Projekta Nr.: 2020-1-LT01-KA203-078070

O1-A2: Rezultāti "PIKŠĶERĒŠANAS UN PRASMJU TRŪKUMA ATPAZĪŠANA"

ZIŅOJUMS

2021

Partnerība

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/

Funded by the Erasmus+ Programme of the European Union

Saturs

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)

Tabulu rādītājs

Attēlu rādītājs

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)

Saīsinājumu saraksts

BEC	Biznesa e-pasta kompromitējums
Izpilddirektors	Galvenais izpilddirektors
ENISA	Eiropas Savienības Kiberdrošības aģentūra
ES	Eiropas Savienība
EUROPOL	Eiropas Savienības Aģentūra tiesībaizsardzības sadarbībai

Funded by the Erasmus+ Programme of the European Union

1. IEVADS

1.1. Kiberdrošība ES: realitāte un vajadzības

Eiropas Komisija ir sagatavojusi un veikusi īpašu Eirobarometra pētījumu[1] 2019. gadā ar mērķi izprast ES pilsoņu zināšanas, pieredzi un priekšstatus par kiberdrošību.
Nav pārsteigums, ka rezultāti liecina, ka interneta izmantošana Eiropā turpina pieaugt, īpaši izmantojot viedtālruņus. Rezultāti[2] arī parādīja, ka ES pilsoņi ir vairāk informēti par iespējamām briesmām, kas rodas, izmantojot internetu, un 52% respondentu norādīja, ka ir diezgan labi vai ļoti labi informēti par kibernoziegumiem, salīdzinot ar 46% 2017. gadā. Saskaņā ar aptaujas rezultātiem bažas par tiešsaistes privātumu un drošību ir pamudinājušas jau vairāk nekā 9 no 10 interneta lietotājus mainīt savu uzvedību tiešsaistē - visbiežāk neatverot nezināmu cilvēku e-pastus, instalējot pretvīrusu programmatūru, apmeklējot tikai zināmas un uzticamas vietnes un piesakoties sistēmā tikai savos datoros.

Lai gan šie rezultāti ir diezgan iepriecinoši, daudzi interneta lietotāji joprojām cieš no krāpšanās tiešsaistē un uzķeras uz e-pasta pikšķerēšanas ēsmas. Saskaņā ar Eurostat datiem 2019. gadā aptuveni katrs trešais ES pilsonis vecumā no 16 līdz 74 gadiem ziņoja par ar drošību saistītiem negadījumiem, izmantojot internetu privātām vajadzībām 2019. gadā pēdējo 12 mēnešu laikā.

Šajā periodā pikšķerēšana bija biežākais drošības incidents, par kuru ziņots 2019. gadā[3] . 25% respondentu ziņoja, ka ir saņēmuši krāpnieciskus ziņojumus, kurus dēvē par pikšķerēšanu, savukārt 12% respondentu ziņoja, ka ir novirzīti uz viltotām vietnēm, pieprasot personas informāciju (domēnsagroze). To cilvēku īpatsvars, kuriem bija problēmas ar drošību, lietojot internetu privātām vajadzībām, dažādās ES dalībvalstīs bija atšķirīgs. Visaugstākais rādītājs novērots Dānijā (50%), kam seko Francija (46%), Zviedrija (45%), Malta un Nīderlande (abas 42%), Somija (41%) un Vācija (40%). Turpretī viszemākais īpatsvars reģistrēts Lietuvā (7%), Polijā (9%), Latvijā (10%), Bulgārijā (13%) un Grieķijā (13%). To cilvēku īpatsvars, kuri piedzīvoja ar drošību saistītas problēmas Igaunijā un Kiprā, bija attiecīgi 32% un 21%.

To var izskaidrot ar atšķirībām starp kibernoziegumu apzināšanās līmeni ES valstīs, vispārējo ES pilsoņu pārliecības samazināšanos par spēju pasargāt sevi no kiberuzbrukumiem, kā arī ar sarežģītākiem kiberuzbrukumiem, kurus ir grūtāk atklāt un no kuriem ir grūtāk izvairīties, jauniem paņēmieniem un pieejamām jaunām platformām šādu uzbrukumu veikšanai.

Runājot par uzņēmējdarbības nozari Eiropā, arī to ietekmē kiberdrošības jautājumi. Eiropas valstis un uzņēmumi arvien biežāk kļūst par mērķiem. Saskaņā ar 2017. gada globālo informācijas drošības apsekojumu aptuveni 80% uzņēmumu Eiropā attiecīgajā gadā ir piedzīvojuši vismaz vienu kiberdrošības incidentu, un darbinieki ir atbildīgi par 27% no visiem kiberdrošības incidentiem.

Visā pasaulē, pamatojoties uz jaunākajiem datiem, 2019. gada pirmajā ceturksnī uzņēmumi kļuva par mērķiem par 120% biežāk nekā gadu iepriekš, kā rezultātā zaudējumi sasniedza pat 22,2 miljardus eiro.

Vairāk nekā 99% e-pastu, kas izplata ļaunprātīgu programmatūru, lai efektīvi darbotos, nepieciešama cilvēka iejaukšanās - sekošana saitēm, dokumentu atvēršana, drošības brīdinājumu pieņemšana un cita rīcība.[4]

---

[1] ES Komisija (2020): Īpašais Eirobarometrs 499: Eiropiešu attieksme pret kiberdrošību, URL https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG (skatīts 11.02.2021.)
[2] Eiropas Savienības Kiberdrošības aģentūra (2020): ENISA drošības apdraudējumu aina 2019. – 2020.
[3] EUROSTAT (2020): Vai interneta lietošana šodien ir drošāka ?, URL https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb/default/table?lang=en (skatīts 11.02.2021.)
[4] Proofpoint (2019): Cilvēka faktora ziņojums 2019, URL https://www.proofpoint.com/us/resources/threat-reports/human-factor (skatīts 12.02.2021.)

Funded by the Erasmus+ Programme of the European Union

Tādējādi, neatkarīgi no tā, vai tas notiek darbā vai mājās, cilvēki, kuri spēj atpazīt brīdinājuma zīmes un pārzina pareizās tehnikas, ir galvenie elementi, kas spēj palēnināt vai novērst kiberuzbrukumus. Tāpēc ir jāatjaunina esošās kiberdrošības programmas vai jāizveido jaunas, lai stiprinātu ES pilsoņu prasmes, izglītību un informētību par jaunākajiem jaunajiem kiberdrošības jautājumiem un draudiem.

Šādas programmas ir jāpiedāvā visiem studentiem, ņemot vērā, ka saskaņā ar ENISA datiem universitātēs ar kiberpasauli saistītie priekšmeti ir nepietiekami pārstāvēti netehniskajās programmās.

1.2. Projekts "Aizsardzība pret pikšķerēšanu 4. industriālās revolūcijas laikmetā"

Kiberdrošība kļūst par vienu no lielākajiem izaicinājumiem digitālajā laikmetā, jo informācija kļūst par dārgu aktīvu, kas saistīts ar milzīgiem datu apjomiem, uzlabojot saziņu ar digitālo vidi. Digitālās ierīces un informācijas sistēmas kļūst arvien pievilcīgāki mērķi kiberuzbrukumiem.

Pikšķerēšana ir viena no lielākajām problēmām, jo kibernoziedznieki pikšķerēšanas kampaņu veikšanai izmanto arvien ātrākus un novatoriskākus tehnoloģiskos rīkus. Tāpēc nepieciešams izstrādāt un padarīt plaši pieejamu cilvēka vadītu pikšķerēšanas aizsardzības sistēmu, kas izmanto cilvēka dabisko instinktu atklāt lietas un tehnoloģijas, lai mērogotu atbildes reakciju. Lai radītu cilvēku vadītu pikšķerēšanas aizsardzību, lietotājam ir nepieciešama izglītība, lai pareizi identificētu pikšķerēšanas uzbrukumus un reaģētu uz tiem.

Viļņas Universitātes Kauņas fakultātes un partneru aizsāktais starptautiskais projekts "Aizsardzība pret pikšķerēšanu 4. industriālās revolūcijas laikmetā" ("CyberPhish") sākās 2020. gada novembra sākumā un ilgs divus gadus.

Projekta mērķis ir izglītot augstskolu studentus, pedagogus, universitāšu darbiniekus (kopienas locekļus), izglītības centrus, uzņēmējdarbības nozari (darba devējus un darbiniekus), kā arī veicināt mērķa grupas kritisko domāšanu kiberdrošības jomā .

Projekta partneri izstrādās mācību programmu, e-mācību materiālus, jaukta tipa mācību vidi, zināšanu un prasmju pašnovērtēšanas un zināšanu novērtēšanas sistēmas simulācijas studentiem un citiem lietotājiem, lai novērstu pikšķerēšanas uzbrukumus, paaugstinātu kompetences, kas palīdzēs vērst uzmanību uz draudiem un veikt atbilstošus profilakses pasākumus.

Projekta partnerību veido sešas organizācijas no piecām Eiropas valstīm:

1. Viļņas universitāte, Lietuva (koordinators)
2. Informācijas tehnoloģiju institūts, Lietuva
3. DOREA izglītības institūts, Kipra
4. Tartu universitāte, Igaunija
5. Altacom SIA, Latvija
6. Macdac Engineering Consultancy Bureau Ltd (MECB), Malta

Lai iegūtu papildinformāciju par projektu un projekta aktivitātēm, lūdzu, apmeklējiet projekta vietni: https://cyberphish.eu/

Funded by the Erasmus+ Programme of the European Union

2. PIKŠĶERĒŠANA

2.1. Kas ir pikšķerēšana?

Pikšķerēšana ir krāpniecisks mēģinājums nozagt lietotāju datus, piemēram, pieteikšanās akreditācijas datus, kredītkaršu informāciju vai pat naudu, izmantojot sociālās inženierijas paņēmienus. Šāda veida uzbrukumi parasti tiek veikti, izmantojot e-pasta ziņojumus, šķiet, ka tie tiek sūtīti no cienījama avota, ar nolūku pārliecināt lietotāju atvērt ļaunprātīgu pielikumu vai sekot krāpnieciskam URL.[5]
Pikšķerēšana ir arī viens no vecākajiem kiberuzbrukumu veidiem, kas datēts ar pagājušā gadsimta 90. gadiem. Neskatoties uz tā gadu desmitiem ilgo pastāvēšanu, tas joprojām ir viens no izplatītākajiem un kaitīgākajiem kiberuzbrukumu veidiem.[6]

Ir daudz dažādu pikšķerēšanas veidu, taču visbiežāk sastopamie ir:

1) *Spray and pray* – ļaunprātīgi e-pasti tiek nosūtīti uz jebkuru e-pasta adresi, mēģinot nozagt sensitīvu informāciju;
2) Viltus personība *(Cat phishing)* - kāda cilvēka ievilināšana attiecībās, uzdodoties par iedomātu tiešsaistes personu;
3) Avansa maksājums *(Advanced fee scam)* - izplatīta krāpšana, kas saistīta ar Nigērijas valstspiederīgajiem, piemēram, palīdzības pieprasīšana lielas naudas summas pārskaitīšanā;
4) Harpunēšana *(Spear fishing)* - ļaunprātīgi e-pasti, kas ir īpaši izstrādāti un nosūtīti konkrētai personai vai organizācijai, mēģinot nozagt sensitīvu informāciju;
5) Vaļu medības *(Whaling)* - mēģinājums nozagt sensitīvu informāciju, bieži tiek mērķēts uz augstāko vadību;
6) *Vishing* - attiecas uz pikšķerēšanu, kas notiek pa tālruni;
7) *Smishing* - attiecas uz pikšķerēšanu, izmantojot īsziņas, nevis e-pastus, lai uzrunātu personas;
8) *Angler Phishing* – salīdzinoši jauns pikšķerēšanas veids, kas attiecas uz uzbrukumiem sociālajos medijos, izmantojot viltotus URL, klonētas vietnes, ziņas un tvītus, kā arī tūlītējo ziņojumapmaiņu;
9) Klonēšanas uzbrukums *(Clone Phishing)* – pikšķerēšanas veids, kura ietvaros tiek izmantoti īsti un iepriekš nosūtīti e-pasti, lai izveidotu identisku e-pastu ar ļaunprātīgu saturu;
10) Ļaunprātīga reklāma *(Malvertising)* - šis pikšķerēšanas veids izmanto tiešsaistes reklāmas vai uznirstošos logus, lai piespiestu cilvēkus noklikšķināt uz saites, kas izskatās īsta, bet vēlāk instalē datorā ļaunprogrammatūru.

Pēdējo pāris gadu laikā novērota aizvien pieaugoša pikšķerēšanas izsmalcinātība, un pikšķerēšanu kļūst arvien grūtāk noteikt, jo daudzi pikšķerēšanas e-pasta ziņojumi un vietnes ir gandrīz identiski patiesajiem. Tajā pašā laikā pikšķerēšanas kampaņas ir kļuvušas ātrākas un automatizētākas, liekot rīkoties ātrāk nekā iepriekš, jo dažos gadījumos no akreditācijas datu noplūdes līdz uzbrukumam ir vajadzīga viena diena.

Balstoties uz Eiropola pētījumu, kibernoziedznieki izmanto holistiskāku pikšķerēšanas stratēģiju, parādot augstu kompetenci attiecībā uz viņu izmantoto rīku, sistēmu un ievainojamību izmantošanu, pieņemot nepatiesu identitāti un strādājot ciešā sadarbībā ar citiem kibernoziedzniekiem.[7]

[5]Eiropas Savienības Kiberdrošības aģentūra (2020): Pikšķerēšana - ENISA drošības apdraudējumu aina 2019. – 2020.
[6] Deloitte (2019): Izpratne par pikšķerēšanas tehniku URL
https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf (skatīts 112.02.2021)

[7] EUROPOL (2020): Organizētās noziedzības draudu novērtējums internetā 2020

Funded by the Erasmus+ Programme of the European Union

Tiek prognozēts, ka e-pasts joprojām būs pikšķerēšanas mehānisms numur viens, taču ne uz ilgu laiku. Eksperti redz, ka palielinās sociālo tīklu ziņojumapmaiņas pielietojums, tostarp WhatsApp un citur, lai veiktu šādus uzbrukumus. Saskaņā ar ENISA teikto, visbūtiskākās izmaiņas būs ziņojumu nosūtīšanas metodēs, kas kļūs sarežģītākas, izmantojot mākslīgo intelektu (AI) ziņojumu sagatavošanai un nosūtīšanai.

2.2.Sociālā inženierija un pikšķerēšana

Informācijas drošības kontekstā sociālo inženieriju definē kā psiholoģisku manipulāciju ar cilvēkiem, lai rosinātu darbību veikšanu vai konfidenciālas informācijas izpaušanu. Sociālā inženierija joprojām ir lielākais drauds cita veida kibernoziegumu atvieglošanai, jo 84% kiberuzbrukumu paļaujas uz sociālo inženieriju (ENISA). Pikšķerēšanas upuru skaits turpina pieaugt, jo tas izmanto cilvēku kā vājāko posmu.

Cilvēka vājo vietu izmantošanai ar sociālās inženierijas palīdzību ir liela ietekme uz sabiedrību, un tas dod iespēju veikt lielāko daļu kibernoziegumu, sākot no krāpšanas līdz slepenas informācijas iegūšanai un augsta līmeņa ļaunprātīgas programmatūras uzbrukumiem. Kibernoziedznieki parasti izmanto sociālo inženieriju, lai pārliecinātu lietotājus neapzināti iesaistīties krāpnieciskās shēmās, bet pikšķerēšanu, lai iegūtu akreditācijas datus un piekļūtu slepeniem kontiem / sistēmām (EUROPOL).

Kibernoziedznieki mācās un ir kļuvuši par sociālās inženierijas ekspertiem, izmantojot cilvēka dabu, lai veiktu krāpšanu. Viņu visbiežāk izmantotās manipulācijas metodes parasti balstās uz bailēm, iebiedēšanu, steidzamības izjūtu, alkatību, zinātkāri, uzticību un iejūtību. Kibernoziedznieki zina, ka rūpīgi sagatavots un personalizēts e-pasts, balss ziņojums / zvans vai īsziņa var maldināt cilvēkus, liekot sniegt sensitīvu informāciju, pārskaitīt naudu vai lejupielādēt failu, kurā ir ļaunprātīga programmatūra, uzņēmuma tīklā.

Lai labāk izprastu sociālās inženierijas jēdzienu, mēs varam apskatīt 6 pārliecināšanas principus, kurus Dr. Roberts B. Cialdīni skaidro grāmatā "Ietekme: Pārliecināšanas psiholoģija"[8]. Lai gan sākotnēji šie principi tika izmantoti mārketingā, tie tika viegli pārņemti un izmantoti arī sociālajā inženierijā un pikšķerēšanā[9] :

1) *Atbildes darbība* - "dot un ņemt". E-pasts, kas piedāvā atlaidi vai kuponu dažiem pirkumiem apmaiņā pret informācijas apmaiņu vai konta reģistrēšanu; e-pasts, kurā solīts piešķirt piekļuvi konfidenciālai informācijai, ja tiek lejupielādēts noteikts pielikums vai saite, ir klasiski piemēri.
2) *Retums* - cilvēka dabā ir vēlēties to, ko grūti iegūt. Pikšķerēšanas e-pasta ziņojumi, kuros uzsvērts, ka konkrēts ieguvums ir pieejams tikai tad, ja darbība tiek veikta īsā laikā. "Konts tiks deaktivizēts 24 stundu laikā, ja nenoklikšķināsit uz saites, lai to atrisinātu" ir šī principa piemērs.
3) *Autoritāte* - cilvēki mēdz sekot autoritātei un uzticamiem ekspertiem kopumā. Tāpēc daudzos pikšķerēšanas e-pasta ziņojumos mēģināts atdarināt vietējos līderus, izpilddirektorus, vecākos darbiniekus, cilvēkresursu vadītājus utt. It kā izpilddirektora nosūtīts e-pasts, kurā finanšu departamentam tiek lūgts nekavējoties pārskaitīt daļu naudas uz departamentam nezināmu kontu, ir viens no piemēriem, kas ir noticis daudzkārt.
4) *Konsekvence* - cilvēki dažādā ziņā ir ieraduma radījumi. Pikšķerēšanas e-pastos, kas izskatās kā oficiāli paziņojumi, tiek izmantots šis fakts, cerot, ka saņēmējs neievēros neparasto pieprasījumu, kas ir iekļauts šādā e-pastā. E-pasts ar Amazon logotipu, kurā teikts, ka sūtījums tiek aizturēts un lūdz saņēmēju apstiprināt viņu mājas adresi, var neradīt aizdomas, pat ja pašlaik netiek gaidīts sūtījums - tas ir plaši atzīta zīmola spēks.

[8] Dr Roberts B. Cialdini ir psiholoģijas un mārketinga profesors Arizonas štata universitātē ASV

[9] NCC grupa (2020): Pikšķerēšanas psiholoģija: Septiņu ietekmes principu izmantošana, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433 (skatīts 20.02.2021.)

Funded by the Erasmus+ Programme of the European Union

5) *Vienprātība* - cilvēki mēdz sekot citiem cilvēkiem, it īpaši, ja viņi par kaut ko nav pārliecināti. Pikšķerēšanas e-pastā, kurā minēts kaut kas līdzīgs "544 no 800 darbiniekiem ir atjauninājuši programmatūru, noklikšķiniet uz šīs saites, lai lejupielādētu", tiek izmantota šī tendence.
6) *Patika* - tas ir diezgan vienkāršs princips - ja cilvēkiem Jūs patīkat vai viņi vēlas iepatikties Jums, viņi, visticamāk, saka "jā". Viens no piemēriem ir e-pasts no IT nodaļas (it kā), kurā jaunajam darbiniekam tiek lūgti personas dati / paroles, lai atjauninātu drošības sistēmu.
7) *Vienotība* - šis princips tika pievienots vēlāk. Tā pamatā ir ideja, ka, jo vairāk mēs identificējamies ar citiem, jo vairāk viņi mūs ietekmē. Pikšķerēšanas e-pastas, kuru, domājams, nosūtījis kāds, kuram ir tādas pašas intereses kā saņēmējam - un šo informāciju ir viegli iegūt ar sociālo mediju starpniecību - ir lielas izredzes gūt panākumus. Piemēram, ja kādam patīk suņi, tad e-pasts no it kā cita suņu mīļotāja, kam šķietami pievienoti jauki suņu attēli, visticamāk tiks atvērts.

Šīs metodes var izraisīt veiksmīgus pikšķerēšanas uzbrukumus, uzbrukumu ietvaros izmantojot ļaunprātīgas saites vai ļaunprātīgu programmatūru. Tāpēc cilvēkiem ir svarīgi atpazīt šos principus un stratēģijas, lai sevi aizsargātu, tomēr tas ir diezgan grūti, jo to pamatā ir cilvēku būtība - veids, kā mēs domājam un uzvedamies.

2.3. Pikšķerēšana COVID-19 laikā

Krīžu un katastrofu laikā mums ir tendence paļauties uz datoriem, mobilajām ierīcēm un internetu, lai strādātu, sazinātos ar citiem cilvēkiem, atrastu, kopīgotu un saņemtu informāciju, iepirktos utt.[10]

COVID-19 pandēmija ir parādījusi mūsu neaizsargātību un parādījusi kibernoziedzības negatīvo ietekmi uz mūsu ikdienas dzīvi visā pasaulē. Tā kā fiziska noslēdze jeb lokdauns kļuva par normu un arvien vairāk cilvēku palika un strādāja mājās, kibernoziedzība kļuva plašāka nekā iepriekš.

Barracude[11] pētnieki ir novērojuši pikšķerēšanas krāpšanas mēģinājumu pieaugumu par 667% tikai viena mēneša laikā kopš pandēmijas sākuma 2020. gada sākumā.

Ir pierādījumi, ka kibernoziedznieki turpina izmantot vājās vietas sev par labu. Kibernoziedznieki ir pielāgojuši esošos kibernoziedzības veidus, lai tie atbilstu pandēmijas naratīvam, ļaunprātīgi izmantojuši situācijas nenoteiktību un sabiedrības vajadzību pēc ticamas informācijas. Noziedznieki ir izmantojuši COVID-19 krīzi, lai veiktu sociālās inženierijas uzbrukumus, proti, sūtītu pikšķerēšanas e-pastus, izmantojot surogātpasta kampaņas, un mērķtiecīgākus mēģinājumus, piemēram, biznesa e-pasta kompromitēšanu (BEC)[12] :

- Pikšķerēšanas kampaņas un ļaunprātīgas programmatūras izplatīšana šķietami oriģinālās vietnēs vai dokumentos, kas sniedz informāciju vai padomus par COVID-19, tiek izmantoti datoru inficēšanai un lietotāju akreditācijas datu iegūšanai.
- Likumpārkāpēji iegūst piekļuvi uzņēmumu vai citu organizāciju sistēmām, mērķējot uz darbiniekiem, kuri strādā attālināti.

Kā ziņo EUROPOL, kiberuzbrukumu skaits ir ievērojams un sagaidāms, ka tas turpinās pieaugt. Kibernoziedznieki turpinās ieviest jauninājumus, ieviešot dažādas ļaunprātīgas programmatūras un izspiedējvīrusu paketes, kuru tematika ir COVID-19 pandēmija un it īpaši vakcīnas.

[10] Eiropas padome (2020): Kibernoziedzība un COVID-19, URL https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (skatīts 12.02.2021.)
[11] Barracuda Networks ir pasaules līderis drošības, lietojumprogrammu piegādes un datu aizsardzības risinājumu jomā
[12] Eiropas padome (2020): [12]Kibernoziedzība un COVID-19, URL https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-12.02.2021 (skatīts 12.02.2021.)

Kibernoziedznieki, visticamāk, mēģinās izmantot arvien vairāk uzbrukuma paņēmienu, jo daudzi darba devēji pašlaik izmanto un turpinās izmantot attālinātu darbu un ļaus izveidot savienojumu ar savas organizācijas sistēmām.[13]

[13] EUROPOL (2020): Peļņas gūšana pandēmijas apstākļos - kā noziedznieki izmanto COVID-19 krīzi

Funded by the Erasmus+ Programme of the European Union

3. STUDENTU, DARBINIEKU UN IZPILDDIREKTORU APTAUJAS

3.1. Datu vākšanas metodika

Lauku darba ietvaros CyberPhish projekta konsorcija partneri[14] sagatavoja un nosūtīja aptauju, kas adresēta studentiem, biznesa pārstāvjiem un vadītājiem no Lietuvas, Latvijas, Igaunijas, Maltas un Kipras. Partneru mērķis bija iesaistīt vismaz 70 dalībniekus (tostarp 20 biznesa pārstāvjus un 10 izpilddirektorus) katrā partnervalstī.

Pamatojoties uz dokumentu pārbaudi un visu partneru atsauksmēm, tika sagatavota anketas versija angļu valodā, kas vēlāk tika lokalizēta un augšupielādēta tiešsaistē angļu, lietuviešu un latviešu valodās. Aptauja tika uzsākta 2020. gada decembra vidū un tika pabeigta 2021. gada janvāra beigās.

Aptaujas galvenie mērķi bija:

- noteikt cilvēku informētību par pikšķerēšanu un dažādiem pikšķerēšanas veidiem;
- noteikt, kā cilvēki atpazīst pikšķerēšanas uzbrukumus;
- noteikt prasmju trūkumus.

Anketā apvienoti jautājumi, kas saistīti ar psiholoģiskām un IT zināšanām, kritiskās domāšanas pieeju, kā arī sniedza pikšķerēšanas piemērus, lai respondenti varētu novērtēt savas zināšanas "praksē". Katrs pikšķerēšanas piemērs tika balstīts uz sešiem pārliecināšanas principiem, ko izstrādājis Dr. Roberts B. Cialdini. Kopumā anketa tika sadalīta vairākās daļās un tika apkopoti šādi dati:

- Personiskā informācija - tostarp dzimums, izglītības līmenis un nodarbinātības statuss;
- Vispārīgas zināšanas un uzvedība pikšķerēšanas jomā;
- Personīgā pieredze ar pikšķerēšanu;
- Pikšķerēšanas uzbrukumu atpazīšana - norādot galvenos sarkanos karogus;
- Praktiski pikšķerēšanas piemēri;
- Kritiskās domāšanas prasmju pašnovērtējums;
- Izvairīšanās no pikšķerēšanas uzbrukumiem - kāpēc pikšķerēšanas uzbrukumi ir veiksmīgi, sociālā inženierija (uzbrucēji izmanto cilvēku emocijas), veicamās darbības;
- Pašnovērtējums par pārliecību par prasmju izmantošanu, kas vajadzīgas pikšķerēšanas uzbrukumu novēršanai.

Apkopotie dati tiks izmantoti, lai identificētu prasmju trūkumus un sagatavotu ieteikumus jaunai mācību programmai, lai stiprinātu interneta lietotāju prasmes, izglītību un informētību par jaunākajiem jaunajiem kiberdrošības jautājumiem un draudiem, jo īpaši - pikšķerēšanu.

Kopumā, pamatojoties uz šīs aptaujas rezultātiem un datorizētu pētījumu par esošo kiberdrošības studiju programmu, partneru konsorcijs izstrādās mācību materiālu, zināšanu pašnovērtēšanas un zināšanu novērtēšanas testus un simulācijas scenārijus apmācībai.

3.2. Rezultātu apkopošana

Anketas rezultāti tika izmantoti, lai izveidotu Nacionālo rezultātu tabulu (strukturēti pa valstīm - Lietuva, Latvija, Igaunija, Malta un Kipra). Šajā tabulā partneri iekļāva visatbilstošākos apkopotos rezultātus, sniedzot informāciju par:

- lauka darbā iesaistīto mērķa grupu raksturojumu;
- aptauju rezultātu analīzi, izmantojot grafikus un tekstu;
- respondentu galvenajiem secinājumiem un ierosinājumiem;

[14] CyberPhish projekta vietne: https://cyberphish.eu/

Funded by the Erasmus+ Programme of the European Union

- Partneru secinājumiem un ieteikumiem, lai atbalstītu partnerus citu rezultātu definēšanā un izstrādē.
- Tabulās tika sniegts pārskats par respondentu zināšanām un rīcību attiecībā uz kiberdrošības, īpaši pikšķerēšanas, tēmu. Šīs tabulas rezultāti ļāva konsorcijam salīdzināt valstis, nosakot prasmju trūkumus un vajadzības.

3.3.Aptauju rezultāti un analīze

3.3.1. Respondentu pārskats

Neskatoties uz īso anketas izplatīšanas periodu, visas valstis ir sasniegušas minimālo 70 respondentu skaitu. Kopumā tika iegūtas 514 atbildes no Kipras, Igaunijas, Latvijas, Lietuvas un Maltas.

	Lietuva	Latvija	Igaunija	Malta	Kipra
Respondenti katrā valstī	93	76	165	104	76

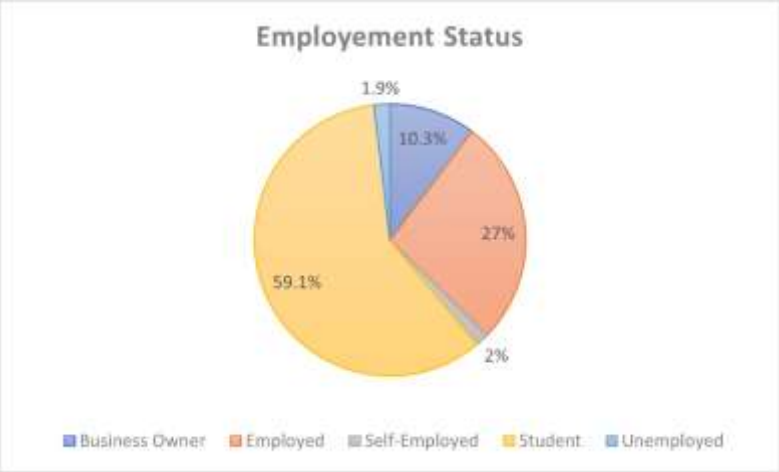
1. tabula Respondenti katrā valstī

No 514 respondentiem - 259 bija sievietes, 248 bija vīrieši, un 7 respondenti izvēlējās nenorādīt savu dzimumu. Visās partnervalstīs, izņemot Igauniju, respondentu sieviešu skaits bija lielāks nekā respondentu vīriešu skaits.

	Lietuva	Latvija	Igaunija	Malta	Kipra
Sieviete	63,4%	57,9 %	34,6%	54,8%	55,3%
Vīrietis	36,6%	40,8%	63%	45,2%	42,1%
Nevēlos atbildēt	-	1,3 %	2,4%	-	2,6%

2. tabula Respondenti pēc dzimuma

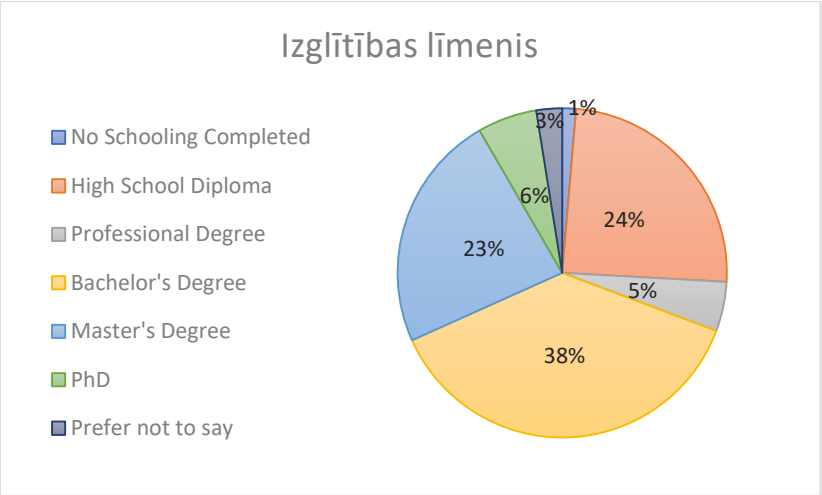
Lielākā daļa respondentu ir studenti (59%), viņiem seko darbinieki (27%), uzņēmumu īpašnieki (10%), bezdarbnieki (2%) un pašnodarbinātie (2%).



1. attēls Aptaujas respondentu nodarbinātības statuss

Aptaujas respondenti ir labi izglītoti - lielākajai daļai respondentu (38%) ir bakalaura grāds, kam seko maģistra grāds (23%) un doktora grāds (6%).

Funded by the Erasmus+ Programme of the European Union

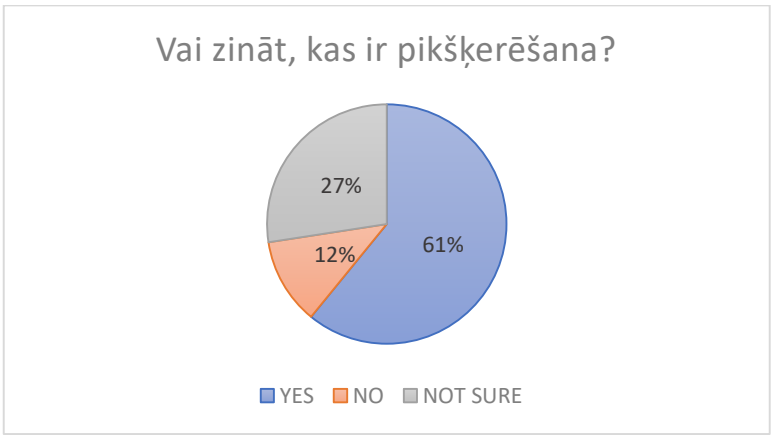


2. attēls Aptaujas respondentu izglītības līmenis

3.3.2. Vispārīgas zināšanas un uzvedība

Lai gan visvairāk respondentu (74%) ir norādījuši, ka nekad nav piedalījušies oficiālās apmācībās / semināros / pētījumos par kiberdrošību vai pikšķerēšanu, vairāk nekā puse respondentu (56%) paši ir pētījuši šo tēmu. Šie rezultāti varētu liecināt, ka kiberdrošības un pikšķerēšanas tēmas ir būtiskas visās aptaujātajās valstīs, un, lai arī respondentiem, iespējams, nav iespējas izpētīt tēmu oficiālā vidē, viņi ir gatavi veltīt laiku tēmas izpētei, lai uzlabotu savas zināšanas un prasmes paši.

61% respondentu atbildēja, ka viņiem ir zināšanas par pikšķerēšanu, 27% nav pārliecināti un 12% nezina, kas ir pikšķerēšana. Kad tiek lūgts izvēlēties pareizo pikšķerēšanas definīciju, 72% aptaujāto cilvēku to ir izvēlējušies pareizi. Maltā un Igaunijā to respondentu skaits, kuri apgalvo, ka zina, kas ir pikšķerēšana, ir vienāds. Lietuvā, Kiprā un Latvijā pareizo atbildi ir izvēlējušies vairāk cilvēku nekā tie, kuri norādīja, ka zina, kas ir pikšķerēšana. Šie rezultāti var norādīt, ka vairāk respondentu no šīm valstīm zina par pikšķerēšanu, taču viņi nav pārliecināti par savām zināšanām.



3. attēls Aptaujas respondentu informētība par pikšķerēšanu

Gandrīz puse respondentu (46%) norādīja, ka bieži baidās atvērt saiti vai pielikumu e-pastā, domājot, ka tas varētu būt viltots, savukārt 13% baidās vienmēr. Tikai 3% respondentu nekad nebaidās atvērt saites / pielikumus, un 8% baidās reti.

Gandrīz trešdaļa respondentu (32%) bieži baidās kļūt par pikšķerēšanas uzbrukumu mērķiem, un 19% vienmēr ir nobijušies. Tikai 5% respondentu norādīja, ka nekad nebaidās kļūt par pikšķerēšanas uzbrukuma mērķi, bet 17% baidās reti.

Funded by the Erasmus+ Programme of the European Union

Iepriekš minētie rezultāti liecina, ka lielākā daļa respondentu apzinās kiberuzbrukumu iespējamību un galvenos hakeru izmantotos rīkus (ļaunprātīgas saites un pielikumi). Turklāt, kaut arī 39% respondentu norādīja, ka nezina vai nav pārliecināti, kas ir pikšķerēšana, tomēr 51% respondentu bieži vai vienmēr baidās kļūt par pikšķerēšanas uzbrukumu mērķiem. Šie rezultāti var nozīmēt, ka pat tiem respondentiem, kuri ir norādījuši, ka zina, kas ir pikšķerēšana, nav obligāti nepieciešamo zināšanu, lai sevi aizsargātu, vai trūkst pārliecības par savām prasmēm.

Jautāti par dažādiem zināmajiem pikšķerēšanas veidiem, respondenti visās aptaujātajās valstīs norādīja, ka viņi visvairāk zina par šiem pikšķerēšanas veidiem: "Spray and Pray", "Cat phishing" un "Malvertising". Visu aptaujāto valstu, izņemot Lietuvu, respondenti arī visvairāk zina par pikšķerēšanas veidu "Advanced fee scam".

4. attēls Respondentiem vislabāk zināmie pikšķerēšanas veidi

No otras puses, respondenti vismazāk zina šos pikšķerēšanas veidus: "Whaling", "Clone phishing" un, izņemot respondentus no Kipras, "Smishing"[15]. Respondenti no Maltas, Kipras, Lietuvas un Latvijas arī vismazāk zina par "Satura ievadīšanu" (*Content injection*), savukārt Igaunijas respondenti norādīja, ka viņi lielākoties zina šo pikšķerēšanas tipu.

5. attēls Respondentiem vismazāk zināmie pikšķerēšanas veidi

Atbildot uz jautājumu, kādas sekas visdrīzāk vai noteikti radīsies pēc veiksmīgā pikšķerēšanas uzbrukuma personai vai uzņēmumam, lielākā daļa respondentu no visām aptaujātajām valstīm nosauca šādas sekas - "sensitīvu datu zādzība", "krāpšana ar kredītkartēm", "klientu informācijas zādzība", "kaitējums reputācijai" un "lietotājvārdu un paroļu pazaudēšana" (izņemot Maltu). Respondenti no visām aptaujātajām valstīm, izņemot Kipru[16] , arī mēdz uzskatīt, ka pēc veiksmīga pikšķerēšanas uzbrukuma viņu dati, visticamāk, tiks pārdoti noziedzīgām trešām personām.

6. attēls Pēc respondentu domām, sekas, kas, visticamāk, radīsies pēc veiksmīga pikšķerēšanas uzbrukuma

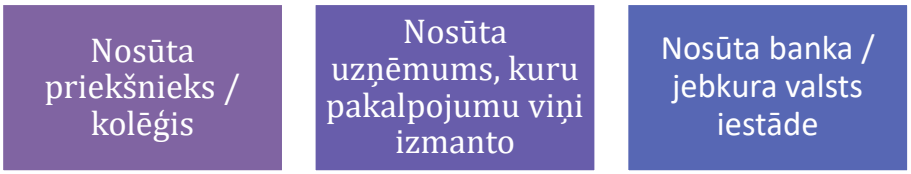
No otras puses, visu aptaujāto valstu respondenti uzskata, ka pēc veiksmīga pikšķerēšanas uzbrukuma "intelektuālā īpašuma zaudēšana" ir maz ticama. Lietuviešu, maltiešu un igauņu

[15] Izņemot respondentus Kiprā
[16] Izņemot respondentus Kiprā

Funded by the Erasmus+ Programme of the European Union

respondenti arī ir skeptiski par "līdzekļu zādzību no biznesa / klientu kontiem", kas varētu notikt pēc pikšķerēšanas uzbrukuma.

Ņemot vērā uzvedības aspektu, respondenti, visticamāk, noklikšķinās uz e-pastā vai ziņojumā esošās saites vai pielikuma, kā arī sniegs slepenu informāciju, ja: "to sūta viņu priekšnieks vai kolēģis", "sūta uzņēmums, kura pakalpojumus viņi izmanto", "sūta banka vai jebkura valsts iestāde". Kiprā respondenti, visticamāk, to darītu arī tad, ja e-pasts/ ziņojums "aicina precizēt datus, piemēram, adresi, pasūtījuma saņemšanai (piemēram, Amazon pasūtījums)". Tajā pašā laikā viedokļi Latvijā un Maltā ir atšķirīgi, un gandrīz vienāds respondentu skaits norāda, ka šāda rīcība ir ļoti iespējama un ka tā ir ļoti maz ticama. Igaunijas un Lietuvas respondentu vidū nav atšķirīgu viedokļu - lielākā daļa uzskata šādu rīcību par maz iespējamu.



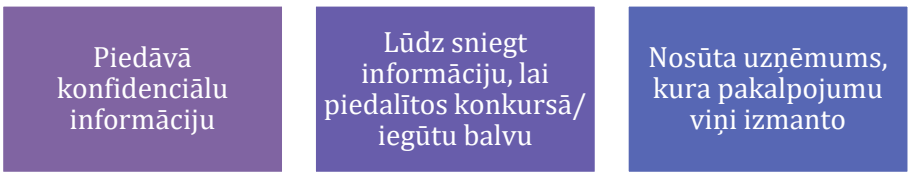
7. attēls E-pastu veidi, kurus saņemot, respondenti visticamāk noklikšķinās uz e-pasta vai ziņojuma saites vai pielikuma un/vai sniegs sensitīvu informāciju

Rezultāti nav pārsteidzoši, ja aplūkojam sešus iepriekš apskatītos pārliecināšanas principus. Kā jau minēts iepriekš, cilvēki mēdz sekot un vairāk uzticēties autoritātēm vai ekspertiem. Tādējādi daudzu hakeru mērķis ir atdarināt vai nu uzticamu valdības iestādi / institūciju, kā arī bankas vai izpilddirektorus. Šī tendence bija redzama arī aptaujā, kur 34% respondentu apgalvoja, ka ļoti bieži vai vienmēr uzticas ziņojumiem, kas, šķiet, saņemti no svarīgas iestādes vai izskatās svarīgi, savukārt 30% dara to dažreiz.

Svarīga loma ir arī "Patikšanas principam", kas nozīmē, ka cilvēki, visticamāk, atbildēs uz kolēģa/ priekšnieka pieprasījumu, pat ja tas izklausās neparasti.

Turklāt cilvēki ir "ieraduma radījumi" un viņiem parasti patīk konsekvence. Pieņemsim, ka e-pastu ir nosūtījis uzņēmums, kuru viņi pazīst kura kādus pakalpojumus viņi izmanto un, iespējams, jau iepriekš ir saņēmuši šāda uzņēmuma e-pastus vai ziņojumus. Tādā gadījumā pasāv lielāka iespējamība, ka viņi to atvērs, noklikšķinās uz saitēm/ pielikumiem u.t.t. nekā tas būtu tāda uzņēmuma gadījumā, kura pakalpojumus viņi neizmanto.

Visās partnervalstīs respondenti visdrīzāk neklikšķinātu uz saites vai pielikuma e-pastā vai ziņojumā un / vai nesniegtu slepenu informāciju, ja tā: "piedāvā viņiem konfidenciālu informāciju (piemēram, informāciju par konkurentiem)", "lūdz viņus aizpildīt aptauju / norādīt savus e-pasta vai tālruņa kontaktus, lai piedalītos konkursā, lai iegūtu balvu" vai "to nosūta uzņēmums / organizācija, kuru viņi pazīst, bet neizmanto tā pakalpojumus".



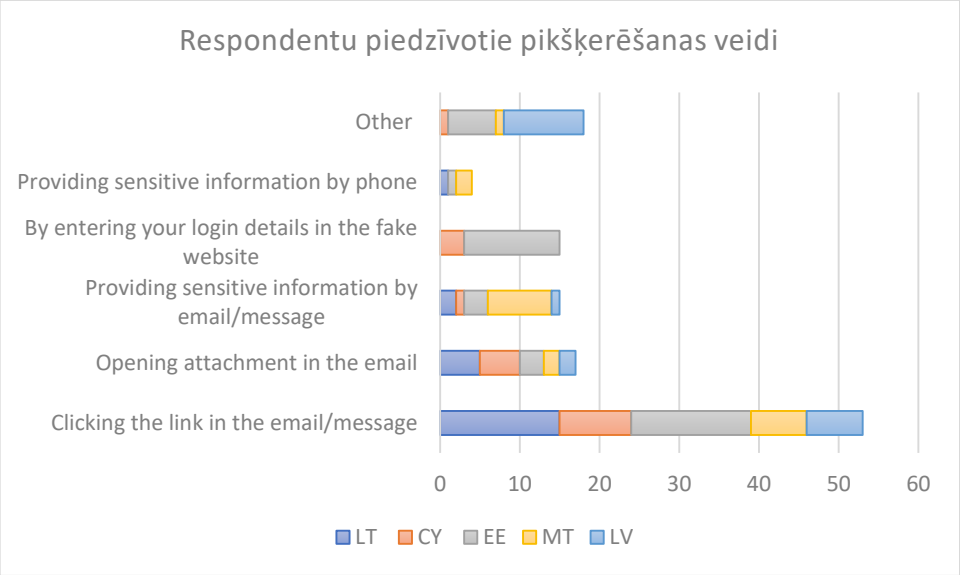
8. attēls E-pastu veidi, kurus saņemot, respondenti visticamāk neklikšķinās uz e-pasta vai ziņojuma saites vai pielikuma un/vai nesniegs sensitīvu informāciju

Arī lielākā daļa respondentu no Igaunijas, Kipras un Maltas norāda, ka ir maz ticams, ka viņi sniegs konfidenciālu informāciju, ja e-pastā vai ziņojumā tiek "lūgts palīdzēt vai ziedot vietējām vai starptautiskām labdarības organizācijām". Respondenti no Kipras, visticamāk, arī noklikšķinātu uz saites / pielikuma un sniegtu konfidenciālu informāciju, ja tajā viņi "tiktu aicināti uz konkrētu tiešsaistes vai bezsaistes pasākumu (piemēram, zoom sapulci). Turpretī Lietuvas, Latvijas, Igaunijas un Maltas respondenti visticamāk to nedarītu.

Funded by the Erasmus+ Programme of the European Union

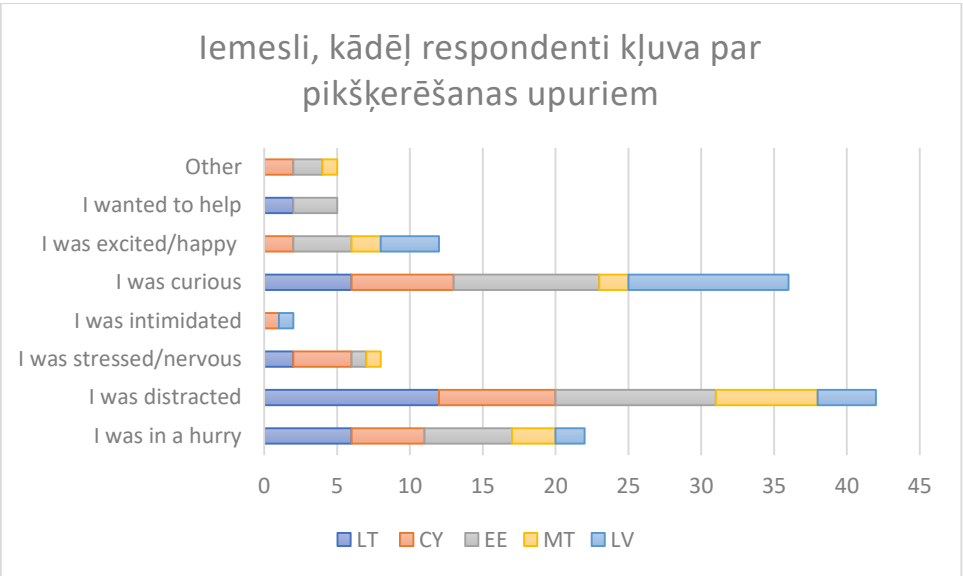
3.3.3. Personīgā pieredze ar pikšķerēšanas uzbrukumiem

19,8% respondentu jeb gandrīz katrs piektais respondents ir piedzīvojis pikšķerēšanas uzbrukumu. Visizplatītākais veids, kā respondenti tiek pakļauti pikšķerēšanas uzbrukumam, ir noklikšķinot uz saites e-pastā vai ziņojumā, e-pastā atverot pielikumu, atbildot uz e-pastu vai ziņojumu un sniedzot sensitīvu informāciju. Pārsteidzoši, ka tikai respondenti Igaunijā un Kiprā ir norādījuši, ka viņi ir piedzīvojuši pikšķerēšanu, viltus vietnē ievadot pieteikšanās datus. Starp "citām" atbildēm vispopulārākās bija "vairāku pikšķerēšanas metožu kombinācija" un "informācijas sniegšana viltus aptaujai".



9. attēls Respondentu iepriekš piedzīvotie pikšķerēšanas veidi

Kad tika lūgts norādīt, kāpēc, viņuprāt, viņi kļuva par pikšķerēšanas upuriem, lielākā daļa respondentu norādīja, ka bijuši apjukuši, ziņkārīgi vai steidzās.



10. attēls Iemesli, kādēļ respondenti kļuva par pikšķerēšanas upuriem

Funded by the Erasmus+ Programme of the European Union

3.3.4. Pikšķerēšanas uzbrukumu atpazīšana

Aptaujā respondentiem tika lūgts novērtēt un norādīt svarīgākos kritērijus, lai atpazītu aizdomīgu e-pastu, īsziņu vai tālruņa zvanu un sociālo mediju ziņojumu.

E-pasts

Runājot par aizdomīgu e-pastu atpazīšanu, visu valstu respondentiem bija vienots viedoklis par svarīgākajiem kritērijiem, kas jāņem vērā. Galvenie norādītie kritēriji ir šādi: 1) Sūtītāja domēns (e-pasts) neizskatās īsts (neatbilst organizācijai, satur pareizrakstības kļūdu, papildu ciparus, burtus u.t.t.); 2) E-pastā iegultās saites nav tādas pašas kā īstā hipersaite; 3) Sūtītājs lūdz apstiprināt / sniegt sensitīvu informāciju (pieteikšanās akreditācijas datus, bankas rekvizītus) pa e-pastu; 4) E-pasta adresēs, saitēs un domēnu nosaukumos ir redzamas neatbilstības; 5) E-pasts satur negaidītu / neparastu pielikumu.

Vismazāk svarīgākie respondentu norādītie kritēriji bija 1) Nekonkrēta uzruna e-pastā; 2) Nav paraksta vai kontaktinformācijas; 3) E-pasta ziņojums rada zinātkāri, jānoskaidro vairāk; 4) E-pasta ziņojums ir pārāk labs, lai būtu patiess. Respondenti no Maltas kā mazāk svarīgu kritēriju izvēlējās arī rakstīšanas un pareizrakstības stilu, kā arī gramatikas kļūdas.

Īsziņa vai tālruņa zvans

Visu respondentu viedoklis bija gandrīz vienbalsīgs visās aptaujātajās valstīs attiecībā uz svarīgākajiem kritērijiem aizdomīgas īsziņas vai tālruņa zvana atpazīšanai. Respondenti no visām valstīm vienojās par šiem svarīgākajiem "sarkanajiem karogiem" - 1) Sūtītājs / zvanītājs lūdz pārbaudīt informāciju vai sniegt sensitīvu informāciju vai nosūtīt naudu; 2) Numurs ar atšķirīgas valsts kodu; un 3) Zvanītājs pienācīgi neiepazīstina ar sevi (vārds, amats, uzņēmums). Respondenti no visām aptaujātajām valstīm, izņemot Igauniju, arī piekrita, ka neparasti garš numurs ir viens no svarīgākajiem "sarkanajiem karogiem". Turklāt visi aptaujas dalībnieki, izņemot tos, kuri bija no Kipras, arī norādīja, ka ziņojums ar brīdinājumu (piemēram, konta derīguma termiņš beidzas) un spiediena izdarīšana uz saņēmēju steidzama lēmuma pieņemšanai ir arī viens no svarīgākajiem galvenajiem sarkanajiem karogiem.

Mazāk svarīgs kritērijs, ko respondenti norādīja Maltā, Igaunijā, Lietuvā un Kiprā, bija pareizrakstības un gramatikas kļūdas. Savukārt, tieši pretēji, Latvijas respondenti kā vienu no svarīgākajiem kritērijiem izvēlējās pareizrakstības un gramatikas kļūdas. Arī aptaujāto valstu respondenti atbildēja, ka tas nav tik svarīgi, ja zvanītājs nenosauc viņus vārdā un uzvārdā, izņemot respondentus no Kipras, kuri uzskatīja, ka tas būs viens no svarīgākajiem kritērijiem, lai atpazītu aizdomīgu zvanu.

Ziņojums sociālo mediju kanālos

Respondentiem bija gandrīz vienots viedoklis par aizdomīgu ziņojumu identificēšanu arī sociālajos medijos. Lielākā daļa respondentu vienojās par šiem svarīgākajiem kritērijiem: 1) Ziņojumā tiek prasīta nauda; 2) Ziņojumā tiek lūgts pārbaudīt informāciju vai sniegt sensitīvu informāciju; 3) Ziņojumā iekļauta apšaubāma saite un 4) Sūtītāja sociālo tīklu profils izskatās aizdomīgs (piemēram, jauns konts, nav draugu u.t.t.). Respondenti, izņemot Maltas respondentus, arī uzskata, ka ziņojums ar aicinājumu instalēt kādu programmu ir viens no galvenajiem sarkanajiem karogiem, kas norāda uz aizdomīgām darbībām.

Pareizrakstības un gramatikas kļūdas, neesošas biznesa attiecības ar sūtītāju vai nepazīstams sūtītājs tika identificēti kā respondentiem vismazāk svarīgie kritēriji.

PIKŠĶERĒŠANAS UZBRUKUMU ATPAZĪŠANA	SVARĪGĀKIE KRITĒRIJI	VISMAZĀK SVARĪGIE KRITĒRIJI

Funded by the Erasmus+ Programme of the European Union

E-PASTS	• Sūtītāja domēns (e-pasts) neizskatās īsts; • E-pastā iegultās saites nav tādas pašas kā īstā hipersaite; • Sūtītājs lūdz apstiprināt / sniegt sensitīvu informāciju; • E-pasta adresēs, saitēs un domēnu nosaukumos ir redzamas neatbilstības; • Negaidīts/ neparasts pielikums.	• Nekonkrēta uzruna; • Nav paraksta vai kontaktinformācijas; • Pats e-pasts rada zinātkāri, jānoskaidro vairāk.
ĪSZIŅA VAI TĀLRUŅA ZVANS	• Sūtītājs / zvanītājs lūdz pārbaudīt informāciju vai sniegt sensitīvu informāciju vai nosūtīt naudu; • Numurs ar atšķirīgu valsts kodu; • Zvanītājs neiepazīstina ar sevi (vārds, amats, uzņēmums); • Neparasti garš tālruņa numurs;[17] • Ziņojumā iekļauts brīdinājums.[18]	• Pareizrakstības un gramatikas kļūdas;[19] • Zvanītājs neuzrunā vārdā, uzvārdā.[20]
ZIŅOJUMS SOCIĀLAJOS MEDIJOS	• Ziņojumā tiek prasīta nauda; • Ziņojumā tiek lūgts sniegt akreditācijas datus vai sensitīvu informāciju; • Ziņojumā iekļauta aizdomīga saite; • Sūtītāja sociālo mediju profils izskatās aizdomīgs (piemēram, jauns konts, nav draugu utt.); • Ziņojumā tiek lūgts instalēt kādu programmu[21]	• Pareizrakstības un gramatikas kļūdas; • Ar sūtītāju nav biznesa attiecību; • Nezināms sūtītājs.

3. tabula Svarīgākie un mazāk svarīgie kritēriji pikšķerēšanas uzbrukumu atpazīšanai

Kopumā, runājot par galveno kritēriju noteikšanu, respondenti, identificējot aizdomīgus e-pastus vai citus, galvenokārt koncentrējas uz "tehniskajiem kritērijiem", piemēram, saitēm, domēniem, pielikumiem, valsts kodu u.t.t., nevis uz cilvēku emocijām (sociālo inženieriju). Pareizrakstības vai gramatikas kļūdas vai vispārēja uzruna ir vieni no pēdējiem punktiem, ko respondenti izvērtē.

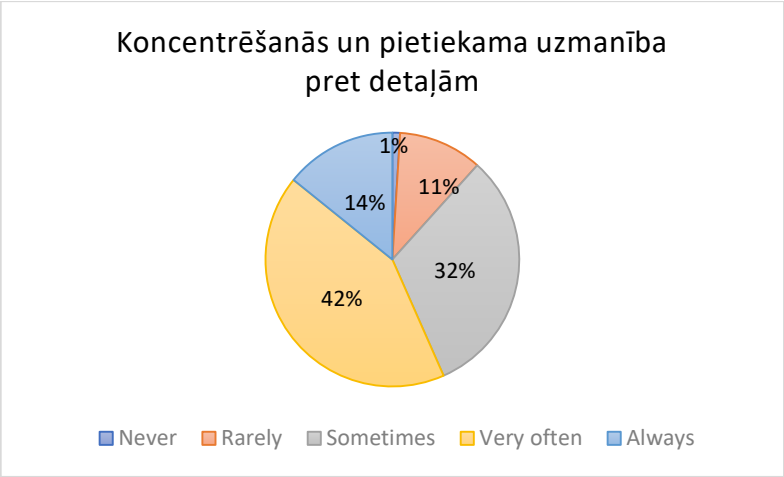
Tomēr ir svarīgi atzīmēt, ka, lai gan "tehniskie kritēriji" ir vieni no pirmajiem aspektiem, ko respondenti pamana un pārbauda, tas nenozīmē, ka, vērtējot e-pastus un ziņojumus, viņi neņem vērā sociālo inženieriju. Kad aptaujā tika lūgts identificēt pikšķerēšanas e-pastus / ziņojumus un galvenos "sarkanos karogus", lielākā daļa respondentu no visām aptaujātajām valstīm izvēlējās gan "tehniskos kritērijus", gan kritērijus, kas vērsti uz cilvēka emocijām (sociālā inženierija).

3.3.5. Kritiskās domāšanas prasmes

Lielākā daļa respondentu ir diezgan optimistiski par savām kritiskās domāšanas prasmēm. Vairāk nekā puse respondentu (57%) paziņoja, ka, atverot e-pastu vai ziņojumu, viņi ļoti bieži vai vienmēr koncentrējas un pievērš pietiekamu uzmanību, atverot e-pastu vai ziņojumu. Salīdzinājumam - 12% apgalvoja, ka viņi nekad nepievērš pietiekami daudz uzmanības vai tas notiek reti.

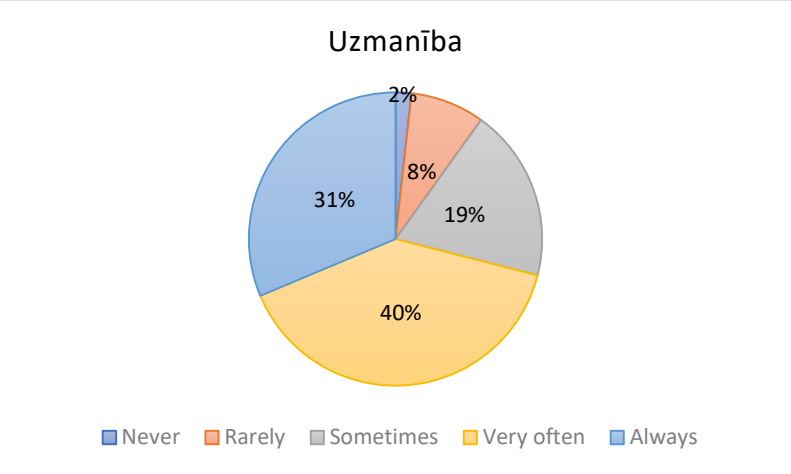
[17] Izņemot respondentus Igaunijā
[18] Izņemot respondentus Kiprā
[19] Izņemot respondentus Latvijā
[20] Izņemot respondentus Kiprā
[21] Izņemot respondentus Maltā

Funded by the Erasmus+ Programme of the European Union



11. attēls Respondentu koncentrēšanās un uzmanība pret detaļām, atverot ziņojumu / e-pastu

71% respondentu apgalvo, ka bieži vien ir piesardzīgi, noklikšķinot uz saites vai pielikuma, savukārt 11% apgalvoja, ka šādā situācijā nekad nepievērš uzmanību vai dara to reti.



12. attēls Respondenti ir uzmanīgi, noklikšķinot uz saites / pielikuma

67% respondentu paziņoja, ka ļoti bieži vai vienmēr var vizualizēt savu lēmumu iespējamās sekas, pamatojoties uz pierādījumiem, saņemot aizdomīga izskata e-pastu vai ziņojumu, savukārt tikai 5% respondentu paziņoja, ka nekad nevar iedomāties šādas sekas vai dara to reti.

77% respondentu arī ļoti bieži vai vienmēr spēj izdarīt secinājumus, balstoties uz pierādījumiem, saņemot aizdomīga izskata e-pastu vai ziņojumu, savukārt tikai 3% respondentu to nespēj nekad vai spēj reti.
Atšķirība starp respondentu, kuri spēj vizualizēt sekas un izdarīt secinājumus, procentuālo apjomu. Turpretī ne visi respondenti zina par pikšķerēšanas sekām. Viņi joprojām spēj izdarīt secinājumus un atpazīt pikšķerēšanas e-pastu / ziņojumu.

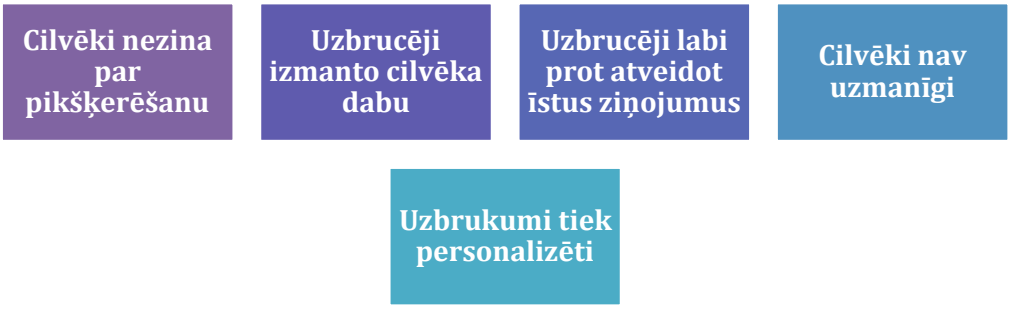
Tomēr ir svarīgi uzsvērt, ka, neraugoties uz diezgan labajiem rezultātiem, apmēram trešdaļa respondentu tikai dažkārt spēj iztēloties sekas un izdarīt secinājumus.

3.3.6. Izvairīšanās no pikšķerēšanas uzbrukumiem

Aptaujas respondentiem tika lūgts norādīt arī galvenos iemeslus, kas, viņuprāt, veicina veiksmīgus pikšķerēšanas uzbrukumus. Respondenti no visām aptaujātajām valstīm ir izvēlējušies 5 galvenos iemeslus: 1) Cilvēki neapzinās / nezina par šādiem uzbrukumiem un to novēršanu; 2) Uzbrucēji izmanto cilvēka dabu, viņi paļaujas uz mijiedarbību un spēlējas ar cilvēka emocijām un vajadzībām; 3) Uzbrucēji patiešām labi atdarina īstu uzņēmumu ziņojumus un e-pastus, padarot tos ļoti ticamus

Funded by the Erasmus+ Programme of the European Union

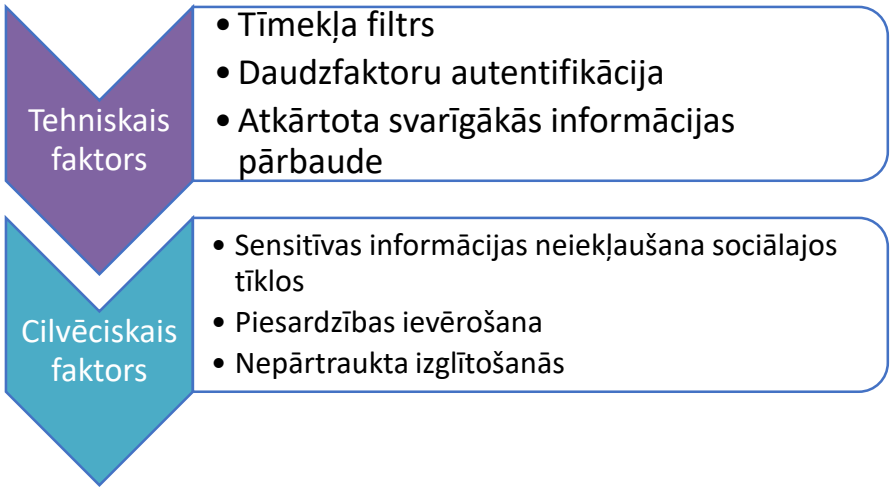
un pārliecinošus; 4) Cilvēki nepievērš pietiekamu uzmanību / ir nezinoši[22] ; 5) Uzbrucēji kļūst arvien progresīvāki, tiek atlasīti konkrēti mērķi, savukārt e-pastu izmantošana ir ļoti personalizēta un izmanto specifisku informāciju[23] .



13. attēls Galvenie iemesli, kāpēc pikšķerēšanas uzbrukumi ir veiksmīgi, pēc respondentu domām

Respondentu visretāk izvēlētie iemesli bija: 1) Cilvēki izmanto novecojušu programmatūru; 2) Pikšķerēšanas rīki ir lēti un plaši izplatīti; un 3) Pati ļaunprātīgā programmatūra kļūst arvien sarežģītāka[24] .
Respondenti bija vienisprātis, ka hakeri parasti izmanto cilvēku emocijas, vajadzības un vēlmes, īpaši rosinot viņu motivāciju, piedāvājot "dāvanas" vai bezmaksas kuponus, rosinot viņu zinātkāri un izraisot bažas / satraukumu.

Lielākā daļa respondentu uzskata, ka, lai izvairītos no pikšķerēšanas uzbrukumiem, ir svarīgi šim jautājumam pievērsties no dažādiem aspektiem: 1) tehniskais faktors - izmantojot tīmekļa filtru ļaunprātīgu vietņu bloķēšanai, daudzfaktoru autentifikāciju / paroļu biežu maiņu, kā arī visu svarīgo detaļu (sūtītāja e-pasta, saites, pielikumi utt.) dubultu pārbaudi, un 2) cilvēciskais faktors - nepublicējot sensitīvu informāciju par sevi sociālajos medijos, ievērojot piesardzību, atverot e-pastus / ziņojumus / atbildot uz tālruni, un pastāvīgi izglītojot sevi šajā jomā."



14. attēls Darbības, kas jāveic, lai novērstu pikšķerēšanas uzbrukumus, pēc respondentu domām

Vismazāk svarīgās darbības, kas jāveic, lai izvairītos no pikšķerēšanas uzbrukumiem, pēc respondentu domām, ir atjauninātas pārlūkprogrammas izmantošana, sekošana līdzi jaunākajai pieejamai programmatūrai un rīkiem vai atjauninātas operētājsistēmas izmantošana[25], kā arī regulāras kiberdrošības apmācības / darbnīcas

[22] Izņemot respondentus Maltā
[23] Izņemot respondentus Kiprā
[24] Izņemot respondentus Maltā
[25] Izņemot respondentus Igaunijā

Funded by the Erasmus+ Programme of the European Union

Lielākā daļa respondentu visdrošāk jūtas šādās jomās: spēja tiešsaistē atrast atbilstošu un uzticamu informāciju, identificēt pikšķerēšanas uzbrukumus un izmantot drošības programmatūru, daudzfaktoru autentifikāciju, kā arī tīmekļa filtru.

Mazāk respondentu jūtas pārliecināti par savām kiberdrošības / pikšķerēšanas terminoloģijas zināšanām un to lietošanu, kā arī par iespēju šifrēt visu sensitīvo uzņēmuma informāciju.

15. attēls Jomas, kurās respondenti jūtas visvairāk pārliecināti

4. KOPSAVILKUMS UN GALVENIE ATZINUMI

Respondentu sociāldemogrāfiskā informācija

- Aptaujā piedalījās 514 cilvēki, no kuriem 259 ir sievietes, 248 vīrieši un septiņi cilvēki nevēlas norādīt savu dzimumu.
- Lielākā daļa respondentu ir studenti (304), viņiem seko darbinieki (139), uzņēmumu īpašnieki (53), bezdarbnieki (10) un pašnodarbinātie (8).
- Lielākā daļa aptaujas respondentu ir labi izglītoti - lielākajai daļai respondentu (38%) ir bakalaura grāds, kam seko maģistra grāds (23%) un doktora grāds (6%).

Vispārīgas zināšanas un uzvedība

- Lai gan 74% respondentu formālā vidē nekad nav piedalījušies nevienā apmācībā / seminārā vai kiberdrošības pētījumā, vairāk nekā puse respondentu (54%) paši ir izpētījuši šo tēmu (lasījuši rakstus, skatījušies videoklipus utt.). Šie rezultāti norāda, ka, lai arī respondentiem ne vienmēr ir iespēja apgūt tēmu formālā vidē, viņi ir motivēti patstāvīgi uzlabot savas zināšanas un prasmes.
- 61% respondentu apgalvoja, ka zina, kas ir pikšķerēšana, savukārt 27% nebija pārliecināti, un 12% to nezināja. Kad tika lūgts izvēlēties pareizo pikšķerēšanas definīciju, vairāk respondentu no Lietuvas, Latvijas un Kipras izvēlējās pareizo atbildi nekā to cilvēku skaits, kuri norādīja, ka zina, kas ir pikšķerēšana. Šie rezultāti var norādīt, ka vairāk respondentu no šīm valstīm ir informēti par pikšķerēšanu, tomēr viņiem, iespējams, nav pietiekamu zināšanu vai pārliecības.
- 59% aptaujāto cilvēku ļoti bieži vai vienmēr baidās atvērt saiti vai pielikumu, domājot, ka tas varētu būt ļaunprātīgs. Salīdzinājumam - 51% ļoti bieži vai vienmēr baidās kļūt par pikšķerēšanas uzbrukumu mērķi. Minētie anketas rezultāti liecina, ka pat tie respondenti, kuri apgalvoja, ka zina, kas ir pikšķerēšana, baidās no pikšķerēšanas, norādot uz nepietiekamām zināšanām vai pārliecības trūkumu par savām prasmēm.
- Respondenti galvenokārt zina pikšķerēšanas veidus “Spray and pray”, “Cat phishing” un “Malvertising”. Turpretī viņiem ir mazāk zināšanu par pikšķerēšanas uzbrukumiem “Whaling”, “Clone phishing” un “Smishing”.
- Respondenti uzskata, ka pēc veiksmīga pikšķerēšanas uzbrukuma, visticamāk, rodas šīs sekas - sensitīvu datu vai klienta informācijas zādzība, krāpšanās ar kredītkartēm un kaitējums reputācijai. Arī lielākā daļa respondentu, izņemot maltiešus, uzskata, ka veiksmīga pikšķerēšanas uzbrukuma rezultātā var pazaudēt lietotājvārdus un paroles. Turklāt datu pārdošanu noziedzīgām trešajām pusēm visu aptaujāto valstu, izņemot Kipru, pārstāvji arī uzskatīja par ļoti iespējamu. Turpretī respondenti uzskata, ka pēc veiksmīga pikšķerēšanas uzbrukuma intelektuālā īpašuma zaudēšana ir mazāk iespējama.
- Lietuviešu, maltiešu un igauņu respondenti arī ir skeptiski par “līdzekļu zādzību no biznesa / klientu kontiem”, kas varētu notikt pēc pikšķerēšanas uzbrukuma.
- Respondenti, visticamāk, noklikšķinātu uz saites vai pielikuma e-pastā vai ziņojumā, ja to nosūtījis priekšnieks vai kolēģis, uzņēmums, kura pakalpojumus viņi izmanto, vai banka vai valsts iestāde. Šķiet, ka autoritātes un patikšanas principi ir tie, uz kuriem respondenti, visticamāk, reaģētu.

Funded by the Erasmus+ Programme of the European Union

- Respondenti retāk noklikšķina uz saites vai pielikuma e-pastā vai ziņojumā, ja tajā tiek piedāvāta konfidenciāla informācija, tiek lūgts sniegt informāciju, lai piedalītos konkursā, lai iegūtu balvu, vai arī to nosūtījis uzņēmums, kura pakalpojumu viņi neizmanto. Šķiet, ka atbildes darbības princips ir viens no pārliecināšanas principiem, kas uz respondentiem iedarbojas mazāk.

Respondentu pieredze pikšķerēšanā

- Gandrīz katrs 5. respondents ir iepriekš piedzīvojis pikšķerēšanas uzbrukumu. Galvenie veidi, kā respondenti tika pakļauti pikšķerēšanai, bija klikšķināšana uz saites vai sensitīvas informācijas sniegšana pa e-pastu vai nosūtot ziņojumu. Tikai respondenti Kiprā un Igaunijā norādīja, ka viņi pakļauti pikšķerēšanai, ievadot savus datus viltus vietnē.

- Galvenie iemesli, kādēļ viņi kļuva par pikšķerēšanas upuriem bija apjukums, ziņkārība vai steiga. Daži respondenti arī minēja, ka nezina, kas ir pikšķerēšana.

Pikšķerēšanas uzbrukumu atpazīšana

- Runājot par galvenajiem kritērijiem, kas izmantoti pikšķerēšanas uzbrukuma atpazīšanai, respondenti kopumā vairāk pievērsās "tehniskajiem kritērijiem", piemēram, sūtītāja domēnam, iegultām saitēm, pielikumiem un redzamām neatbilstībām starp tiem, kā arī neparasti garam tālruņa numuram vai atšķirīgam valsts kodam. Respondenti arī norādīja, ka sūtītājs / zvanītājs, kurš lūdz sensitīvu informāciju vai naudu, ir viens no galvenajiem aizdomas raisošajiem kritērijiem. Pareizrakstības vai gramatikas kļūdas vai vispārēja uzruna lielākajā daļā gadījumu ir vieni no pēdējiem punktiem, ko respondenti izvērtē.

- Tomēr, lai gan respondenti vispirms ievēro un pārbauda "tehniskos kritērijus", viņi ņem vērā arī "cilvēciskos kritērijus" (sociālā inženierija), izvērtējot e-pastus un ziņojumus. Kad aptaujā tika lūgts identificēt pikšķerēšanas e-pastus / ziņojumus un galvenos "sarkanos karogus", lielākā daļa respondentu no visām aptaujātajām valstīm izvēlējās gan "tehniskos kritērijus", gan kritērijus, kas vērsti uz cilvēka emocijām (sociālā inženierija).

Kritiskās domāšanas prasmes

- Lielākā daļa respondentu ir diezgan optimistiski par savām kritiskās domāšanas prasmēm. 57% respondentu paziņoja, ka, atverot e-pastus vai ziņojumus, viņi ļoti bieži vai vienmēr pievērš nepieciešamo uzmanību. Salīdzinājumam - 71% apgalvoja, ka ļoti bieži vai vienmēr ir uzmanīgi, noklikšķinot uz saites vai pielikuma.

- 67% respondentu teica, ka, saņemot aizdomīgu e-pastu vai ziņojumu, viņi ļoti bieži vai vienmēr spēj iztēloties iespējamās savas rīcības sekas. Salīdzinājumam - 77% respondentu ļoti bieži vai vienmēr spēj izdarīt secinājumus. Atšķirība starp to respondentu procentuālo daudzumu, kuri var iztēloties sekas un spēj izdarīt secinājumus, var liecināt, ka, kaut arī ne visi respondenti zina par pikšķerēšanas sekām, tomēr viņi spēj izdarīt secinājumus un atpazīt pikšķerēšanas e-pastu / ziņojumu.

- Tomēr ir svarīgi uzsvērt, ka, neraugoties uz diezgan labajiem rezultātiem, apmēram trešdaļa respondentu tikai dažkārt spēj iztēloties sekas un izdarīt secinājumus.

Funded by the Erasmus+ Programme of the European Union

Izvairīšanās no pikšķerēšanas uzbrukumiem

- Respondenti izvēlējās šos galvenos iemeslus, kas, viņuprāt, noved pie veiksmīgiem pikšķerēšanas uzbrukumiem - cilvēki nezina par pikšķerēšanu un to, kā to novērst, uzbrucēji izmanto cilvēka dabu. Viņi labi prot reproducēt īstu uzņēmumu e-pastus un ziņojumus, un cilvēki nepievērš pietiekamu uzmanību vai viņiem trūkst zināšanu. Mazāk respondentu uzskata, ka pikšķerēšanas uzbrukumu galvenie iemesli ir cilvēki, kas izmanto novecojušu programmatūru, pikšķerēšanas rīku izmantošana ir lēta vai plaši izplatīta, un ļaunprogrammatūra kļūst arvien sarežģītāka.

- Respondenti uzskata, ka hakeri galvenokārt izmanto cilvēka zinātkāri, rūpes vai satraukumu un izmanto stimulus, piemēram, "bezmaksas dāvanas" vai "vaučerus".

- Lai izvairītos no pikšķerēšanas uzbrukumiem, respondenti uzskata, ka ir svarīgi tam tuvoties no 2 dažādiem skatupunktiem, piemēram, "tehniskais faktors" un "cilvēciskais faktors", izmantojot atbilstošus rīkus un stratēģijas, kas aptvertu abus šos aspektus. Piemēram, "tehniskais faktors" ietver tīmekļa filtra izmantošanu, daudzfaktoru autentifikāciju un svarīgu detaļu pārbaudi, piemēram, sūtītāja e-pasta, saites un pielikumu utt. pārbaudi. "Cilvēciskais faktors" ir sensitīvas informācijas nepublicēšana sociālajos medijos, piesardzība un pastāvīga izglītošanās.

- Interesanti, ka, lai gan lielākā daļa respondentu uzskata, ka ir svarīgi sevi nepārtraukti izglītot šajā jomā, mazāk respondentu uzskata, ka ir nepieciešamas regulāras kiberdrošības mācības vai semināri. Tomēr tas atbilst datiem, ka gandrīz puse respondentu pēta šo tēmu patstāvīgi.

- Kopumā respondenti uzsver cilvēka spēju novērtēt un identificēt pikšķerēšanas uzbrukumus, nevis paļaujas uz datora operētājsistēmu, programmatūru un pieejamajiem rīkiem.

- Lielākā daļa respondentu visdrošāk jūtas šādās jomās: spēja tiešsaistē atrast atbilstošu un uzticamu informāciju, identificēt pikšķerēšanas uzbrukumus un izmantot drošības programmatūru, daudzfaktoru autentifikāciju, kā arī tīmekļa filtru.

- Mazāk respondentu jūtas pārliecināti par savām kiberdrošības / pikšķerēšanas terminoloģijas zināšanām un to lietošanu, kā arī par iespēju šifrēt visu sensitīvo uzņēmuma informāciju.

Funded by the Erasmus+ Programme of the European Union

5. BIBLIOGRĀFIJA:

1. ES Komisija (2020): Īpašais Eirobarometrs 499: Eiropiešu attieksme pret kiberdrošību, URL https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG
2. Eiropas Savienības Kiberdrošības aģentūra (2020): ENISA drošības apdraudējumu aina 2019. – 2020.
3. https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb/default/table?lang=en EUROSTAT (2020): Vai interneta lietošana šodien ir drošāka ?, URL https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb/default/table?lang=en (skatīts 11.02.2021.)
4. Proofpoint (2019): Cilvēka faktora ziņojums 2019, URL https://www.proofpoint.com/us/resources/threat-reports/human-factor (skatīts 12.02.2021.)
5. Eiropas Savienības Kiberdrošības aģentūra (2020): Pikšķerēšana - ENISA drošības apdraudējumu aina 2019. – 2020.
6. Deloitte (2019): Izpratne par pikšķerēšanas tehniku URL https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf (skatīts 112.02.2021)
7. EUROPOL (2020): Organizētās noziedzības draudu novērtējums internetā 2020
8. NCC grupa (2020): Pikšķerēšanas psiholoģija: Septiņu ietekmes principu izmantošana, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433 (skatīts 20.02.2021.)
9. Eiropas padome (2020): Kibernoziedzība un COVID-19, URL https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-12.02.2021 (skatīts 12.02.2021.)
10. EUROPOL (2020): Peļņas gūšana pandēmijas apstākļos - kā noziedznieki izmanto COVID-19 krīzi

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. PIELIKUMS Aptauja “Pikšķerēšanas prasmju novērtēšana un atpazīšana”

1. DAĻA Personas dati

1. **Vārds:** ..... *(nav obligāti)*

2. **E-pasta adrese:** .... *(nav obligāti - ja vēlaties saņemt jaunumus par projektu un piedalīties apmācības programmas izmēģinājuma testēšanā lūdzu, norādiet savu e-pastu.)*

3. **Dzimums**
- Vīrietis
- Sieviete
- Nevēlos atbildēt

4. **Izglītības līmenis**
- Nav iegūta izglītība
- Vidusskolas diploms
- Profesionālā izglītība (tehniskā / profesionālā izglītība)
- Bakalaura grāds
- Maģistra grāds
- Doktora grāds
- Nevēlos atbildēt
- Cits:.....

5. **Nodarbinātības statuss**

- Biznesa īpašnieks
- Darbinieks
- Pašnodarbinātais
- Students
- Pensionējies
- Bezdarbnieks
- Cits:.....

2. IEDAĻA: Vispārīgas zināšanas un uzvedības

6. **Cik lielā mērā iespējams, ka noklikšķināsiet uz e-pastā vai ziņojumā iekļautas saites vai e-pielikuma un/vai sniegsiet sensitīvu informāciju, ja:**

Funded by the Erasmus+ Programme of the European Union

	Ļoti maz iespējams	Maz iespējams	Neitrāli	Iespējams	Ļoti iespējams
Tajā tiek piedāvāts kupons vai atlaides noteiktiem pirkumiem					
Piedāvā piekļuvi noteiktiem ekskluzīviem piedāvājumiem					
Aicina uz konkrētu pasākumu tiešsaistē vai bezsaistē (piemēram, zoom sapulce)					
Ietver uzaicinājumu aizpildīt aptauju/ norādīt savu e-pastu vai tālruni, lai piedalītos konkursā un saņemtu balvu					
Piedāvā konfidenciālu informāciju (piemēram, informāciju par konkurentiem)					
Aicina precizēt personisko un / vai konta informāciju, lai tas netiktu slēgts / deaktivizēts (piemēram, bankas konts, Netflix konts, Facebook konts utt.)					
Aicina precizēt informāciju, piemēram, adresi pasūtījuma saņemšanai (piemēram, Amazon piegāde)					
Informē par jaunākajiem notikumiem saistībā ar svarīgiem sociālajiem jautājumiem un dabas katastrofām (piemēram, jauna informācija par Covid-19)					
Aicina palīdzēt / ziedot vietējām vai starptautiskām labdarības organizācijām					
Ietver informāciju par Jūsu vaļaspriekiem					
To nosūtījusi banka vai jebkura valsts iestāde					
To nosūtījis Jūsu priekšnieks vai kolēģis					
To nosūtījis uzņēmums, kura pakalpojumus izmantojat					
To nosūtījis uzņēmums/ organizācija, kura ir pazīstama, bet kuras pakalpojumus neizmantojat					

7. **Vai esat kādreiz piedalījies oficiālās apmācībās / semināros / pētījumos par kiberdrošību vai pikšķerēšanu?**

- Jā
- Nē

Funded by the Erasmus+ Programme of the European Union

8. **Vai esat pats pētījis / mācījies par kiberdrošību vai pikšķerēšanu? (lasījis rakstu, skatījies videoklipus utt.)**
- Jā
- Nē

9. **Vai zināt, kas ir pikšķerēšana?**
- Jā
- Nē
- Neesmu drošs

10. **Kurš no šiem piemēriem, Jūsuprāt, atbilst pikšķerēšanas definīcijai?**
- Kibernoziegums, ar kura mērķi sazinās pa e-pastu, lai maldinātu personu un liktu tai sniegt sensitīvus datus par tās kontiem
- Tas ir sava veida sports priekam vai sacensībām
- Nevēlami un/vai atkārtoti personas vai uzņēmuma e-pasti, kas piedāvā produktus vai pakalpojumus
- Kibernoziegums, ar kura mērķi sazinās pa e-pastu, tālruni vai īsziņu, lai maldinātu personu un liktu tai sniegt sensitīvus datus par tās kontiem

11. **Vai Jūs zināt par šiem pikšķerēšanas veidiem?**

1) Spray and pray – ļaunprātīgi e-pasti tiek nosūtīti uz jebkuru e-pasta adresi, mēģinot nozagt sensitīvu informāciju;
2) Avansa maksājums (Advanced fee scam) - izplatīta krāpšana, kas saistīta ar Nigērijas valstspiederīgajiem, piemēram, palīdzības pieprasīšana lielas naudas summas pārskaitīšanā;
3) Viltus personība (Cat phishing) - kāda cilvēka ievilināšana attiecībās, uzdodoties par iedomātu tiešsaistes personu;
4) Harpunēšana (Spear fishing) - ļaunprātīgi e-pasti, kas ir īpaši izstrādāti un nosūtīti konkrētai personai vai organizācijai, mēģinot nozagt sensitīvu informāciju;
5) Vaļu medības (Whaling) - mēģinājums nozagt sensitīvu informāciju, bieži tiek mērķēts uz augstāko vadību;
6) Vishing - attiecas uz pikšķerēšanu, kas notiek pa tālruni;
7) Smishing - attiecas uz pikšķerēšanu, izmantojot īsziņas, nevis e-pastus, lai uzrunātu personas;
8) Klonēšanas uzbrukums (Clone Phishing) – pikšķerēšanas veids, kura ietvaros tiek izmantoti īsti un iepriekš nosūtīti e-pasti, lai izveidotu identisku e-pastu ar ļaunprātīgu saturu;
9) Satura ievietošana (Content injection) - kibernoziedznieki uzlauž pazīstamu vietni un ievieto viltotu vietnes pieteikšanās lapu vai uznirstošo logu, kas vietnes apmeklētājus novirza uz viltotu vietni.
10) Ļaunprātīga reklāma (Malvertising) - šis pikšķerēšanas veids izmanto tiešsaistes reklāmas vai uznirstošos logus, lai piespiestu cilvēkus noklikšķināt uz saites, kas izskatās īsta, bet vēlāk instalē datorā ļaunprogrammatūru.

	Nezinu	Nedaudz zinu	Viduvējas zināšanas	Labi zinu	Ļoti labi zinu
Spray and Pray					
Advanced fee scam					
Cat phishing					
Spear phishing					
Whaling					
Whishing					

Funded by the Erasmus+ Programme of the European Union

Smishing					
Clone phishing					
Content Injection					
Malvertising					

12. Kādas sekas varētu rasties pēc veiksmīga pikšķerēšanas uzbrukuma personai vai uzņēmumam?

	Noteikti nē	Visticamāk nē	Iespējams	Ļoti iespējams	Noteikti
Identitātes zādzība					
Krāpšana ar kredītkartēm					
Sensitīvu datu zādzība					
Lietotājvārdu un paroļu zaudēšana					
Ļaunprātīgas programmatūras un izspiedējvīrusa instalēšana					
Intelektuālā īpašuma zaudēšana					
Klienta informācijas zādzība					
Līdzekļu zādzība no uzņēmuma un klientu kontiem					
Piekļuve sistēmām, lai veiktu turpmākus uzbrukumus					
Dati tiek pārdoti noziedzīgām trešām personām					
Kaitējums reputācijai					

3. DAĻA - Personīgā pieredze

13. Vai esat kādreiz baidījies e-pastā vai ziņojumā atvērt saiti, domājot, ka tā varētu būt viltota?

1 - Nekad
2 - Reti
3 - Dažreiz
4 - Bieži
5 - Vienmēr

14. Vai Jūs kopumā baidāties kļūt par pikšķerēšanas uzbrukuma mērķi?

1 - Nekad
2 - Reti
3 - Dažreiz
4 - Bieži

Funded by the Erasmus+ Programme of the European Union

5 - Vienmēr

15. Vai kādreiz esat kļuvis par pikšķerēšanā cietušo?

Apraksts: Šeit domājam, vai esat kādreiz noklikšķinājis uz ļaunprātīgas saites/ pielikuma, iesniedzis sensitīvus datus u.t.t.

- Jā
- Nē

4. DAĻA - Pikšķerēšanas uzbrukums (tikai tiem, kuri uz 15. jautājumu atbildēja "jā")

16. Kā kļuvāt par pikšķerēšanas upuri?

- Noklikšķinot uz e-pastā vai ziņojumā iekļautas saites
- Atbildot uz e-pastu vai ziņojumu un sniedzot sensitīvu informāciju (piemēram, pieteikšanās datus)
- Atverot pielikumu e-pastā
- Sniedzot sensitīvu informāciju pa tālruni
- Cits.....

17. Kāpēc, Jūsuprāt, tas notika?

- Es steidzos
- Es biju apjucis / nepievērsu uzmanību
- Es biju saspringts / nervozs
- Mani iebiedēja
- Es biju ziņkārīgs
- Es biju aizrāvies / laimīgs (piemēram, domāju, ka ieguvu balvu)
- Es gribēju palīdzēt
- Cits.....

5. DAĻA - Pikšķerēšanas uzbrukuma atpazīšana

19. Cik svarīgi ir šie kritēriji, lai atpazītu aizdomīgu e-pastu?

	Nav svarīgi	Nedaudz svarīgi	Vidēji svarīgi	Svarīgi	Ļoti svarīgi
Vispārīga uzruna e-pastā (piem., cienījamais klient)					
Sūtītājs lūdz apstiprināt / sniegt sensitīvu informāciju (pieteikšanās akreditācijas datus, bankas rekvizītus) pa e-pastu vai tālruni					
Sūtītāja domēns (e-pasts) neizskatās īsts (neatbilst organizācijai, satur slēptu pareizrakstības kļūdu, papildu ciparus, burtus tajā utt.)					
E-pastā iegultās saites nav tādas pašas kā īstā hipersaite					
E-pasta adresēs, saitēs un domēnu nosaukumos ir redzamas neatbilstības					
E-pasts satur negaidītu/ neparastu pielikumu					

Funded by the Erasmus+ Programme of the European Union

E-pastā ir pareizrakstības un gramatikas kļūdas					
E-pasta rakstīšanas stils neatbilst personai / uzņēmumam, kas parasti nosūta šādus e-pastus					
Nav paraksta vai kontaktinformācijas					
E-pasta ziņojums rada steidzamības izjūtu, prasa tūlītēju rīcību un liek krist panikā un izjust stresu					
Pats ziņojums rada zinātkāri, jānoskaidro vairāk.					
E-pasta ziņojums ir pārāk labs, lai būtu patiess					

20. Cik svarīgi ir šie kritēriji, lai atpazītu aizdomīgu īsziņu / tālruņa zvanu?

	Nav svarīgi	Nedaudz svarīgi	Vidēji svarīgi	Svarīgi	Ļoti svarīgi
Neparasti garš tālruņa numurs					
Numurs ar atšķirīgu valsts kodu					
Sūtītājs / zvanītājs lūdz pārbaudīt informāciju vai sniegt sensitīvu informāciju vai nosūtīt naudu					
Zvanītājs neiepazīstina ar sevi (vārds, amats, uzņēmums)					
Zvanītājs neuzrunā vārdā, uzvārdā					
Ziņojumā iekļauta saite					
Jūs neesat sūtītāja / zvanītāja (uzņēmuma) klients					
Jums nav nekādu attiecību vai biznesa attiecību ar sūtītāju / zvanītāju					
Ziņojumā ir cits tālruņa numurs, uz kuru zvanīt					
Pareizrakstības un gramatikas kļūdas					
Pats ziņojums satur brīdinājumu (piemēram, konta derīguma termiņš beidzas) un rada spiedienu uz saņēmēju, lai pieņemtu steidzamu lēmumu					

21. Cik svarīgi ir šie kritēriji, lai atpazītu aizdomīgu ziņojumu sociālo mediju kanālos?

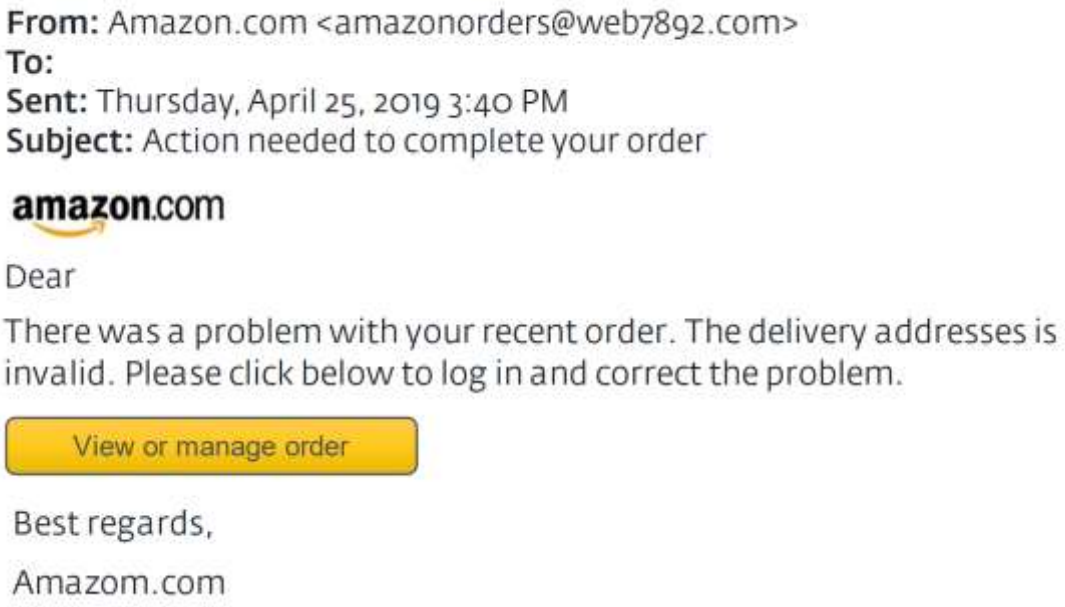
Funded by the Erasmus+ Programme of the European Union

	Nav svarīgi	Nedaudz svarīgi	Vidēji svarīgi	Svarīgi	Ļoti svarīgi
Ziņojumā tiek lūgts sniegt akreditācijas datus vai sensitīvu informāciju					
Ziņojumā tiek prasīta nauda					
Ziņojumā tiek lūgts instalēt kādu programmu					
Ziņojumā iekļauta aizdomīga saite					
Jūs nepazīstat sūtītāju					
Jums nav biznesa attiecību ar sūtītāju					
Sūtītāja sociālo mediju profils izskatās aizdomīgs (piemēram, jauns konts, nav draugu utt.);					
Ziņojumā ir uzmanību piesaistošs nosaukums (piemēram, Jūs neticēsiet šim videoklipam!)					
Ziņojuma stils neatbilst sūtītājam (pārāk formāls / neformāls utt.)					
Pareizrakstības un gramatikas kļūdas					

6. DAĻA - Pikšķerēšanas piemēri

Pikšķerēšanas 1. piemērs

Funded by the Erasmus+ Programme of the European Union



22. Vai augstāk redzamajā attēlā redzams īsts e-pasts vai pikšķerēšanas e-pasts?

- Īsts e-pasts
- Pikšķerēšanas e-pasts

7. DAĻA:

1. piemērs (tikai tad, ja iepriekšējā jautājumā sniegta atbilde "Pikšķerēšanas e-pasts")

23. Kāpēc domājat, ka šis ir pikšķerēšanas e-pasts? Izvēlieties aizdomīgās pazīmes

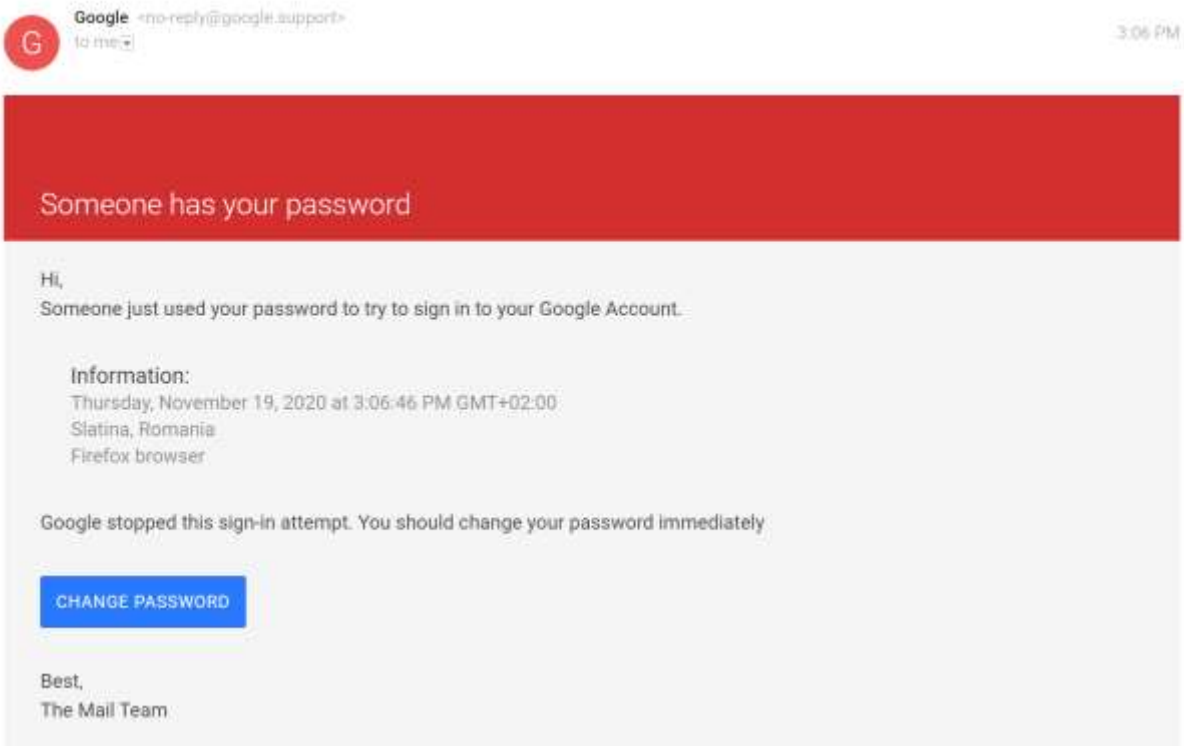
- Nekonkrēta uzruna
- Tiek pieprasīts apstiprināt/ verificēt/ norādīt sensitīvu informāciju
- Sūtītāja domēns / e-pasts
- Aizdomīgas saites
- Neatbilstības e-pasta adresēs, saitēs un domēnu nosaukumos
- Pareizrakstības un gramatikas kļūdas
- Aizdomīgs rakstīšanas stils
- Steidzamības sajūta / nepieciešamība veikt tūlītējas darbības
- Pārāk labi, lai būtu patiesība

Cits.....

8. DAĻA:

Pikšķerēšanas 2. piemērs

Funded by the Erasmus+ Programme of the European Union



24. Vai augstāk redzamajā attēlā redzams īsts e-pasts vai pikšķerēšanas e-pasts?

- Īsts e-pasts
- Pikšķerēšanas e-pasts

9. DAĻA:

2. piemērs (tikai tad, ja iepriekšējā jautājumā sniegta atbilde "Pikšķerēšanas e-pasts")

25. Kāpēc domājat, ka šis ir pikšķerēšanas e-pasts? Izvēlieties aizdomīgās pazīmes

- Nekonkrēta uzruna
- Tiek pieprasīts apstiprināt/ verificēt/ norādīt sensitīvu informāciju
- Sūtītāja domēns / e-pasts
- Aizdomīgas saites
- Neatbilstības e-pasta adresēs, saitēs un domēnu nosaukumos
- Pareizrakstības un gramatikas kļūdas
- Aizdomīgs rakstīšanas stils
- Steidzamības sajūta / nepieciešamība veikt tūlītējas darbības
- Pārāk labi, lai būtu patiesība

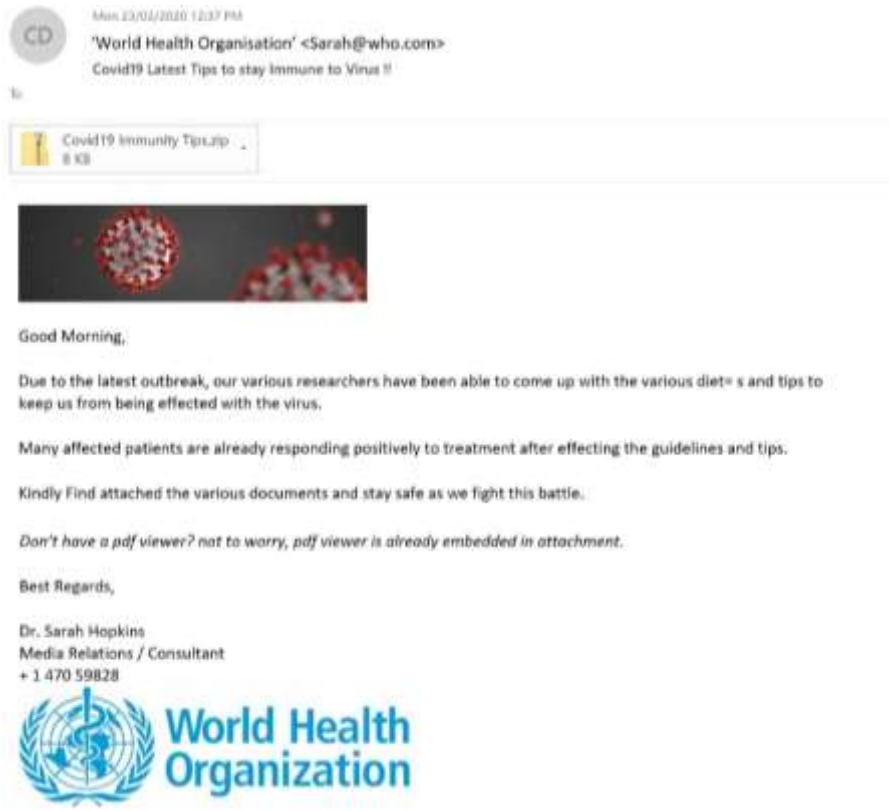
Cits.....

10. DAĻA:

Pikšķerēšanas 3. piemērs

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)



26. Vai augstāk redzamajā attēlā redzams īsts e-pasts vai pikšķerēšanas e-pasts?

- Īsts e-pasts
- Pikšķerēšanas e-pasts

11. DAĻA:

3. piemērs (tikai tad, ja iepriekšējā jautājumā sniegta atbilde "Pikšķerēšanas e-pasts")

27. Kāpēc domājat, ka šis ir pikšķerēšanas e-pasts? Izvēlieties aizdomīgās pazīmes

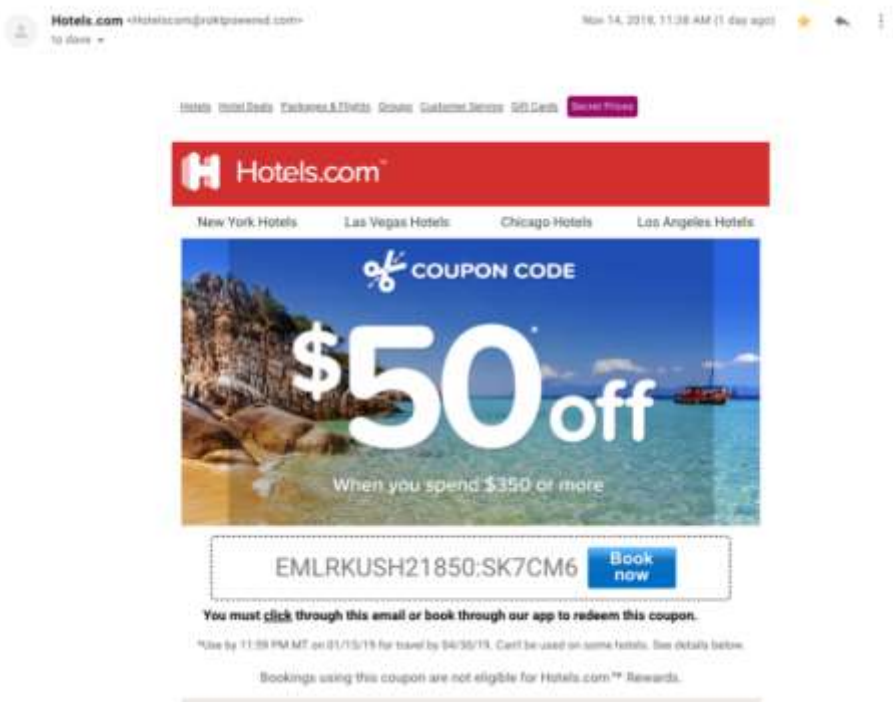
- Nekonkrēta uzruna
- Tiek pieprasīts apstiprināt/ verificēt/ norādīt sensitīvu informāciju
- Sūtītāja domēns / e-pasts
- Aizdomīgas saites
- Neatbilstības e-pasta adresēs, saitēs un domēnu nosaukumos
- Pareizrakstības un gramatikas kļūdas
- Aizdomīgs rakstīšanas stils
- Steidzamības sajūta / nepieciešamība veikt tūlītējas darbības
- Pārāk labi, lai būtu patiesība

Cits.....

12. DAĻA:

Pikšķerēšanas 4. piemērs

Funded by the Erasmus+ Programme of the European Union



28. Vai augstāk redzamajā attēlā redzams īsts e-pasts vai pikšķerēšanas e-pasts?

- Īsts e-pasts
- Pikšķerēšanas e-pasts

13. DAĻA:

4. piemērs (tikai tad, ja iepriekšējā jautājumā sniegta atbilde "Pikšķerēšanas e-pasts")

29. Kāpēc domājat, ka šis ir pikšķerēšanas e-pasts? Izvēlieties aizdomīgās pazīmes

- Nekonkrēta uzruna
- Tiek pieprasīts apstiprināt/ verificēt/ norādīt sensitīvu informāciju
- Sūtītāja domēns / e-pasts
- Aizdomīgas saites
- Neatbilstības e-pasta adresēs, saitēs un domēnu nosaukumos
- Pareizrakstības un gramatikas kļūdas
- Aizdomīgs rakstīšanas stils
- Steidzamības sajūta / nepieciešamība veikt tūlītējas darbības
- Pārāk labi, lai būtu patiesība

Cits.....

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)

14. DAĻA:

Pikšķerēšanas 5. piemērs

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. Vai augstāk redzamajā attēlā redzams īsts e-pasts vai pikšķerēšanas e-pasts?

- Īsts e-pasts
- Pikšķerēšanas e-pasts

15. DAĻA:

5. piemērs (tikai tad, ja iepriekšējā jautājumā sniegta atbilde "Pikšķerēšanas e-pasts")

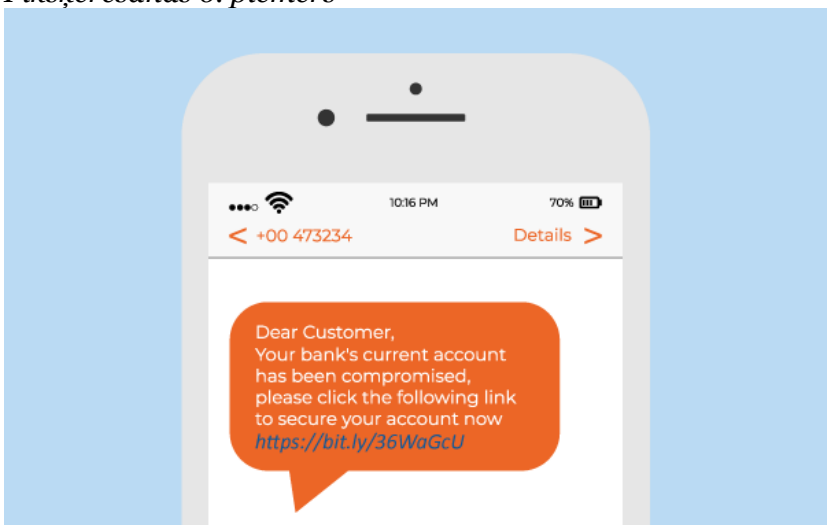
31. Kāpēc domājat, ka šis ir pikšķerēšanas e-pasts? Izvēlieties aizdomīgās pazīmes

- Nekonkrēta uzruna
- Tiek pieprasīts apstiprināt/ verificēt/ norādīt sensitīvu informāciju
- Sūtītāja domēns / e-pasts
- Aizdomīgas saites
- Neatbilstības e-pasta adresēs, saitēs un domēnu nosaukumos
- Pareizrakstības un gramatikas kļūdas
- Aizdomīgs rakstīšanas stils
- Steidzamības sajūta / nepieciešamība veikt tūlītējas darbības
- Pārāk labi, lai būtu patiesība

Cits.....

16. DAĻA:

Pikšķerēšanas 6. piemērs



Funded by the Erasmus+ Programme of the European Union

32. Vai augstāk redzamajā attēlā redzama īsta īsziņa vai pikšķerēšanas īsziņa?

- Īsta īsziņa
- Pikšķerēšanas īsziņa

17. DAĻA:

6. piemērs (tikai tad, ja iepriekšējā jautājumā sniegta atbilde "Pikšķerēšanas īsziņa")

33. Kāpēc domājat, ka šī ir pikšķerēšanas īsziņa? Izvēlieties aizdomīgās pazīmes

- Nekonkrēta uzruna
- Tiek pieprasīts apstiprināt/ verificēt/ norādīt sensitīvu informāciju
- Sūtītāja domēns / e-pasts
- Aizdomīgas saites
- Neatbilstības e-pasta adresēs, saitēs un domēnu nosaukumos
- Pareizrakstības un gramatikas kļūdas
- Aizdomīgs rakstīšanas stils
- Steidzamības sajūta / nepieciešamība veikt tūlītējas darbības
- Pārāk labi, lai būtu patiesība

Cits.....

18. DAĻA - Pašnovērtējums: Kritiskā domāšana

34. Izmantojiet skalu no 1 līdz 5, lai novērtētu:

1) Nekad
2) Reti
3) Dažreiz
4) Ļoti bieži
5) Vienmēr

	Nekad	Reti	Dažreiz	Ļoti bieži	Vienmēr
Vai Jūs parasti uzticaties ziņojumiem, kas šķietami saņemti no svarīga sūtītāja vai izskatās svarīgi?					
Vai, atverot e-pastu/ziņojumu, pietiekami koncentrējaties un pievēršat uzmanību detaļām?					
Vai pievēršat uzmanību tam, uz kā klikšķināt, kad saņemat e-pastu/ ziņojumu ar saiti/ pielikumu?					

35. Kad saņemat aizdomīga izskata e-pastu, vai Jūs novērtējat:

	Nekad	Reti	Dažreiz	Ļoti bieži	Vienmēr
Kas ir sūtītājs					
Kāds ir sūtītāja e-pasts					
Kāds ir e-pasta temats					
E-pasta stils (formāls, neformāls, izmantotie vārdi)					

Funded by the Erasmus+ Programme of the European Union

Attēli					
Gramatikas un pareizrakstības kļūdas					
Saites/pielikumi					
Paraksts un amats					

36. Kad saņemat aizdomīga izskata e-pastu / ziņojumu, vai, pamatojoties uz pierādījumiem, varat iztēloties sava lēmuma iespējamās sekas?

- Nekad
- Reti
- Dažreiz
- Ļoti bieži
- Vienmēr

37. Kad saņemat aizdomīga izskata e-pastu / ziņojumu, vai Jūs varat izdarīt secinājumus, pamatojoties uz pierādījumiem?

- Nekad
- Reti
- Dažreiz
- Ļoti bieži
- Vienmēr

19. DAĻA - Izvairīšanās no pikšķerēšanas uzbrukumiem

38. Kāpēc pikšķerēšanas uzbrukumi ir veiksmīgi? (Izvēlieties 5 galvenos iemeslus)

- Uzbrucēji patiešām labi spēj atveidot īstu uzņēmumu ziņojumus un e-pastus, padarot tos ļoti ticamus un pārliecinošus
- Uzbrucēji izmanto cilvēka dabu, viņi paļaujas uz mijiedarbību un spēlējas ar cilvēku emocijām un vajadzībām
- Uzbrucēji var viegli piekļūt personas datiem un informācijai par konkrēto personu vai uzņēmumu sociālo mediju / uzņēmuma tīmekļa vietnēs, presē utt.
- Uzbrucēji kļūst arvien progresīvāki, tiek atlasītas konkrētas personas, izmantojot e-pastos ļoti personalizētu un specifisku informāciju
- Cilvēki nepievērš pietiekamu uzmanību / ir nezinoši
- Cilvēki neapzinās / nezina par šādiem uzbrukumiem un to novēršanu
- Cilvēki izmanto novecojušu programmatūru
- Organizācijas / uzņēmumi nedara pietiekami daudz, lai novērstu šos uzbrukumus
- Kiberdrošības un pikšķerēšanas jomā trūkst apmācības
- Pikšķerēšanas rīki ir lēti un plaši izplatīti
- Pati ļaunprogrammatūra kļūst arvien sarežģītāka
- Cits.....

39. Kādas emocijas, vajadzības un vēlmes uzbrucēji parasti izmanto?

- Bailes
- Bažas / trauksme
- Panika
- Ziņkārība
- Mantkārība
- Motivācija (dāvana / bezmaksas kupons)
- Vēlme pēc emocionāla piepildījuma
- Uzticēšanās

Funded by the Erasmus+ Programme of the European Union

- Izpalīdzība
- Cits.....

40. Kādas darbības ir svarīgi veikt, lai izvairītos no pikšķerēšanas uzbrukumiem?

	Nav svarīgi	Nedaudz svarīgi	Vidēji svarīgi	Svarīgi	Ļoti svarīgi
Izmantot atjauninātu pārlūku					
Izmantojot atjauninātu operētājsistēmu					
Sekot līdzi jaunākajai pieejamajai programmatūrai un rīkiem					
Drošības programmatūras izmantošana					
Nepublicēt sensitīvu informāciju par sevi sociālajos medijos					
Izmantot daudzfaktoru autentifikāciju/ bieži mainīt paroles					
Izmantošana tīmekļa filtru ļaunprātīgu vietņu bloķēšanai					
Regulāras kiberdrošības apmācības / semināri					
Izstrādāt drošības politiku					
Šifrēt visu sensitīvo uzņēmuma informāciju					
Ievērot piesardzību, atverot e-pastus/ ziņojumus/ atbildot uz tālruni					
Vēlreiz pārbaudīt visu svarīgo informāciju (sūtītāja e-pastu, saites, pielikumus utt.)					
Uzticēties saviem instinktiem un pielietot spriestspēju					
Nepārtraukti izglītoties par šo tēmu					

41. Cik lielā mērā Jūs piekrītat šādiem apgalvojumiem: Es jūtos pārliecināts par:

	Vispār neesmu pārliecināts	Drīzāk neesmu pārliecināts	Jūtos gana pārliecināts	Jūtos nedaudz pārliecināts	Esmu pilnīgi pārliecināts
Kiberdrošības / pikšķerēšanas terminoloģijas pārzināšana un izmantošana					
Attiecīgas un uzticamas informācijas atrašana tiešsaistē					

Funded by the Erasmus+ Programme of the European Union

Pareizu darbību / pasākumu veikšana pikšķerēšanas uzbrukumu novēršanai					
Pikšķerēšanas uzbrukumu identificēšana					
Manas programmatūras / programmu atjaunināšana					
Daudzfaktoru autentifikācijas izmantošana					
Drošības programmatūras izmantošana					
Izmantošana tīmekļa filtru ļaunprātīgu vietņu bloķēšanai					
Šifrēt visu sensitīvo uzņēmuma informāciju					

42.Citi komentāri / ieteikumi

Funded by the Erasmus+ Programme of the European Union