Funded by the Erasmus+ Programme of the European Union

Kibernetinių atakų atpažinimas ir apsauga

Kibernetinių atakų atpažinimas

Kaip atpažinti sukčiavimo (angl. Phishing) atakas?

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

Mokymosi tikslai

Paaiškinti e. saugumo sąvoką ir aktyvaus požiūrio į kibernetines grėsmes svarbą taikant kibernetinės higienos koncepciją.

Atpažinti ir valdyti kibernetines atakas.

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Studento darbo krūvis

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

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Turinys


2
Suprasti URL
1
Suprasti sukčiavimą
Sukčiavimo atakų atpažinimas
3
Atpažinti pagrindinius požymius
4
Kritinis mąstymas

Turinys

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kas yra sukčiavimo ataka?

Sukčiavimas tai socialinės inžinerijos būdas, dėl kurios žmonės ir organizacijos gali prarasti duomenis, sugadinti savo reputaciją, patirti tapatybės vagystę, prarasti pinigus ir patirti daugybę kitų nuostolių. Sukčiavimas paprastai prasideda nuo elektroninio laiško, kuriuo bandoma įgyti potencialios aukos pasitikėjimą ir įtikinti ją atlikti užpuoliko pageidaujamus veiksmus.

[*Abroshan, 2021*]

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo šaltiniai

Photo by Google

- El. laiškas
- Interneto svetainės
- Socialiniai tinklai
- Mobilusis ryšys (SMS, balsas)
- *Bet kokia bendravimo forma...*

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo žinučių anatomija

- Žinutės šaltinis
  - *kas siunčia man žinutę?*
- Žinutės turinys
  - *apie ką rašoma žinutėje?*
- Nuorodos / Priedai
  - *į ką dar ši žinutė nurodo?*

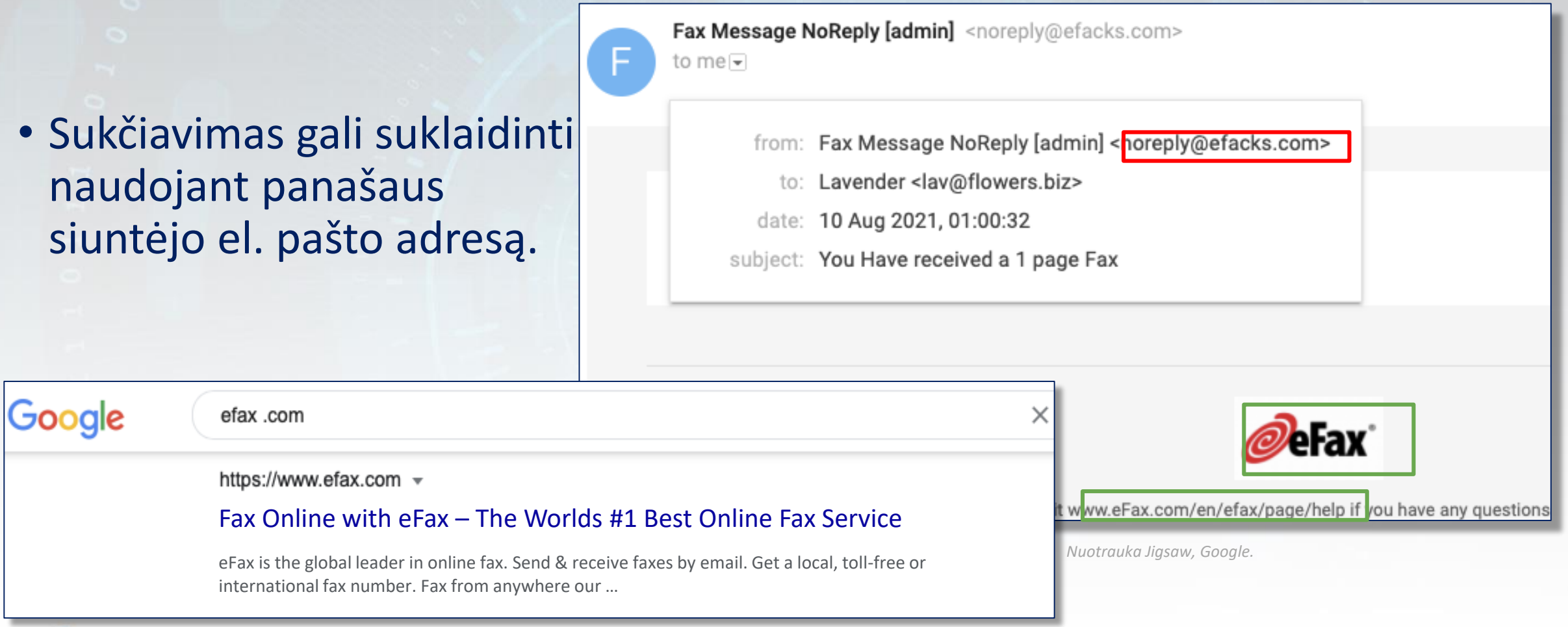
Nuotrauka iš istockphoto.com

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Žinutės šaltinis

- Sukčiavimas gali suklaidinti naudojant panašaus siuntėjo el. pašto adresą.

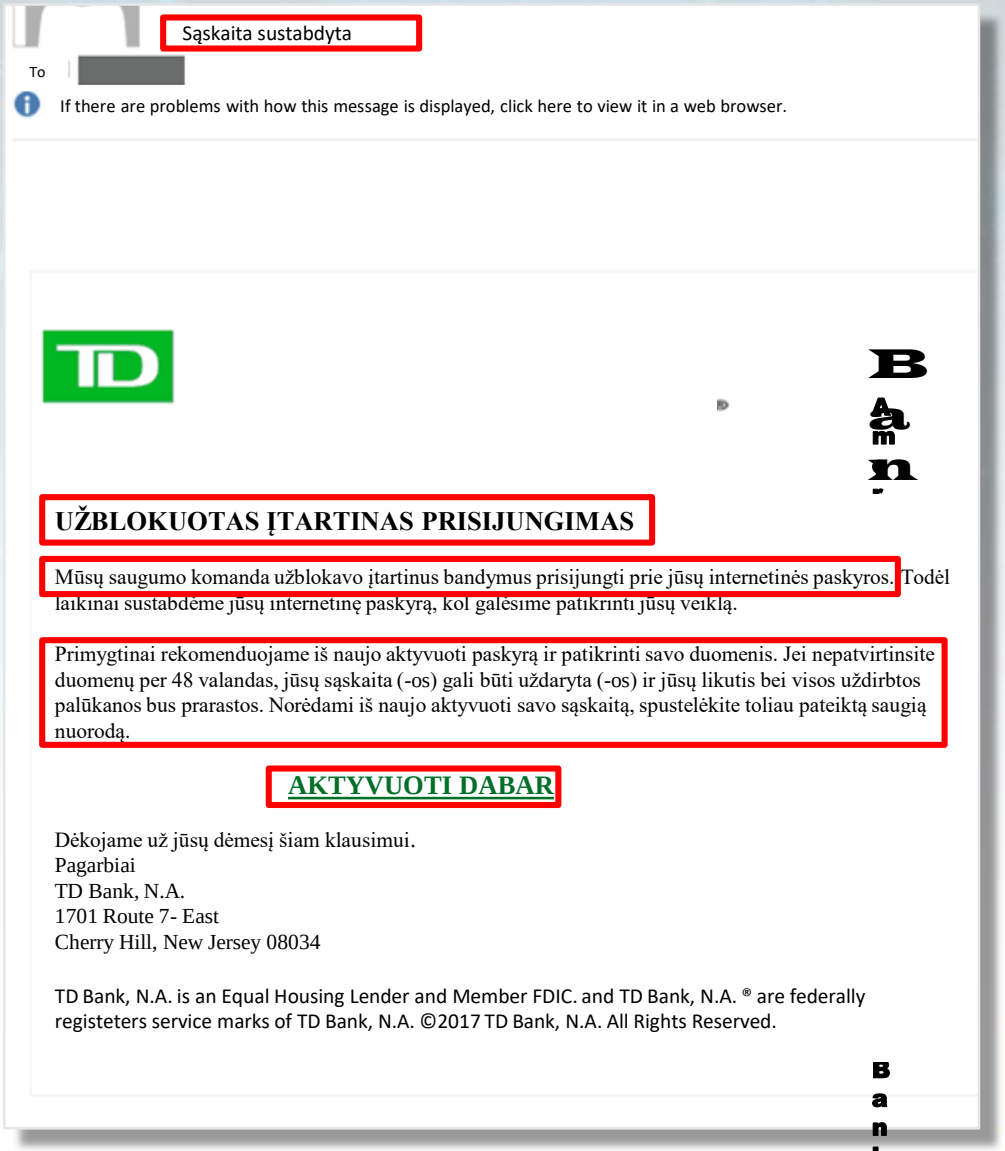


Nuotrauka Jigsaw, Google.

Funded by the Erasmus+ Programme of the European Union

Žinutės turinys

- Apgaulė per baimę, skubą, valdžią, godumą, draugystę, pagalbą ir neviltį



Sąskaita sustabdyta

To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

TD Bank

UŽBLOKUOTAS ĮTARTINAS PRISIJUNGIMAS

Mūsų saugumo komanda užblokavo įtartinus bandymus prisijungti prie jūsų internetinės paskyros. Todėl laikinai sustabdėme jūsų internetinę paskyrą, kol galėsime patikrinti jūsų veiklą.

Primygtinai rekomenduojame iš naujo aktyvuoti paskyrą ir patikrinti savo duomenis. Jei nepatvirtinsite duomenų per 48 valandas, jūsų sąskaita (-os) gali būti uždaryta (-os) ir jūsų likutis bei visos uždirbtos palūkanos bus prarastos. Norėdami iš naujo aktyvuoti savo sąskaitą, spustelėkite toliau pateiktą saugią nuorodą.

AKTYVUOTI DABAR

Dėkojame už jūsų dėmesį šiam klausimui.
Pagarbiai
TD Bank, N.A.
1701 Route 7- East
Cherry Hill, New Jersey 08034

TD Bank®

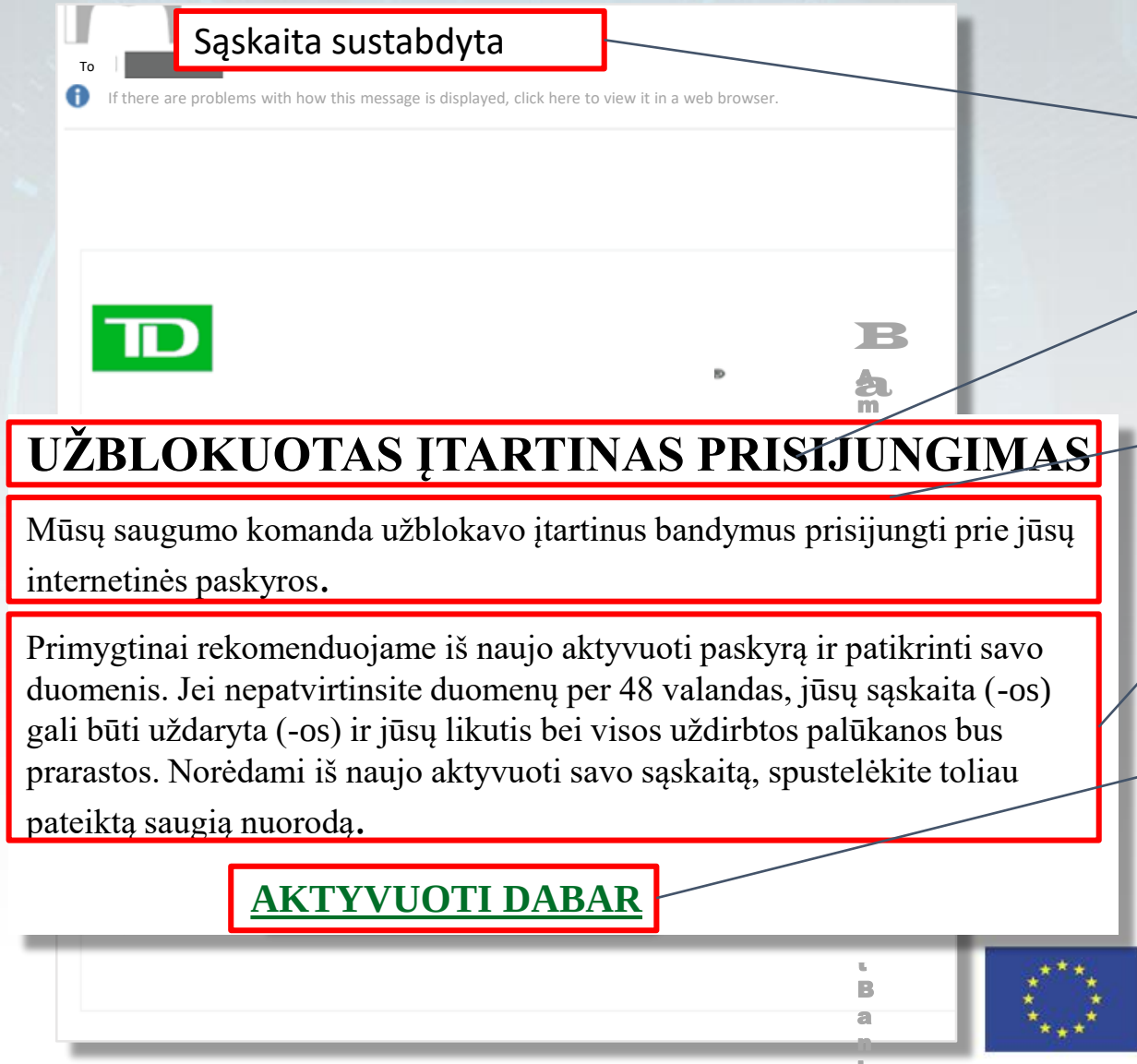
Nuotrauka Sonicwall Phishing Test

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Žinutės tyrinys

- Apgaulė per baimę, skubą, valdžią, godumą, draugystę, pagalbą ir neviltį



Baimė

Baimė

Pagalba

Skubinimas + Desperacija

Skubinimas

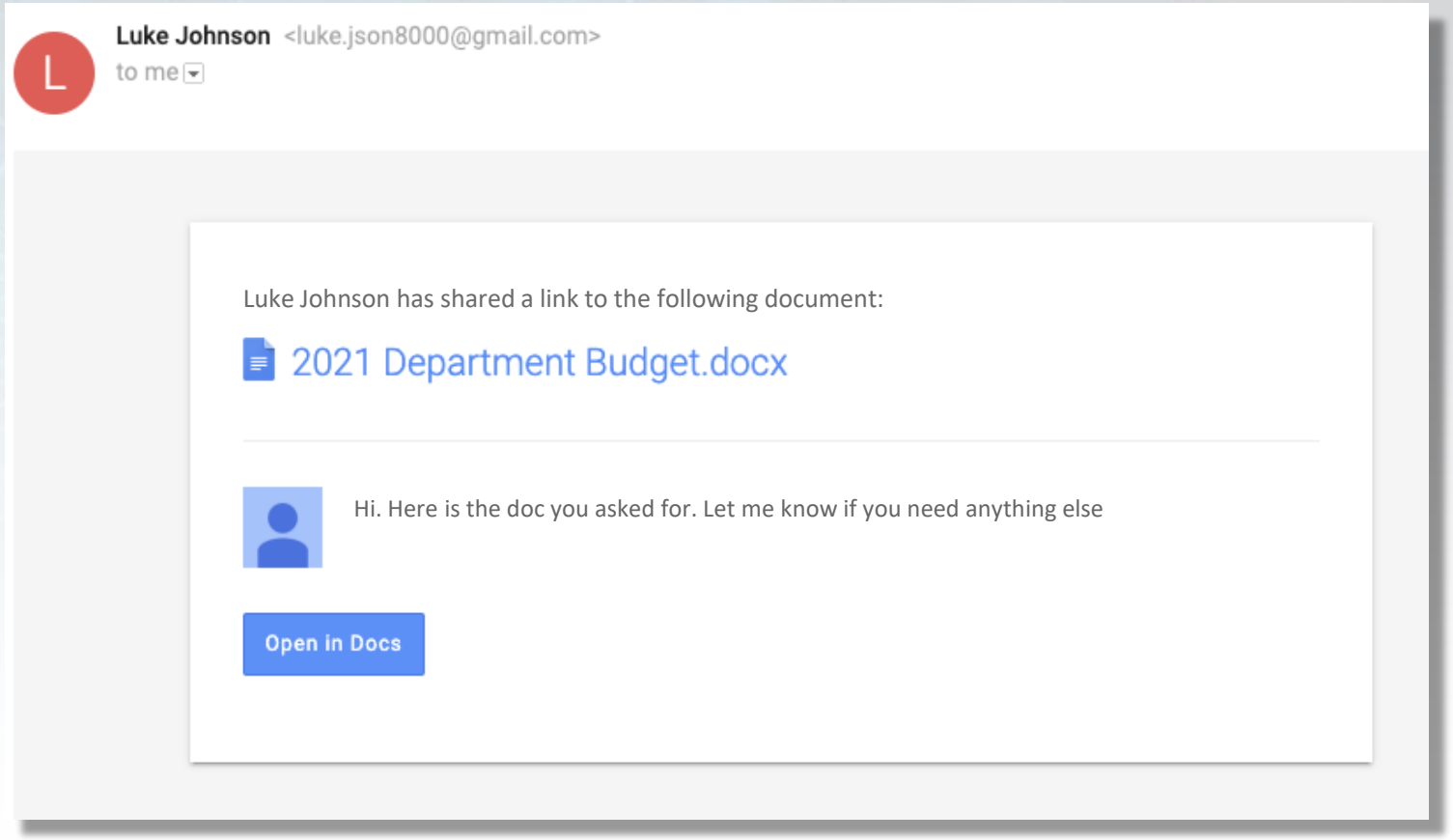
Nuotrauka Sonicwall Phishing Test

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Hipersaitai / Priedai

- Prieduose gali būti įvairių tipų failų, kurie gali būti kenkėjiški.
- Hipersaitai nurodo failo vietą žiniatinklyje ir gali nukreipti aukas į kenkėjiškas svetaines arba atsiųsti kenkėjiškus failus.



Nuotrauka Jigsaw, Google.

CyberPhish
Safeguarding your digital future

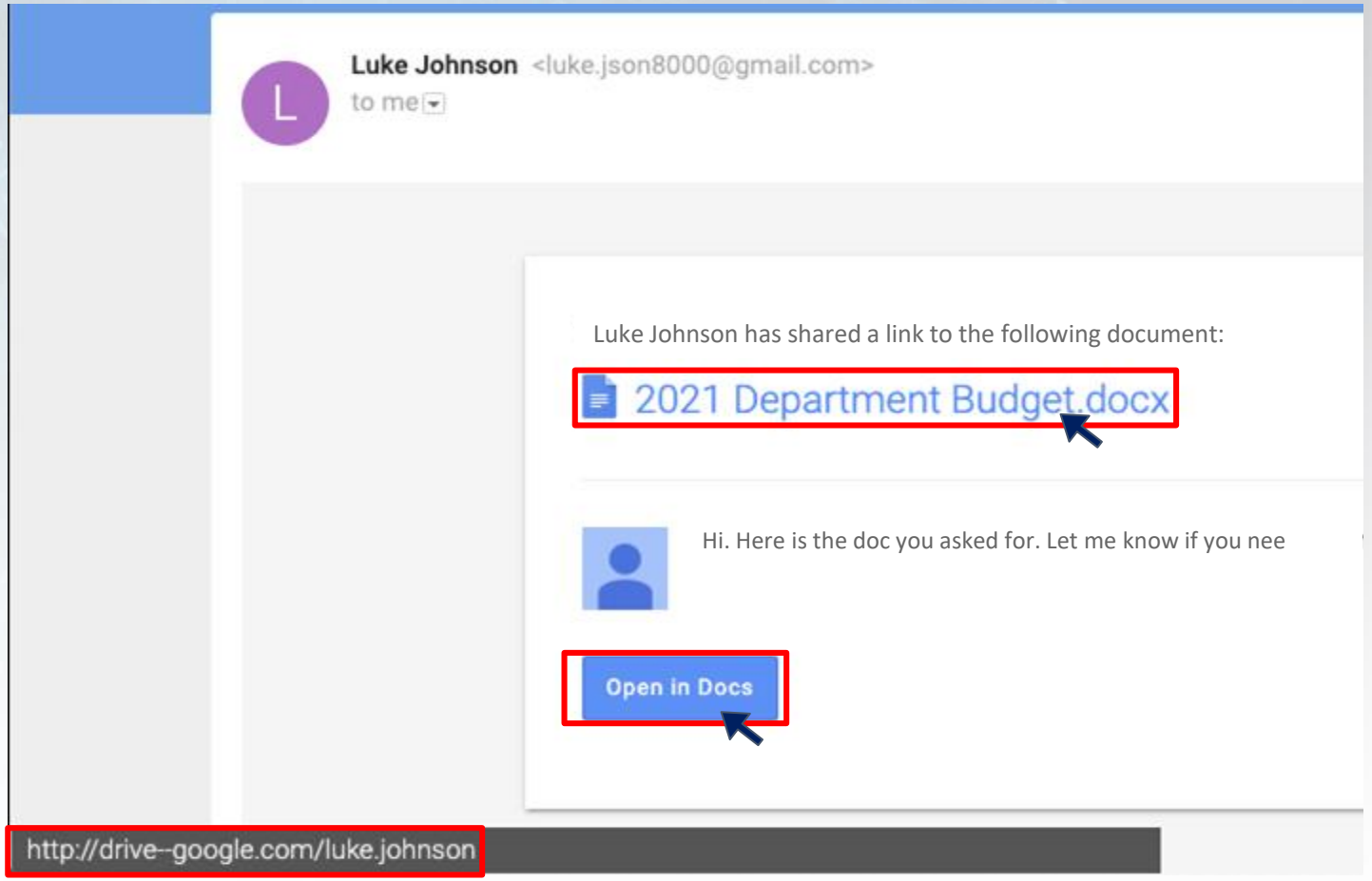
Funded by the Erasmus+ Programme of the European Union

Hipersaitai / Priedai

- Užvedus pelės žymeklį ant šių hipersaitų, galima pamatyti jų URL.

- Rodomas URL yra nesaugus „Google“ disko domeno imitavimas.

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

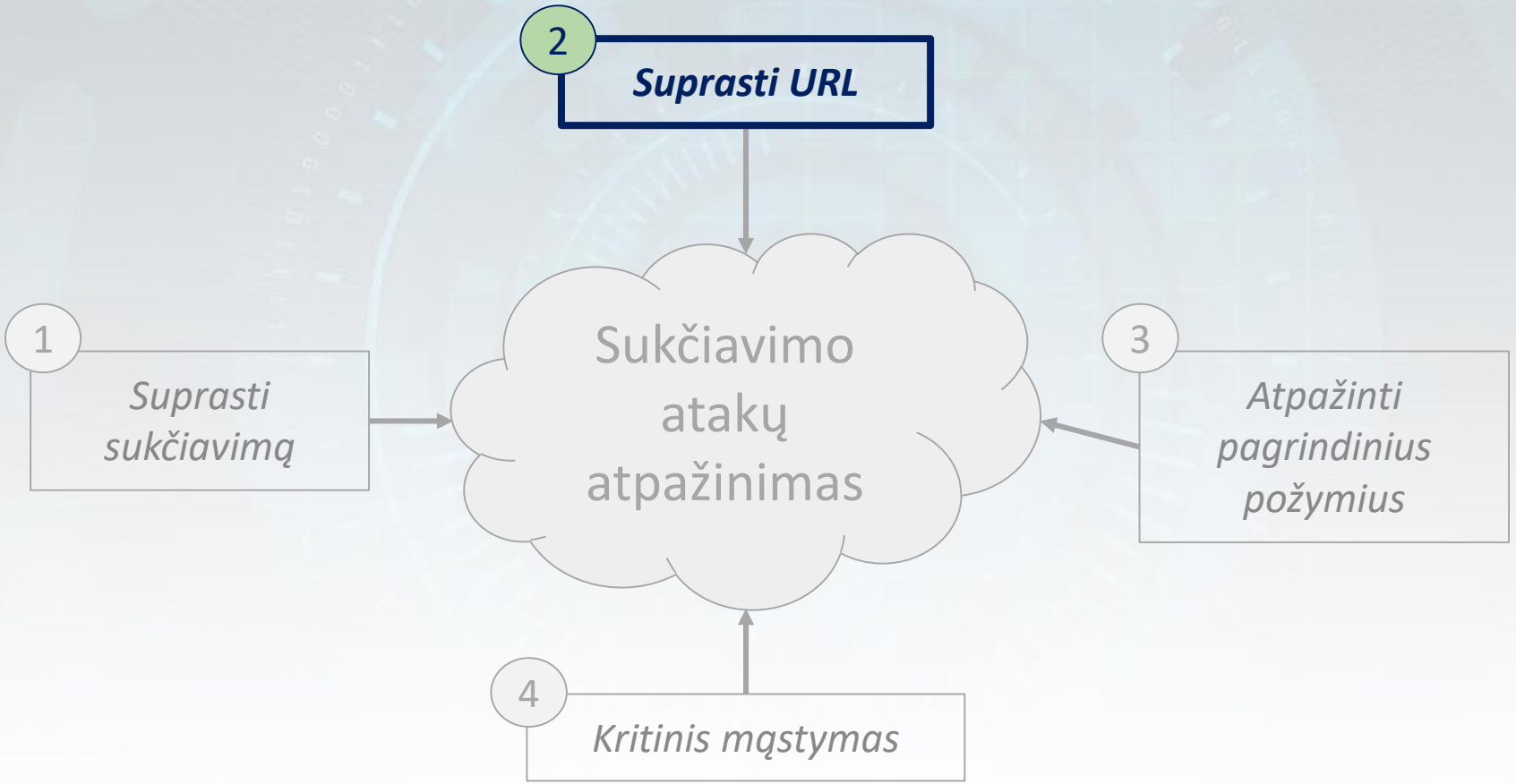


Nuotrauka Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Turinys

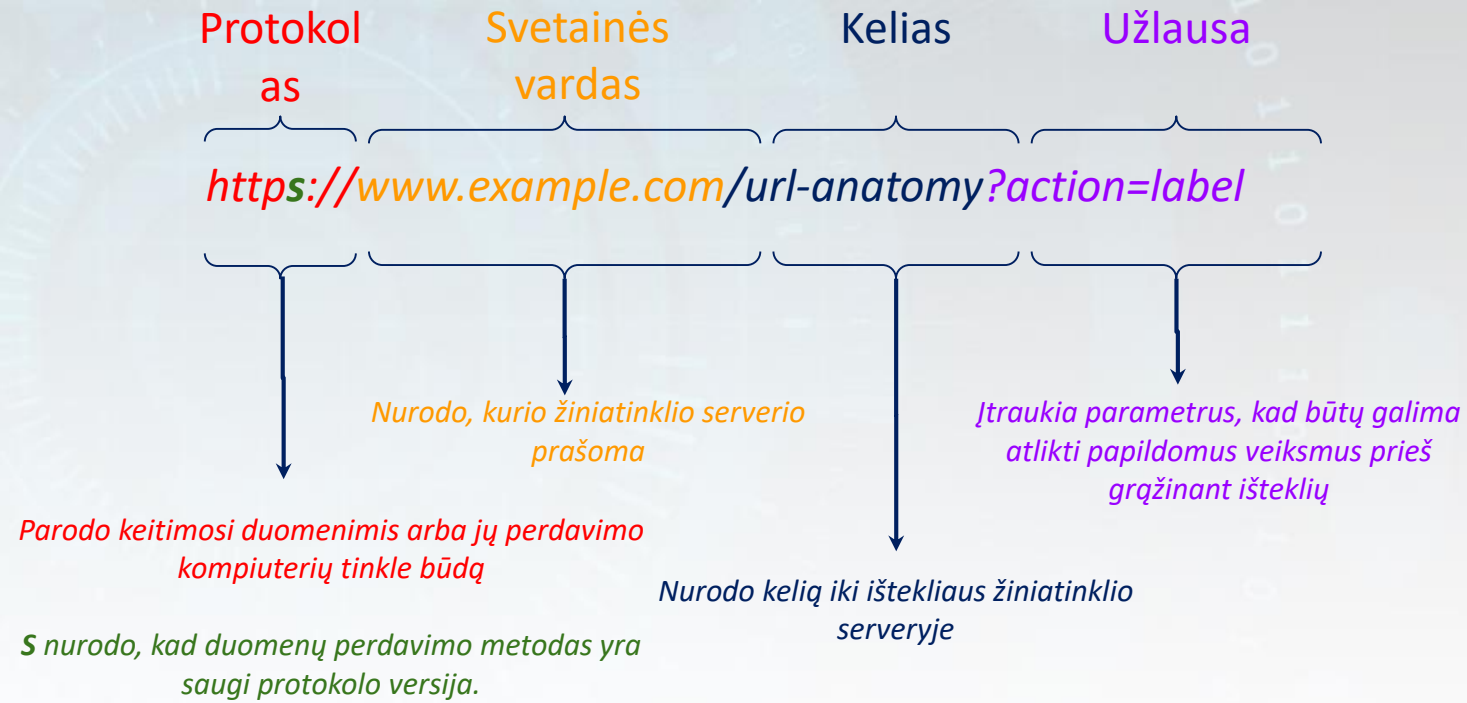


CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Suprasti URL

- Uniform Resource Locator (URL) yra tam tikro unikalaus išteklius adresas internete

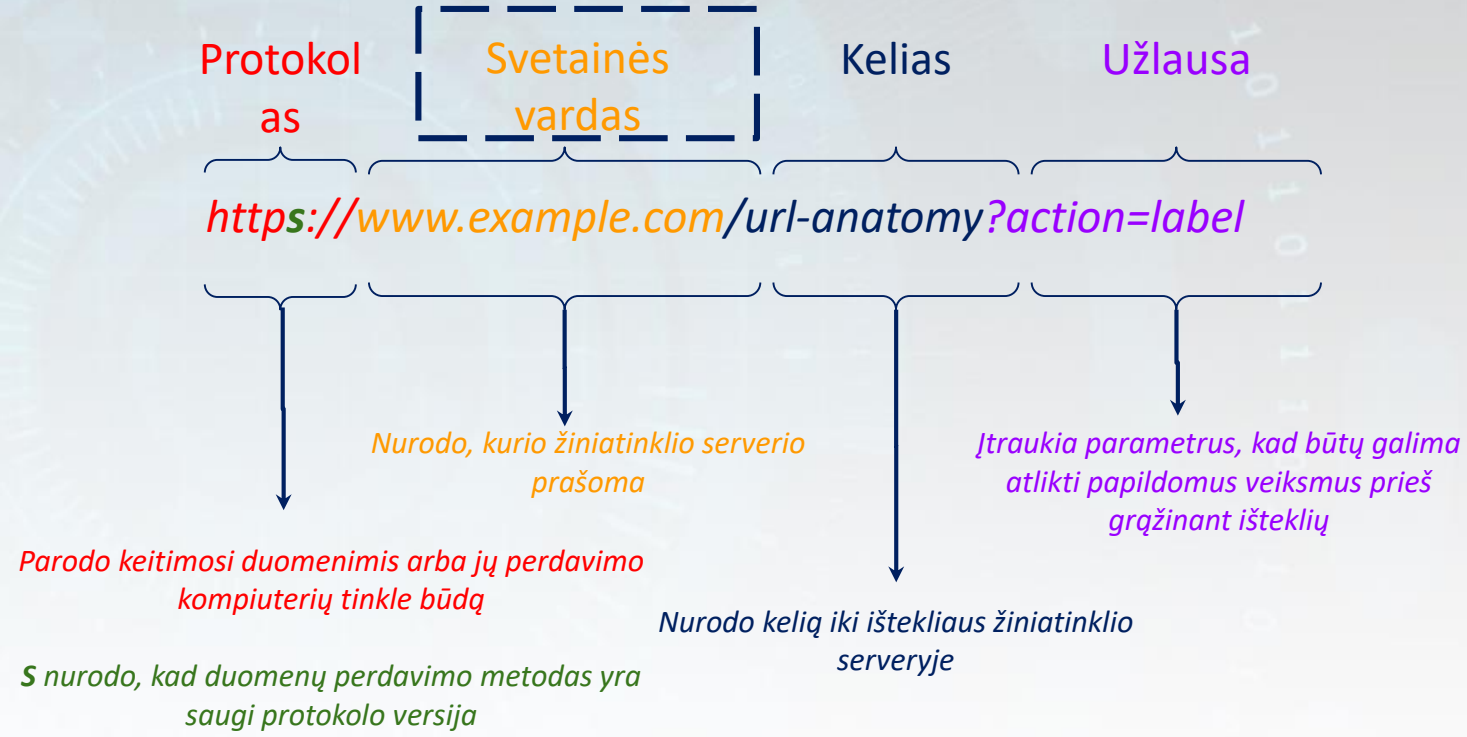


https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL
Protocol, Simple Object Access. "URL." (2007).

Funded by the Erasmus+ Programme of the European Union

Suprasti URL

- Uniform Resource Locator (URL) yra tam tikro unikalaus išteklius adresas internete.

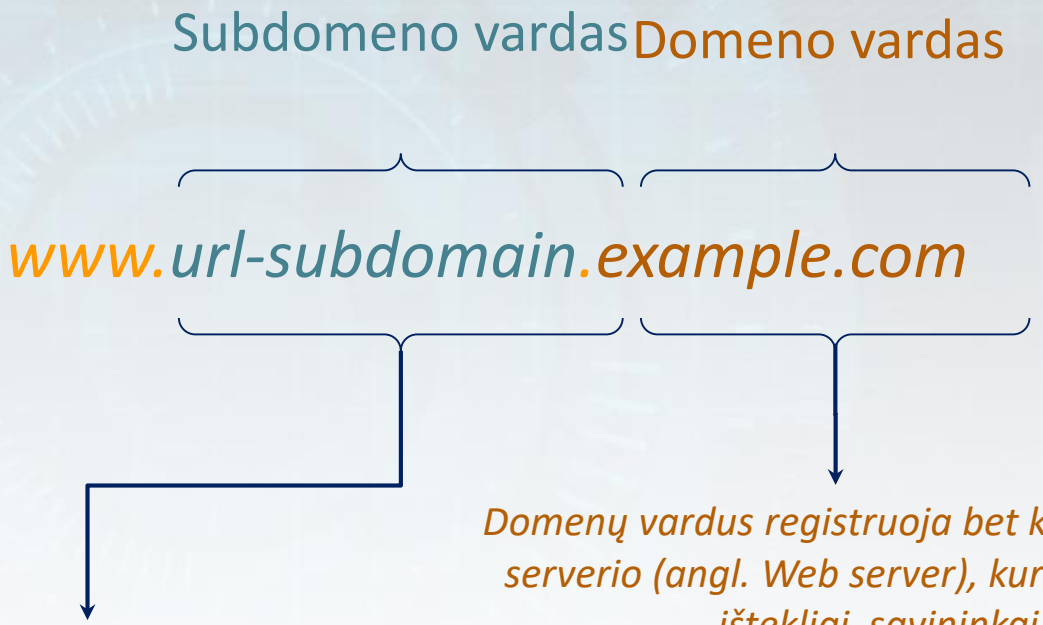


https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL
Protocol, Simple Object Access. "URL." (2007).

Funded by the Erasmus+ Programme of the European Union

Suprasti URL

- Svetainės vardas URL adrese gali turėti kelis subdomenus



https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL
Protocol, Simple Object Access. "URL." (2007).

Funded by the Erasmus+ Programme of the European Union

Suprasti URL

Sukčiavimo atveju dažnai bandoma apgauti aukas naudojant URL adresus.

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

Protokolas	*http*
Svetainės vardas	*amazon.com.mailru382.co*
Kelias	*/packagedelivery/2017Dk25RE3*
Domeno vardas	*mailru382.co*
Subdomeno elementas 1	com
Subdomeno elementas 2	*amazon*

Funded by the Erasmus+ Programme of the European Union

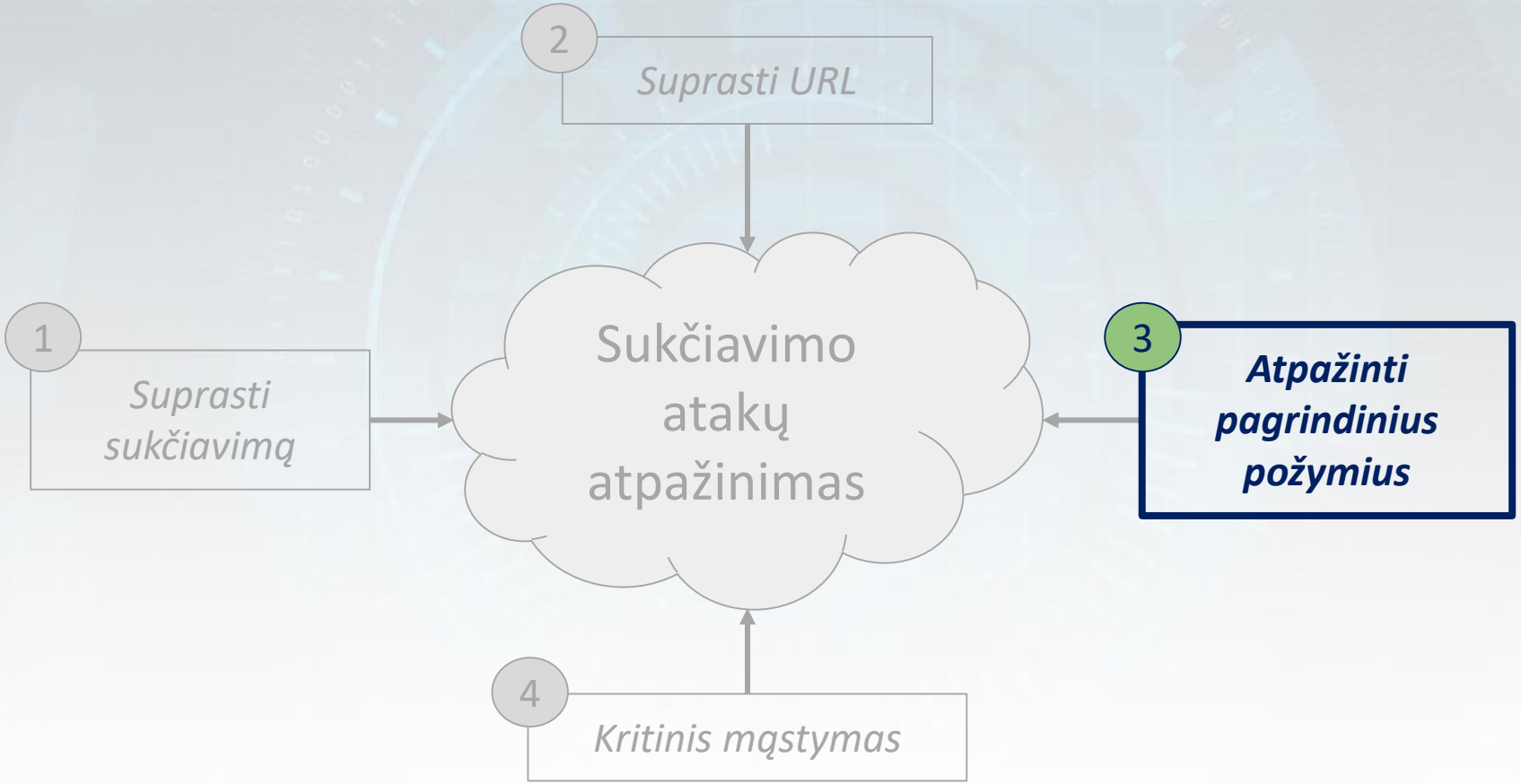
Suprasti URL

Kitos gudrybės su URL ...	Pavyzdys
• URL protokole nėra saugaus protokolo indikatoriaus.	URL naudojama *http* vietoje *https*
• Domenas akivaizdžiai panašus į gerai žinomą domeną, tačiau iš tikrųjų skiriasi.	*google.com* neteisingai parašyta kaip *googgle.com*
• Sudėtingai atrodantis domeno vardas, kad suklaidintų auką, t. y. IP adresas, šešioliktainiai ar dešimtainiai simboliai, simbolis domene.	IP adresas - http://20.85.220.142/telas/caixa/ Simboliai - https://epic.app/#con@sceneworld.org Skaičiai - http://2130706433/evil.com
• URL gali apimti gerai žinomą domeno pavadinimą, tačiau jis nepriklauso teisėtam šaltiniui.	"*Instagram*" įtrauktas į *http://instagramsupport.it/*

Rupa, D.C.C., Srivastava, G., Bhattacharya, S., Reddy, P., Gadekallu, T.R.R. (2021, August)

Funded by the Erasmus+ Programme of the European Union

Turinys


2
Suprasti URL
1
Suprasti sukčiavimą
Sukčiavimo atakų atpažinimas
3
Atpažinti pagrindinius požymius
4
Kritinis mąstymas

Pagrindinių požymių atpažinimas

- Teisėti el. pašto šaltiniai (t. y. įmonės) neprašo jūsų neskelbtinos informacijos el. paštu.

SUSTAINABLE DEVELOPMENT GOALS

Jungtinės Tautos jums skyrė **950 000,00 $ (devyni šimtai penkiasdešimt tūkstančių JAV dolerių)** švietimo darbuotojo stipendiją. Jungtinių Tautų valdžia nusprendė Jums pasiūlyti šią stipendiją, nes ji yra pasaulinio tikslo padėti švietimo darbuotojams ir studentams per šį Covid-19 pandemijos laikotarpį dalis.

Darnaus vystymosi tikslai (SDG) gimė 2012 m. Rio de Žaneire vykusioje Jungtinių Tautų tvaraus vystymosi konferencijoje. Tikslas buvo sukurti visuotinių tikslų rinkinį, kuris atitiktų neatidėliotinus aplinkos, politinius ir ekonominius iššūkius, su kuriais susiduria mūsų pasaulis.

JT atitinkamas biuras suteiks dotacijos lėšas, kai pateiksite šį prašymą. Sveikiname ir dėkojame už jūsų paslaugas.

Pateikite prašymą ir gaukite švietimo dotacijos lėšas

Vardas, Pavardė (privaloma)
El. paštas (ne Edu) (privaloma)
Telefono numeris (privaloma)
Gyvenamosios vietos ir darbo adresas (privaloma)

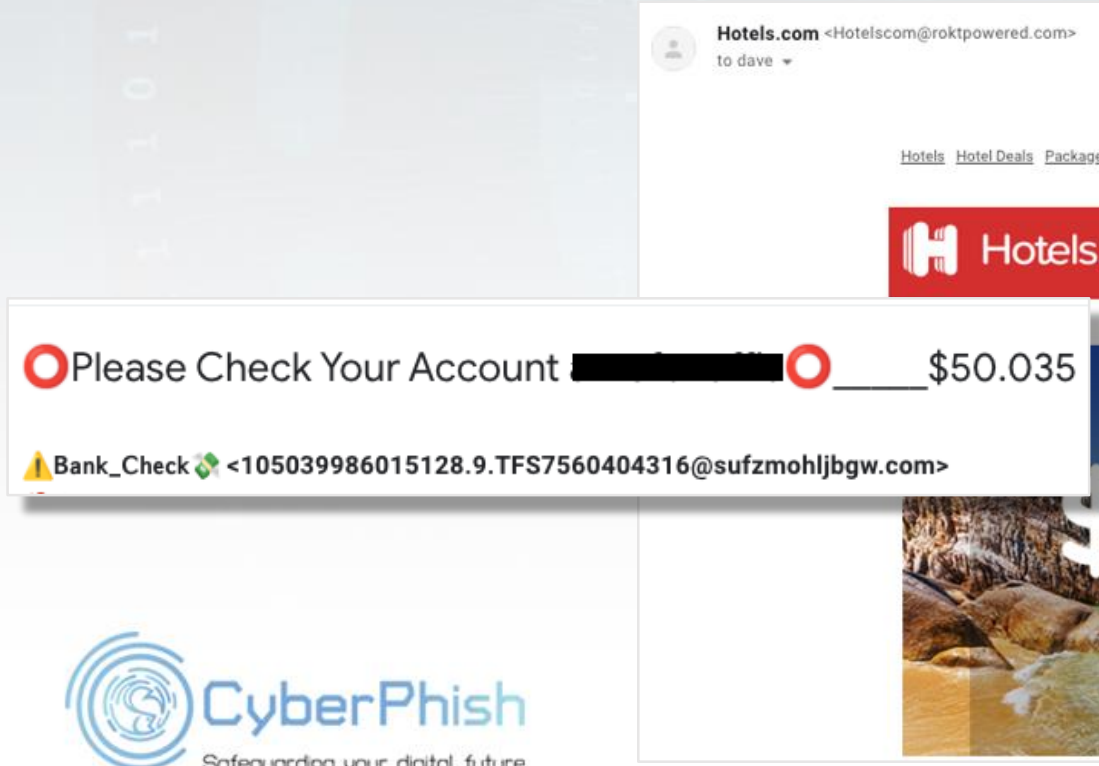
Prašymas turėtų būti siunčiamas iš jūsų asmeninio (ne edu) el. pašto.

Nuotrauka Stanford Edu.

Funded by the Erasmus+ Programme of the European Union

Pagrindinių požymių atpažinimas

- Teisėti el. pašto šaltiniai paprastai neturi:
  - sudėtingų el. pašto adresų
  - el. pašto adreso, el. pašto domeno arba el. pašto siuntėjo vardo neatitikimo



CyberPhish
Safeguarding your digital future

Nuotrauka Security Metrics.

Funded by the Erasmus+ Programme of the European Union

Pagrindinių požymių atpažinimas

- Teisėti el. pašto šaltiniai paprastai kreipiasi į jus vardu

Nuo: No Reply <sarahrk@unm.edu>
Išsiųsta: Monday, June 8, 2020 9:03 AM
Tema: Pastaba

Nauji pranešimai yra laikomos laikinajame aplanke dėl sinchronizavimo klaidos.

Norėdami pasiekti laukiančius pranešimus ir pasirinkti, ką su jais daryti, vadovaukitės toliau pateikta nuoroda.

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

© 2020 cs.stanford.edu

Nuotrauka Stanford Edu.

Pagrindinių požymių atpažinimas

- Teisėti el. pašto šaltiniai neturi rašybos ir gramatikos problemų

From: noreply@stanford.edu <noreply@stanford.edu>
Sent: Monday, May 11, 2020 10:59 AM
Subject: stanford.edu De pasaulinės Covid-19 epidemijos mes tikriname visus musu el. pašto paskyros naudotojus musu serveryje.

Mail.stanford.edu Notification

De pasaulinės Covid-19 epidemijos mes tikriname visus musu el. pašto paskyros naudotojus musu serveryje.

jusu paskyra turi buti patvirtinta ir nedelsiant apsaugota pas mus, atsisiunte pridedama patvirtinimo programa mail.stanford.edu ir patvirtinkite savo el. pašto paskyra, kad paskyra nebutu išjungta musu serveryje. atkreipkite demesi, kad jei neatsisiusite musu pridedamos programos ir nepatvirtinsite paskyros pas mus, jusu paskyra bus automatiškai laikoma paveikta Covid-19 epidemijos ir jusu paskyra bus išjungta iš karto po musu sistemos patvirtinimo.

Email INC www.stanford.edu
© 2020 S ecurity Email Verification All Rights Reserved.

Nuotrauka Stanford Edu.

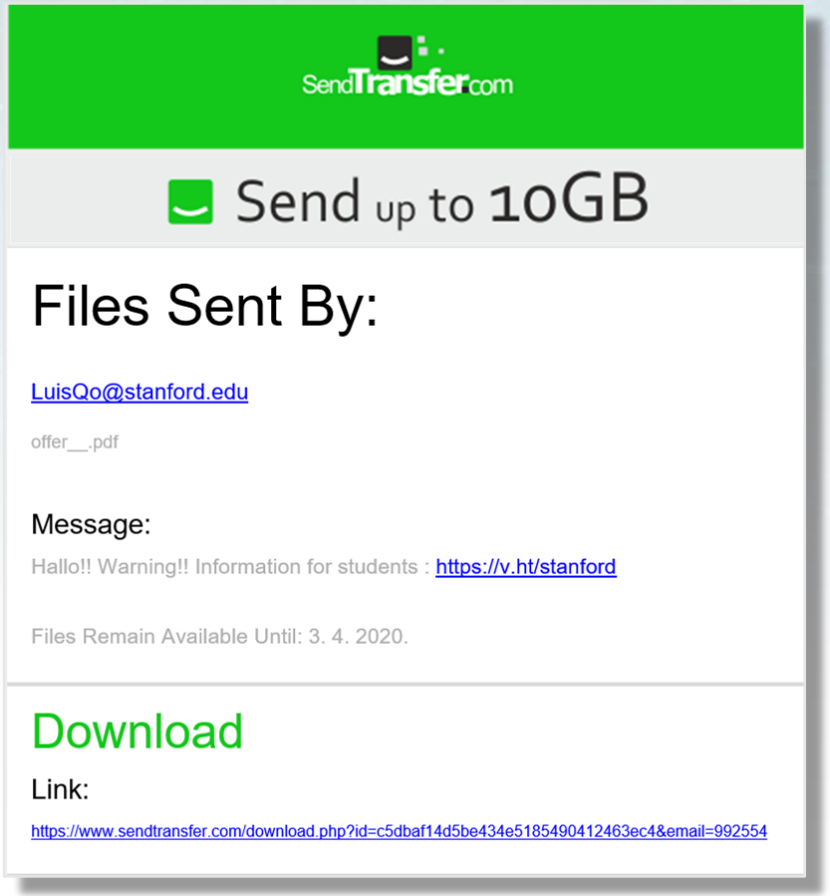
CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Pagrindinių požymių atpažinimas

- Teisėti el. pašto šaltiniai nesiunčia nepageidaujamų priedų

Nuotrauka Sonicwall Phishing Test

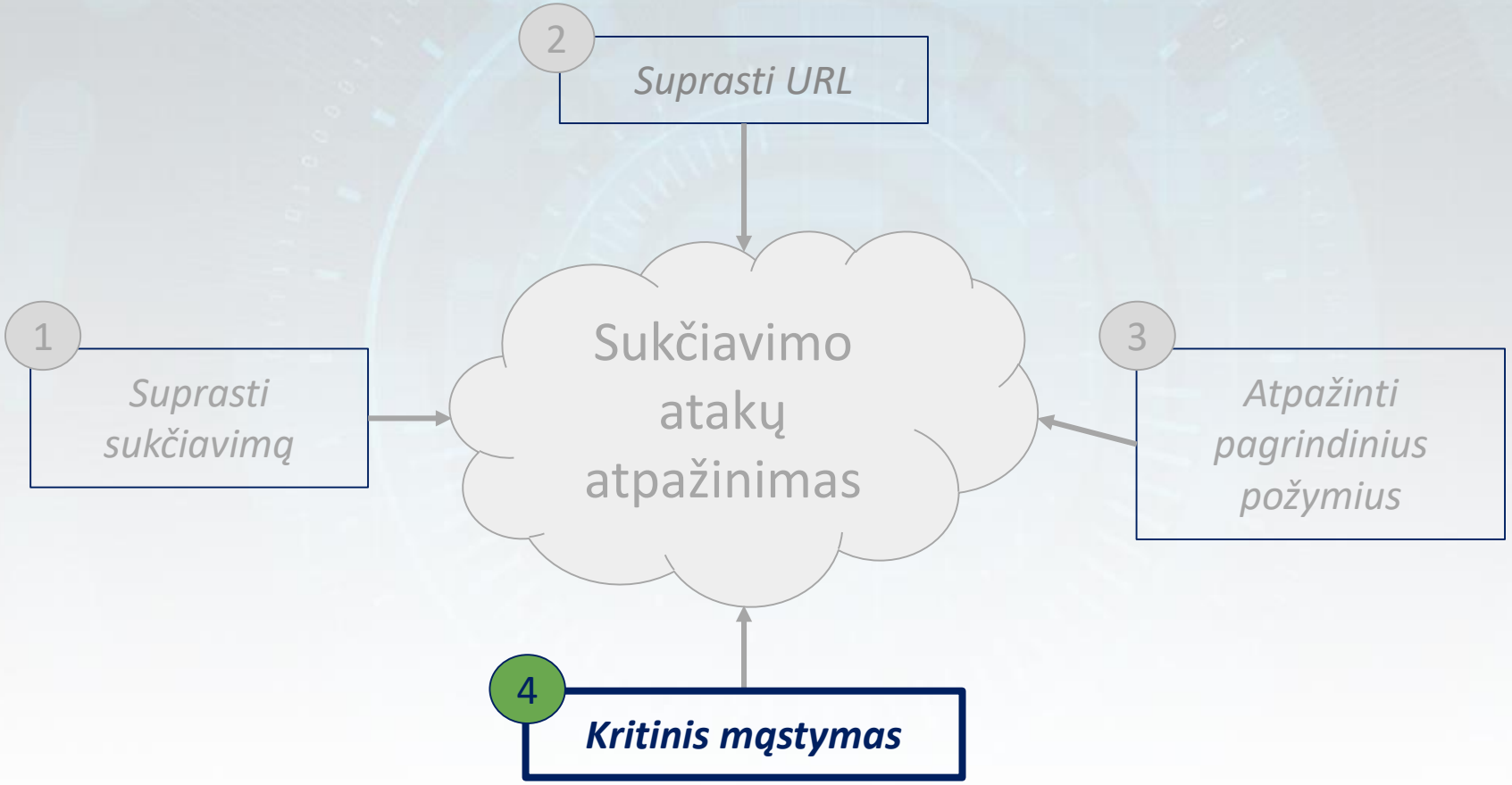


Nuotrauka Stanford Edu.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Turinys


2
Suprasti URL
1
Suprasti sukčiavimą
Sukčiavimo atakų atpažinimas
3
Atpažinti pagrindinius požymius
4
Kritinis mąstymas

Kritinis mąstymas

Sukčiavimo (angl. phishing) aptikimas apima apgaulės aptikimą.

Prieš imdamiesi veiksmų skirkite daugiau laiko pranešimų peržiūrai

Patikrinimas vietoje: Ar žinutėje tikrinami visi pagrindiniai požymiai?

Kritinis mąstymas

- Būkite ypač atsargūs, jei nesate tikri, kad pažįstate siuntėją.

  Prisimeni TK iš mokyklos?

- Apsimestinis žinomumas gali sukelti pakankamą pasitikėjimą, kad galėtumėte spustelėti kenkėjiškus URL adresus.

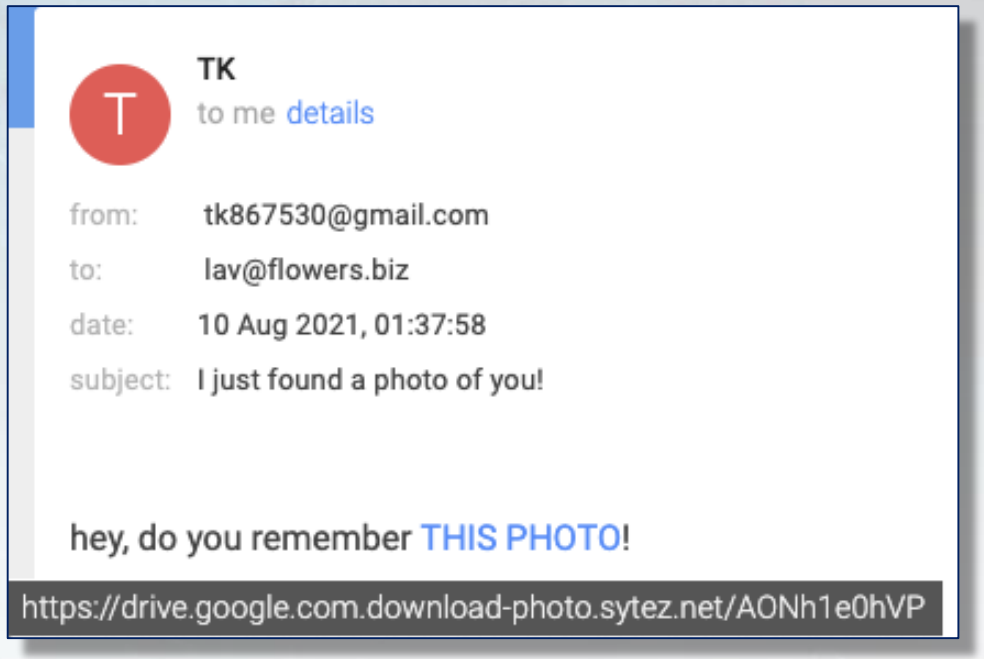
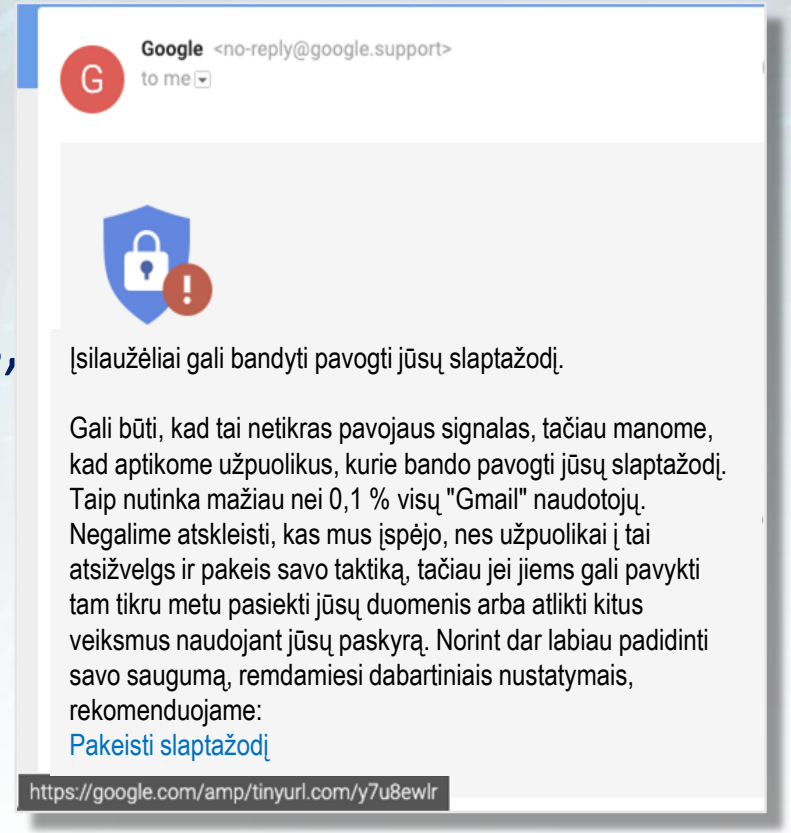


Photo by Jigsaw, Google.

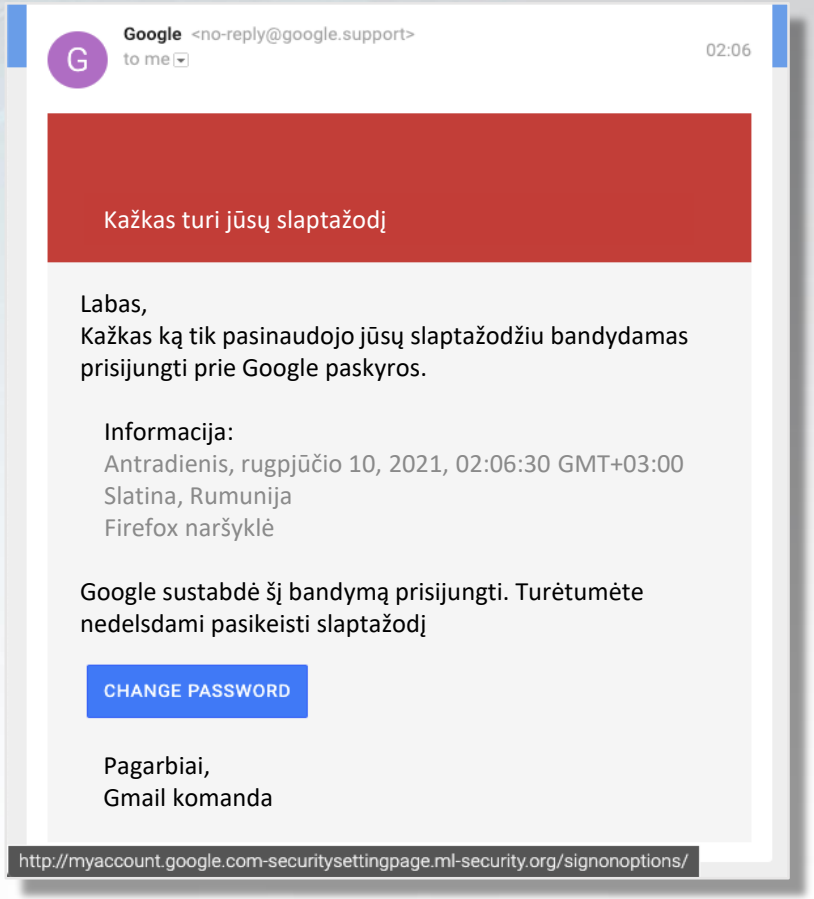
Be to, tikrasis domeno vardas yra „*sytez.net*“, ne „Google drive“.

Kritinis mąstymas

- Atidžiau žiūrėkite į el. laiškus, kuriuose prašoma imtis skubių veiksmų



Nuotrauka Jigsaw, Google.

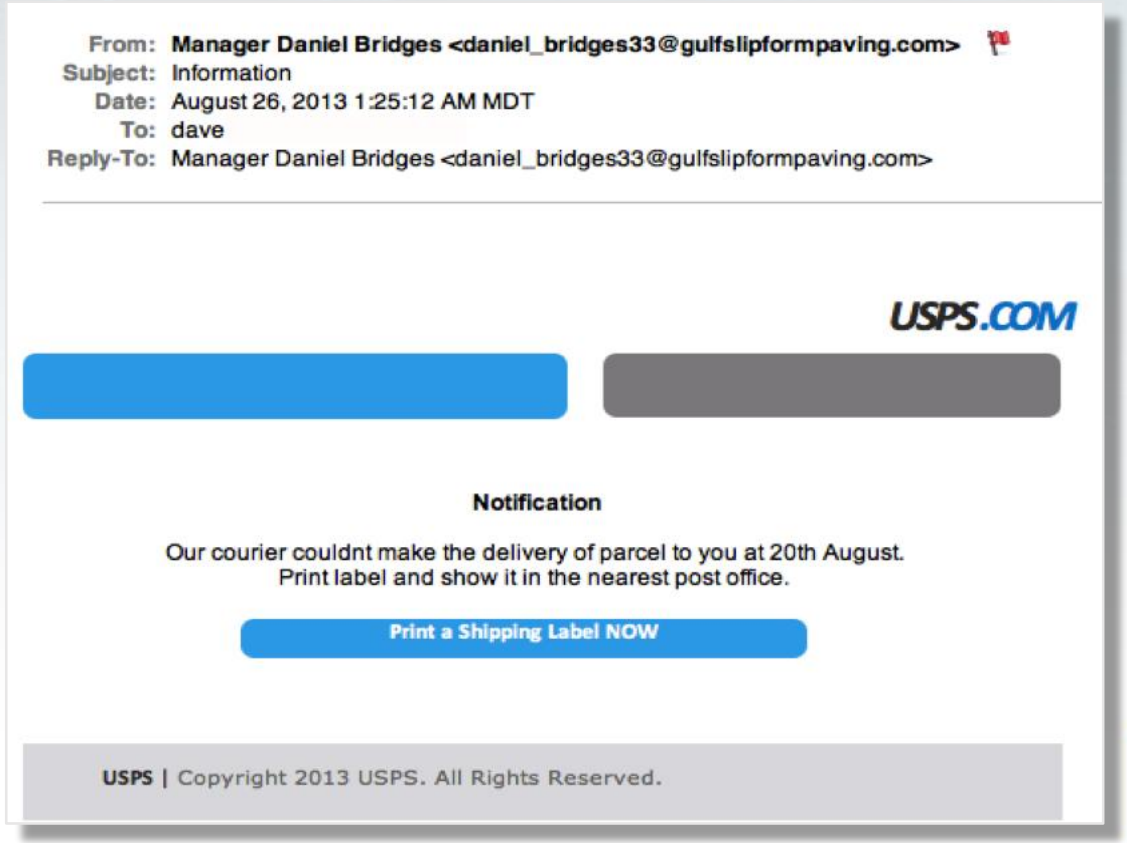


CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kritinis mąstymas

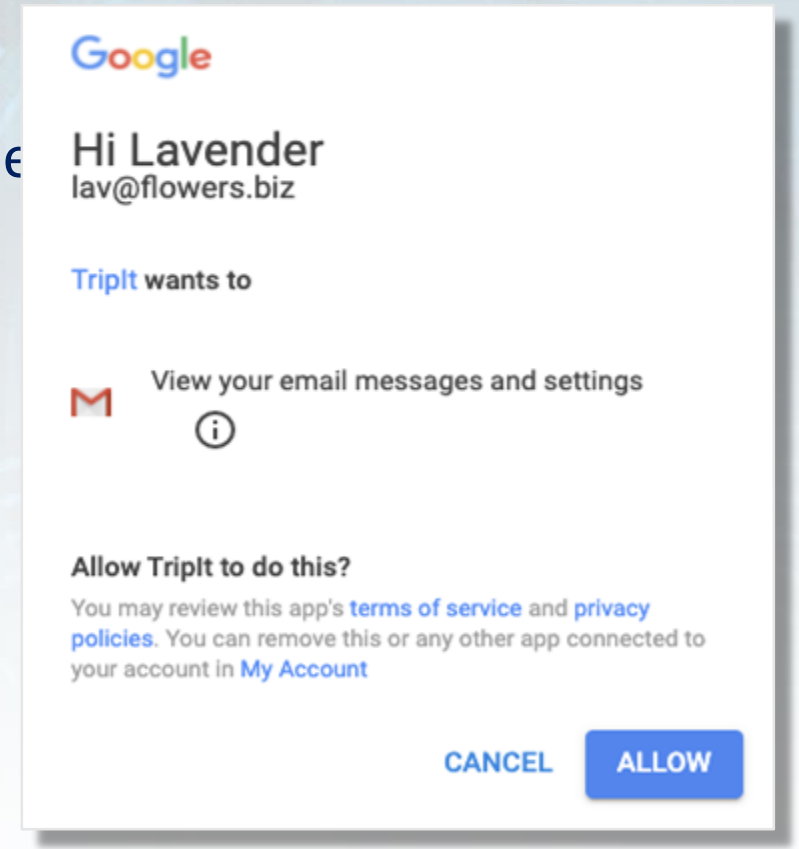
- Atkreipkite dėmesį į el. laiškus, kuriuose raginama pereiti į išorinę svetainę. Užvedus pelės žymeklį ne tik ant akivaizdžių nuorodų, bet ir ant viso el. laiško rėmo, gali būti rodomas paslėptas URL adresas.

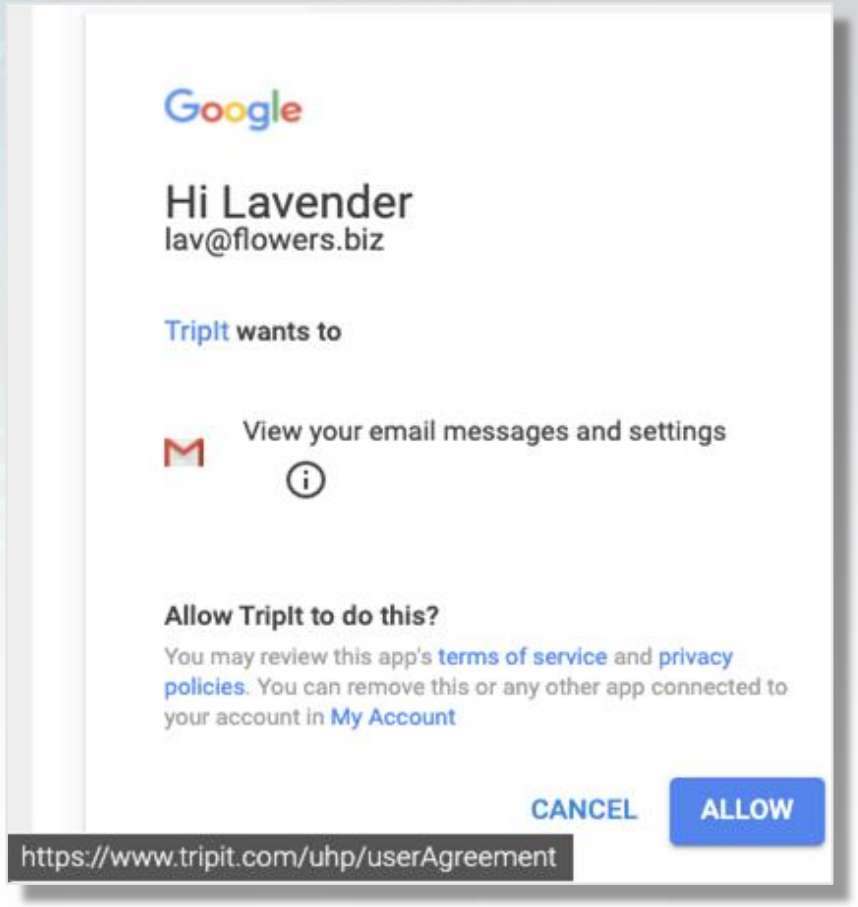


Nuotrauka Security Metrics.

Kritinis mąstymas

- Prieš suteikdami prieigą prie paskyros užklausas patikrinkite, ar pasitikite programėlių kūrėjais





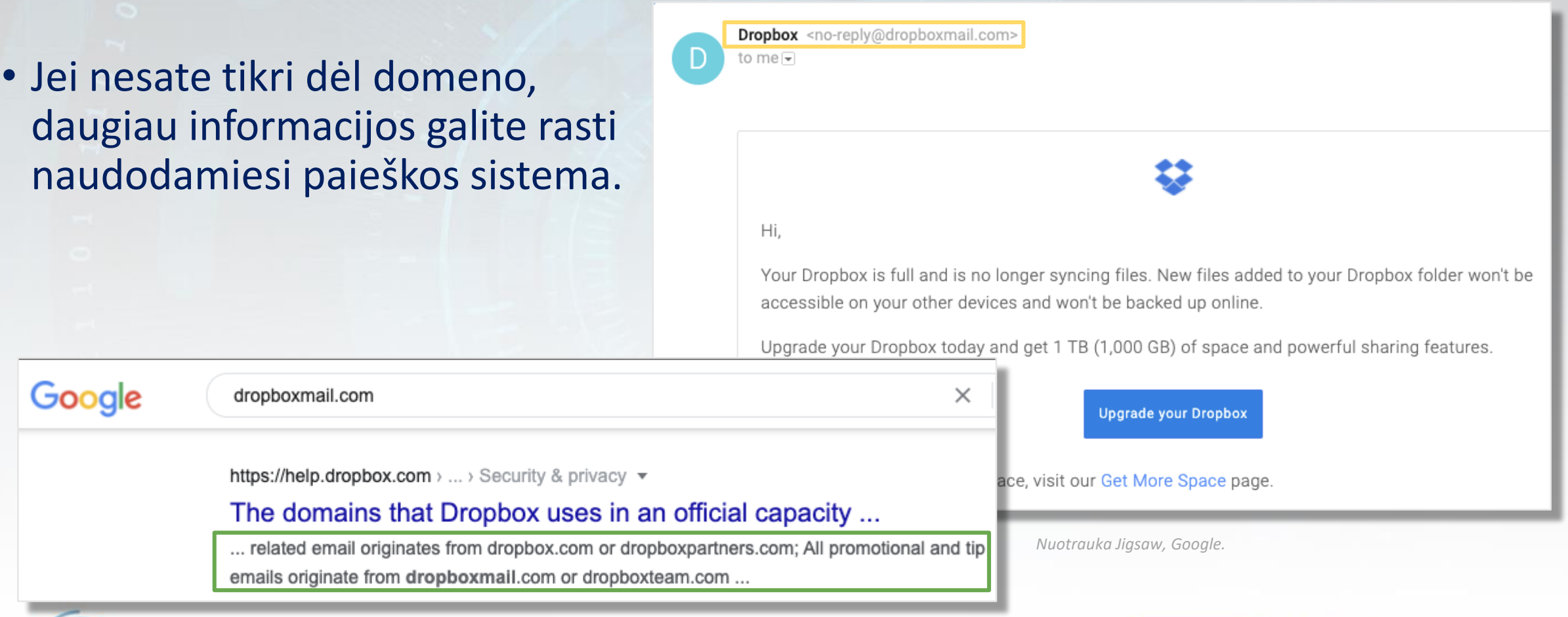
Nuotrauka Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kritinis mąstymas

- Jei nesate tikri dėl domeno, daugiau informacijos galite rasti naudodamiesi paieškos sistema.



Nuotrauka Jigsaw, Google.

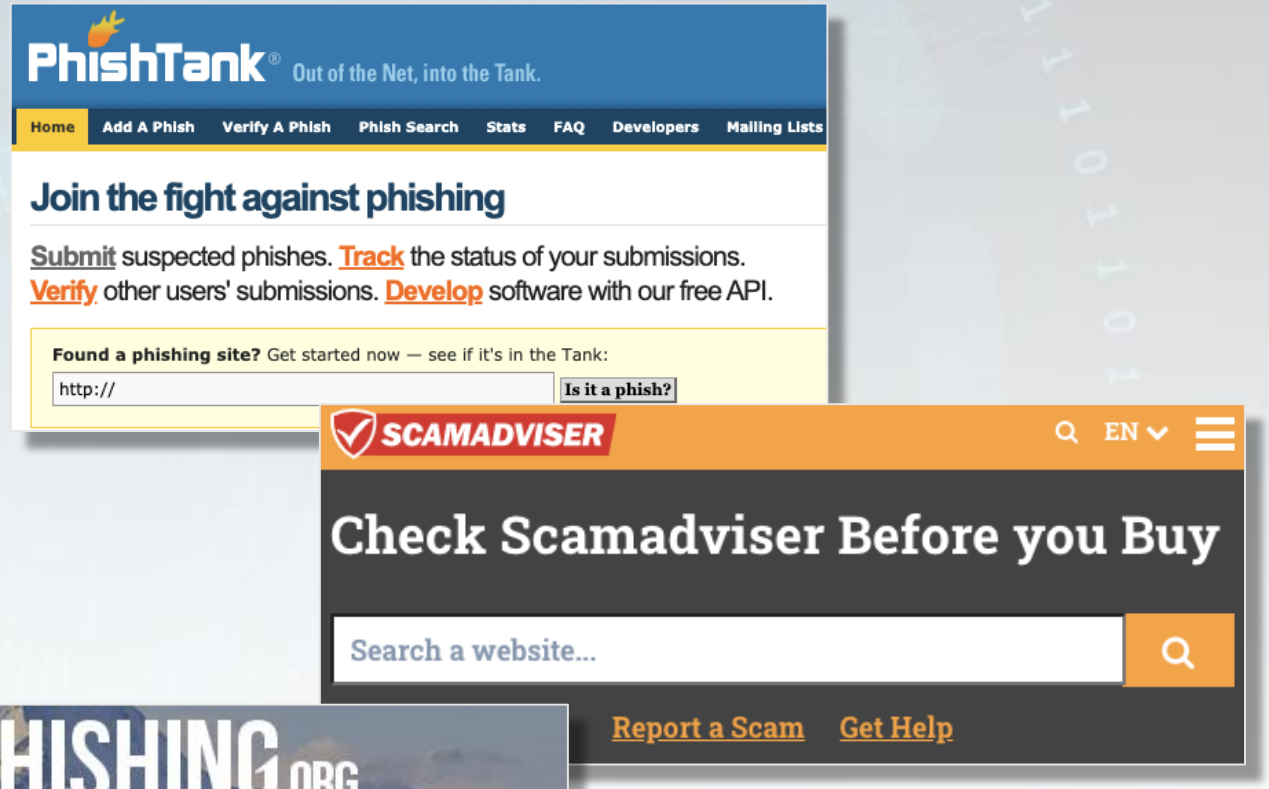
Funded by the Erasmus+ Programme of the European Union

Kritinis mąstymas

- Jei nesate tikri dėl URL adreso, yra nemokamų internetinių įrankių, skirtų ieškoti galimai apgaulingų URL adresų.

Pavyzdžiai:

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



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Santrauka


2
Suprasti URL
1
Suprasti sukčiavimą
Sukčiavimo atakų atpažinimas
3
Atpažinti pagrindinius požymius
4
Kritinis mąstymas

Užduotis

Ar galite atpažinti, kurie iš toliau pateiktų URL adresų yra sukčiavimo adresai?

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

Užduotis

Aptarkite kitus, šioje paskaitoje nepaminėtus, pagrindinius požymius (angl. red flags), su kuriais susidūrėte realiame gyvenime arba kuriuos atpažinote iš pateiktų sukčiavimo pavyzdžių.

Užduotis

Eikite į ***PhishTank*** ir pasirinkite sukčiavimo analizės pavyzdį iš neseniai pateiktų duomenų („Recent submissions“).

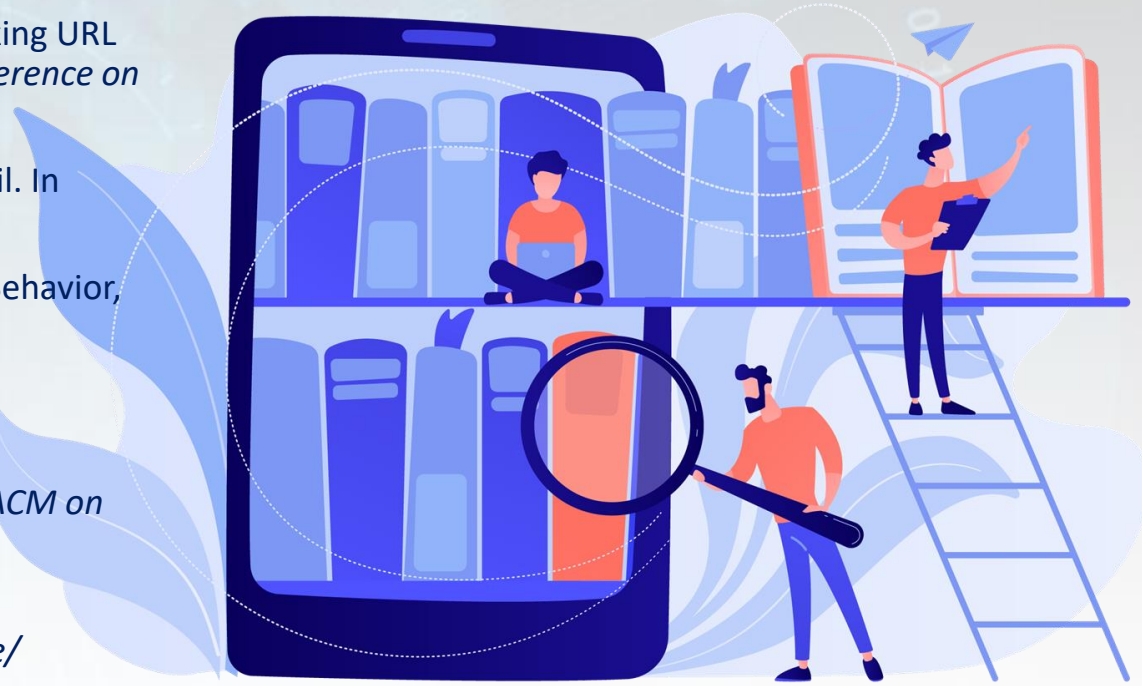
- *Ar galite pasakyti, ar tai sukčiavimo atvejis, ar ne?*
- *Kokie buvo sukčiavimo požymiai?*
- *Spustelėkite „view technical details“ (peržiūrėti techninę informaciją). Ko galite iš jo pasimokyti?*

https://phishtank.org

Papildomi skaitiniai

Medžiaga, naudota rengiant šią paskaitą

- **Rupa, D.C.C., Srivastava, G., Bhattacharya, S., Reddy, P., Gadekallu, T.R.R.** (2021, August). A machine learning driven threat intelligence system for malicious url detection. In: *The 16th International Conference on Availability, Reliability and Security. ARES 2021*, Article 154, 1–7. *https://doi.org/10.1145/3465481.3470029*
- **Althobaiti, K., Meng, N., & Vaniea, K.** (2021, May). I Don't Need an Expert! Making URL Phishing Features Human Comprehensible. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-17).
- **Drake, C. E., Oliver, J. J., & Koontz, E. J.** (2004, July). Anatomy of a Phishing Email. In CEAS.
- **Abroshan H.:** Root Causes of Falling Victim to Phishing – The Effects of Human Behavior, Emotions, and Demographics., *PhD thesis*, Ghent University, 2021
- **Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I.** (2021). Phishing Attacks: Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science, 3, 6.*
- **Wash, R.** (2020). How experts detect phishing scam emails. *Proceedings of the ACM on Human-Computer Interaction, 4 (CSCW2), 1-28*.
- **SavvySecurity** (2021). 10 Phishing Email Examples You Need to See. *https://cheapsslsecurity.com/blog/10-phishing-email-examples-you-need-to-see/*
- **Ellis, D**. 7 Ways to Recognize a Phishing Email: Email Phishing Examples. *https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email*



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Trumpi vaizdo įrašai

- Sukčiavimo el. laiškų anatomija
  - ***https://youtu.be/3gpOM9c6mmA***
- Sukčiavimo atakos paaiškinimai
  - ***https://youtu.be/Y7zNlEMDmI4***
  - ***https://youtu.be/gqhPkeXMeh0***
- Kaip atpažinti ir apsisaugoti nuo sukčiavimo
  - ***https://youtu.be/R12_y2BhKbE***

Funded by the Erasmus+ Programme of the European Union

Dėkojame!