Maltą). Respondentai iš visų apklaustų šalių, išskyrus Kiprą15, taip pat linkę manyti, kad po sėkmingos sukčiavimo atakos jų duomenys greičiausiai bus parduoti nusikalstamoms trečiosioms šalims.



6 pav. Respondentų įvardintos pasekmės, kurios greičiausiai atsirastų po sėkmingos sukčiavimo atakos

Kita vertus, visų apklaustų šalių respondentai mano, kad „intelektinės nuosavybės praradimas“ po sėkmingos sukčiavimo atakos vargu ar įvyksta. Respondentai iš Lietuvos, Maltos ir Estijos taip pat skeptiškai vertina „lėšų vagystes iš verslo ar klientų sąskaitų“ galimybę įvykus sukčiavimo atakai.

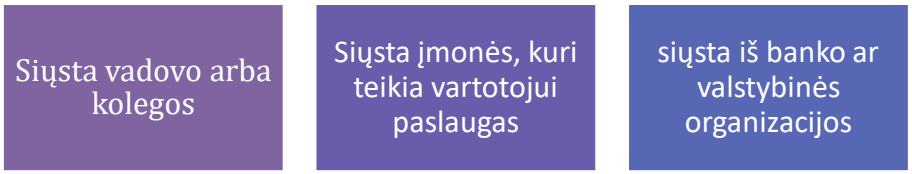
Atsižvelgiant į elgsenos aspektą, respondentai greičiausiai spustelės el. laiške ar žinutėje esančią nuorodą ar priedą ir pateiks neskelbtiną informaciją, jei tokį laišką: „atsiuntė jų viršininkas ar kolega“, „atsiuntė įmonė, kurios paslaugas jie naudoja“, „atsiuntė bankas ar bet kuri valstybinė institucija“. Kipre respondentai taip pat greičiausiai taip elgtųsi, jei el. laiške ar žinutėje būtų „prašoma patikslinti

14 Except for the respondents in Cyprus

15 Except for the respondents in Cyprus

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

detales, tokias kaip jų adresas užsakymo siuntimui (pvz., „Amazon“ užsakymui). Tuo pat metu Latvijoje ir Maltoje nuomonės išsiskiria: beveik vienodas skaičius respondentų, kurie labai tikėtina, kad taip pasielgtų, ir labai mažai tikėtina, kad taip pasielgtų. Tarp Estijos ir Lietuvos respondentų nėra skirtingų nuomonių, ir dauguma jų greičiausiai to nedarytų.



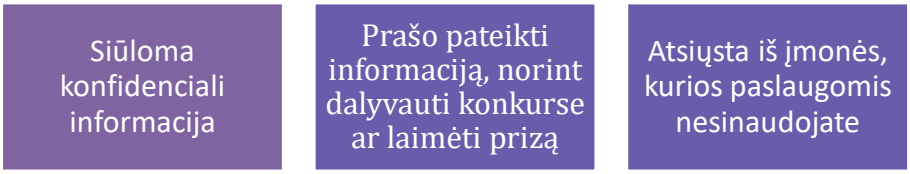
7 pav. El. laiškų tipai, kuriuose respondentai greičiausiai spustelės el. laiške ar žinutėje esančią nuorodą ar priedą ir (ar) pateiks neskelbtiną informaciją

Rezultatai nėra tokie stebinantys, jei pažvelgtume į šešis anksčiau aprašytus įtikinėjimo principus. Kaip minėta anksčiau, žmonės linkę sekti ir pasitikėti daugiau autoritetu ar ekspertais. Taigi daugelis įsilaužėlių siekia apsimesti arba patikima valstybine institucija ar organizacija ir bankais arba aukščiausio lygio vadovais. Ši tendencija buvo matoma ir apklausoje, kur 34% respondentų teigė, kad labai dažnai arba visada pasitiki žinutėmis, kurios atrodo atsiųstos iš svarbaus subjekto ar atrodo svarbūs, tuo tarpu 30% taip elgiasi kartais.

„Patikimo principas“ (angl. liking principle) taip pat vaidina svarbų vaidmenį, tai reiškia, kad žmonės daug dažniau atsakys į prašymą iš savo kolegų ar vadovų, net jei tas prašymas skamba neįprastai.

Be to, žmonės yra „įpročio būtybės“ (angl. creatures of habits) ir linkę mėgti nuoseklumą. Tarkime, kad el. laišką siunčia kompanija, kurią jie žino ir, kurios paslaugas naudoja ir tikriausiai jau yra gavę el. laiškų ar pranešimų anksčiau. Tokiu atveju jie bus labiau linkę jį atidaryti, spustelėti nuorodas ar priedus ir pan., nei tai darytų gavę laišką iš įmonės, kurios paslaugomis nesinaudoja.

Visose šalyse partnerėse respondentai mažiausiai linkę spustelėti el. laiške ar žinutėje esančią nuorodą ar priedą ir (arba) pateikti neskelbtiną informaciją, jei jame: „siūloma jiems konfidenciali informacija (pvz., informacija apie konkurentus)“, „prašoma jų užpildyti apklausą ar pateikti savo el. pašto adresą arba telefono numerį, tam kad galėtų dalyvauti konkurse ir laimėti prizą“ arba laišką „atsiunčia kompanija ar organizacija, kurią jie žino, bet nenaudoja jos paslaugų“.



8 pav. El. laiškų tipai, kuriuose respondentai mažiausiai linkę spustelėti el. laiške ar žinutėje esančią nuorodą ar priedą ir (ar) pateikti neskelbtiną informaciją

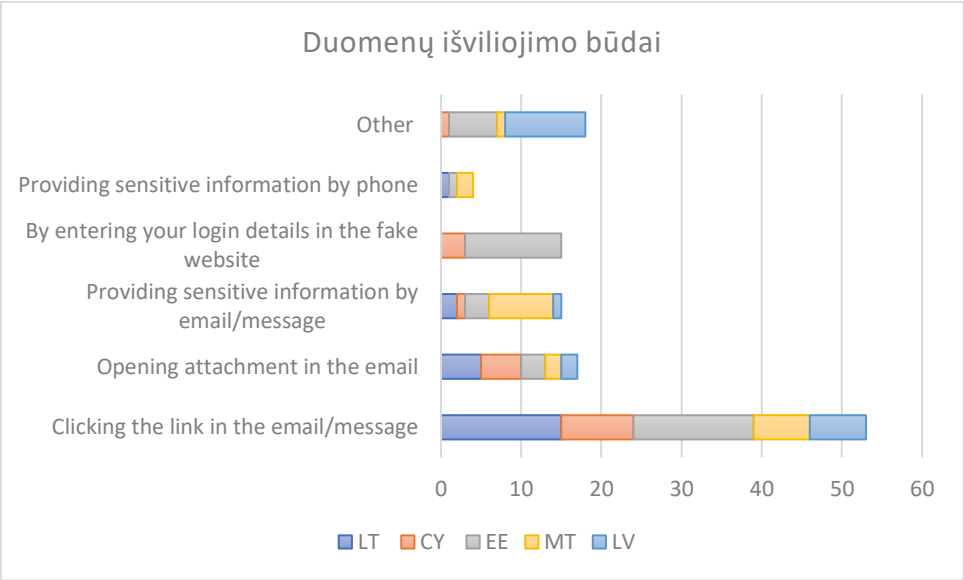
Dauguma respondentų iš Estijos, Kipro ir Maltos taip pat vargu ar pateiks konfidencialią informaciją, jei el. laiške ar žinutėje „prašoma padėti arba paaukoti vietos ar tarptautinėms labdaros organizacijoms“. Respondentai iš Kipro taip pat greičiausiai spustelės nuorodą ar priedą ir pateiks neskelbtiną informaciją, jei laiškas „pakvies juos į konkretų renginį internetu (pvz., Zoom susitikimas) arba kontaktiniu būdu. Priešingai, respondentai iš Lietuvos, Latvijos, Estijos ir Maltos veikiausiai to nedarytų.

3.3.3. Asmeninė patirtis susijusi su sukčiavimu (angl. phishing) atakomis

19,8 %. respondentų (arba beveik kas penktas asmuo, dalyvavęs apklausoje) praeityje nukentėjo nuo sukčiavimo (angl. phishing) atakos. Rezultatai rodo, jog dažniausiai tai įvykdavo todėl, nes žmonės paspausdavo nuorodas el. laiškuose ar žinutėse, atverdavo priedus arba atsakydavo į

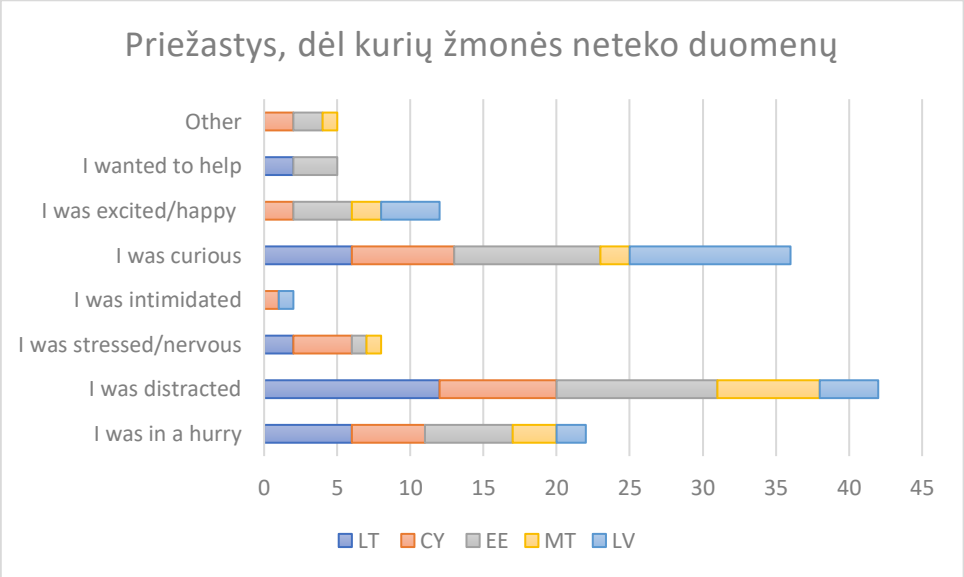
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project №.: 2020-1-LT01-KA203-078070)

laiškus pateikdami konfidencialius duomenis. Netikėta, kad tik apklaustieji iš Estijos ir Kipro įvardijo, jog svarbius duomenis prarado įvedę savo prisijungimo duomenis į suklastotas svetaines. Tarp „kita“ atsakymų populiariausi buvo „kelių sukčiavimo būdų derinys“ ir „informacijos pateikimas suklastotoje apklausoje“.



9 iliustracija. Būdai, kaip praeityje iš žmonių išvilioti duomenis

Didžiosios apklaustųjų dalies nuomone, jie nuo sukčiavimo nukentėjo kadangi buvo išsiblaškę, smalsūs arba kur nors skubėjo.



10 pav. Apklaustųjų nuomonė, dėl kokių priežasčių jie neteko duomenų

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

3.3.4. Sukčiavimo (angl. phishing) atakų atpažinimas

Apklausos dalyvių buvo paprašyta įvertinti ir įvardinti pagrindinius kriterijus, siekiant atpažinti įtartiną elektroninį laišką, skambutį, trumpąją žinutę, ar žinutę socialiniame tinkle.

Elektroninis laiškas

Kalbant apie įtartinus elektroninius laiškus, apklaustieji iš visų šalių turi bendrą nuomonę apie pačius svarbiausius kriterijus, siekiant atpažinti tokio pobūdžio ataką. Pagrindiniai iš jų yra:

1) siuntėjo domenas (elektroninis paštas) neatrodo autentiškas (neatitinka tikrojo organizacijos pašto, jame paslėpta rašybos klaida, jame yra daug skaičių ar raidžių, ir t. t.);
2) nuorodos patalpintos el. laiške nesutampa su realiomis nuorodomis;
3) siuntėjas prašo elektroniniu laišku patvirtinti ar pateikti konfidencialią informaciją (prisijungimo duomenis, banko duomenis);
4) yra akivaizdžių neatitikimų elektroninio pašto adresuose, nuorodose bei domenų varduose;
5) kartu su elektroniniu laišku yra atsiunčiamas įtartinas ar neįprastas priedas.

Mažiausiai svarbūs kriterijai, kuriuos nurodė respondentai, buvo šie:

1) laiške pasisveikinama nuasmenintai;
2) nėra jokio parašo ar kontaktinės informacijos;
3) laiškas sužadina smalsumą, norą juo pasidomėti daugiau;
4) informacija pateikiama laiške skamba pernelyg gerai, jog tai būtų tiesa.

Tyrimo dalyviai iš Maltos prie šių kriterijų taip pat prideda, jog laiško rašymo stilius, kuris neatitinka to žmogaus ar kompanijos, iš kurios asmuo paprastai gauna tokius laiškus stiliaus bei gramatinės ir rašybos klaidos esančios tekste, taip pat nėra itin reikšmingi signalai.

Trumpoji žinutė ar skambutis

Beveik vienoda visų apklaustų šalių respondentų nuomonė taip pat sutapo, kai reikėjo nurodyti svarbiausius kriterijus, pagal kuriuos galima atpažinti įtartiną SMS žinutę ar skambutį.

Toliau išvardinti požymiai (angl. red flags), pasak apklaustųjų, gali išduoti, jog nusikaltėliai bando išgauti asmeninę informaciją:

1) siuntėjas ar skambintojas prašo patvirtinti tam tikrus duomenis, pateikti asmeninę informaciją ar pervesti pinigų;
2) skambintojo pirmieji numerio skaičiai nesutampa su šalies kodu;
3) skambintojas tinkamai neprisistato, neaišku koks jo vardas, pavardė, kompanijoje užimamos pareigos ir pan.

Apklaustieji iš Estijos papildo šį sąrašą dar vienu kriterijumi – neįprastai ilgas telefono numeris taip pat signalizuoja apie galimą bandymą sukčiauti. Be to, tyrimo dalyviai iš visų šalių, išskyrus Kiprą, įvardina, jog trumposios žinutės su įspėjimais, pavyzdžiui, jog žmogaus sąskaita greitai nustos galioti bei spaudimas gavėją priimti kuo skubesnį sprendimą, taip pat yra požymis apie galimą sukčiavimo ataką.

Mažiau svarbus kriterijus, kurį nurodė Maltos, Estijos, Lietuvos ir Kipro respondentai, buvo rašybos ir gramatikos klaidos. Latviai, savo ruožtu, mano priešingai – gramatines ir rašybos klaidas įvardina kaip viena iš didžiausių požymių apie galima sukčiavimą. Tyrimo dalyviai iš daugumos šalių teigia,

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project №.: 2020-1-LT01-KA203-078070)

kad nėra itin reikšminga, jog skambintojas nesikreipia į juos vardu ar pavarde. Kaip vieną iš svarbiausių signalų, tai įvardino tik respondentai iš Kipro.

Žinutė socialiniame tinkle

Respondentų nuomonė dėl įtartinų žinučių socialinėje žiniasklaidoje atpažinimo taip pat buvo beveik vieninga. Dauguma respondentų pritarė šiems svarbiausiems kriterijams:

1) žinutėje prašoma pinigų;
2) žinutėje prašoma patvirtinti duomenis arba pateikti konfidencialią informaciją;
3) žinutėje yra įtartina interneto nuoroda;
4) siuntėjo asmeninis profilis nekelia pasitikėjimo, pavyzdžiui, jo paskyra sukurta neseniai, asmuo neturi nei vieno draugo ir pan.

Respondentai, išskyrus respondentus iš Maltos, taip pat mano, kad žinutė, kurioje prašoma įdiegti kokią nors programą, yra viena iš pagrindinių požymių, rodančių įtartiną veiklą (sukčiavimą).

Mažiausiai svarbiais kriterijais respondentai įvardijo rašybos ir gramatikos klaidas, tai, kad su siuntėju neturi jokių verslo ryšių arba nepažįsta siuntėjo.

Sukčiavimo atakos atpažinimas	Patys svarbiausi kriterijai	Mažiau svarbūs kriterijai
Elektroninis laiškas	• Siuntėjo domenas (el. paštas) neatrodo tikras. • Nuorodos patalpintos el. laiške nesutampa su realiomis nuorodomis. • Siuntėjas prašo patvirtinti ar pateikti asmeninę ar konfidencialią informaciją. • Akivaizdūs neatitikimai el. pašto adresuose, interneto nuorodose ir domeno varduose. • El. laiškas turi netikėtą ar neįprastą priedą.	• Nuasmenintas pasisveikinimas laiške. • Nėra parašo ar kontaktinės informacijos. • Laiško turinys sukelia smalsumą, norą sužinoti daugiau.
Trumpoji žinutė ar skambutis	• Siuntėjas ar skambintojas prašo patvirtinti duomenis, pateikti asmeninę informaciją. • Numeris su kitos šalies kodu. • Siuntėjas tinkamai neprisistato (vardas, pareigos, kompanija). • Neįprastai ilgas numeris.16 • Žinutėje yra perspėjimas.17	• Gramatikos ar rašybos klaidos.18 • Skambintojas tinkamai neprisistato.19
Žinutė socialiame tinkle	• Žinutėje prašoma pervesti pinigų. • Žinutėje prašoma patvirtinti duomenis arba pateikti konfidencialią informaciją. • Žinutėje yra abejotina interneto nuoroda.	• Gramatinės ir rašybos klaidos.

16 Išskyrus apklaustuosius iš Estijos

17 Išskyrus apklaustuosius iš Kipro

18 Išskyrus apklaustuosius iš Latvijos

19 Išskyrus apklaustuosius iš Kipro

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Sukčiavimo atakos atpažinimas	Patys svarbiausi kriterijai	Mažiau svarbūs kriterijai
	• Siuntėjo socialinio tinklo profilis yra įtartinas (pvz. nauja paskyra, nėra jokių draugų). • Žinutėje prašoma įdiegti kokią nors programą.20	• Asmuo neturi jokių verslo santykių su siuntėju. • Asmuo siuntėjo nepažįsta.

3 lentelė. Svarbiausi ir mažiau reikšmingi kriterijai, siekiant atpažinti sukčiavimo atakas

20 Išskyrus apklaustuosius iš Maltos

Co-funded by the Erasmus+ Programme of the European Union

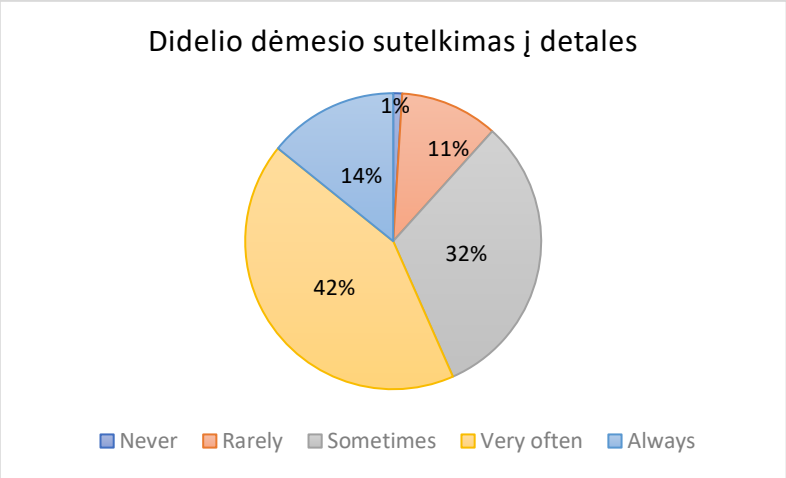
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Apskritai, nurodydami pagrindinius kriterijus, respondentai daugiausia dėmesio skiria „techniniams kriterijams“, pavyzdžiui, nuorodoms, domenams, priedams, šalies kodui ir t. t., o ne žmogiškoms emocijoms (socialinei inžinerijai) atpažįstant įtartinus el. laiškus ar pranešimus. Rašybos ar gramatikos klaidos arba bendrinis pasveikinimas yra vieni iš paskutinių punktų, kuriuos respondentai vertina.

Tačiau verta pažymėti, kad nepaisant to, jog „techniniai kriterijai“ apklaustųjų yra laikomi vienais iš pagrindinių požymių, kurie įspėja apie galimą sukčiavimą, tai nereiškia, jog asmenys neįvertina socialinės inžinerijos grėsmės. Paprašyti atpažinti sukčiavimo laiškus ar pranešimus bei pagrindinius bruožus, kurie rodo, kad tai bandymas sukčiauti, dauguma apklaustųjų iš visų šalių nurodė, jog tai išduoda tiek techniniai kriterijai, tiek su žmogaus emocijomis susiję kriterijai (socialinė inžinerija).

3.3.5. Kritinio mąstymo gebėjimai

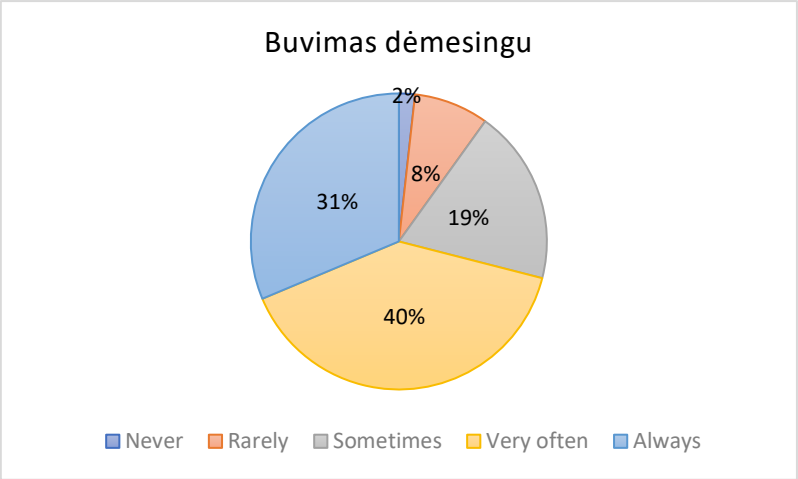
Dauguma respondentų gana optimistiškai vertina savo kritinio mąstymo įgūdžius. Daugiau nei pusė respondentų (57 %) teigė, kad labai dažnai arba visada atidarydami el. laišką ar žinutę jie pakankamai susikaupia ir atkreipia dėmesį į detales. Palyginimui, 12% žmonių atsakė, jog jie niekada arba retai koncentruojasi į tokius dalykus.



11 pav. Respondentų didelio dėmesio sutelkimas į detales, atidarant žinutę/elektroninį laišką

71 % respondentų teigia, jog jie dažnai yra dėmesingi, kuomet atidaro nuorodą ar priedą, tuo tarpu 11 % teigia, jog tai darydami, atidžiais būna labai retai arba net niekada.

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)



12 pav. Respondentų dėmesingumas spaudžiant ant nuorodos/priedo

67 % respondentų teigė, kad labai dažnai arba visada, gavę įtartinai atrodantį el. laišką ar žinutę, gali tinkamai vertinti galimas savo sprendimų pasekmes, remdamiesi įrodymais, ir tik 5% teigia, jog retai arba niekada negalėtų įvertinti savo veiksmų pasekmių.

77 % atsakiusiųjų taip pat gali daryti tinkamas išvadas, atsižvelgdami į įtartino laiško/pranešimo parametrus/duomenis, o tik 3 % respondentų niekada arba retai gali tai padaryti.

Skirtumas tarp respondentų, galinčių įsivaizduoti pasekmes ir galinčių daryti išvadas, procentinės dalies yra nedidelis. Priešingai, ne visi respondentai suvokia, kokios gali sukčiavimo (angl. phishing) pasekmės. Vis tik, jie gali daryti tinkamas išvadas ir atpažinti sukčiavimo laišką/žinutę.

Tačiau svarbu pabrėžti, kad, nepaisant gana gerų rezultatų, maždaug trečdalis respondentų dar tik kartais geba įvertinti gresiančias pasekmes bei padaryti tinkamas išvadas.

3.3.6. Apsisaugojimas nuo sukčiavimo atakų

Apklausos dalyvių buvo paprašyta pasirinkti pagrindines priežastis, dėl kurių, jų nuomone, sukčiavimo atakos būna sėkmingos. Asmenys iš visų šalių išskyrė penkias:

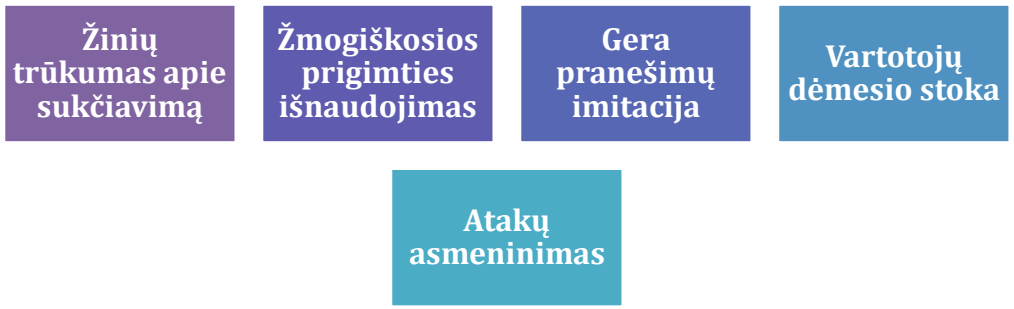
1) Vartotojai neturi žinių apie tokias atakas ir nežino kaip jų išvengti;
2) Atakų organizatoriai naudojasi žmogiškąja prigimtimi, emocijomis bei poreikiais;
3) Atakų organizatoriai labai gerai imituoja realių įmonių pranešimus ir el. laiškus, jie parengiami tikroviškai bei įtikinamai;
4) Vartotojai neskiria tam pakankamai dėmesio[21];
5) Atakų organizatoriai tampa vis labiau pažengę, atakuoja atskirus asmenis naudodami personalizuotą ir specifinę informaciją[22].

21 Išskyrus apklaustuosius iš Maltos

22 Išskyrus apklaustuosius iš Kipro

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)



13 pav. Pagrindinės priežastys, kodėl sukčiavimo atakos būna sėkmingos

Rečiausiai pasirinktos priežastys yra šios:

1) žmonės naudoja pasenusias programines priemones;
2) sukčiavimo priemonės pigios bei plačiai paplitusios;
3) kenkėjiškos programos tampa sudėtingesnėmis23.

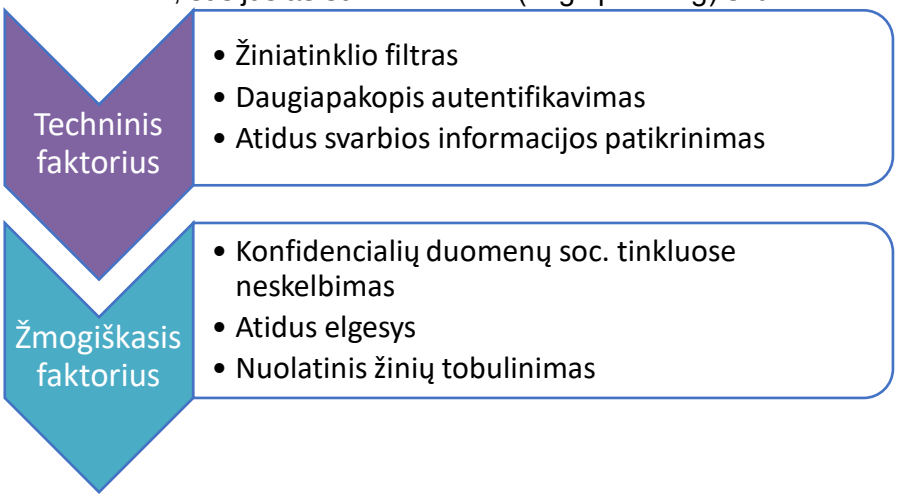
Atsakiusieji sutinka su mintimi, jog atakuotojai naudojasi žmogiškosiomis emocijomis, poreikiais bei potraukiais, kalbant konkrečiai, motyvuoja žmones „dovanomis“, nemokamais laimėjimais, žadina smalsumą bei sukelia nerimą ar jaudulį.

23 Išskyrus apklaustuosius iš Maltos

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Didžioji dalis apklaustųjų mano, kad siekiant išvengti sukčiavimo atakų, į šį klausimą reikia žvelgti iš skirtingų perspektyvų:

1) techninis – naudoti žiniatinklio filtrą kenkėjiškų svetainių blokavimui, naudoti daugiapakopį autentifikavimą ir dažnai keisti slaptažodžius, atidžiai patikrinti visą svarbią informaciją (siuntėjo pašto adresą, nuorodas, priedus ir t. t.);
2) žmogiškasis – konfidencialios informacijos neskelbti socialiniuose tinkluose, elgtis atidžiai atidarant elektroninius laiškus ir pranešimus ar atsiliepiant į telefoninius skambučius bei nuolat tobulinti žinias, susijusias su sukčiavimo (angl. phishing) sritimi.

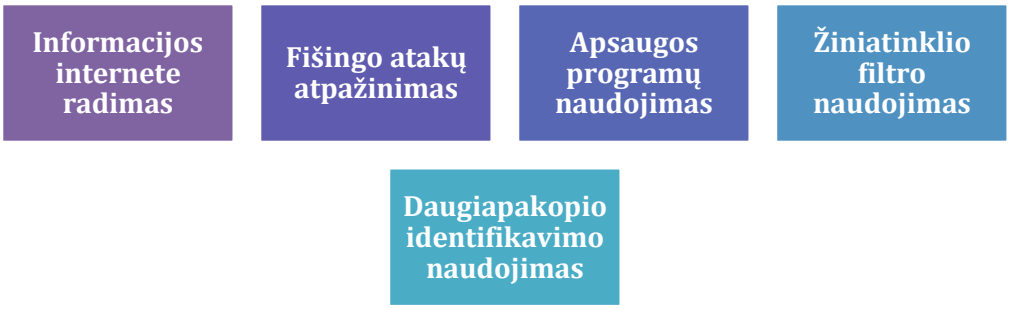


14 pav. Faktoriai, padedantys apsisaugoti nuo sukčiavimo atakų

Svarbūs veiksmai, kurių reikėtų imtis siekiant išvengti sukčiavimo atakų, respondentų nuomone, yra naudoti atnaujintą naršyklę, sekti naujausią turimą programinę įrangą ir įrankius, naudoti atnaujintą operacinę sistemą, taip pat reguliariai tobulintis kibernetinio saugumo mokymuose ar seminaruose.

Apklaustieji teigia, jog randa tinkamą ir patikimą informaciją internete, atpažįsta sukčiavimo atakas, laiku atnaujiną programinę įrangą, naudoja daugiapakopį autentifikavimą, apsaugos programas bei žiniatinklio filtrą. Šiose srityse tyrimo dalyviai labiausiai užtikrinti.

Mažesnė dalis respondentų jaučiasi užtikrinti, jog tinkamai išmano kibernetinio saugumo ar sukčiavimo terminiją bei naudoją ją, be to šifruoja visa konfidencialią kompanijos ar asmeninę informaciją.



15 pav. Sritys, kuriose apklaustieji jaučiasi labiausiai užtikrinti

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project №.: 2020-1-LT01-KA203-078070)

4. Apklausos apibendrinimas ir pagrindinės išvados

Apklaustųjų socialinė demografija

- Apklausoje iš viso dalyvavo 514 žmonių, iš kurių 259 moterys, 248 vyrai bei 7 žmonės, kurie lyties atskleisti nenorėjo.
- Dauguma apklaustųjų – studentai (304), toliau seka samdomi darbuotojai (139), darbo neturintys asmenys (10) bei žmonės kurie dirba savarankiškai (8).
- Dauguma tyrimo dalyvių yra įgiję aukštąjį išsilavinimą: 38 % turi bakalauro laipsnį, 23 % turi magistro laipsnį, o 6 % turi daktaro laipsnį.

Bendrosios žinios ir elgsena

- Nors 74 % apklaustųjų niekada nedalyvavo jokiuose oficialiuose ar formaliuose kibernetinio saugumo mokymuose ar seminaruose, 54 % teigia, jog domėjosi šia sritimi patys (skaitė straipsnį, žiūrėjo vaizdo įrašus ir pan.). Šie rezultatai parodo, kad nepaisant to, jog apklaustieji ne visada turi galimybę dalyvauti oficialiuose kibernetinio saugumo mokymuose, jie turi motyvacijos patys gilinti savo žinias bei įgūdžius.
- 61% apklaustųjų teigia, jog žino, kas yra sukčiavimas (angl. phishing), 27 % nėra dėl to tikri, o 12 % atsakė, kad negali atsakyti kas tai yra. Paprašyti įvardinti tinkamą šio žodžio reikšmę, daugiau žmonių iš Lietuvos, Latvijos ir Kipro pasirinko tikslų jo apibrėžimą, nei bendras skaičius apklaustųjų, kurie teigė, jog žino kas yra sukčiavimas (angl. phishing). Šis rezultatas parodo, kad galimai daugiau žmonių iš šių šalių žino, ką reiškia ši sąvoka, tačiau jiems trūksta žinių arba pasitikėjimo savo įgomis.
- 59 % apklausoje dalyvavusių žmonių labai dažnai ar net visada bijo paspausti ant nuorodos ar priedo, manydami, jog tai gali būti sukčiavimas. Palyginimui, 51 % teigia, jog labai dažnai ar net visuomet baiminasi tapti sukčiavimo (angl. phishing) atakos taikiniu. Tai sufleruoja, kad net ir tie apklaustieji, kurie teigia, jog žino kas yra sukčiavimas (angl. phishing), bijo nuo jo nukentėti. Dėl to galima manyti, kad šiems žmonėms trūksta tinkamų žinių arba pasitikėjimo savo įgomis.
- Atsakiusieji labiausiai atpažįsta šiuos sukčiavimo (angl. phishing) būdus: „*Spray and pray*“, „*Cat phishing*“ ir „*Malvertising*“. Tačiau tyrimo dalyviai turi mažiau žinių apie „*Whaling*“, „*Clone phishing*“ ir „*Smishing*“ atakas.
- Atsakiusieji mano, jog po sėkmingo sukčiavimo (angl. phishing) atakos, gali atsirasti šios pasekmės: konfidencialių duomenų vagystė, sukčiavimai, susiję su kreditinėmis kortelėmis bei žala reputacijai. Didelė dalis tyrimo dalyvių, išskyrus Maltos respondentus, taip pat mano, jog po sėkmingos atakos galima netekti prisijungimo vardų ir slaptažodžių. Dauguma apklaustųjų, išskyrus Kipro respondentus, įvardija, kad duomenys gali būti parduodami nusikalstamosioms trečiosioms šalims. Kalbant apie mažiausiai tikėtiną pasekmę, respondentai teigia, jog intelektinės nuosavybės praradimo tikimybė yra nedidelė.

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project №.: 2020-1-LT01-KA203-078070)

- Lietuvos, Maltos ir Estijos respondentai mano, jog lėšų vagystė iš verslo ir klientų sąskaitų yra menkai tikėtina pasekmė, kuri gali kilti po sėkmingos kibernetinės atakos.

- Tyrimo dalyviai labiau linkę spausti el. laiške ar žinutėje esančią nuorodą ar priedą, jeigu jį atsiunčia vadovas, kolega, įmonė, kuri asmeniui teikia paslaugas, bankas ar valstybinė organizacija. Remiantis dr. Robert B. Cialdini įtikinėjimo principais, tokioje situacijoje žmonės labiau linkę pasitikėti valdžios atstovais, t. y. pasitiki asmenimis, kuriuos gerbia bei mieliau pildo prašymus tų, kurie jiems patinka.

- Mažesnė tikimybė, kad respondentai spragtelės nuorodą ar priedą el. laiške ar žinutėje, jei joje bus siūloma konfidenciali informacija, prašoma pateikti informaciją, kad galėtų dalyvauti konkurse ir laimėti prizą, arba ją atsiųs įmonė, kurios paslaugomis jie nesinaudoja. Atrodo, kad įtikinėjimo „abipusiškumo“ principas yra tas, į kurį respondentai būtų mažiau linkę reaguoti.

Tyrimo dalyvių asmeninė patirtis susijusi su sukčiavimu

- Beveik kas penktas asmuo įvardijo, jog praeityje nukentėjo nuo sukčiavimo (angl. phishing) atakos. Pagrindinės to priežastys – asmenys paspaudė nuorodą elektroniniame laiške, žinutėje arba atsakė į sukčiavimo (angl. phishing) laišką, pateikdami konfidencialią informaciją. Tik respondentai iš Kipro ir Estijos teigia, kad į sukčiavimo (angl. phishing) pinkles papuolė įvedę savo duomenis į suklastotą svetainę.

- Pagrindinės priežastys, kodėl asmenys nuo sukčiavimo (angl. phishing) nukentėjo yra tos, kad tuo metu jie buvo išsiblaškę, smalsūs arba skubėjo. Kai kurie dalyviai atsakė, jog nežinojo kas yra sukčiavimas (angl. phishing).

Sukčiavimo (angl. phishing) atakų atpažinimas

- Kalbėdami apie pagrindinius kriterijus, pagal kuriuos galima nustatyti, kad įvykdyta sukčiavimo ataka, respondentai apskritai daugiau dėmesio skyrė „techniniams kriterijams“, pavyzdžiui, siuntėjo domenui, įterptoms nuorodoms, priedams ir matomiems jų neatitikimams, taip pat neįprastai ilgam numeriui ar kitokiam šalies kodui. Respondentai taip pat nurodė, kad siuntėjas ar skambintojas, prašantis pateikti neskelbtinos informacijos arba pinigų, yra vienas iš pagrindinių atpažinimo kriterijų apie galimą sukčiavimą. Gramatinės ar rašybos klaidos, nuasmeninti pasisveikinimai atsakiusiųjų buvo įvardinti rečiausiai.

- Tačiau, nors respondentai pirmiausia pastebi ir tikrina „techninius kriterijus“, vertindami el. laiškus ir pranešimus jie atsižvelgia ir į „žmogiškuosius kriterijus“ (socialinę inžineriją). Apklausoje paprašyti nurodyti apgaulingus el. laiškus ar žinutes ir pagrindines pagrindinius sukčiavimo (angl. phishing) bruožus, dauguma respondentų iš visų tirtų šalių pasirinko tiek „techninius kriterijus“, tiek kriterijus, orientuotus į žmogiškąjį faktorių (socialinę inžineriją).

Kritinio mąstymo gebėjimai

- Dauguma respondentų gana palankiai vertina savo kritinio mąstymo gebėjimus. 57 % respondentų sutelkia didelį dėmesį į detales, kuomet atidaro elektroninius laiškus ar pranešimus. Palyginimui, 71 % teigia, jog jie labai dėmesingi, kuomet paspaudžia ant nuorodos ar atveria priedą.

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project №.: 2020-1-LT01-KA203-078070)

- 67 % respondentų teigia, jog labai dažnai ar visuomet gali įvertinti galimas pasekmes, kurios gali kilti priklausomai nuo jų veiksmų, kuomet gauna įtartinai atrodantį laišką ar pranešimą. Palyginimui, 77 % respondentų labai dažnai arba visada sugeba padaryti išvadas. Procentinis skirtumas tarp šių duomenų parodo, jog nors ne visi žmonės pilnai supranta, kokios gali būti sėkmingo sukčiavimo (angl. phishing) atakos pasekmės, jie vis tiek gali padaryti tinkamas išvadas ir atpažinti sukčiavimo (angl. phishing) laišką.

- Tačiau svarbu pabrėžti, jog nepaisant pakankamai gerų rezultatų, maždaug viena trečioji atsakiusiųjų tik kartais geba įvertinti galimas pasekmes ir padaryti tinkamas išvadas.

Sukčiavimo (angl. phishing) atakų išvengimas

- Respondentai pasirinko pagrindines priežastis, kurios, jų nuomone, lemia sėkmingas sukčiavimo atakas: žmonės nežino apie sukčiavimą ir kaip nuo jo apsisaugoti, užpuolikai naudojasi žmogaus prigimtimi. Be to, jie gerai sugeba atkartoti teisėtų bendrovių el. laiškus ir pranešimus, o žmonės neskiria pakankamai dėmesio arba yra neišprusę. Mažesnė respondentų dalis mano, kad tam įtaką daro tai, jog kai kurie vartotojai naudojasi pasenusiomis programinėmis priemonėmis, taip pat faktas, kad sukčiavimo (angl. phishing) priemonės yra pigios, plačiai paplitusios, o pačios kenkėjiškos programos tampa vis sudėtingesnėmis.

- Respondentai mano, jog atakuotojai stengiasi išnaudoti žmonių smalsumą, nerimą, jaudulį, taip pat bando sudominti nemokamais laimėjimais, kuponais ar nuolaidomis pirkiniams.

- Kaip išskiria apklausos dalyviai, siekiant atpažinti sukčiavimo (angl. phishing) ataką, būtinas tiek techninis, tiek žmogiškasis faktoriai. Pavyzdžiui, „techninis veiksnys“ apima žiniatinklio filtro naudojimą, daugiapakopį autentiškumo patvirtinimą ir svarbių duomenų, tokių kaip, siuntėjo el. pašto, nuorodų, priedų ir pan. tikrinimą. „Žmogiškasis veiksnys“ – asmenims nepatartina skelbti konfidencialių duomenų socialiniuose tinkluose, be to reikia būti atsargiems ir nuolat tobulintis šioje srityje.

- Įdomu tai, jog nors dauguma tyrimo dalyvių mano, kad svarbu nuolat tobulintis šioje srityje, tik mažesnė dalis pasisako už tai, jog reikia reguliariai dalyvauti kibernetinio saugumo mokymuose ar seminaruose. Tačiau tai galima paaiškinti tuo, jog beveik pusė dalyvių žinias apie kibernetinį saugumą gilina savarankiškai.

- Apskritai tyrimo dalyviai mano, jog siekiant atpažinti sukčiavimo (angl. phishing) ataką, žmogiškieji gebėjimai yra svarbesni, nei tai, kokią operacinę sistemą, įrangą ar įrankius tuo metu naudoja vartotojas.

- Dauguma respondentų labiausiai pasitiki gebėjimu rasti svarbią ir patikimą informaciją internete, atpažinti sukčiavimo (angl. phishing) atakas ir naudotis saugumo programine įranga, daugiapakopiu autentifikavimu bei interneto filtru.

- Mažesnė dalis apklaustųjų yra įsitikinę, jog žino kibernetinio saugumo ar sukčiavimo (angl. phishing) terminiją ir naudoja ją bei šifruoja visa konfidencialią kompanijos ar asmeninę informaciją.

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project №.: 2020-1-LT01-KA203-078070)

5. Bibliografija

1. EU Commission (2020): Special Eurobarometer 499: Europeans' attitudes towards cyber security, URL https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG
2. European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020
3. EUROSTAT (2020): Is internet use safer today?, URL https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb/default/table?lang=en (žiūrėta 11.02.2021)
4. Proofpoint (2019): Human Factor Report 2019, URL https://www.proofpoint.com/us/resources/threat-reports/human-factor (žiūrėta 12.02.2021)
5. European Union Agency for Cybersecurity (2020): Phishing - ENISA threat landscape 2019-2020
6. Deloitte (2019): Understanding Phishing Techniques, URL https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf (žiūrėta 112.02.2021)
7. EUROPOL (2020): Internet Organised Crime Threat Assessment 2020
8. NCC group (2020) :Psychology of the Phish: Leveraging the Seven Principles of Influence, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433 (žiūrėta 12.02.2021)
9. Council of Europe (2020): Cybercrime and Covid, URL: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (žiūrėta 12.02.2021)
10. EUROPOL (2020): Pandemic profiteering - how criminals exploit the COVID-19 crisis

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

PRIEDAS 1. Apklausa „Kaip atpažįstame sukčiavimo (angl. phishing) atakas?“

1 Sekcija Asmeniniai duomenys

1. **Vardas:**…… *(neprivaloma)*

2. **E-pašto adresas:**……*(neprivaloma - jei norite gauti naujausią informaciją apie projektą ir dalyvauti pilotiniuose mokymuose, pateikite savo el. paštą)*

3. **Lytis**

- Vyras
- Moteris
- Nenorėčiau atskleisti

4. **Išsilavinimas**

- Nebaigtas vidurinis
- Aukštojo mokslo diplomas
- Profesinis išsilavinimas (techninis / profesinis mokymas)
- Bakalauro laipsnis
- Magistro laipsnis
- Daktaro laipsnis
- Nenorėčiau atskleisti
- Kita:……

5. **Užimtumas**

- Verslininkas
- Samdomas darbuotojas
- Savarankiškai dirbantis
- Studentas
- Senjoras
- Bedarbis
- Kita:……

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

6. **Kokia tikimybė, kad paspausite nuorodą ar atversite priedą el. laiške ar žinutėje ir / ar pateiksite konfidencialią asmeninę informaciją, kai:**

	Labai maža	Maža	Vidutinė	Didelė	Labai didelė
Jums siūlomas kuponas ar nuolaidos pirkiniams					
Jums siūloma prieiga prie išskirtinių pasiūlymų					
Jus kviečia į ypatingą internetinį susitikimą (pvz., zoom susitikimas)					
Jūsų prašo užpildyti anketą / pateikti savo el. pašto adresą ar telefono numerį, norint laimėti prizą					
Jums siūloma konfidenciali informacija (pvz., apie konkurentus)					
Jūsų prašo patikslinti asmeninę informaciją ir / ar sąskaitos duomenis. Neatnaujinus duomenų paskyra ar sąskaita būtų uždaroma/blokuojama (pvz., banko sąskaita, internetinio filmų portalo (Netflix, Go3), Facebook paskyra ir pan.)					
Jūsų prašo patikslinti namų adresą tam, kad pristatytų prekes (pvz., iš Amazon)					
Pateikiama informacija apie naujausius įvykius, susijusius su stichinėmis nelaimėmis ar su svarbiomis socialinėmis problemomis (pvz., Covid-19 naujausia informacija)					
Jūsų prašoma padėti / paaukoti labdaros organizacijoms					
Pateikiama informacija susijusi su jūsų pomėgiais					
Laiškas / žinutė atsiųsta iš banko ar vyriausybinės organizacijos					
Laiškas / žinutė atsiųsta vadovo ar kolegos					
Laiškas / žinutė atsiųsta įmonės, kuri jums teikia paslaugas					
Laiškas / žinutė atsiųsta iš įmonės, kurios paslaugomis nesinaudojate					

7. **Ar kada nors dalyvavote oficialiuose/formaliuose kibernetinio saugumo ar konkrečiai sukčiavimo (angl. phishing) mokymuose / seminaruose / tyrimuose?**

- Taip
- Ne

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project №.: 2020-1-LT01-KA203-078070)

8. **Ar kada nors pats asmeniškai domėjotės / mokėtės apie kibernetinį saugumą ar konkrečiai sukčiavimą (angl. phishing) (skaitėte straipsnį, žiūrėjote vaizdo įrašus ir pan.)?**

- Taip
- Ne

9. **Ar žinote kas yra sukčiavimas (angl. phishing)?**

- Taip
- Ne
- Nesu tikras

10. **Kuris iš pateiktų teiginių, jūsų manymu, atitinka sukčiavimo (angl. phishing) apibrėžimą?**

- Elektroninis nusikaltimas, kai el. paštu susisiekiama su potencialia auka, siekiant išvilioti iš asmens konfidencialią informaciją apie jo paskyras.
- Tai savotiškas sportas malonumui ar varžyboms.
- Nepageidaujami ir (arba) pasikartojantys el. laiškai iš produktus ar paslaugas siūlančio asmens ar įmonės.
- Elektroninis nusikaltimas, kai el. paštu, telefonu ar teksto pranešimu žinute susisiekiama su potencialia auka, siekiant išvilioti iš asmens konfidencialią / asmeninę informaciją.

11. **Ar žinote šiuos sukčiavimo (angl. phishing) būdus?**

1) Spray and pray – kenkėjiški el. laiškai, siunčiami bet kuriuo ir visais el. pašto adresais, bandant pavogti konfidencialią informaciją;
2) Advanced fee scam – dažnas sukčiavimas, susijęs su Nigerijos piliečiais, pvz., prašymas padėti pervesti didelę pinigų sumą;
3) Cat phishing – kieno nors įviliojimas į santykius su išgalvota internetine asmenybe;
4) Spear fishing - kenkėjiški el. laiškai, specialiai sukurti ir siunčiami konkrečiam asmeniui ar organizacijai, siekiant pavogti konfidencialią informaciją;
5) Whaling - bandymas pavogti konfidencialią informaciją ir dažnai nukreiptas į aukščiausią vadovybę;
6) Vishing - sukčiavimas, kuris vyksta telefonu;
7) Smishing - sukčiavimas, siunčiant asmeniui SMS žinutes;
8) Clone Phishing - sukčiavimo tipas, kai teisėtas/tikras ir anksčiau/seniau gautas el. laiškas panaudojamas identiško el. laiško sukūrimui su kenkėjišku turiniu;
9) Content Injection - sukčiavimo tipas kai kibernetiniai nusikaltėliai įsilaužia į atpažįstamą svetainę ir patalpina suklastotą svetainės prisijungimo puslapį arba iššokantį langą, nukreipiantį svetainės lankytojus į suklastotą svetainę;
10) Malvertising - šis sukčiavimo tipas naudoja internetines reklamas ar iššokančius (angl. pop-up) langus, kad priverstų žmones paspausti ant įtarimo nekeliančios nuorodos, siekiant įdiegti kenkėjišką programą kompiuteryje.

	Visiškai nežinau	Šiek tiek žinau	Vidutiniškai žinau	Gerai žinau	Labai gerai žinau
Spray and pray					
Advanced fee scam					
Cat phishing					
Spear phishing					

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project №.: 2020-1-LT01-KA203-078070)

Whaling					
Whishing					
Smishing					
Clone phishing					
Content Injection					
Malvertising					

12. Kokios pasekmės gali atsirasti po sėkmingo sukčiavimo (angl. phishing) atakos prieš asmenį ar įmonę?

	Tikrai ne	Tikriausiai ne	Tikėtina	Tikriausiai taip	Tikrai taip
Tapatybės vagystė					
Sukčiavimai, susiję kreditine kortele					
Konfidencialių duomenų vagystė					
Prisijungimo vardų (*username*) ir slaptažodžių praradimas					
Kenkėjiškų ir išpirkos reikalaujančių programų įdiegimas					
Intelektinės nuosavybės praradimas					
Kliento informacijos vagystė					
Lėšų vagystės iš verslo ir klientų sąskaitų					
Prieiga prie sistemų būsimoms atakoms pradėti					
Duomenų pardavimas nusikalstamoms trečiosioms šalims					
Žala reputacijai					

3 sekcija Asmeninė patirtis

13. Ar kada nors bijojote paspausti ant nuorodos el. laiške ar žinutėje, galvodami, kad tai gali būti klastotė?

1 – Niekada
2 – Retai
3 – Kartais
4 – Dažnai
5 – Visada

14. Ar Jūs apskritai bijote tapti sukčiavimo (angl. phishing) atakos auka?

1 – Niekada
2 – Retai
3 – Kartais
4 – Dažnai
5 – Visada

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

15. Ar Jūs kada nors patekote į sukčiavimo (angl. phishing) pinkles?

Patikslinimas: Kalbėdami apie sukčiavimą (angl. phishing), turime omenyje – paspaudėte ant kenkėjiškos nuorodos / el. laiško priedo / pateikėte konfidencialius duomenis ir kt.

- Taip
- Ne

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

4 Sekcija (tik tiems, kurie į 15 klausimą atsakė „taip“) sukčiavimo (angl. phishing) atakos

16. Kaip Jūs patekote į sukčiavimo (angl. phishing) pinkles?

- Paspaudėte ant nuorodos el. laiške ar žinutėje
- Atsakėte į el. laišką ar žinutę pateikdami konfidencialią informaciją (pvz., prisijungimo duomenis)
- Atvėrėte el. laiško priedą
- Telefonu pateikėte konfidencialius duomenis
- Kita……

17. Kodėl, Jūsų manymu, taip atsitiko?

- Skubėjote
- Buvote išsiblaškęs / nekreipėte dėmesio
- Buvote įsitempęs / nervingas
- Buvote įbaugintas
- Buvote smalsus
- Buvote susijaudinęs / laimingas (pvz., pagalvojote, kad laimėjote prizą)
- Norėjote padėti
- Kita……

5 Skyrius sukčiavimo (angl. phishing) atakų atpažinimas

19. Kiek svarbūs yra šie kriterijai įtartinų el. laiškų atpažinimui?

	Nesvarbūs	Šiek tiek svarbūs	Vidutiniškai svarbūs	Svarbūs	Labai svarbūs
Nuasmenintas pasisveikinimas laiške (pvz., Gerb. kliente)					
Siuntėjas prašo jūsų patvirtinti / pateikti asmeninę / konfidencialią informaciją (prisijungimo duomenis, banko duomenis) el. paštu ar telefonu					
Siuntėjo domenas (el. paštas) neatrodo tikras (neatitinka organizacijos, jame yra paslėpta rašybos klaida, papildomi skaičiai ar raidės ir pan.)					
Nuorodos patalpintos/ pateikiamos el. laiške nesutampa su realiomis nuorodomis					
Yra akivaizdžių neatitikimų el. pašto adresuose, interneto nuorodose ir domeno varduose					
El. laiškas turi netikėtą / neįprastą priedą					
Laiške yra gramatinių ir rašybos klaidų					
Laiško rašymo stilius neatitinka to asmens ar kompanijos, iš kurios paprastai gaunate tokius laiškus, stiliaus					

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project №.: 2020-1-LT01-KA203-078070)

Nėra parašo ar kontaktinės informacijos					
Laiško turinys iššaukia neatidėliotinos reakcijos įspūdį, reikalauja skubaus veiksmo ir sukelia paniką ar stresą					
Laiško turinys sukelia smalsumą, poreikį sužinoti daugiau					
Tai, kas parašyta laiške, atrodo per gerai, kad būtų tiesa					

20. Kiek svarbūs yra šie kriterijai, atpažįstant įtartiną tekstinę žinutę ar telefono skambutį?

	Nesvarbūs	Šiek tiek svarbūs	Vidutiniškai svarbūs	Svarbūs	Labai svarbūs
Neįprastai ilgas numeris					
Numeris su kitos šalies kodu					
Siuntėjas / skambintojas prašo patvirtinti duomenis, pateikti asmeninę informaciją arba pervesti pinigus					
Skambintojas tinkamai neprisistato (vardas, pareigos, kompanija)					
Skambintojas nesikreipia į Jus vardu, pavarde					
Tekstinėje žinutėje yra interneto nuoroda					
Jūs nesate siuntėjo / skambintojo (kompanijos) klientas					
Jūs neturite jokių ryšių ar verslo santykių su siuntėju / skambintoju					
Žinutėje yra kitas telefono numeris perskambinimui					
Gramatinės ir rašybos klaidos					
Žinutėje yra perspėjimas (pvz., apie besibaigiantį sąskaitos galiojimą) ir reikalaujama priimti skubų sprendimą					

Kita: ……..……

21. Kiek svarbūs yra šie kriterijai, atpažįstant įtartiną žinutę socialinių tinklų kanaluose?

	Nesvarbūs	Šiek tiek svarbūs	Vidutiniškai svarbūs	Svarbūs	Labai svarbūs
Žinutėje Jūsų prašoma patvirtinti duomenis arba pateikti konfidencialią informaciją					
Žinutėje prašoma pervesti pinigų					

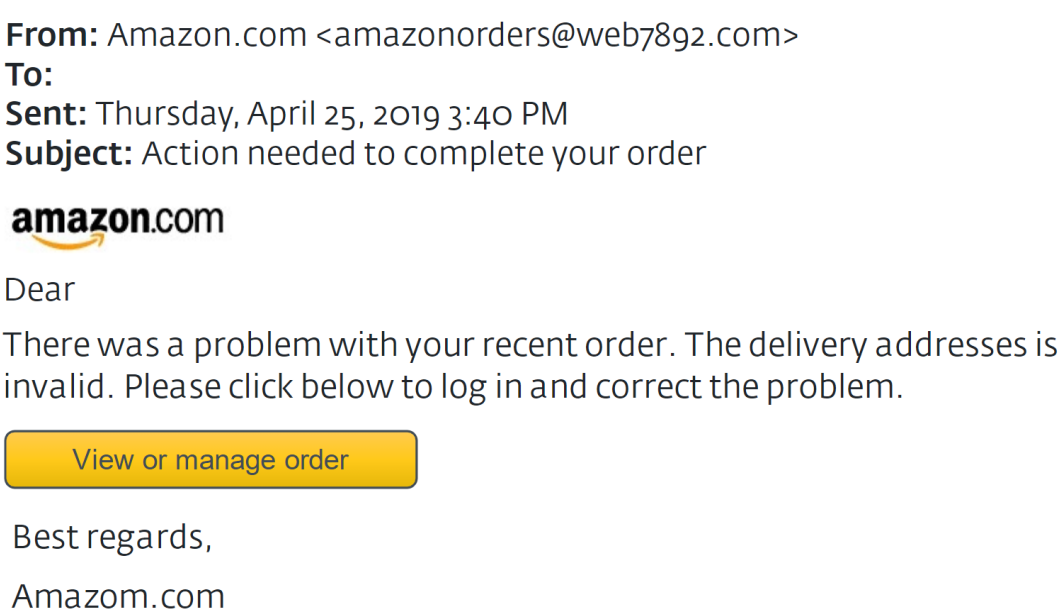
Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Žinutėje prašoma įdiegti kokią nors programą					
Žinutėje yra abejotina interneto nuoroda					
Jūs nepažįstate siuntėjo					
Jūs neturite jokių verslo santykių su siuntėju					
Siuntėjo socialinio tinklo profilis atrodo įtartinas (pvz., nauja paskyra, neturi draugų ir pan.)					
Žinutė turi dėmesį patraukiančią antraštę (pvz., Jūs nepatikėsite šiuo video!)					
Žinutės stilius neatitinka siuntėjo (per daug formalus / neformalus ir pan.)					
Gramatinės ir rašybos klaidos					

Kita: ……..……

SEKCIJA 6

Sukčiavimo (angl. phishing) pavyzdys 1



Paveikslėlis

22. Ar aukščiau pateiktas el. laiško pavyzdys yra:

- Tikras el. laiškas
- Sukčiavimo (angl. phishing)laiškas

Sekcija7

Pavyzdys 1 (tik jei į ankstesnį klausimą atsakyta „sukčiavimo (angl. phishing) laiškas“)

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project №.: 2020-1-LT01-KA203-078070)

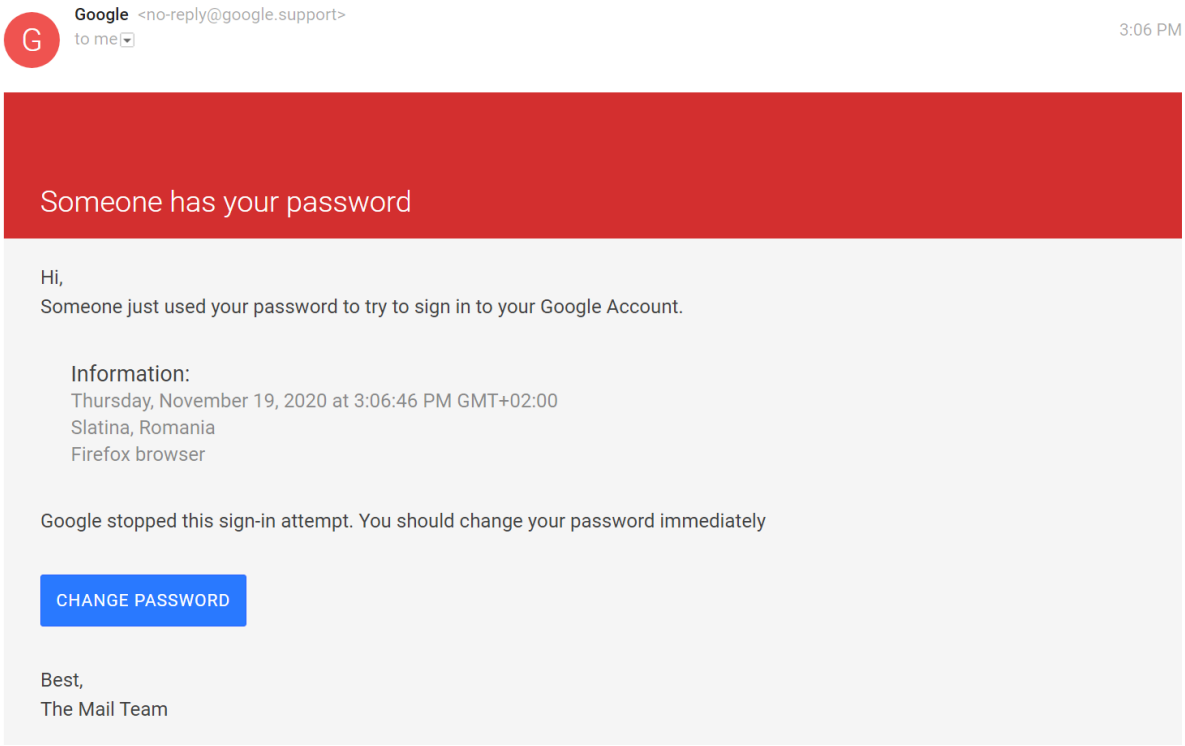
23. Kodėl nusprendėte, kad tai yra sukčiavimo (angl. phishing) laiškas? Pažymėkite atpažinimo požymius.

- Nuasmenintas pasisveikinimas
- Prašymas pateikti konfidencialią / patvirtinimo / asmeninę informaciją
- Siuntėjo domeno / el. pašto adresas
- Įtartinos nuorodos
- Neatitikimai el. pašto adresuose, nuorodose ir domenų pavadinimuose
- Rašybos ir gramatinės klaidos
- Įtartinas rašymo stilius
- Raginimas skubėti / imtis veiksmų nedelsiant
- Per gerai, kad būtų tiesa

Kita……

8 sekcija

Sukčiavimo (angl. phishing) pavyzdys 2
Paveikslėlis



24. Ar aukščiau pateiktas el. laiško pavyzdys yra:

- Tikras el. laiškas
- sukčiavimo (angl. phishing) laiškas

9 sekcija

Pavyzdys 2 (tik jei į ankstesnį klausimą atsakyta „sukčiavimo (angl. phishing) laiškas“)

25. Kodėl nusprendėte, kad tai yra sukčiavimo (angl. phishing) laiškas? Pažymėkite atpažinimo požymius.

- Nuasmenintas pasisveikinimas
- Prašymas pateikti konfidencialią / patvirtinimo / asmeninę informaciją
- Siuntėjo domeno / el. pašto adresas

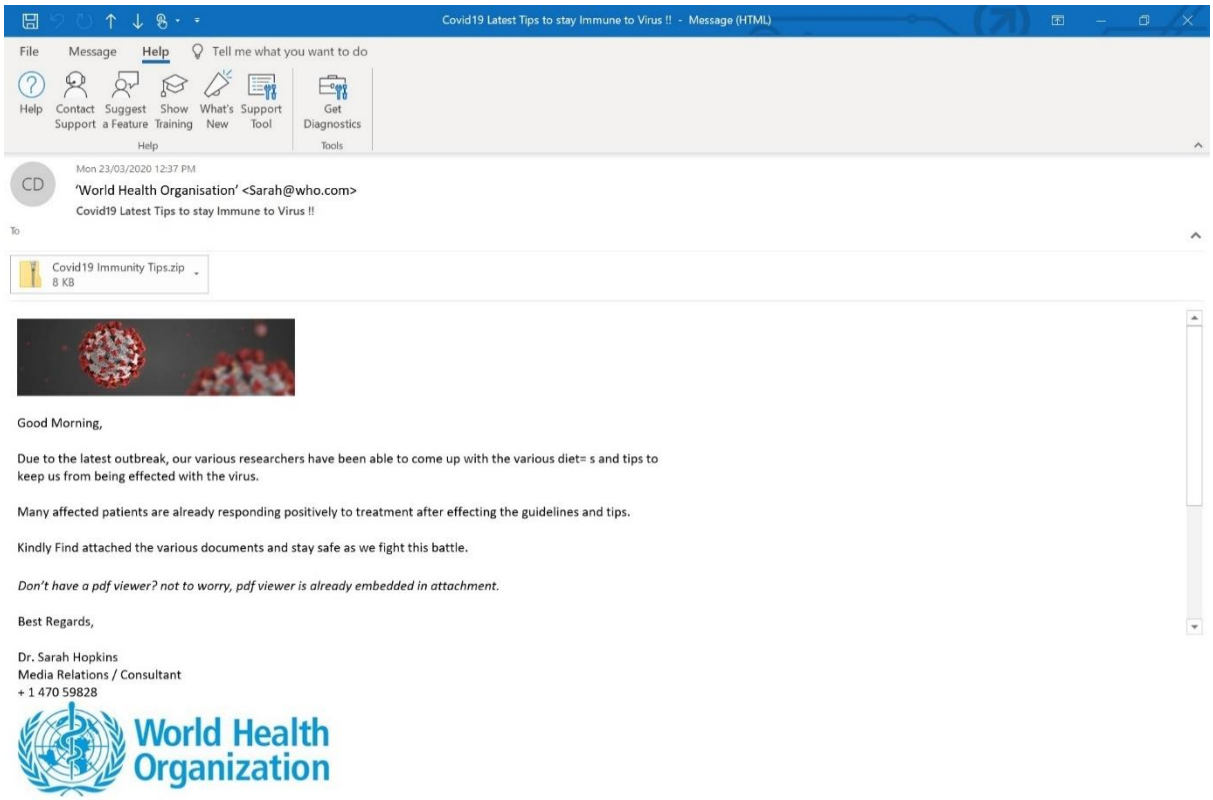
Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

- Įtartinos nuorodos
- Neatitikimai el. pašto adresuose, nuorodose ir domenų pavadinimuose
- Rašybos ir gramatinės klaidos
- Įtartinas rašymo stilius
- Raginimas skubėti/ imtis veiksmų nedelsiant
- Per gerai, kad būtų tiesa

Kita……

10 sekcija

Sukčiavimo (angl. phishing) pavyzdys 3
Paveikslėlis



26. Ar aukščiau pateiktas el. laiško pavyzdys yra:
- Tikras el. laiškas
- Sukčiavimo (angl. phishing)laiškas

11sekcija

Pavyzdys 3 (tik jei į ankstesnį klausimą atsakyta „sukčiavimo (angl. phishing) laiškas“)

27. Kodėl nusprendėte, kad tai yra sukčiavimo (angl. phishing) laiškas? Pažymėkite atpažinimo požymius.
- Nuasmenintas pasisveikinimas
- Prašymas pateikti konfidencialią / patvirtinimo / asmeninę informaciją
- Siuntėjo domeno / el. pašto adresas
- Įtartinos nuorodos

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

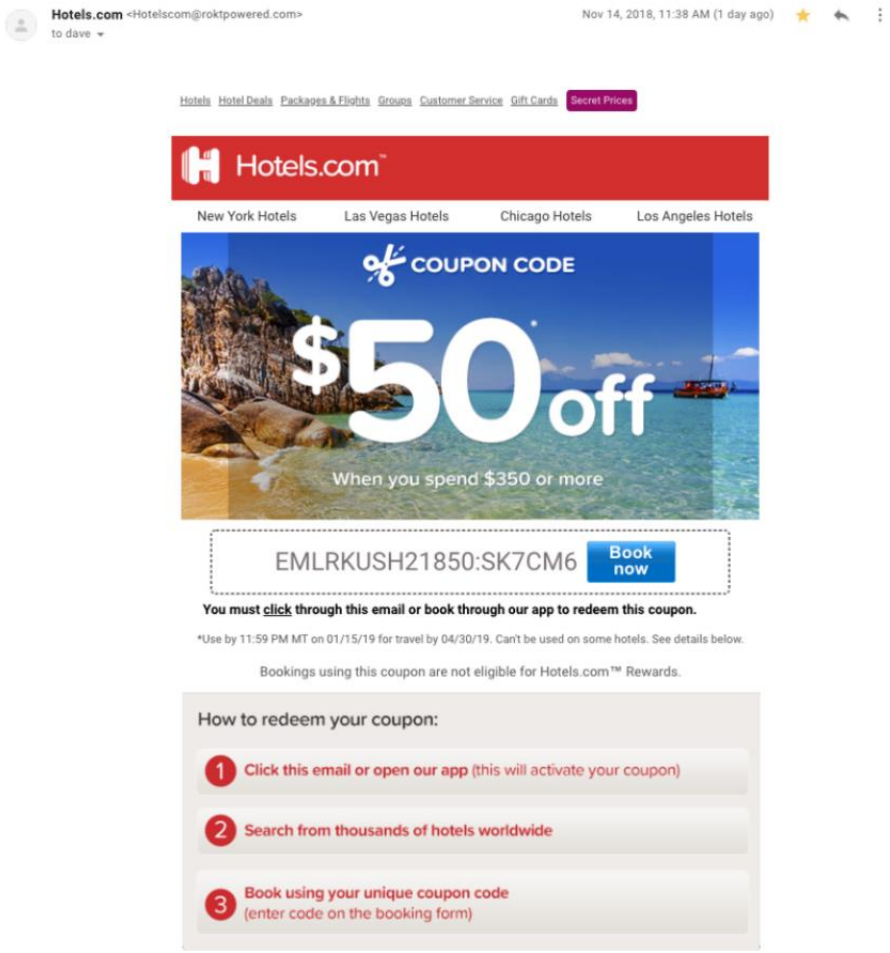
- Neatitikimai el. pašto adresuose, nuorodose ir domenų pavadinimuose
- Rašybos ir gramatinės klaidos
- Įtartinas rašymo stilius
- Raginimas skubėti/ imtis veiksmų nedelsiant
- Per gerai, kad būtų tiesa

Kita……

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

12 sekcija

Sukčiavimo (angl. phishing) pavyzdys 4
Paveikslėlis



28. Ar aukščiau pateiktas el. laiško pavyzdys yra:

- Tikras el. laiškas
- Sukčiavimo (angl. phishing)laiškas

13 sekcija

Pavyzdys 4 (tik jei į ankstesnį klausimą atsakyta „sukčiavimo (angl. phishing)laiškas“)

29. Kodėl nusprendėte, kad tai yra sukčiavimo (angl. phishing) laiškas? Pažymėkite atpažinimo požymius.

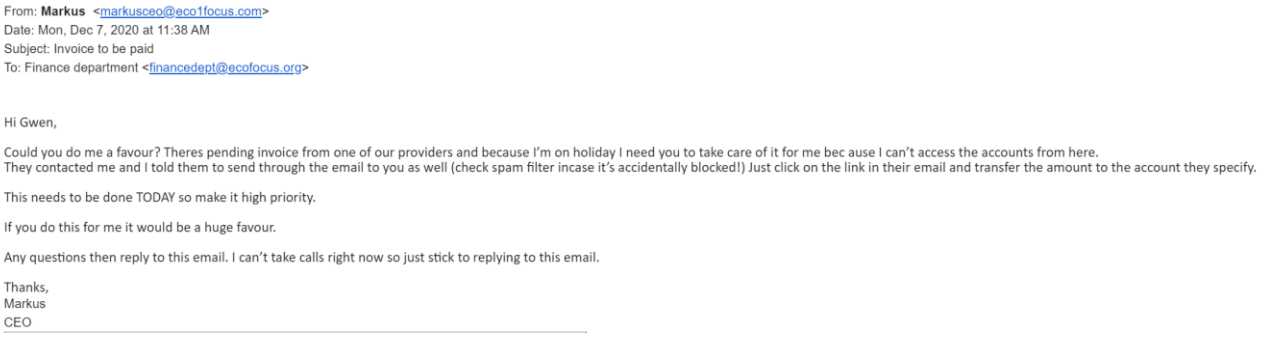
- Nuasmenintas pasisveikinimas
- Prašymas pateikti konfidencialią / patvirtinimo / asmeninę informaciją
- Siuntėjo domeno / el. pašto adresas
- Įtartinos nuorodos
- Neatitikimai el. pašto adresuose, nuorodose ir domenų pavadinimuose
- Rašybos ir gramatinės klaidos
- Įtartinas rašymo stilius
- Raginimas skubėti/ imtis veiksmų nedelsiant
- Per gerai, kad būtų tiesa

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Kita……

14 sekcija

Sukčiavimo (angl. phishing) pavyzdys 5
Paveikslėlis



From: **Markus** <markusceo@eco1focus.com>
Date: Mon, Dec 7, 2020 at 11:38 AM
Subject: Invoice to be paid
To: Finance department <financedept@ecofocus.org>

Hi Gwen,

Could you do me a favour? Theres pending invoice from one of our providers and because I'm on holiday I need you to take care of it for me bec ause I can't access the accounts from here.
They contacted me and I told them to send through the email to you as well (check spam filter incase it's accidentally blocked!) Just click on the link in their email and transfer the amount to the account they specify.

This needs to be done TODAY so make it high priority.

If you do this for me it would be a huge favour.

Any questions then reply to this email. I can't take calls right now so just stick to replying to this email.

Thanks,
Markus
CEO

30. Ar aukščiau pateiktas el. laiško pavyzdys yra:

- Tikras el. laiškas
- Sukčiavimo (angl. phishing) el. laiškas

15 sekcija

Pavyzdys 5 (tik jei į ankstesnį klausimą atsakyta „sukčiavimo (angl. phishing) laiškas“)

31. Kodėl nusprendėte, kad tai yra sukčiavimo (angl. phishing) laiškas? Pažymėkite atpažinimo požymius.

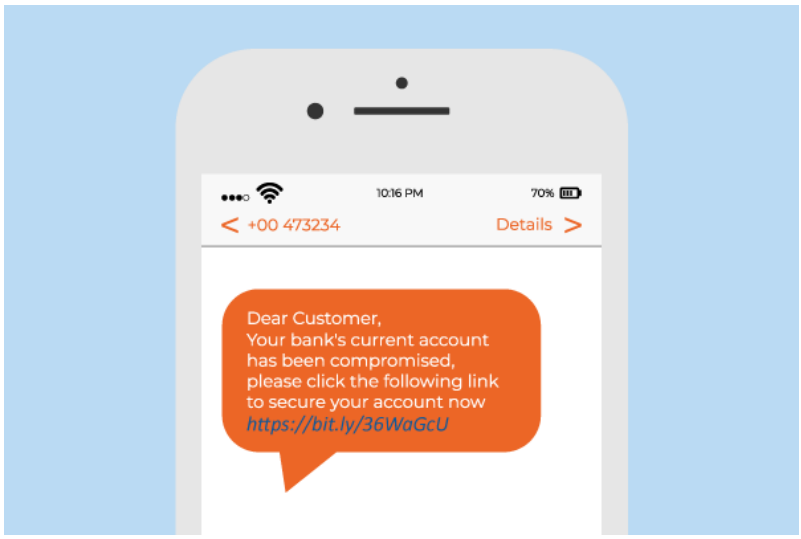
- Nuasmenintas pasisveikinimas
- Prašymas pateikti konfidencialią / patvirtinimo / asmeninę informaciją
- Siuntėjo domeno / el. pašto adresas
- Įtartinos nuorodos
- Neatitikimai el. pašto adresuose, nuorodose ir domenų pavadinimuose
- Rašybos ir gramatinės klaidos
- Įtartinas rašymo stilius
- Raginimas skubėti/ imtis veiksmų nedelsiant
- Per gerai, kad būtų tiesa

Kita……

16 sekcija

Sukčiavimo (angl. phishing) pavyzdys 6
Paveikslėlis

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)



32. Ar aukščiau pateiktas SMS žinutės pavyzdys yra:

- Reali SMS žinutė
- Sukčiavimo (angl. phishing) SMS žinutė

17 sekcija

Pavyzdys 6 (tik jei į ankstesnį klausimą atsakyta „sukčiavimo (angl. phishing) žinutė“)

33. Kodėl nusprendėte, kad tai yra sukčiavimo (angl. phishing) SMS žinutė? Pažymėkite atpažinimo požymius.

- Nuasmenintas pasisveikinimas
- Prašymas pateikti konfidencialią / patvirtinimo / asmeninę informaciją
- Siuntėjo domeno/ el. pašto adresas
- Įtartinos nuorodos
- Neatitikimai nuorodose ir domenų pavadinimuose
- Rašybos ir gramatinės klaidos
- Įtartinas rašymo stilius
- Raginimas skubėti / imtis veiksmų nedelsiant
- Per gerai, kad būtų tiesa

Kita……

18 Sekcija

Savęs vertinimas įsivertinimas. Kritinis mąstymas

34. Skalėje nuo 1 iki 5 įvertinkite:

1) Niekada
2) Retai
3) Kartais
4) Labai dažnai
5) Visada

	Niekada	Retai	Kartais	Labai dažnai	Visada
Ar jūs paprastai pasitikite pranešimais, kurie atrodo pasiekę Jūs iš svarbių ar					

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

atrodančių svarbiomis organizacijų / institucijų?					
Kuomet atidarote el. laišką / žinutę ar jūs sutelkiate reikiamą dėmesį į detales?					
Ar jūs atkreipiate dėmesį, ką spaudžiate, kuomet gaunate laišką su laiško priedu (angl. attachment)?					

35. Kuomet gaunate įtartinai atrodantį laišką / pranešimą, ar jūs įvertinate:

	Niekada	Retai	Kartais	Labai dažnai	Visada
Kas yra siuntėjas					
Siuntėjo el. paštą					
Laiško temą					
Laiško teksto stilių (formalus, neformalus žodžių naudojimas)					
Paveikslėlius					
Gramatiką ir rašybos klaidas					
Nuorodas / laiško priedus (angl. attachment)					
Kas laiško pabaigoje pasirašo ir ar pateikiami rekvizitai					

36. Kuomet gaunate įtartinai atrodantį laišką / pranešimą, ar galite įvertinti galimus savo sprendimo rezultatus / pasekmes pagal laiško parametrus / duomenis?

- Niekada
- Retai
- Kartais
- Labai dažnai
- Visada

37. Kuomet gaunate įtartinai atrodantį laišką / pranešimą, ar galite padaryti tinkamas išvadas pagal laiško parametrus / duomenis?

- Niekada
- Retai
- Kartais
- Labai dažnai
- Visada

SEKCIJA 19

Sukčiavimo (angl. phishing) atakų išvengimas

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

38. Kodėl sukčiavimo (angl. phishing) atakos būna sėkmingos? (Pasirinkite 5 svarbiausias priežastis)

- Atakų organizatoriai labai gerai imituoja realių kompanijų pranešimus ir el. laiškus, sukuria juos labai tikroviškai ir įtikinamai
- Atakų organizatoriai išnaudoja žmogišką prigimtį, žmogiškas emocijas ir poreikius
- Atakų organizatoriai gali lengvai gauti asmeninius duomenis ir informaciją apie asmenį ar įmonę socialiniuose tinkluose / kompanijos puslapiuose, spaudoje, ir t. t.
- Atakų organizatoriai tampa labiau pažengę, atakuoja atskirus asmenis laiškais su personalizuota ir specifine informacija
- Vartotojai neskiria tam pakankamo dėmesio
- Vartotojai neturi žinių apie tokias atakas ir kaip jų išvengti
- Žmonės naudoja pasenusias programines priemones
- Organizacijos ir įmonės nesiima pakankamų priemonių išvengti šių atakų
- Trūksta mokymų kibernetinio saugumo ir sukčiavimo (angl. phishing) srityje
- sukčiavimo (angl. phishing) priemonės yra pigios ir plačiai paplitusios
- Kenkėjiškos programos tampa sudėtingesnėmis
- Kita……

39. Kokias emocijas / poreikius ir potraukius paprastai išnaudoja atakų organizatoriai?

- Baimę
- Nerimą / jaudulį
- Paniką
- Smalsumą
- Godumą
- Motyvavimą (Dovanos / Laimėjimai)
- Emocinio pasitenkinimo poreikį
- Patiklumą
- Paslaugumą
- Kita……

40. Kokių veiksmų reikia imtis, kad būtų išvengta sukčiavimo (angl. phishing) atakų?

	Nesvarbu	Šiek tiek svarbu	Vidutiniškai svarbu	Svarbu	Labai svarbu
Naudoti naujausią naršyklės versiją					
Naudoti atnaujintą operacinę sistemą					
Naudoti naujausias programas ir priemones					
Naudoti apsaugos programas					
Neskelbti konfidencialios asmeninės informacijos soc. tinkluose					
Naudoti daugiapakopį autentifikavimą / dažnai keisti slaptažodžius					

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Kenkėjiškų svetainių blokavimui naudoti žiniatinklio filtrą					
Reguliariai dalyvauti kibernetinio saugumo mokymuose / seminaruose					
Turėti patvirtintą saugumo politiką ir ja vadovautis					
Šifruoti visą konfidencialią įmonės informaciją					
Elgtis atidžiai atidarant el. laiškus / pranešimus / atsakant telefonu					
Patikrinti visą svarbią informaciją (siuntėjo pašto adresą, nuorodas, priedus ir t. t.)					
Pasikliauti savo instinktais ir nuojauta					
Nuolat tobulintis šioje srityje					

41. Kiek sutinkate su sekančiais teiginiais. Jaučiuosi įsitikinęs, kad:

	Visai neįsitikinęs	Šiek tiek įsitikinęs	Kažkiek įsitikinęs	Gana įsitikinęs	Visiškai
Žinau kibernetinio saugumo / sukčiavimo (angl. phishing) terminiją ir naudoju ją					
Randu tinkamą ir patikimą informaciją internete					
Imuosi tinkamų veiksmų / priemonių apsisaugoti nuo sukčiavimo (angl. phishing) atakų					
Atpažįstu sukčiavimo (angl. phishing) atakas					
Laiku atnaujinu savo programinę įrangą					
Naudoju daugiapakopį autentifikavimą					
Naudoju apsaugos programas					
Kenkėjiškų svetainių blokavimui naudoju žiniatinklio filtrą					

Co-funded by the Erasmus+ Programme of the European Union
The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Šifruoju visą konfidencialią kompanijos / asmeninę informaciją					

42. **Kiti komentarai / pasiūlymai**

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)