Funded by the Erasmus+ Programme of the European Union

Pārskats par kiberuzbrukumu izpratni un apiešanos ar tiem

Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana

Kā atpazīt pikšķerēšanas uzbrukumus?

Safeguarding against Phishing in the age of 4th Industrial Revolution
www.cyberphish.eu
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CyberPhish
Safeguarding your digital future

Apmācību mērķis

Izskaidrot e-drošības jēdzienu un to, cik svarīgi ir pieņemt proaktīvu pieeju kiberdraudiem, izmantojot kibernētiskās higiēnas koncepciju

Atpazīt un rīkoties ar kiberuzbrukumiem

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kursantu darba slodze

Lekcija	2 st.
Audio un video materiāli	2 st.
Pētījumi	2 st.
Papildu lasīšana	4 st.
Sagatavošanās eksāmenam	2 st.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Saturs


2
URL saišu saprašana
1
Pikšķerēšanas saprašana
Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana
3
Aizdomīgo momentu atpazīšana
4
Kritiskā domāšana

Saturs


2
URL saišu saprašana
Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana
1
Pikšķerēšanas saprašana
3
Aizdomīgo momentu atpazīšana
4
Kritiskā domāšana

Kas ir pikšķerēšanas uzbrukums?

Pikšķerēšana jeb personas datu izmānīšana *ir sociālās inženierijas krāpniecība, kas var izraisīt datu zudumu, reputācijas bojājumus, identitātes zādzību, naudas zaudējumus un daudzus citus negatīvus efektus indivīdiem un organizācijām. Pikšķerēšanas krāpniecība parasti sākas ar e-pasta ziņojumu, kurā tiek mēģināts iegūt potenciālā upura uzticību un pārliecināt viņu veikt uzbrucējam vēlamās darbības.*

[Abrošans *[Abroshan]*, 2021. gads]

Funded by the Erasmus+ Programme of the European Union

Pikšķerēšanas avots

Google fotoattēls

- E-pasts
- Mājaslapas
- Sociālie mediji
- Mobilās ierīces (SMS, balss)
- *Jebkura saziņas forma...*

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

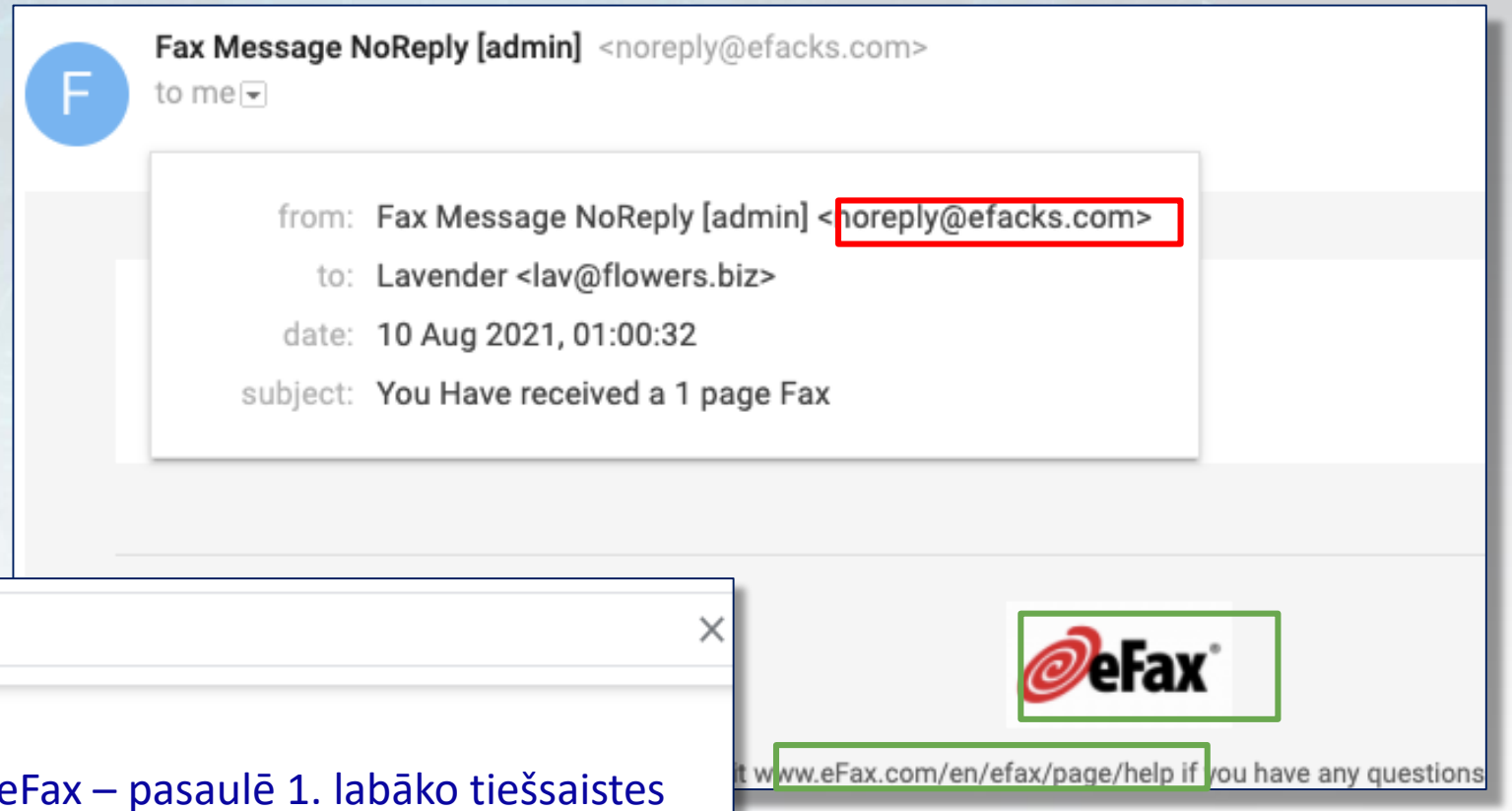
Pikšķerēšanas ziņojumu anatomija

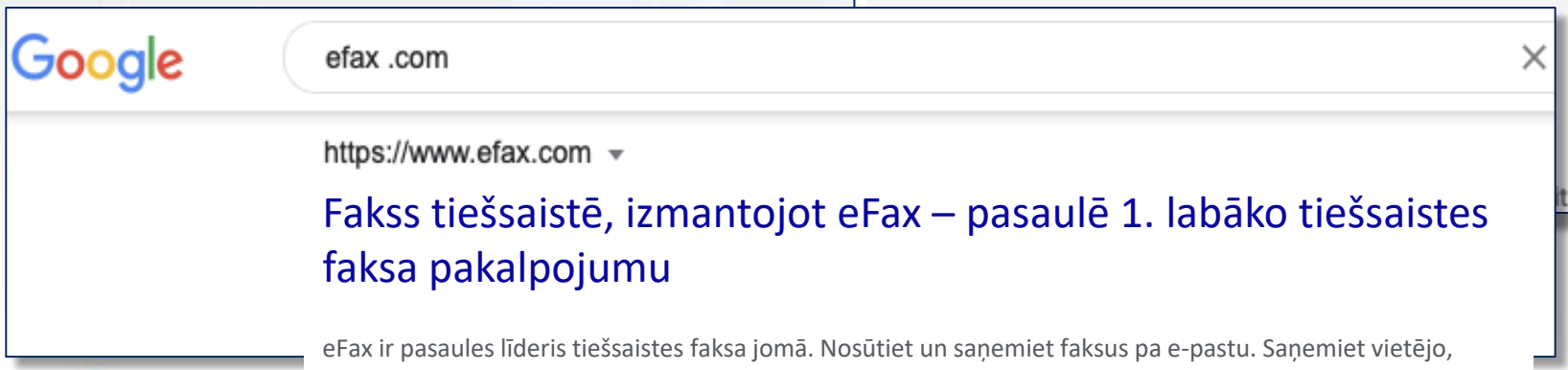
- Ziņojuma avots
  - *kas nosūta man šo ziņu?*
- Ziņojuma saturs
  - *kas ir ietvers ziņas saturā?*
- Hipersaites/pielikumi
  - *Uz ko vēl šajā ziņā sniegtas saites?*

Fotoattēls no istockphoto.com

Ziņojuma avots

- Pikšķerēšana var būt viltīga, izmantojot līdzīgu sūtītāja e-pastu.





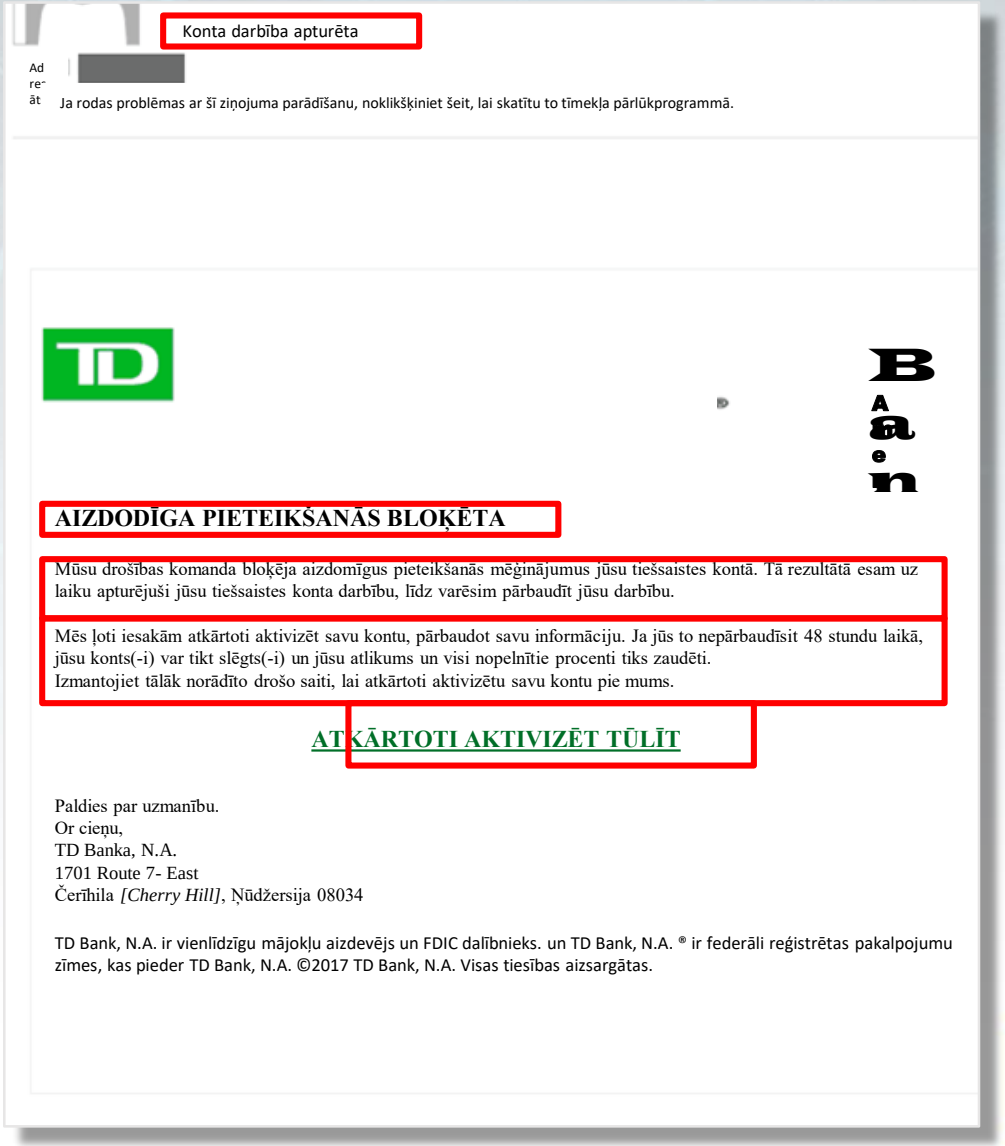
Fotoattēli no Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Ziņojuma saturs

- Maldināšana ar bailēm, steidzamību, autoritāti, alkatību, draudzību, palīdzību un izmisumu



Konta darbība apturēta

Ad re- āt

Ja rodas problēmas ar šī ziņojuma parādīšanu, noklikšķiniet šeit, lai skatītu to tīmekļa pārlūkprogrammā.

TD

B A a e n

AIZDODĪGA PIETEIKŠANĀS BLOĶĒTA

Mūsu drošības komanda bloķēja aizdomīgus pieteikšanās mēģinājumus jūsu tiešsaistes kontā. Tā rezultātā esam uz laiku apturējuši jūsu tiešsaistes konta darbību, līdz varēsim pārbaudīt jūsu darbību.

Mēs ļoti iesakām atkārtoti aktivizēt savu kontu, pārbaudot savu informāciju. Ja jūs to nepārbaudīsit 48 stundu laikā, jūsu konts(-i) var tikt slēgts(-i) un jūsu atlikums un visi nopelnītie procenti tiks zaudēti.
Izmantojiet tālāk norādīto drošo saiti, lai atkārtoti aktivizētu savu kontu pie mums.

ATKĀRTOTI AKTIVIZĒT TŪLĪT

Paldies par uzmanību.
Or cieņu,
TD Banka, N.A.
1701 Route 7- East
Čerīhila *[Cherry Hill]*, Ņūdžersija 08034

TD Bank, N.A. ir vienlīdzīgu mājokļu aizdevējs un FDIC dalībnieks. un TD Bank, N.A. ® ir federāli reģistrētas pakalpojumu zīmes, kas pieder TD Bank, N.A. ©2017 TD Bank, N.A. Visas tiesības aizsargātas.

Fotoattēls no Sonicwall Phishing Test

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Ziņojuma saturs

- Maldināšana ar bailēm, steidzamību, autoritāti, alkatību, draudzību, palīdzību un izmisumu

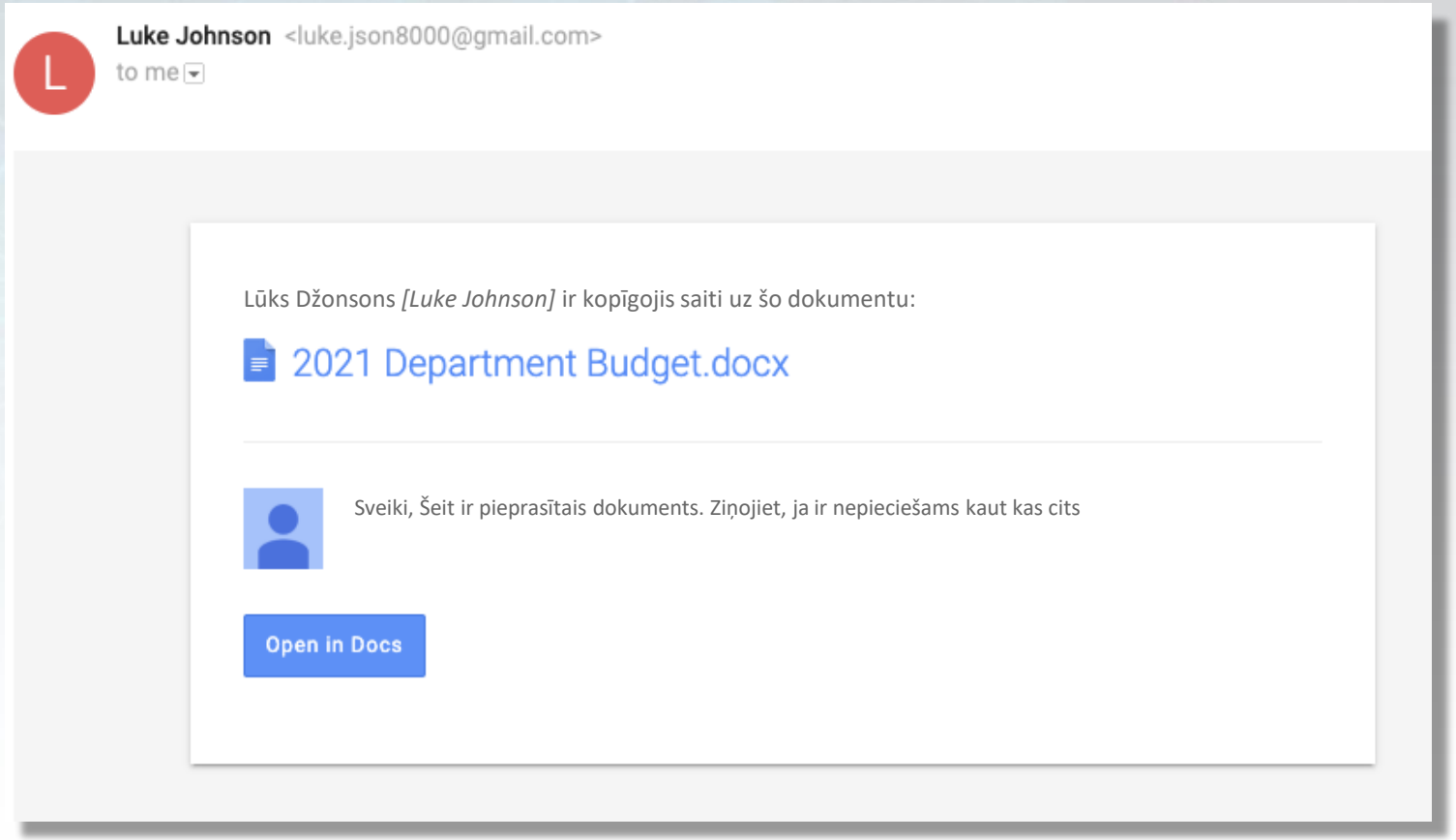
Fotoattēls no Sonicwall Phishing Test

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Hipersaites/pielikums

- Pielikumos var būt ietverti dažāda veida faili, kas var būt ļaunprātīgi
- Hipersaites norāda faila atrašanās vietu tīmeklī un var novirzīt upurus uz ļaunprātīgām vietnēm vai lejupielādēt ļaunprātīgus failus.



Fotoattēli no Jigsaw, Google.

CyberPhish
Safeguarding your digital future

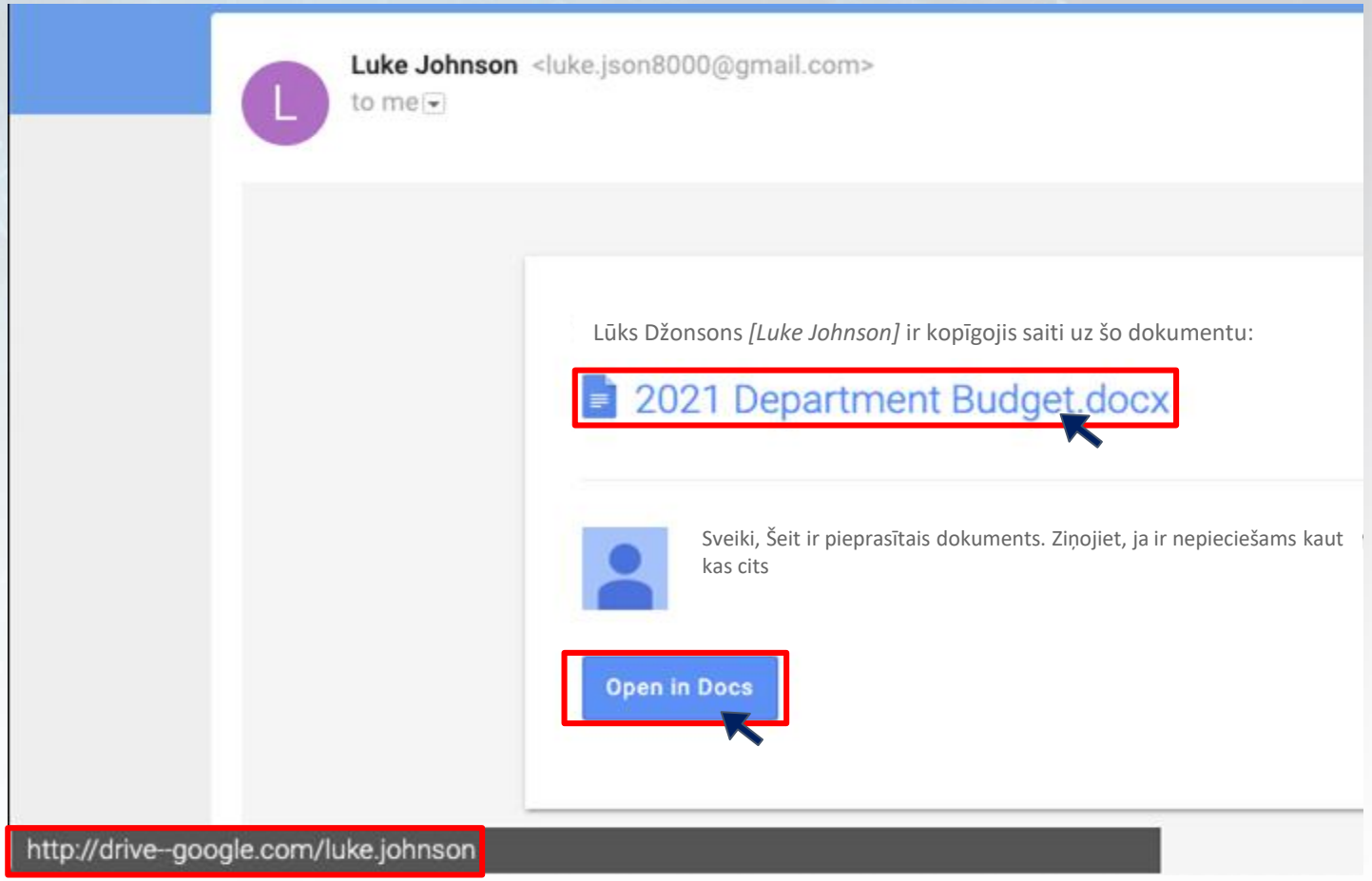
Funded by the Erasmus+ Programme of the European Union

Hipersaites/pielikums

- Novietojiet peles kursoru virs šīm hipersaitēm, lai atklātu to URL saiti.

- Parādītais URL ir nedroša Google diska domēna imitācija

http*://drive--google.com/luke.johnson*



Fotoattēli no Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

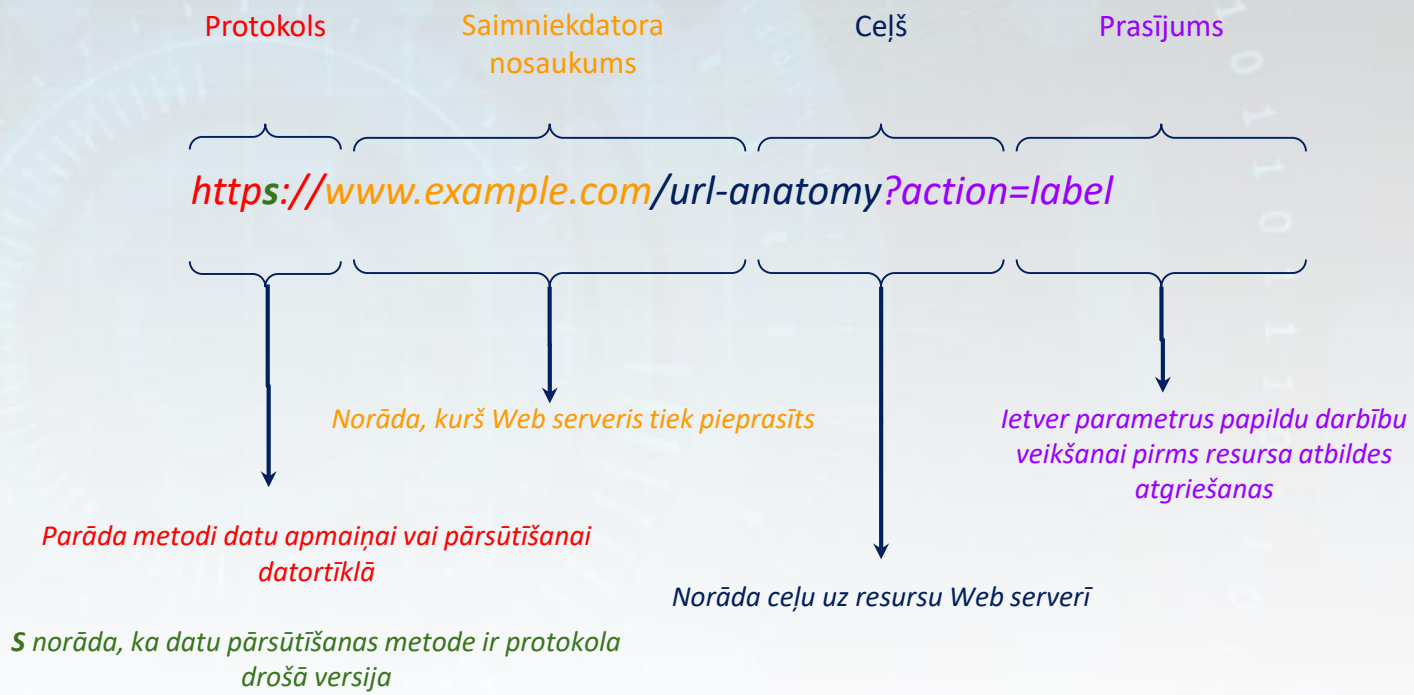
Saturs

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

URL saišu saprašana

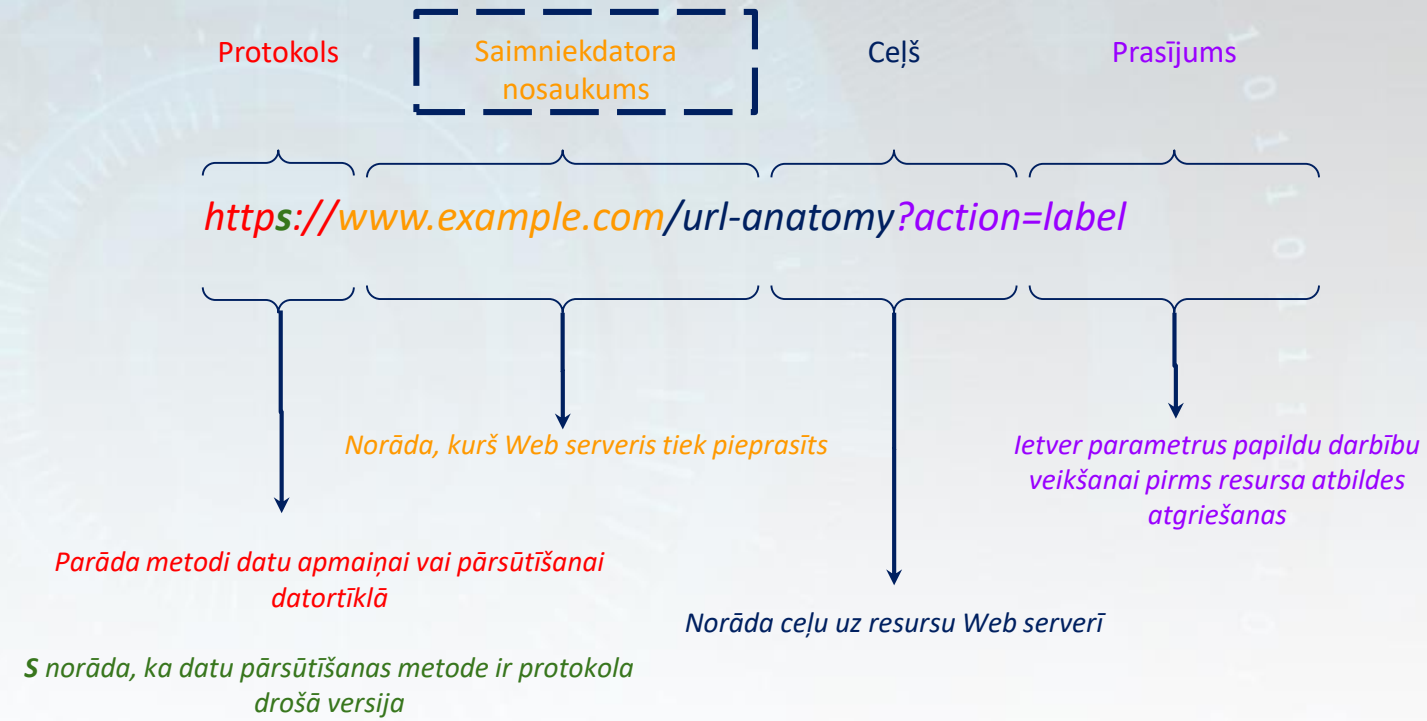
- Uniform Resource Locator (URL) ir noteikta unikāla resursa adrese tīmeklī.



https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL
Protokols, vienkārša objektu piekļuve. "URL." (2007. gads).

URL saišu saprašana

- Uniform Resource Locator (URL) ir noteikta unikāla resursa adrese tīmeklī.

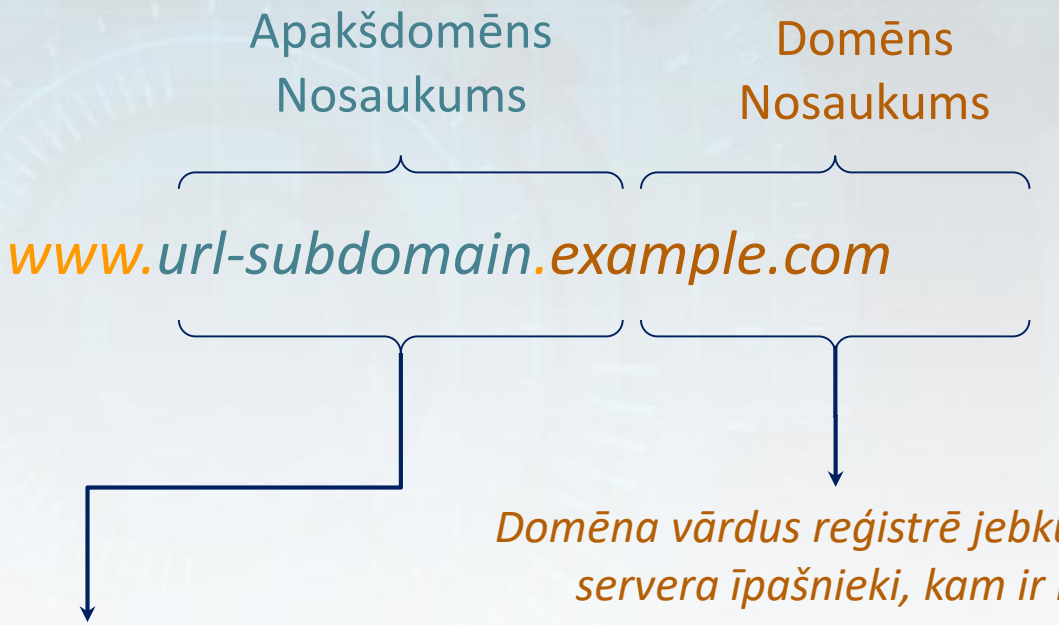


https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL
Protokols, vienkārša objektu piekļuve. "URL." (2007. gads).

Funded by the Erasmus+ Programme of the European Union

URL saišu saprašana

- Vietrādī URL resursdatora nosaukums var ietvert vairākus apakšdomēnu nosaukumus



Apakšdomēnu nosaukumi ir saistīti ar atbilstošo domēna nosaukumu un norāda resursa sadaļu, kas pieejama, izmantojot domēna nosaukumu.

https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL
Protokols, vienkārša objektu piekļuve. "URL." (2007. gads).

Funded by the Erasmus+ Programme of the European Union

URL saišu saprašana

Pikšķerēšana ietvaros bieži vien tiek mēģināts apmānīt upurus ar URL vietrāžiem.

http://amazon.com.mailru382.co/packagedelivery/2017Dk25RE3

Protokols	*http*
Saimniekdatora nosaukums	*amazon.com.mailru382.co*
Ceļš	*/packagedelivery/2017Dk25RE3*
Domēna nosaukums	*mailru382.co*
Apakšdomēna vienums Nr. 1	com
Apakšdomēna vienums Nr. 2	*amazon*

Funded by the Erasmus+ Programme of the European Union

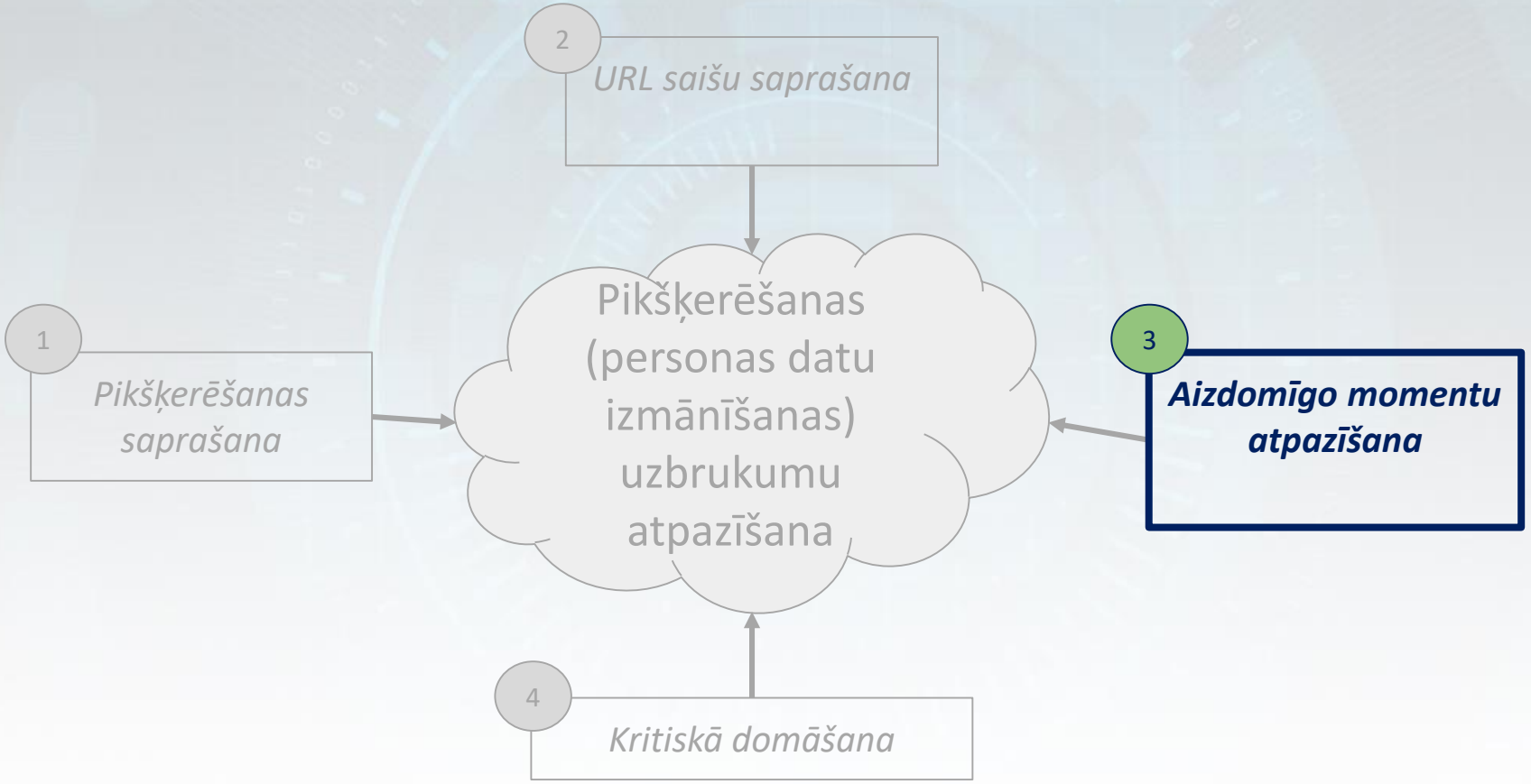
URL saišu saprašana

Citi triki ar URL saitēm ...	Piemērs
• URL protokolam trūkst drošā protokola indikatora.	URL izmantots *http*, nevis *https*
• Domēns ir acīmredzami līdzīgs labi zināmam domēnam, taču patiesībā atšķiras.	*google.com* nepareizi rakstīts kā *googgle.com*
• Sarežģīts domēna nosaukums, lai maldinātu un mulsinātu upuri, piemēram, IP adrese, heksa vai decimālzīmes, simbols domēnā.	IP adrese - http://20.85.220.142/telas/caixa/ Simboli - https://epic.app/#con@sceneworld.org Decimālzīmes - http://2130706433/evil.com
• URL var ietvert labi zināmu domēna nosaukumu, taču tas nepieder legālam avotam.	"*Instagram*" ietverts adresē *http://instagramsupport.it/*

Rupa D. C. C. [Rupa, D.C.C.], Srivastava G. [Srivastava, G.], Batačaraja S. [Bhattacharya, S.], Redijs P. [Reddy, P.], Gadekalu T. R. R. [Gadekallu, T.R.R.] (2021. gada augusts)

Funded by the Erasmus+ Programme of the European Union

Saturs



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Aizdomīgo momentu atpazīšana

- Legāli e-pasta avoti (t.i., uzņēmumi) nepieprasa jūsu sensitīvo informāciju pa e-pastu

SUSTAINABLE DEVELOPMENT GOALS

Izglītības darbinieka stipendija **USD 950,000.00 (deviņi simti piecdesmit tūkstošu dolāru)** apmērā ir jums piešķirta no Apvienoto Nāciju Organizācijas. Apvienoto Nāciju varas iestādes ir nolēmušas jums piedāvāt šo stipendiju kā daļu no globālā mērķa palīdzēt izglītības darbiniekiem un studentiem Covid-19 epidēmijas laikā.

Ilgtspējīgas attīstības mērķi (SDG) radās Apvienoto Nāciju Organizācijas konferencē par ilgtspējīgu attīstību Riodežaneiro 2012. gadā. Mērķis bija izstrādāt universālu mērķu kopumu, kas atbilstu steidzamajām vides, politiskajām un ekonomiskajām problēmām, ar kurām saskaras mūsu pasaule.

Dotāciju līdzekļus padarīs pieejamus ANO korespondējošais birojs, tiklīdz jūs iesniegsiet šo prasību. Apsveicam un pateicamies par jūsu pakalpojumiem.

Iesniedziet prasību un pieprasiet izglītības dotācijas līdzekļus

Vārds, (vidējais vārds), uzvārds (obligāti)
E-pasts (ne-izglītības e-pasts (obligāts))
Tālruņa numurs (obligāts)
Iedzīvotāja un biroja adrese (obligāti)

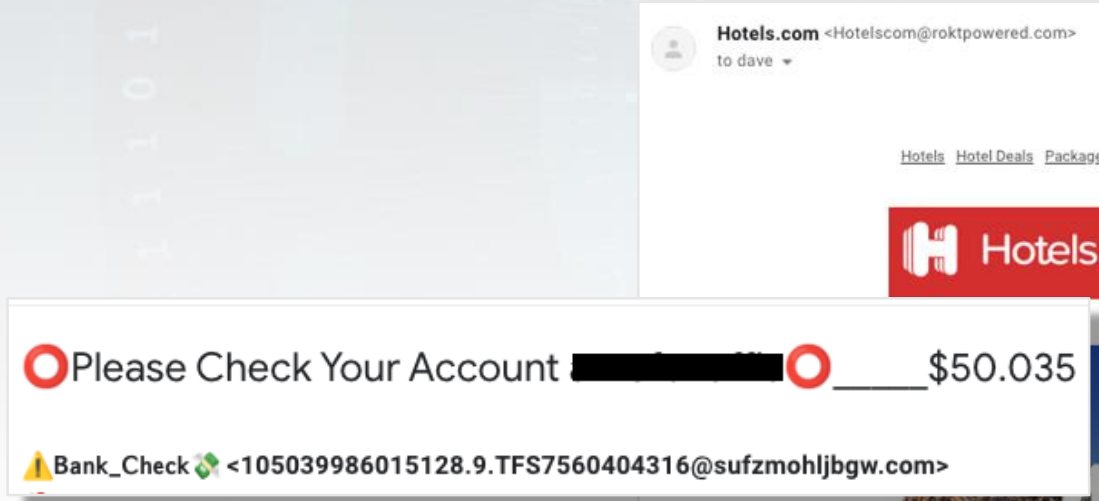
Atbilde uz prasību ir jānosūta no jūsu privātā e-pasta, kas nav izglītības iestādes adrese.

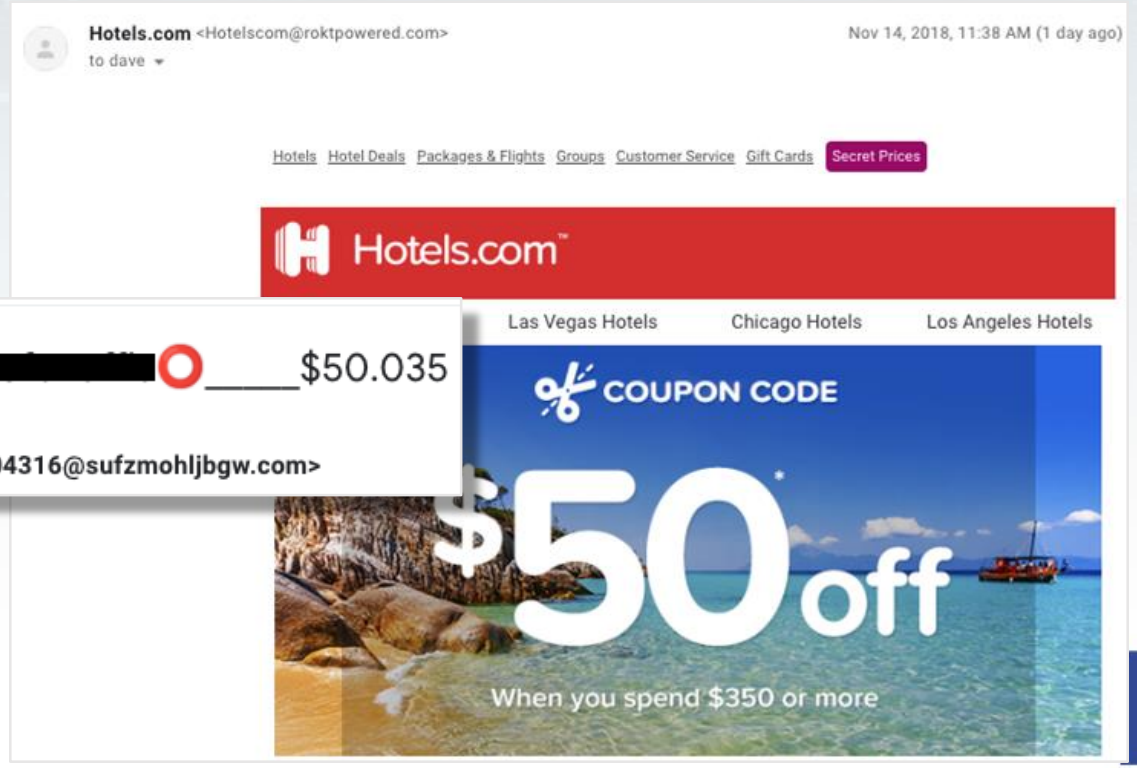
Fotoattēls no Stanford Edu.

Funded by the Erasmus+ Programme of the European Union

Aizdomīgo momentu atpazīšana

- Legāliem e-pasta avotiem parasti nav:
  - sarežģītas e-pasta adreses
  - neatbilstība starp e-pasta adresi, e-pasta domēnu vai e-pasta sūtītāja vārdu





CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Fotoattēls no Security Metrics.

Aizdomīgo momentu atpazīšana

- Leģitīmi e-pasta avoti parasti sauc jūs jūsu vārdā.

Nosūtītājs: Neatbildēt <sarahrk@unm.edu>
Nosūtīšanas datums: Pirmdiena, 2020. gada 8. jūnijs, plkst. 9:03
Tēma: Paziņojums

Sinhronizācijas kļūdas dēļ jūsu pagaidu mapē tiek aizturēts jauns ziņojums.

Sekojiet tālāk norādītajai informācijai, lai piekļūtu neapstiprinātajiem ziņojumiem un izvēlētos, ko ar tiem darīt.

http://www.cs.stanford.edu/msg_panel/

© 2020 cs.stanford.edu

Fotoattēls no Stanford Edu.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Aizdomīgo momentu atpazīšana

- Leģitīmiem e-pasta avotiem nav problēmu ar pareizrakstību un gramatiku.

From: noreply@stanford.edu <noreply@stanford.edu>
Sent: Monday, May 11, 2020 10:59 AM
Subject: stanford.edu Pasaules Covid-19 epidēmijas dē mēs pārbaudām visus mūsu e-pasta konta lietotājus mūsu severī

Mail.stanford.edu Notification

Pasaules Covid-19 epidēmijas dē mēs pārbaudām visus mūsu e-pasta konta lietotājus mūsu severī

Jūsu kontu nepieciešams apstip ripināt un nekavējoties sazinieties ar mums, lejupielādējot pievienoto verifikācijas lietotni mail.stanford.edu, un verificējiet savu e-pasta kontu, laiizvairītos no konta slēgšanas mūsu severī. Ņemiet vērā, ka, ja nelejupielādēsiet mūsu pievienoto lietotni un nepārbaudīsit savu kontu, jūsu koponts tiks automātiski uzskatīts par Covid-19 epidēmijas ietekmētu, un tas novedīs pie jupūsu konta slēgšanas tūlīt pēc mūspu sistēmas verifikācijas.

Epasts INC www.stanford.edu

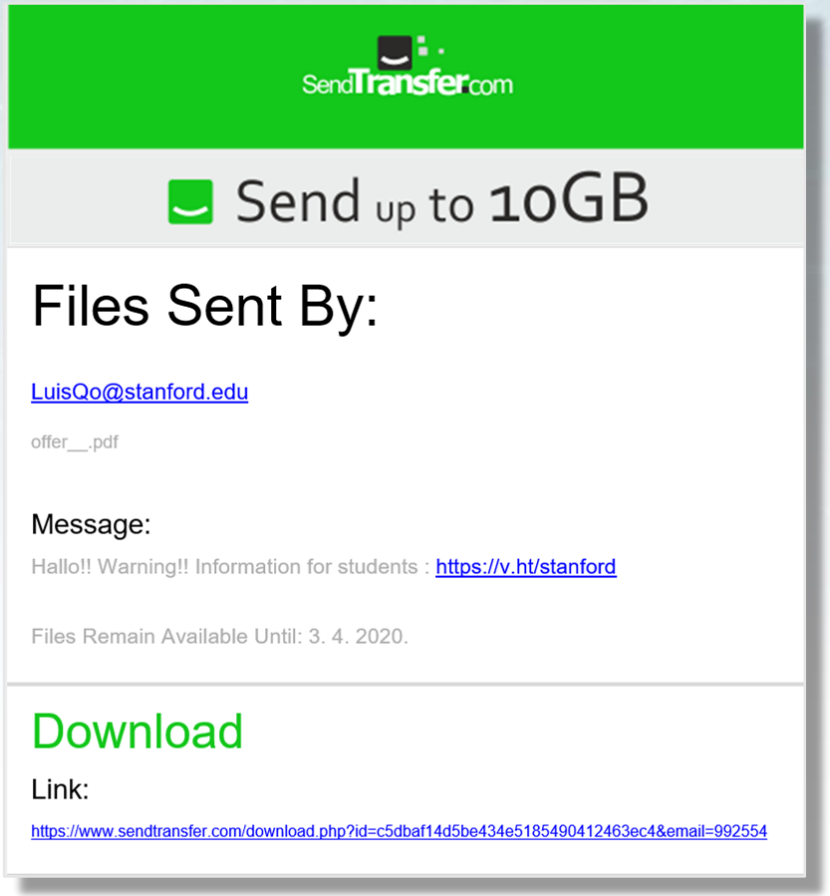
© 2020 Dr ošības e-pastapārbaude Visas tiesības rezervētas

Fotoattēls no Stanford Edu.

Aizdomīgo momentu atpazīšana

- Legāli e-pasta avoti nesūta nevēlamus pielikumus

Fotoattēls no Sonicwall Phishing Test

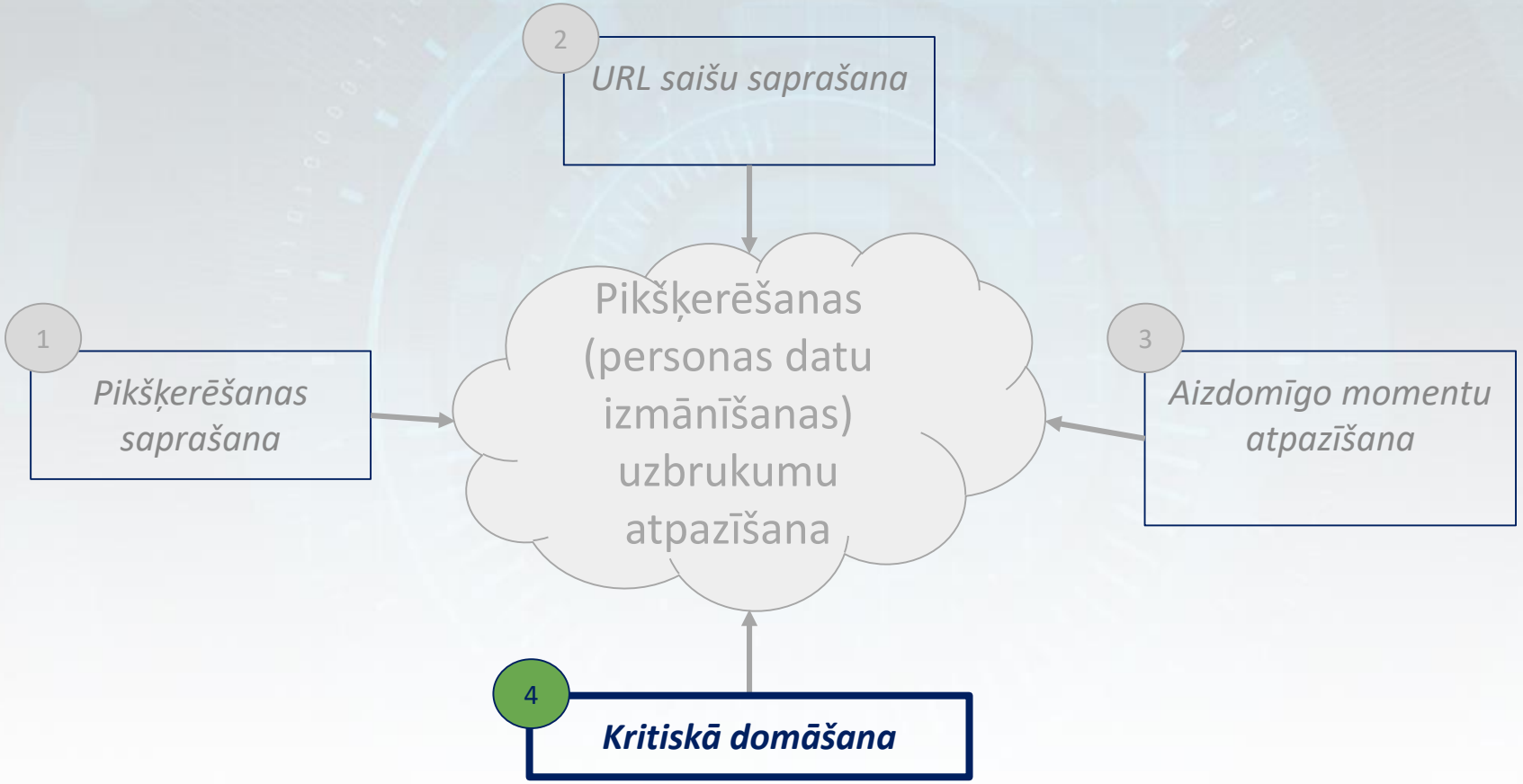


Fotoattēls no Stanford Edu.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Saturs


2
URL saišu saprašana
1
Pikšķerēšanas saprašana
Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana
3
Aizdomīgo momentu atpazīšana
4
Kritiskā domāšana

Kritiskā domāšana

Pikšķerēšanas noteikšana ietver maldināšanas atklāšanu.

Pirms darbību veikšanas veltiet vairāk laika ziņojuma pārskatīšanai

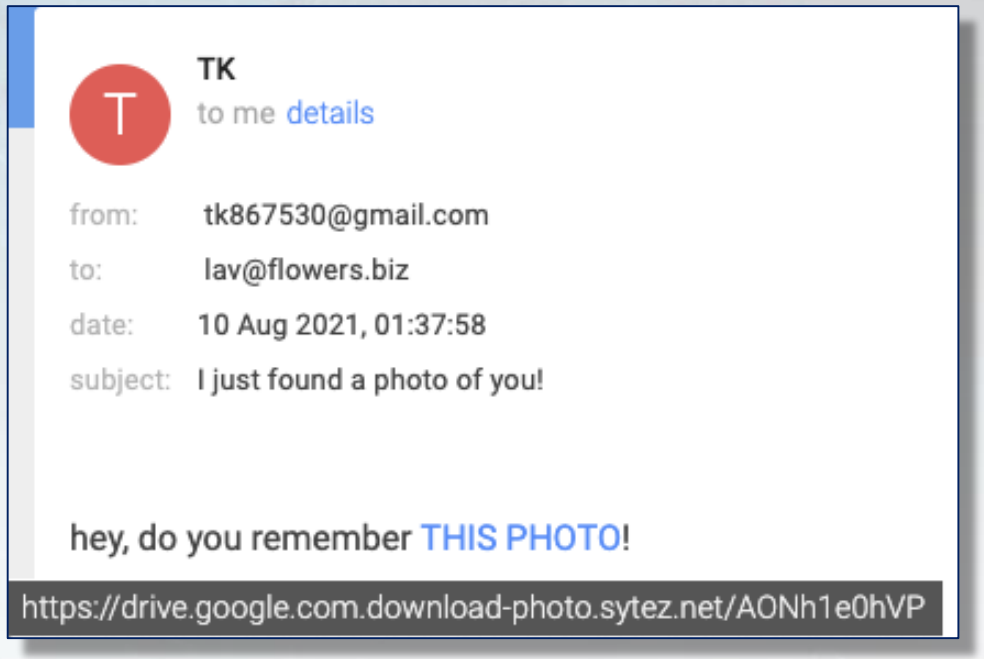
Mirkļa pārbaude:
Vai ziņojumā pastāv aizdomīgi momenti?

Kritiskā domāšana

- Esiet īpaši piesardzīgs, ja neesat pārliecināts, ka pazīstat sūtītāju.

  Vai atceries TK no skolas laikiem?

- Familiaritātes maska var radīt pietiekamu uzticību, lai noklikšķinātu uz ļaunprātīgiem URL.

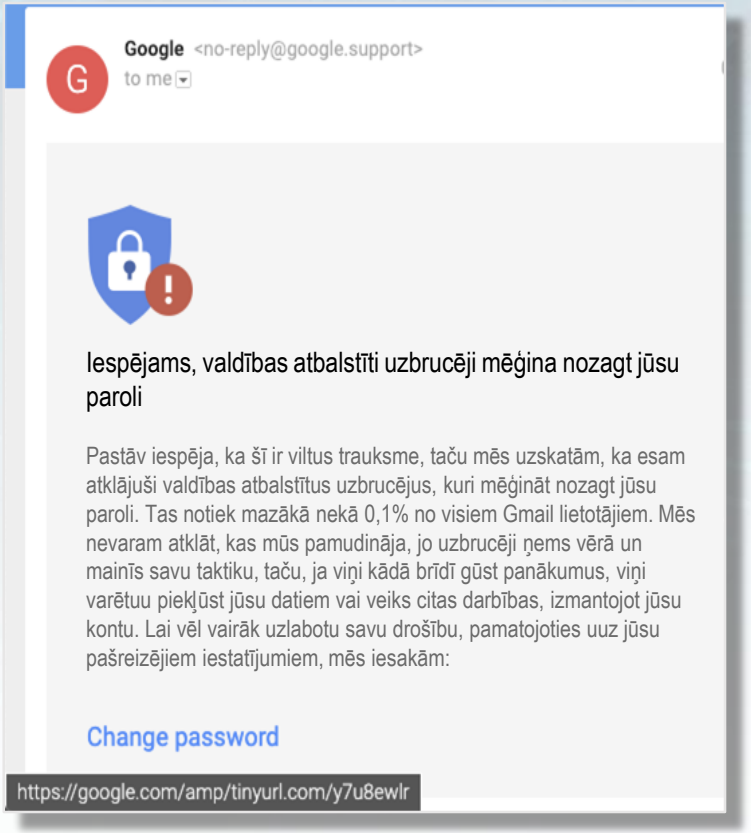


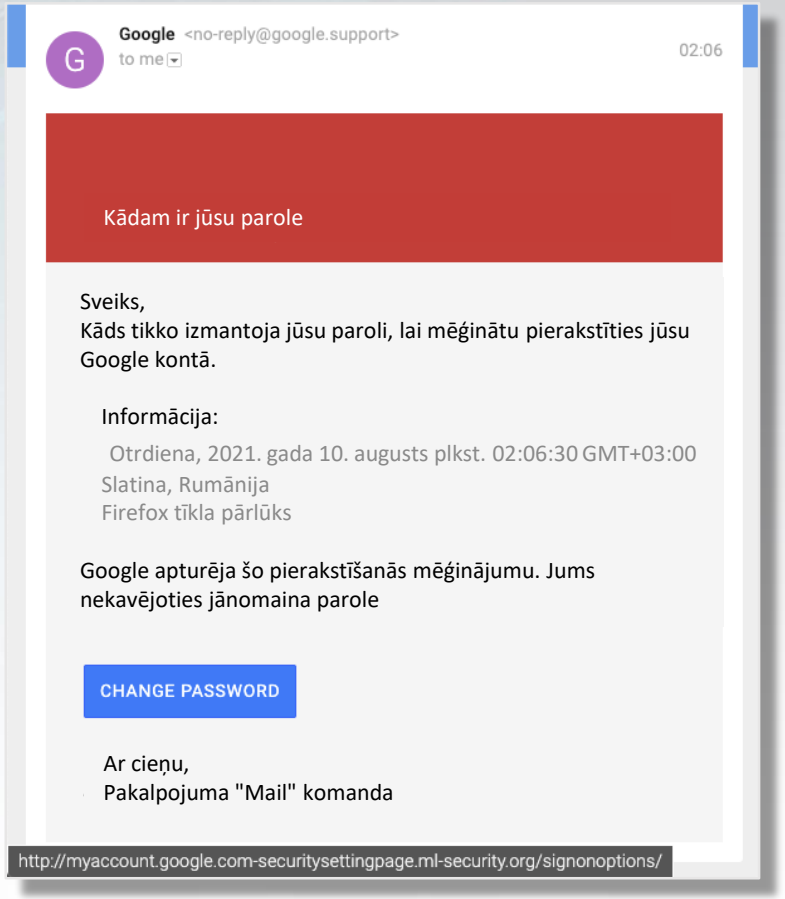
Fotoattēli no Jigsaw, Google.

Turklāt īstais fotoattēlu domēns '*sytez.net*' nav iekļauts Google Drive pakalpojumā.

Kritiskā domāšana

- Skatieties uzmanīgāk, kad e-pastā tiek pieprasītas darbības ar steidzamības sajūtu





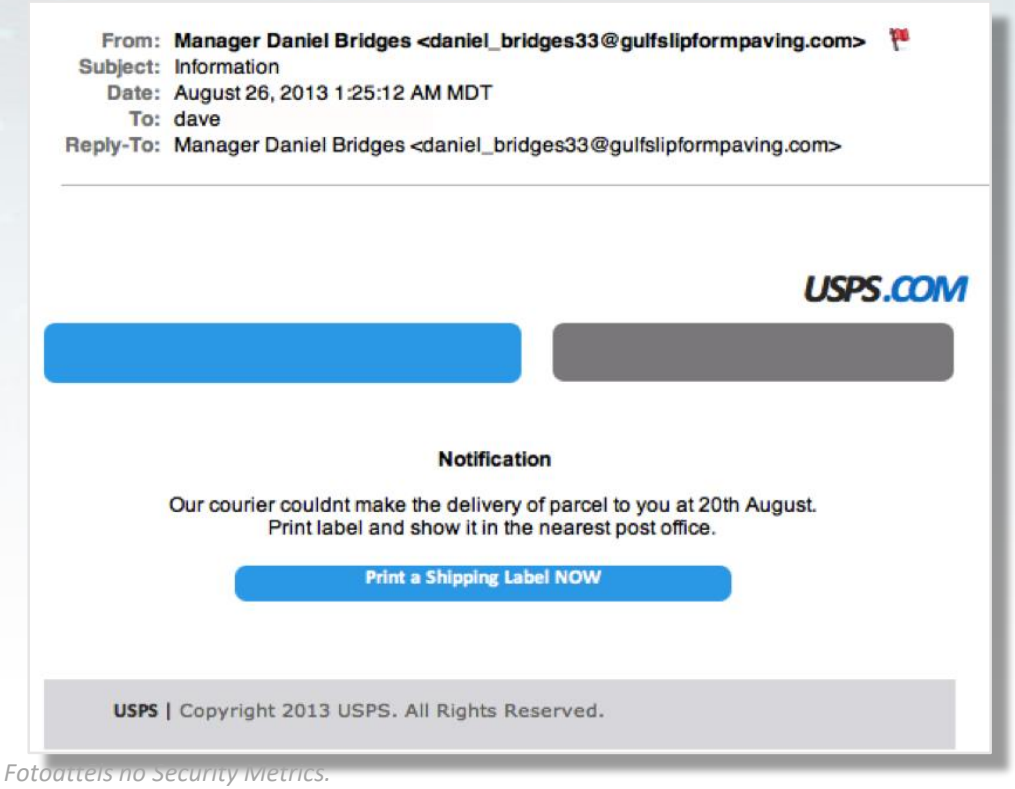
Fotoattēli no Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kritiskā domāšana

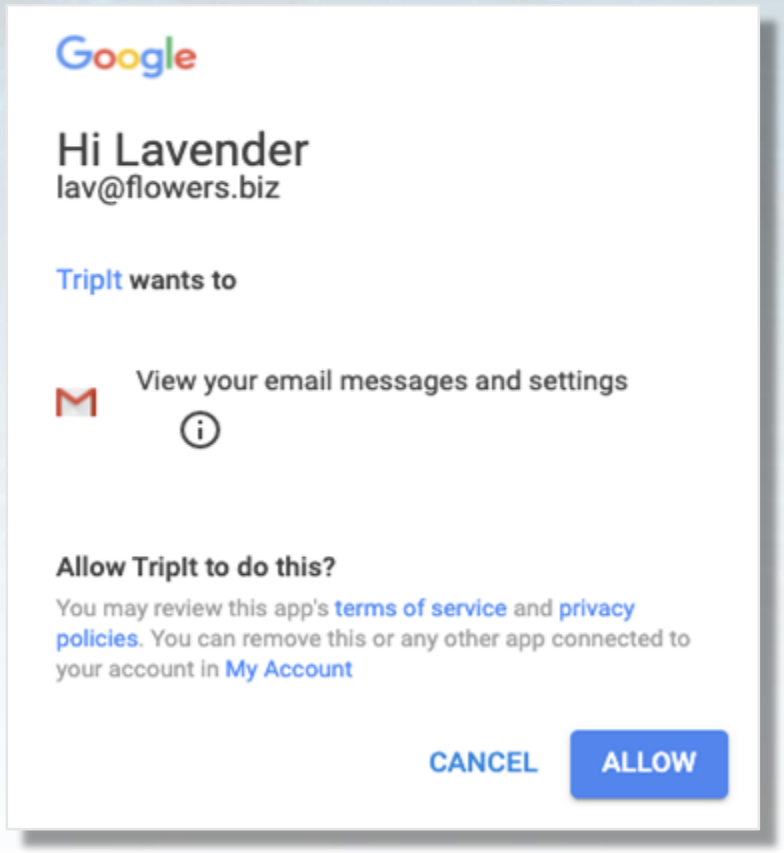
- Esiet apzinīgi attiecībā pret e-pasta ziņojumiem, kas liek atvērt ārēju vietni. Virzot kursoru ne tikai virs šķietamām saitēm, bet virs visa e-pasta ietvara, var tikt parādīts slēpts URL

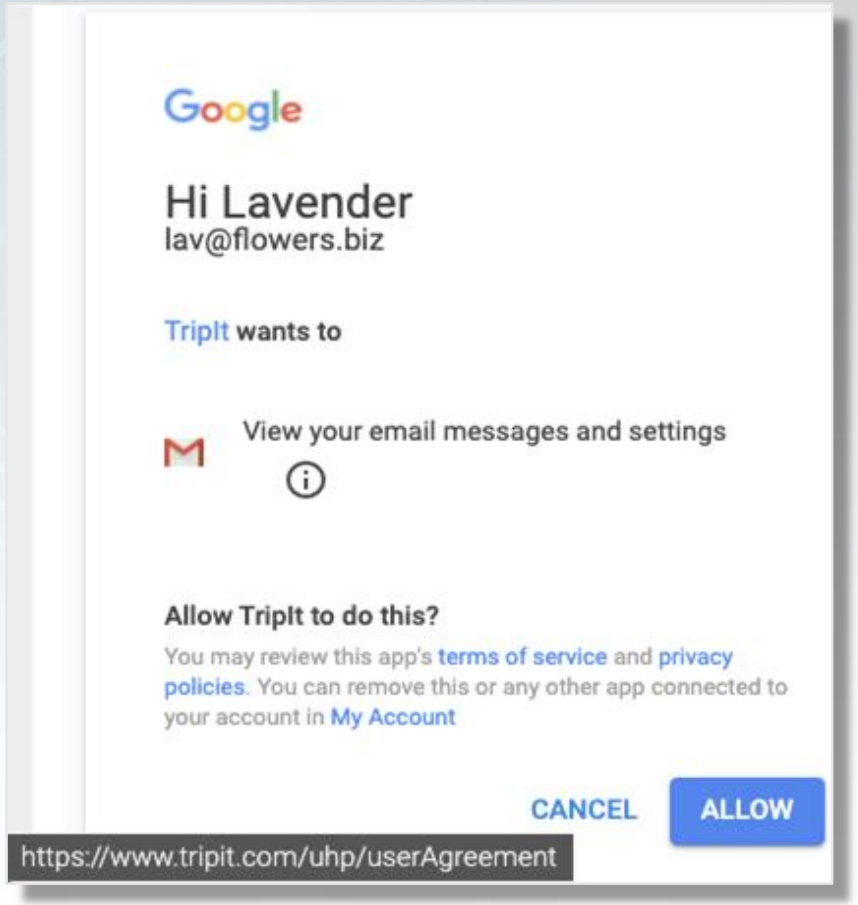


Fotoattēls no Security Metrics.

Kritiskā domāšana

- Pirms piešķirat konta piekļuves pieprasījumus, pārbaudiet, vai uzticaties lietotņu izstrādātājiem





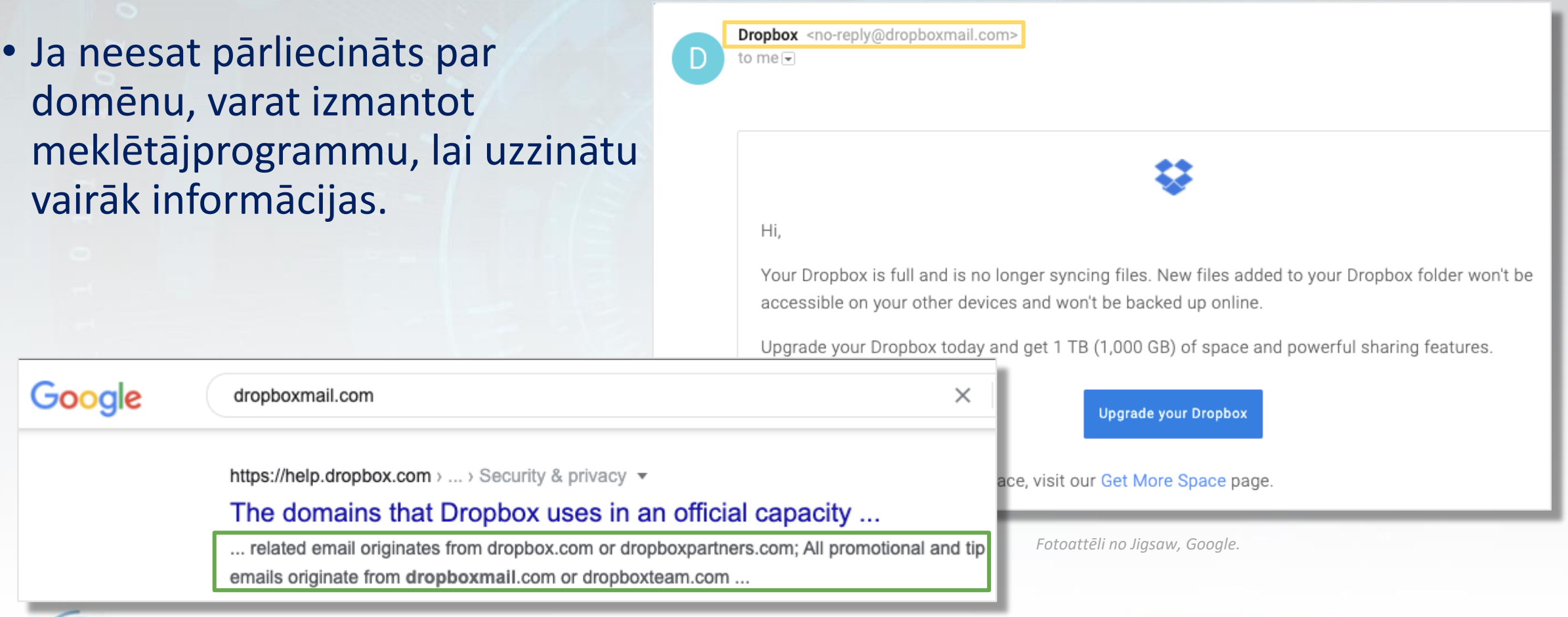
Fotoattēli no Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kritiskā domāšana

- Ja neesat pārliecināts par domēnu, varat izmantot meklētājprogrammu, lai uzzinātu vairāk informācijas.



Fotoattēli no Jigsaw, Google.

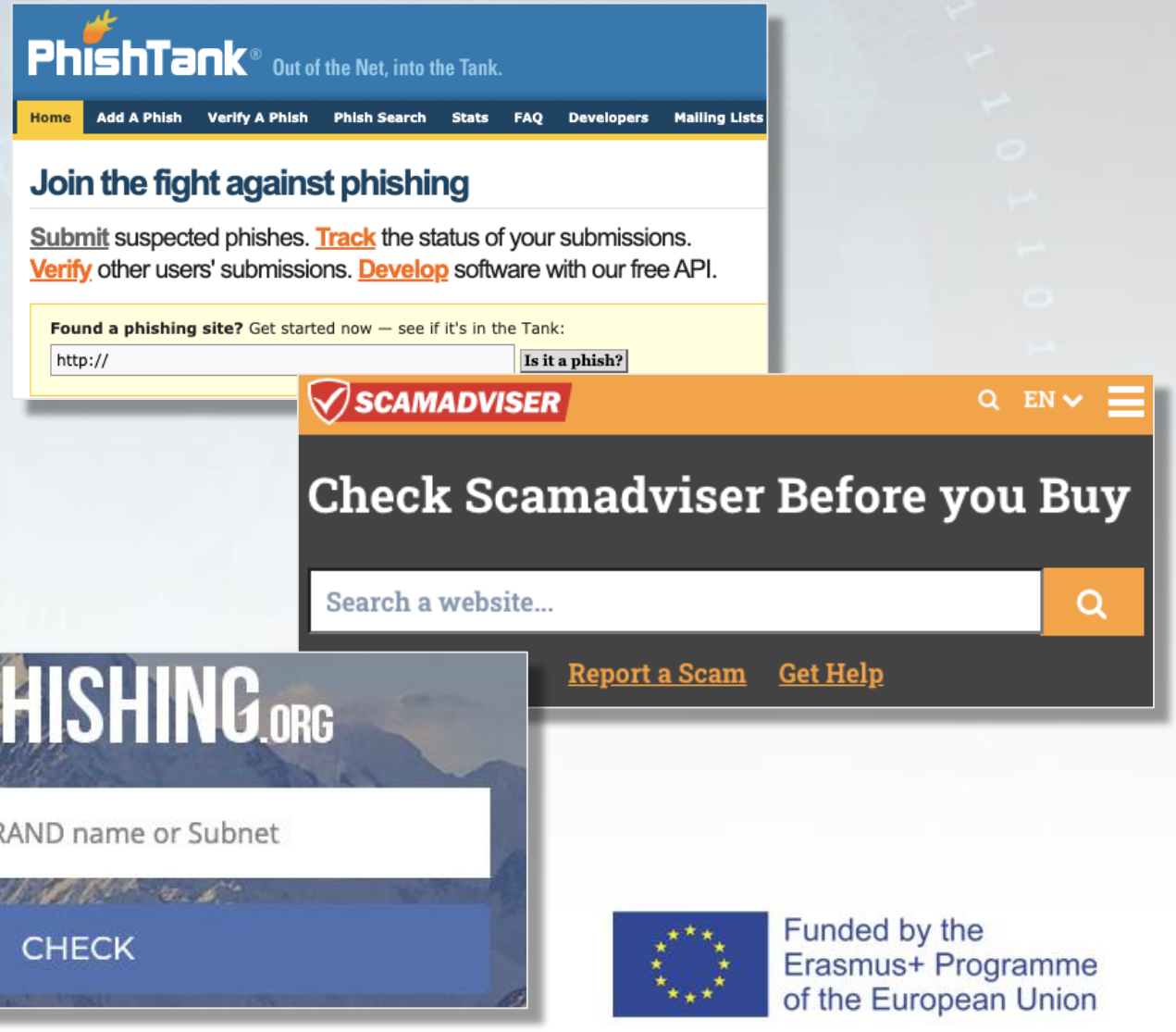
Funded by the Erasmus+ Programme of the European Union

Kritiskā domāšana

- Ja neesat pārliecināts par URL, ir pieejami bezmaksas tiešsaistes rīki potenciāli pikšķerētu vietrāžu URL meklēšanai

Daži piemēri:

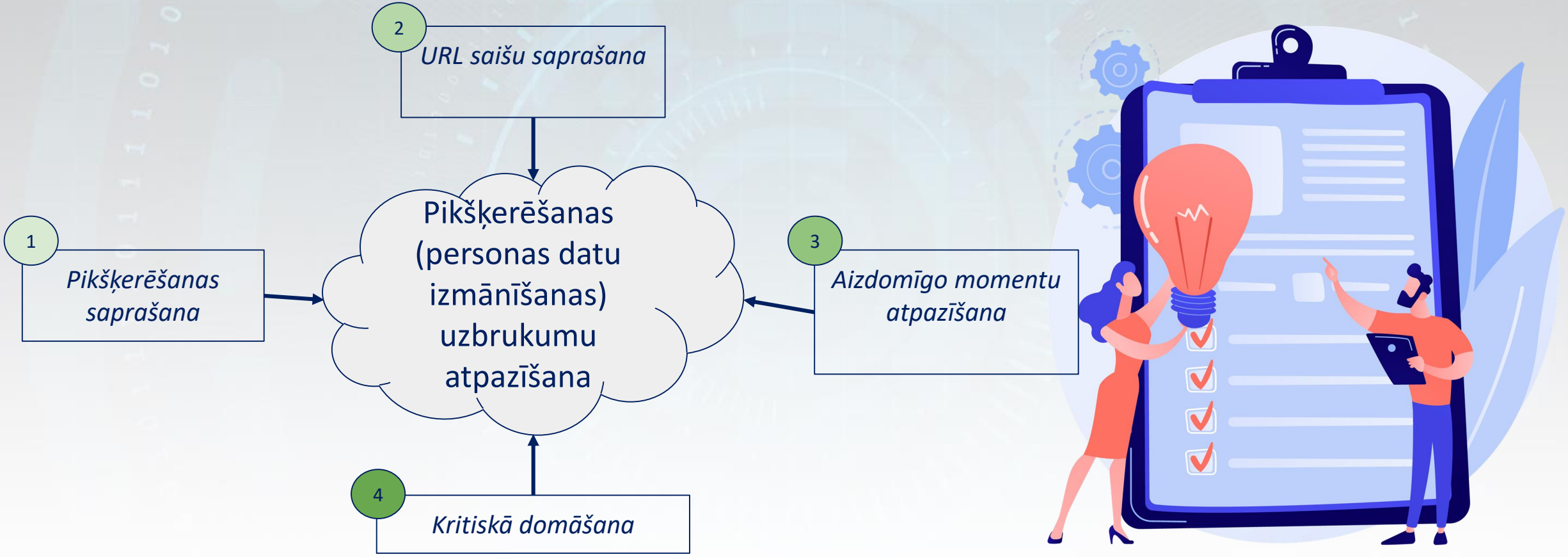
- *PhishTank*
- *CheckPhish*
- *IsItPhishing*
- *MalwareURL*
- *ScamAdviser*



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kopsavilkums



Uzdevums

Vai varat pamanīt, kuri no tālāk norādītajiem ir pikšķerēšanas URL?

http://drive--google.com

https://yahoomailservlce.weebly.com/

https://amacon-bldr.ga/

https://support.google.com/faqs/answer/10122684

páypal.com

https://storage.googleapis.com/random1992/redirectgffd.html#rd/jOp8EI39NGje0739co9

https://dropboxmail.com

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Uzdevums

Diskutējiet par citiem aizdomīgajiem momentiem, par kuriem šajā lekcijā nav runāts, un kurus esat pieredzējis reālajā dzīvē vai atpazinis dažos sniegtajos pikšķerēšanas piemēros

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Uzdevums

Pārejiet uz vietni ***PhishTank*** un atlasiet pikšķerēšanas analīzes paraugu no “nesenajiem iesniegumiem”

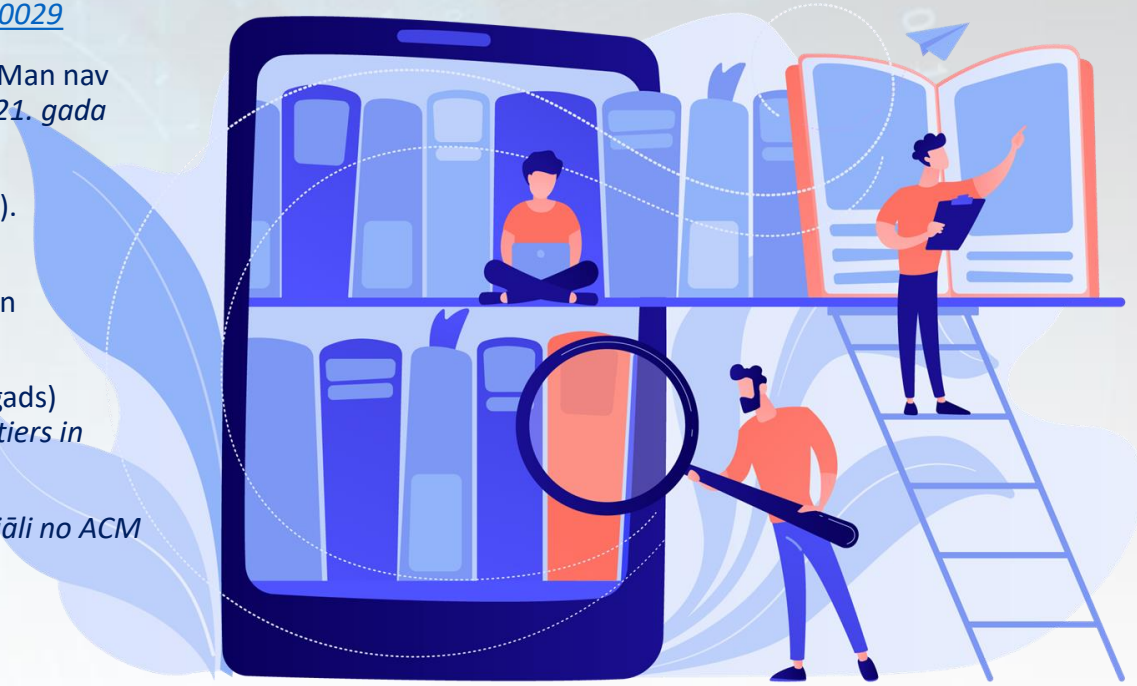
- *Vai varat pateikt, vai tā ir pikšķerēšana vai nē?*
- *Kādi bija pikšķerēšanas rādītāji?*
- *Noklikšķiniet uz "Skatīt tehnisko informāciju". Ko no tā var mācīties?*

https://phishtank.org

Papildu lasīšana

Šīs lekcijas sagatavošanā izmantotie materiāli

- **Rupa D. C. C.** ***[Rupa, D.C.C.]*****, Srivastava G.** ***[Srivastava, G.]*****, Batačaraja S.** ***[Bhattacharya, S.]*****, Redijs P.** ***[Reddy, P.]*****, Gadekalu T. R. R.** ***[Gadekallu, T.R.R.]*** (2021. gada augusts) Mašīnmācību vadīta draudu izlūkošanas sistēma ļaunprātīgu URL noteikšanai. Materiālā: *16. starptautiskā konference par pieejamību, uzticamību un drošību. ARES 2021*, Raksts Nr. 154, 1–7. https://doi.org/10.1145/3465481.3470029
- **Altobaiti K.** *[Althobaiti, K.]*, **Mengs N.** *[Meng, N.]*, **& Venīja K.** *[Vaniea, K.]* (2021. gada maijs). Man nav vajadzīgs eksperts! URL pikšķerēšanas funkciju padarīšana cilvēkiem saprotama. Materiālā *2021. gada CHI konferences par cilvēciskajiem faktoriem skaitļošanas sistēmās* (1-17. lpp.).
- **Driks C. E.** *[Drake, C. E.]*, **Oliver J. J.** *[Oliver, J. J.]* **un Kūncs E. J.** *[Koontz, E. J.]* (2004. gada jūlijs). Pikšķerēšanas e-pasta anatomija. Materiālos CEAS.
- **Abrošans H.** ***[Abroshan H.]*****:** Pikšķerēšanas upuru pamatcēloņi — cilvēka uzvedības, emociju un demogrāfijas ietekme, Promocijas darbs, Gentes Universitāte, 2021. gads
- **Alkhalils Z.** [Alkhalil Z.], **Hjūidžs C.** *[Hewage C.]*, **Navafs L.** *[Nawaf L.]*, **Hans I.** *[Khan I.]* (2021. gads) Pikšķerēšanas uzbrukumi: Nesen veikts visaptverošs pētījums un jauna anatomija, Front. *Frontiers in Computer Science, 3, 6.*
- **Vašs R.** *[Wash, R.]* (2020. gads). Kā eksperti atklāj pikšķerēšanas krāpniecības e-pastus. *Materiāli no ACM par cilvēka un datora mijiedarbību, 4 (CSCW2), 1-28*.
- **SavvySecurity** (2021. gads). 10 pikšķerēšanas e-pasta piemēri, kas jums jāredz. https://cheapsslsecurity.com/blog/10-phishing-email-examples-you-need-to-see/
- **Eliss D.** *[Ellis, D]*. 7 veidi, kā atpazīt pikšķerēšanas e-pastu: E-pasta pikšķerēšanas piemēri. https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Īsi video

- Pikšķerēšanas e-pasta krāpniecības anatomija
  - ***https://youtu.be/3gpOM9c6mmA***
- Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu skaidrojums
  - ***https://youtu.be/Y7zNlEMDml4***
  - ***https://youtu.be/gqhPkeXMeh0***
- Pikšķerēšanas atpazīšana un aizsardzība pret to
  - ***https://youtu.be/R12_y2BhKbE***

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Pateicamies!