Funded by the
Erasmus+ Programme
of the European Union

Küberrünnakute mõistmise ja nendega toimetuleku ülevaade

Andmepüügirünnakute äratundmine

Kuidas andmepüügirünnakuid ära tunda?

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

Õppe-eesmärgid

Selgitage e-ohutuse kontseptsiooni ja küberohtudele ennetava lähenemise tähtsust küberhügieeni kontseptsiooni kaudu

Tuvastada ja käsitleda küberrünnakuid

CyberPhish
Safeguarding your digital future

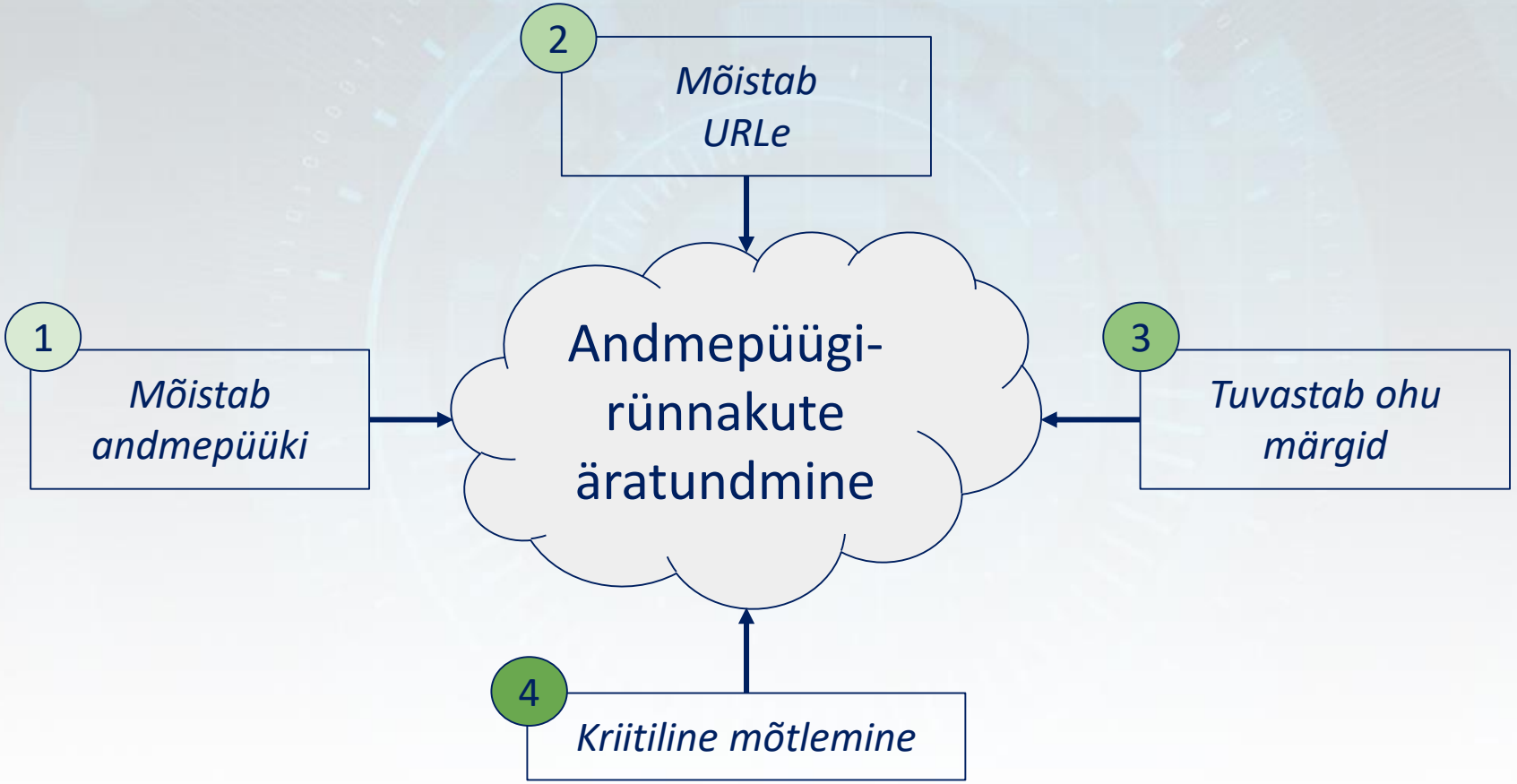
Funded by the Erasmus+ Programme of the European Union

Õpilase töökoormus

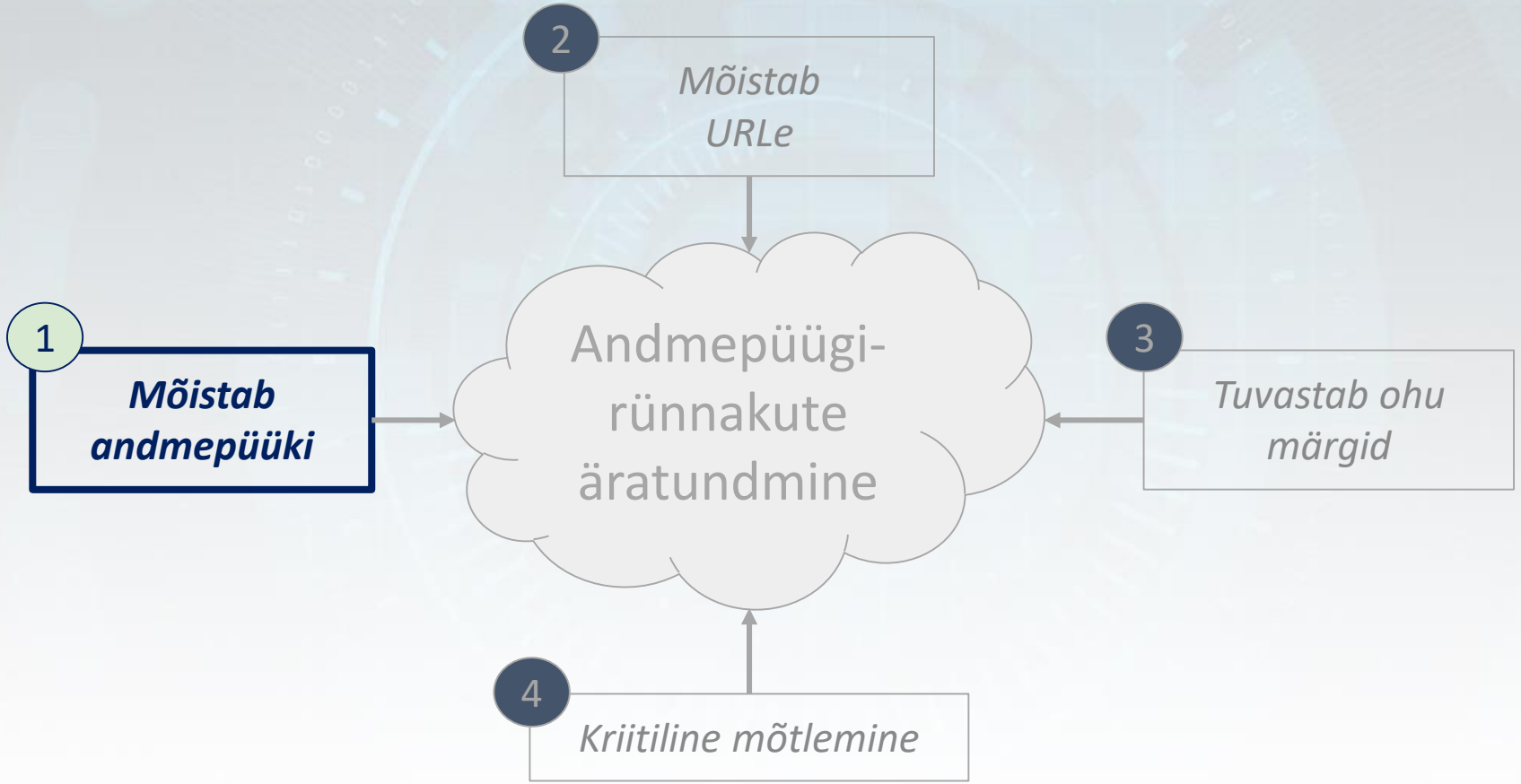
Loengud	2 h
Audio- ja videomaterjal	2 h
Juhtumiuuringud	2 h
Lisalugemine	4 h
Eksamiks valmistumine	2 h

Funded by the Erasmus+ Programme of the European Union

Loenguteemad



Loenguteemad



Mis on andmepüügirünnak?

Andmepüük *on sotsiaalse manipuleerimise pettus, mille tagajärjeks võib olla andmete kadu, maine kahjustamine, identiteedivargus, rahakaotus ja palju muud kahju inimestele ja organisatsioonidele. Andmepüügipettus algab tavaliselt e-kirjaga, mis püüab võita potentsiaalse ohvri usaldust ja veenda teda ründaja soovitud toiminguid tegema.*

[*Abroshan, 2021*]

Funded by the Erasmus+ Programme of the European Union

Andmepüügirünnaku allikad

Photo by Google

- E-mail
- Veebisaidid
- Sotsiaalmeedia
- Mobiil (SMS, hääl)
- Igasugune suhtlusvorm...

Funded by the Erasmus+ Programme of the European Union

Andmepüügisõnumi anatoomia

- Sõnumi allikas
  - *kes mulle sõnumi saadab?*
- Sõnumi sisu
  - *millest sõnum räägib?*
- Hüperlingid/manused
  - millele see sõnum veel viitab?

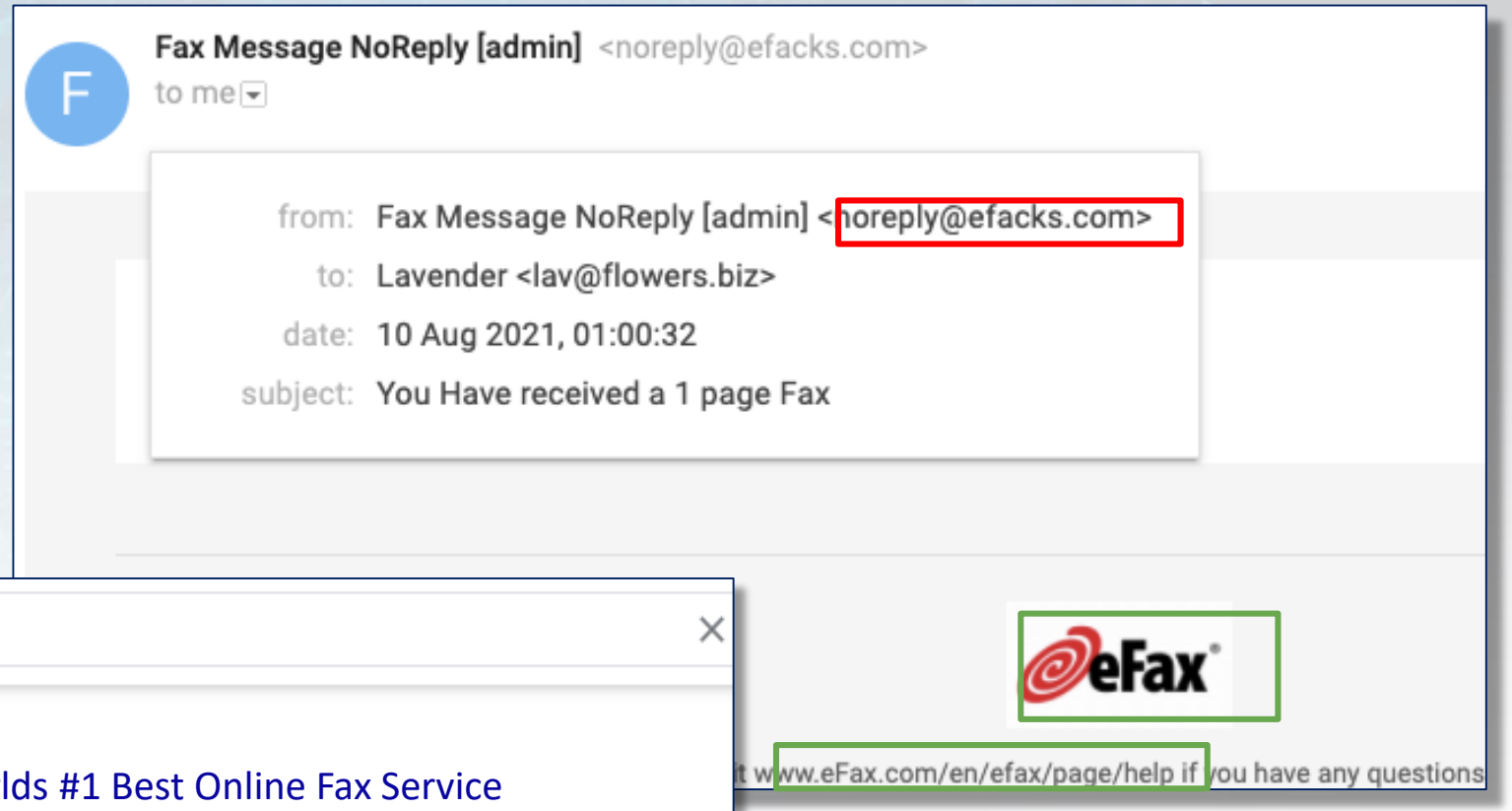
Photo by istockphoto.com

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Sõnumi allikas

- Andmepüük võib trikitada sarnase saatja meiliga.



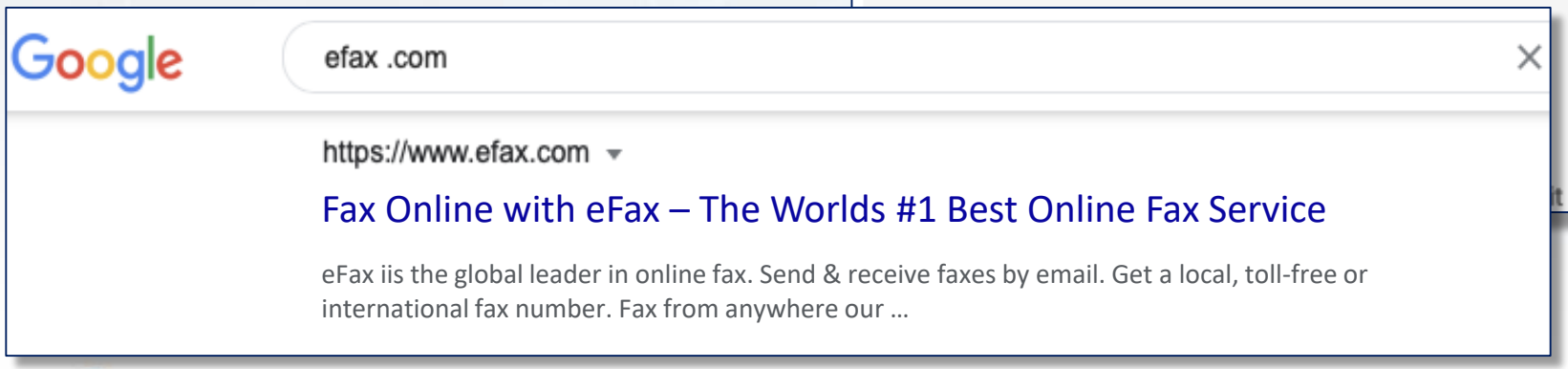


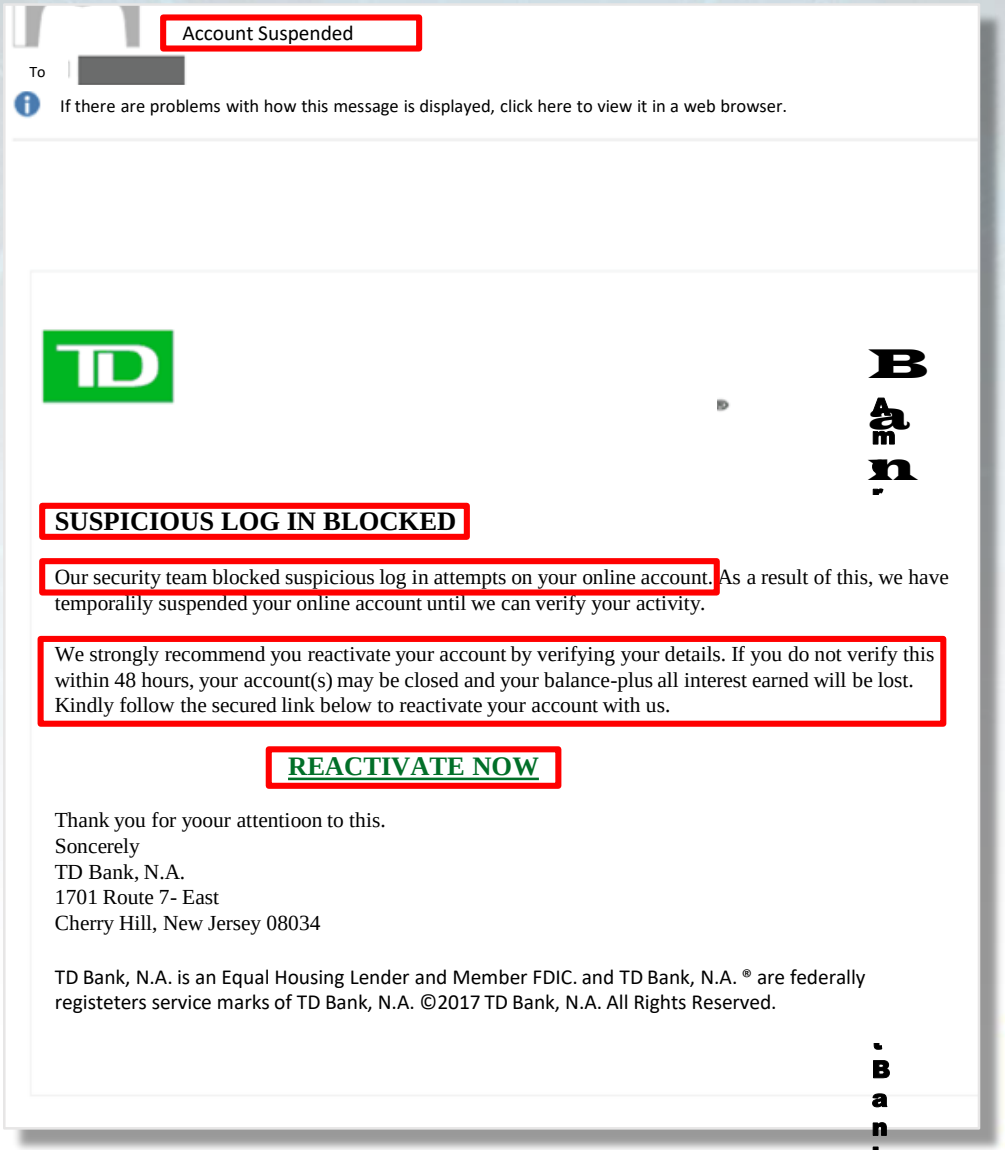
Photo by Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Sõnumi sisu

- Pettus hirmu, kiireloomulisuse, autoriteedi, ahnuse, sõpruse, abi ja meeleheite kaudu.



Account Suspended

To [redacted]

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

TD Bank

SUSPICIOUS LOG IN BLOCKED

Our security team blocked suspicious log in attempts on your online account. As a result of this, we have temporalily suspended your online account until we can verify your activity.

We strongly recommend you reactivate your account by verifying your details. If you do not verify this within 48 hours, your account(s) may be closed and your balance-plus all interest earned will be lost. Kindly follow the secured link below to reactivate your account with us.

REACTIVATE NOW

Thank you for yoour attentioon to this.
Soncerely
TD Bank, N.A.
1701 Route 7- East
Cherry Hill, New Jersey 08034

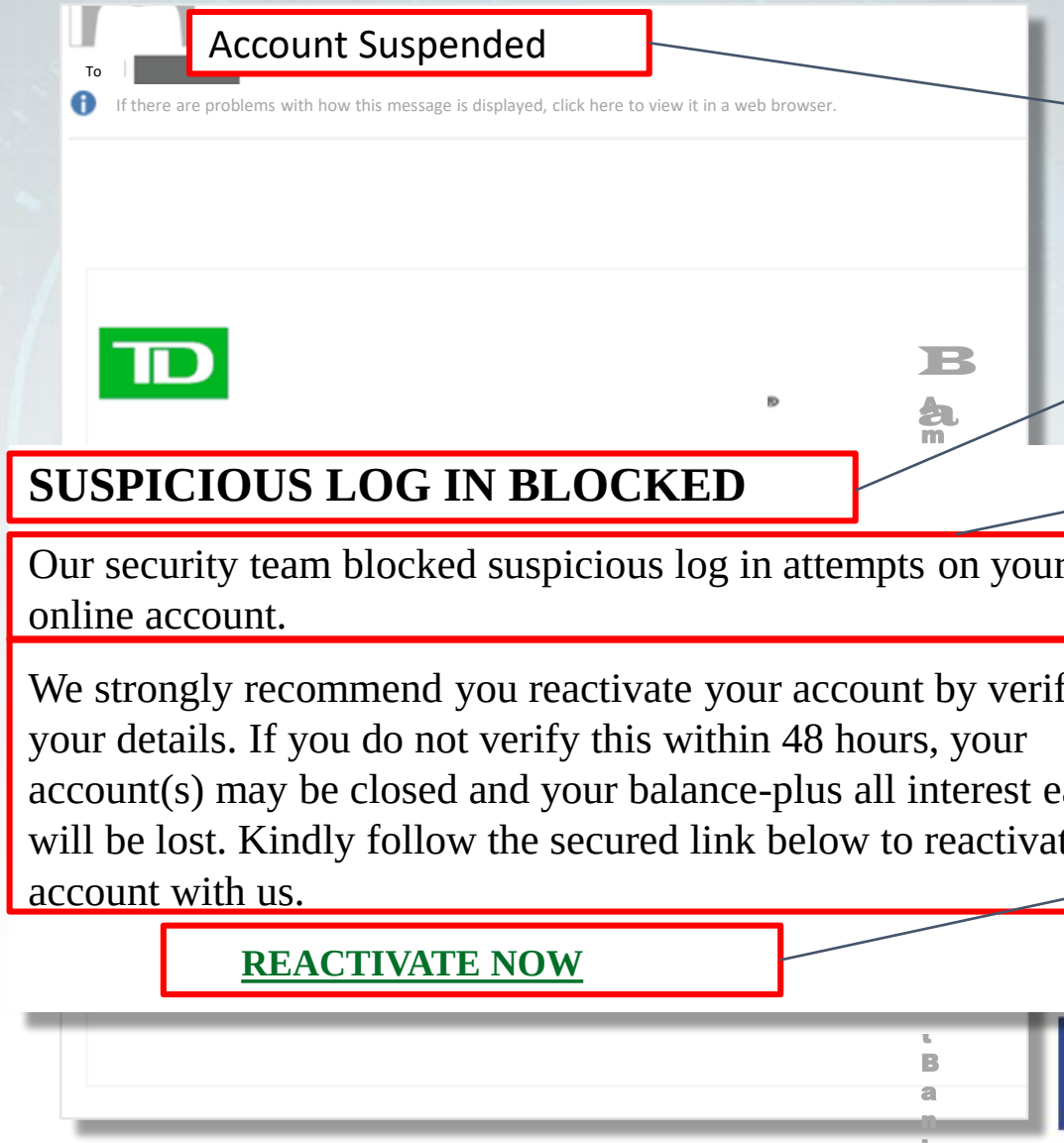
TD Bank, N.A. is an Equal Housing Lender and Member FDIC. and TD Bank, N.A. ® are federally registeters service marks of TD Bank, N.A. ©2017 TD Bank, N.A. All Rights Reserved.

TD Bank®

Photo by Sonicwall Phishing Test

Sõnumi sisu

- Pettus hirmu, kiireloomulisuse, autoriteedi, ahnuse, sõpruse, abi ja meeleheite kaudu



Hirm

Hirm

Abi

Kiireloomulisus + meeleheide

Kiireloomulisus

Photo by Sonicwall Phishing Test

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Hüperlingid/manused

- Manused võivad sisaldada erinevat tüüpi faile, mis võivad olla pahatahtlikud
- Hüperlingid näitavad faili asukohta veebis ja võivad ohvreid suunata pahatahtlikele veebisaitidele või pahatahtlikke faile alla laadima.

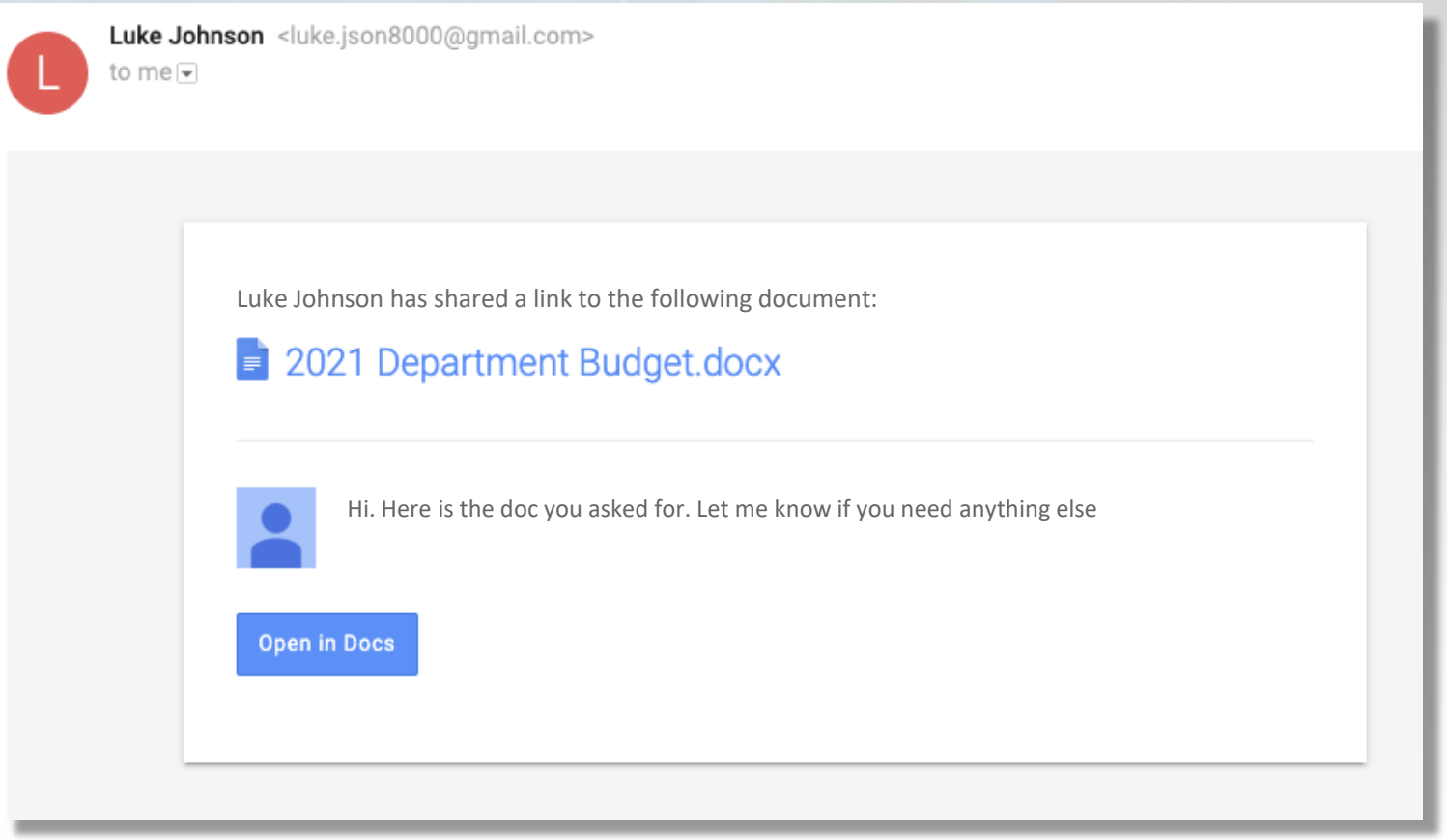


Photo by Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Hüperlingid/manused

- URL-i kuvamiseks hõljutage kursorit nende hüperlinkide kohal (või hõljutage kursorit nende kohal).
- Kuvatav URL on Google Drive'i domeeni ebaturvaline imitatsioon

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

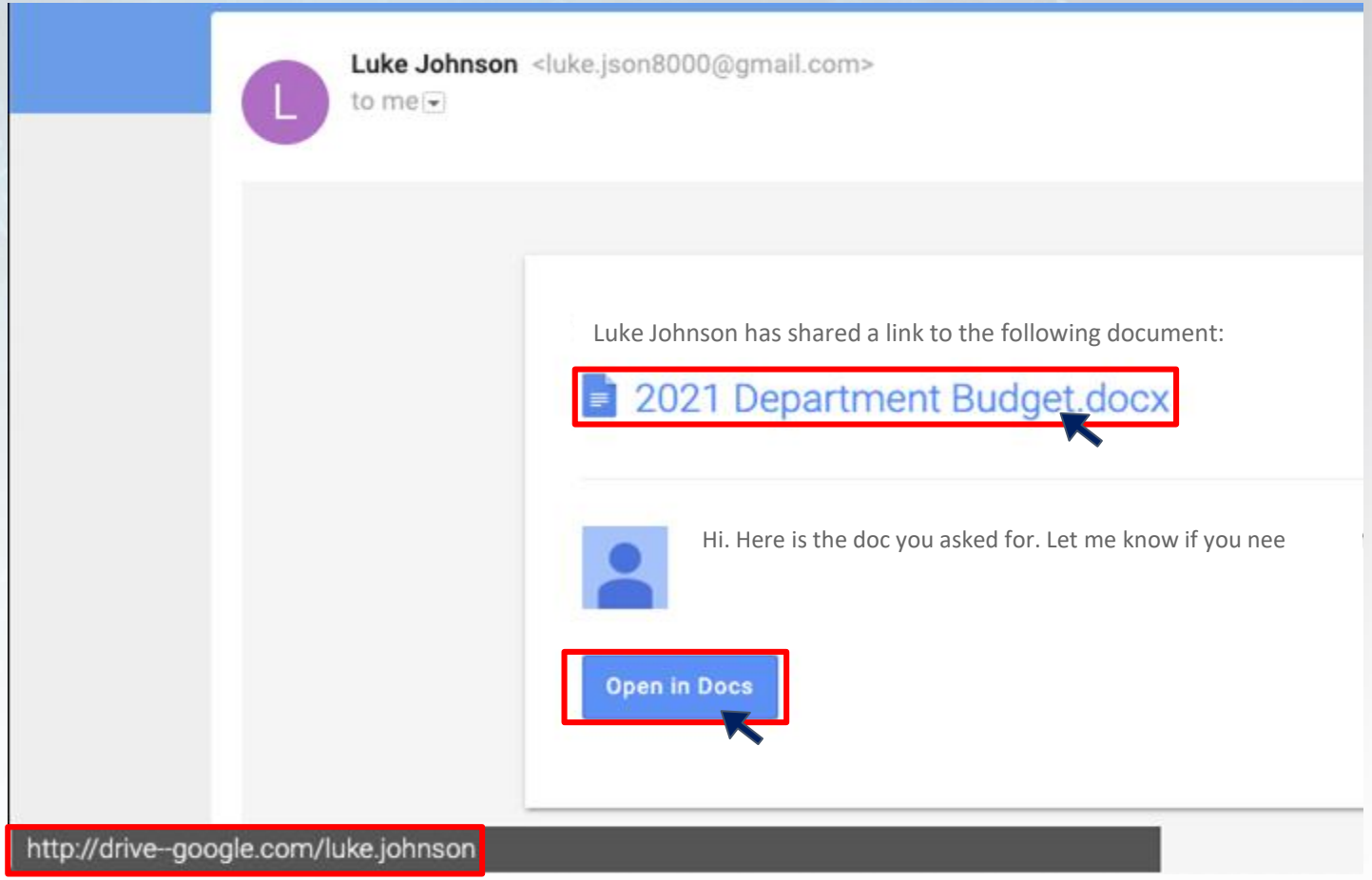
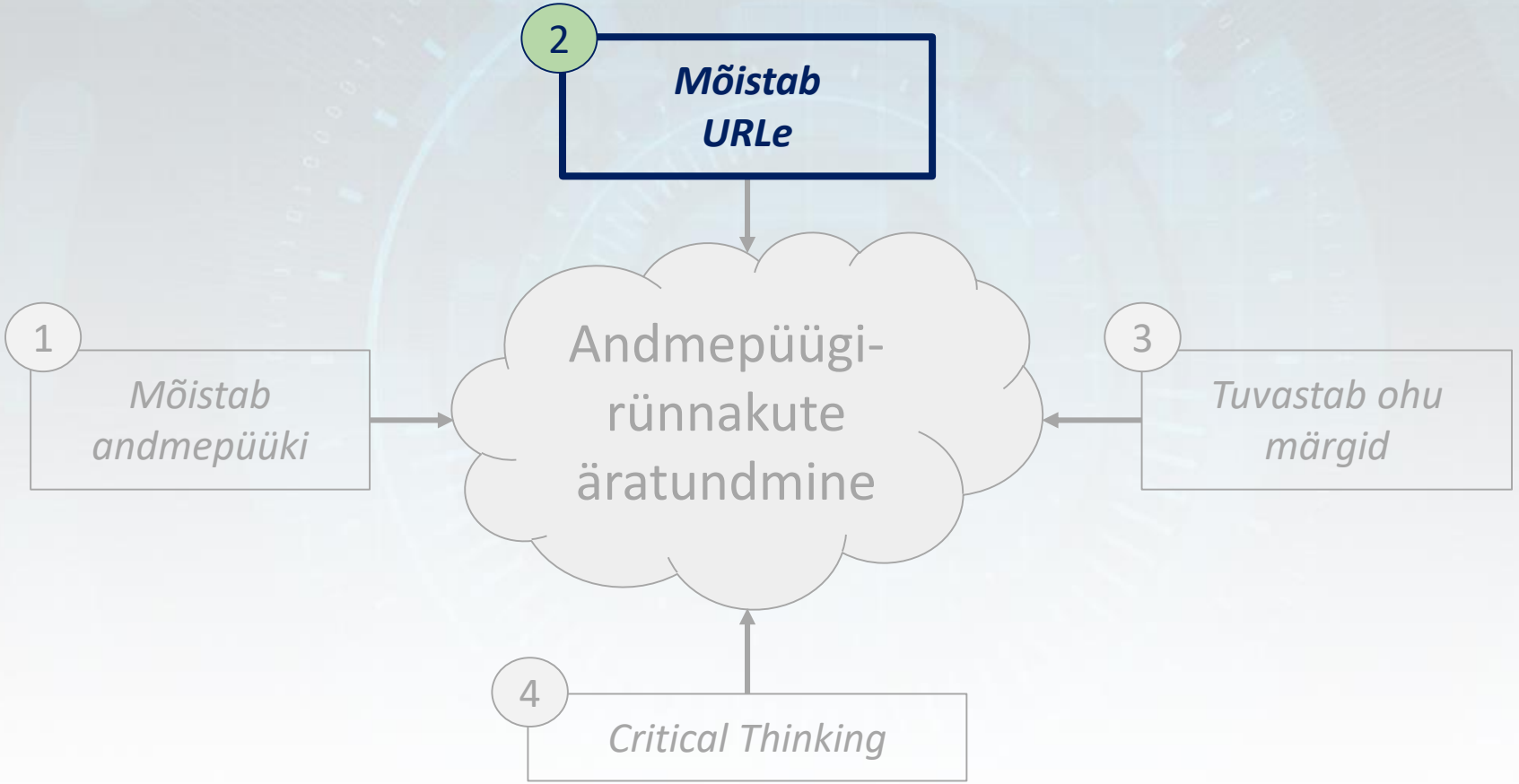


Photo by Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Loenguteemad

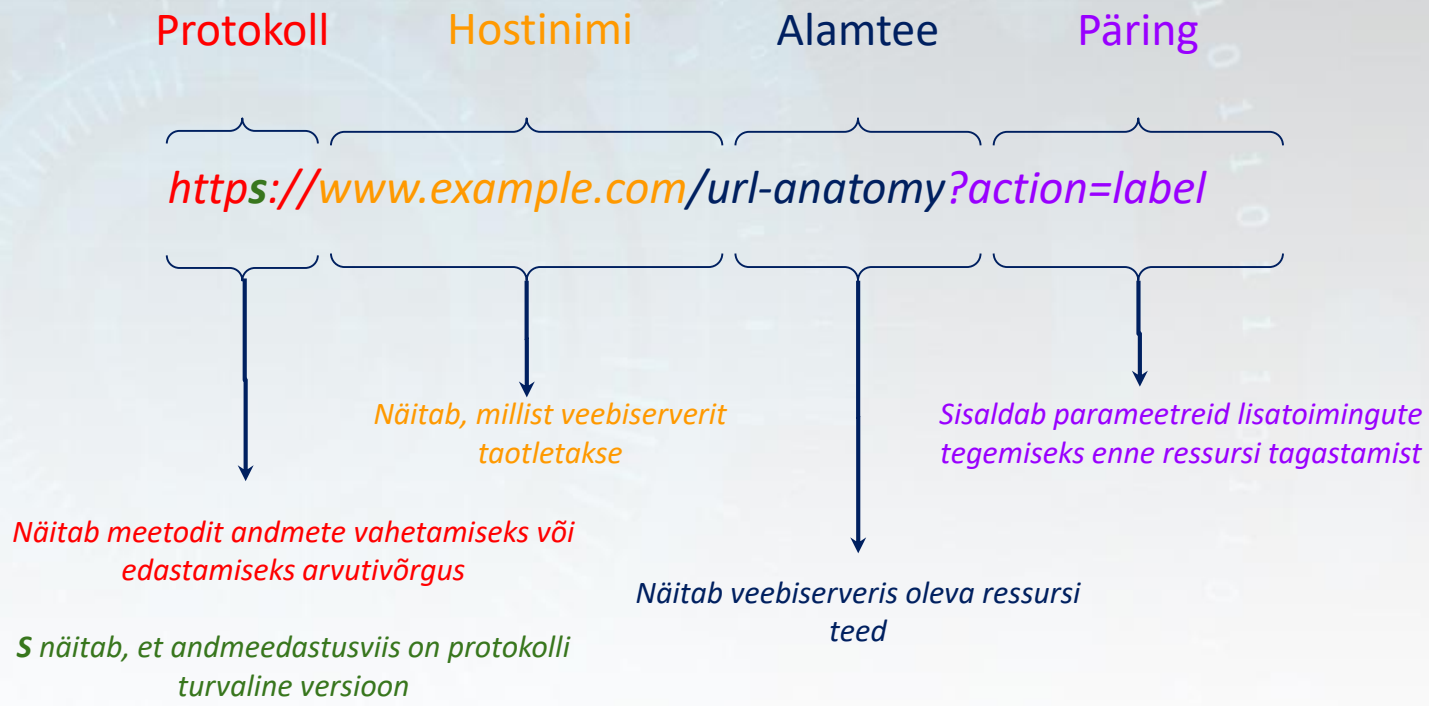


CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Mõistab URLe

- Uniform Resource Locator (URL) on defineeritud unikaalse ressursi aadress veebis.

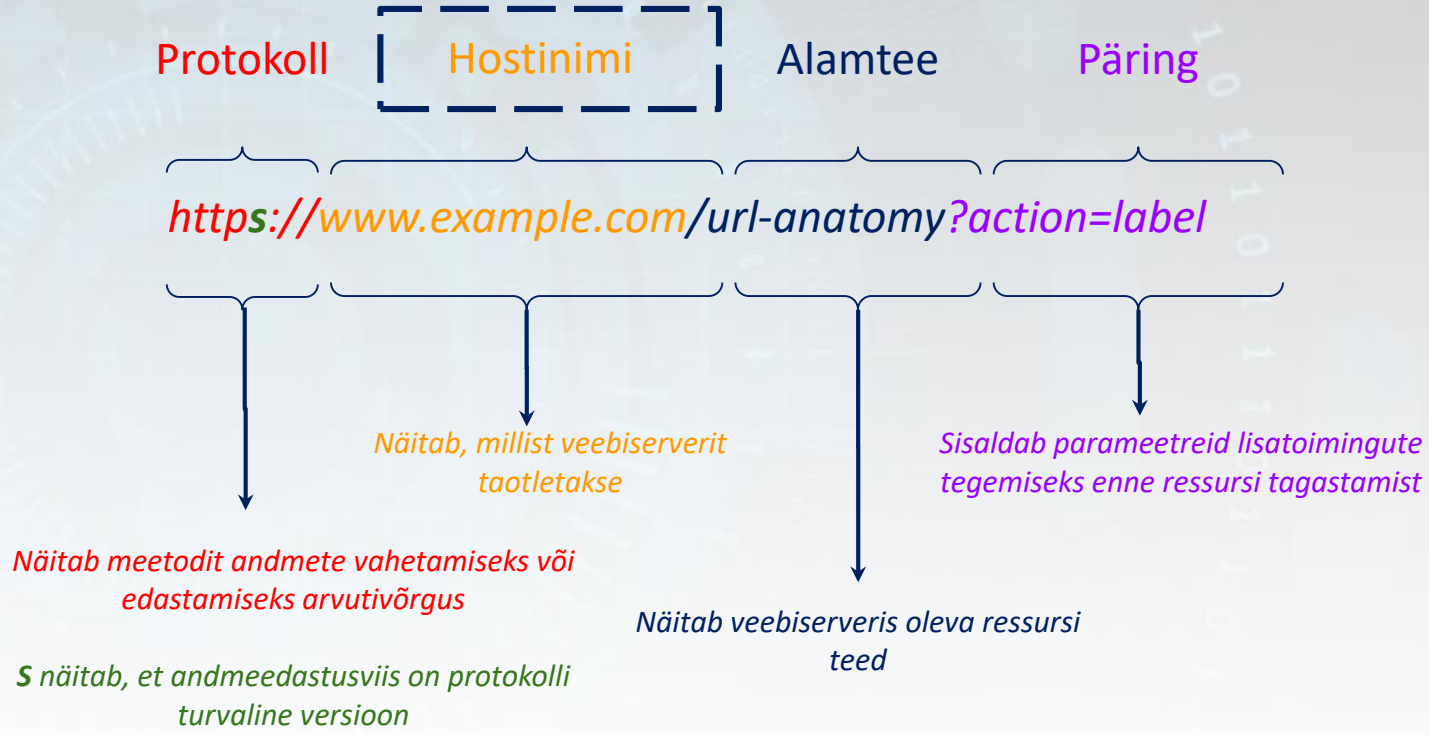


https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL
Protocol, Simple Object Access. "URL." (2007).

Funded by the Erasmus+ Programme of the European Union

Mõistab URLe

- Uniform Resource Locator (URL) on defineeritud unikaalse ressursi aadress veebis.

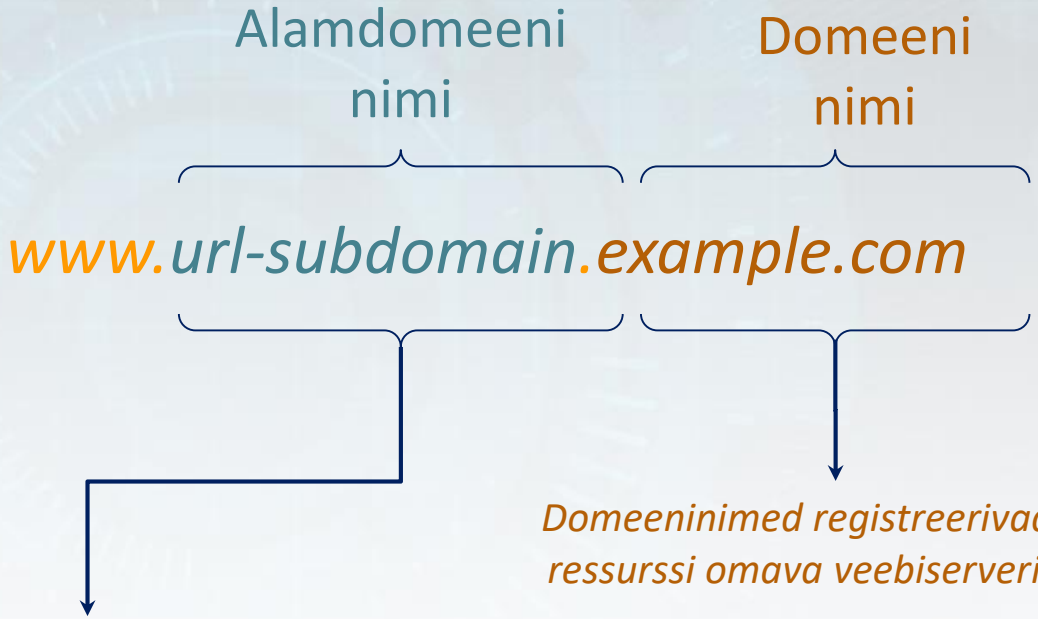


https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL
Protocol, Simple Object Access. "URL." (2007).

Funded by the Erasmus+ Programme of the European Union

Mõistab URLe

- URL-is oleva hosti nimi võib sisaldada mitut alamdomeeni nime



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

Mõistab URLe

Andmepüügiga püütakse sageli ohvreid URL-idega petta.

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

Protokoll	*http*
Hostinimi	*amazon.com.mailru382.co*
Alamtee	*/packagedelivery/2017Dk25RE3*
Domeeni nimi	*mailru382.co*
Alamdomeen 1	com
Alamdomeen 2	*amazon*

Funded by the Erasmus+ Programme of the European Union

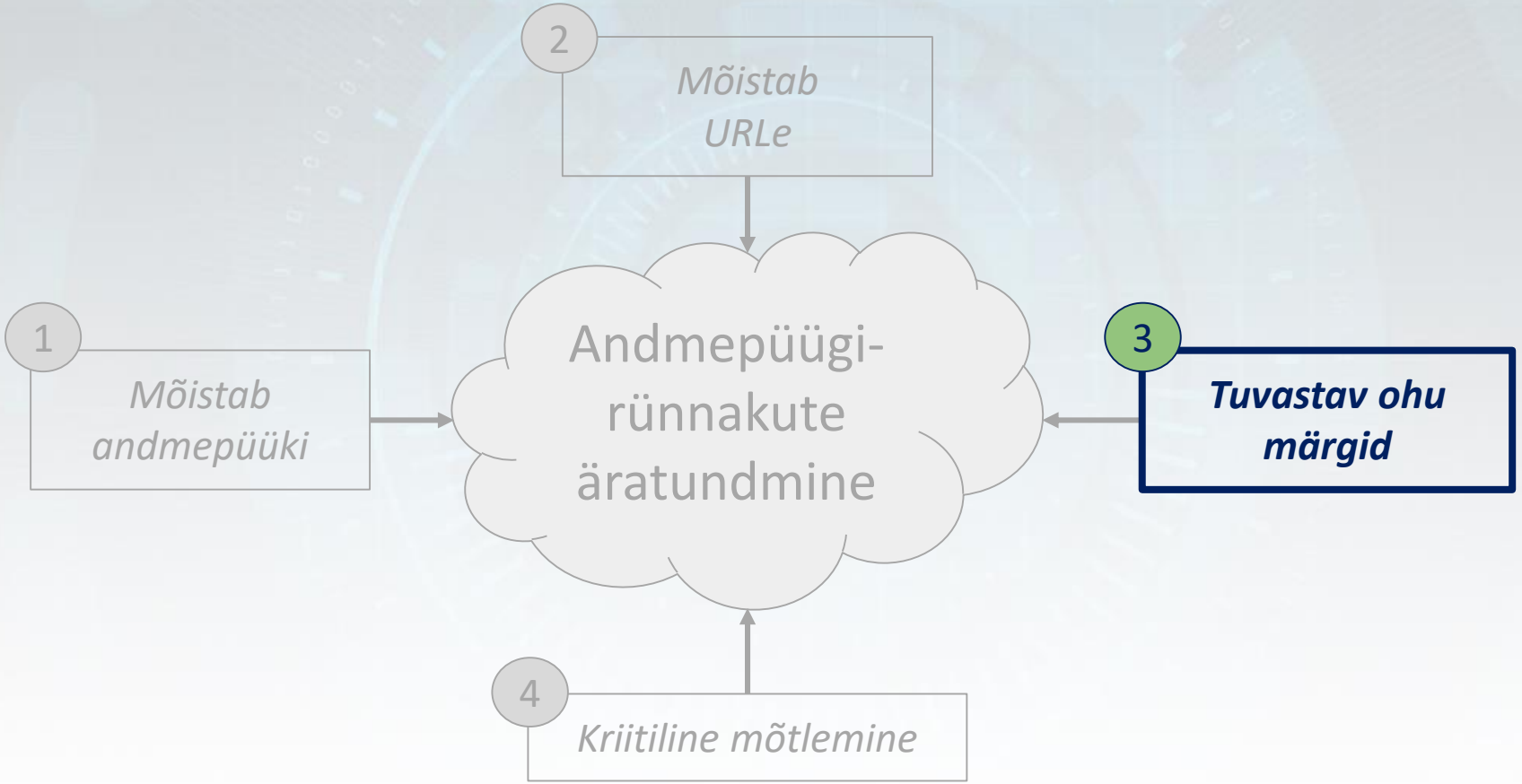
Mõistab URLe

Muud nipid URL-iga ...	Näide
• URL-i protokollil puudub turvalise protokolli indikaator.	URL kasutab *http* mitte *https*
• Domeen on nähtavalt sarnane tuntud domeeniga, kuid tegelikult erinev.	*google.com* valesti kirjutatud kui *googgle.com*
• Keerulise välimusega domeeninimi, mis ajab ohvri segadusse, st IP-aadress, kuueteistkümnend- või kümnendmärgid, sümbol domeenis.	IP aadress - http://20.85.220.142/telas/caixa/ Sümbolid - https://epic.app/#con@sceneworld.org Numbrid- http://2130706433/evil.com
• URL võib sisaldada domeenis hästi tuntud nime, kuid see ei kuulu seaduslikule allikale.	"*Instagram*" nimekujus *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

Loenguteemad



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Tuvastab ohu märgid

- Õiguspärased meiliallikad (nt ettevõtted) ei küsi teie tundlikku teavet meili teel

SUSTAINABLE DEVELOPMENT GOALS

An education employee grant on **$ 950,000.00 (Nive Hundred and fifty Thousand Dollars)** has been awarded to you by the United Nations. The united nations authorities has decided to offer you this grant as part of the global goal to assist education workers and students during this Covid-19 pademic.

The Sustainable Development Goals (SDGs) were born at the United Nations Conference on Suistainable Development in Rio de Janeiro in 2012. The objective was to produce a set of universal goals that meet the urgent environmental, political and economic challenges facing our world.

Grant funds would be made available by the UN correspondiing office once you file for this claim. Congratulations and thank you for your services.

File and Claim Education Grant Funds

First Name, (Middle name), Last Name(required)
Email(Non-Edu Email(required)
Phone number(required)
Resident and Office Address(required)

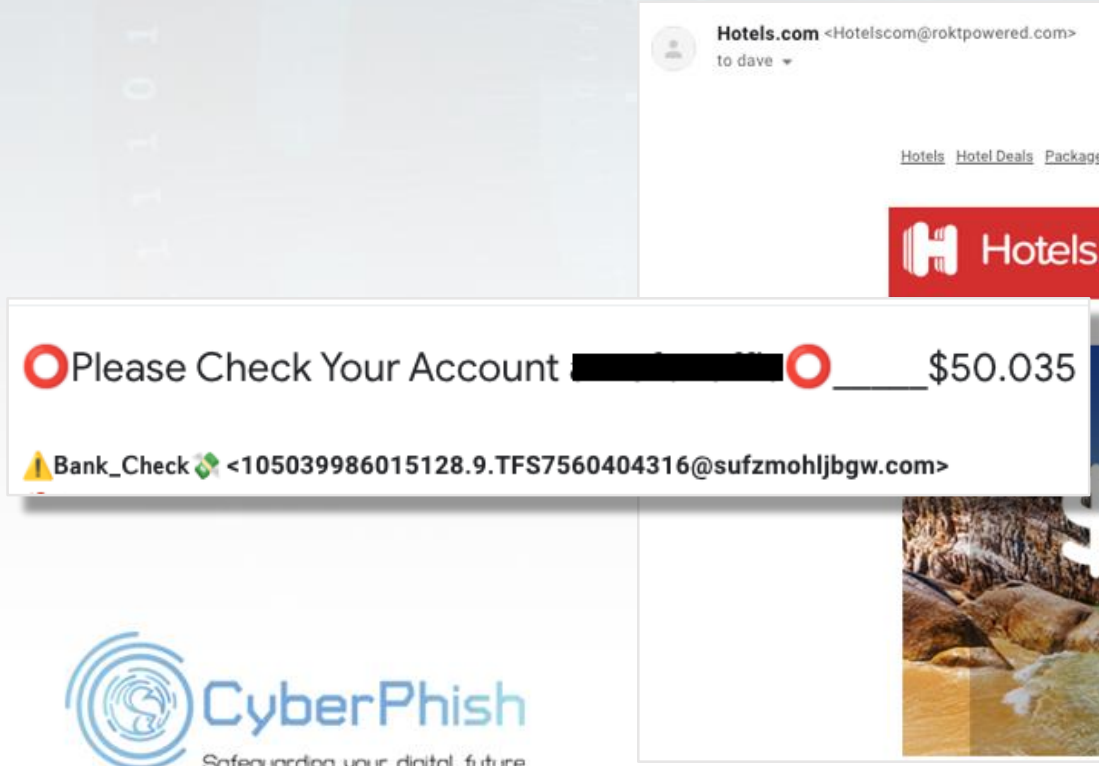
Claim response should be sent from your private Non-edu email.

Photo by Stanford Edu.

Funded by the Erasmus+ Programme of the European Union

Tuvastab ohu märgid

- Õigustatud meiliallikatel pole tavaliselt:
  - keerulised meiliaadressid
  - e-posti aadressi, e-posti domeeni või meili saatja nime mittevastavus



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Photo by Security Metrics.

Tuvastab ohu märgid

- Õigustatud meiliallikad kutsuvad teid tavaliselt teie nime järgi

From: No Reply <sarahrk@unm.edu>
Sent: Monday, June 8, 2020 9:03 AM
Subject: Notice

New message are being held in your temp folder due to a sync error.

Follow below liin to access pending messages and choose what to do with them.

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

© 2020 cs.stanford.edu

Photo by Stanford Edu.

Tuvastab ohu märgid

- Usaldus-väärsetel meiliallikatel ei ole probleeme õigekirja ja grammatikaga

From: noreply@stanford.edu <noreply@stanford.edu>
Sent: Monday, May 11, 2020 10:59 AM
Subject: stanford.edu Du to the world Covid-19 epidemic we are verifying all our Email Account users on our sever

Mail.stanford.edu Notification

Du to the world Covid-19 epidemic we are verifying all our Email Account users on our sever.

your account need to be verifiedand be secured with us immediately by download our mail.stanford.edu verification app attached and verify your email account to avoid account froom been shutdown on our sever. please note that failing to download our attached app and verify your account with us will automatically regard youor accoountt with us as affected by the Covid-19 epidemic and will lead to youor account shutdown immediately after oour system verification.

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

Photo by Stanford Edu.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Tuvastab ohu märgid

- Õiguspärased meiliallikad ei saada soovimatuid manuseid

Photo by Sonicwall Phishing Test

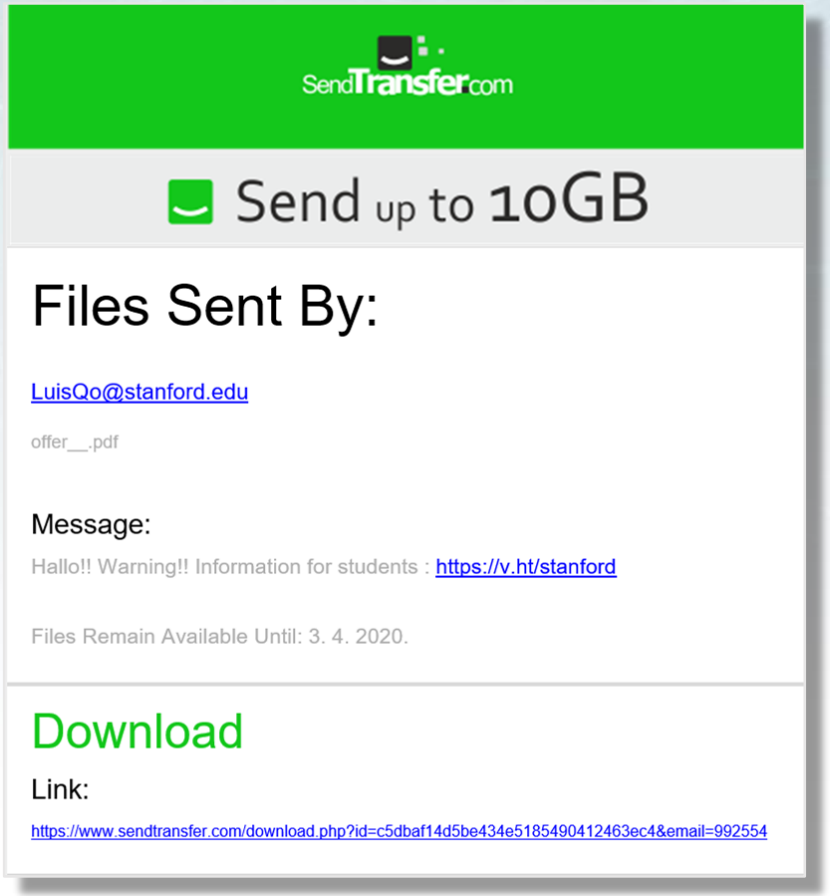
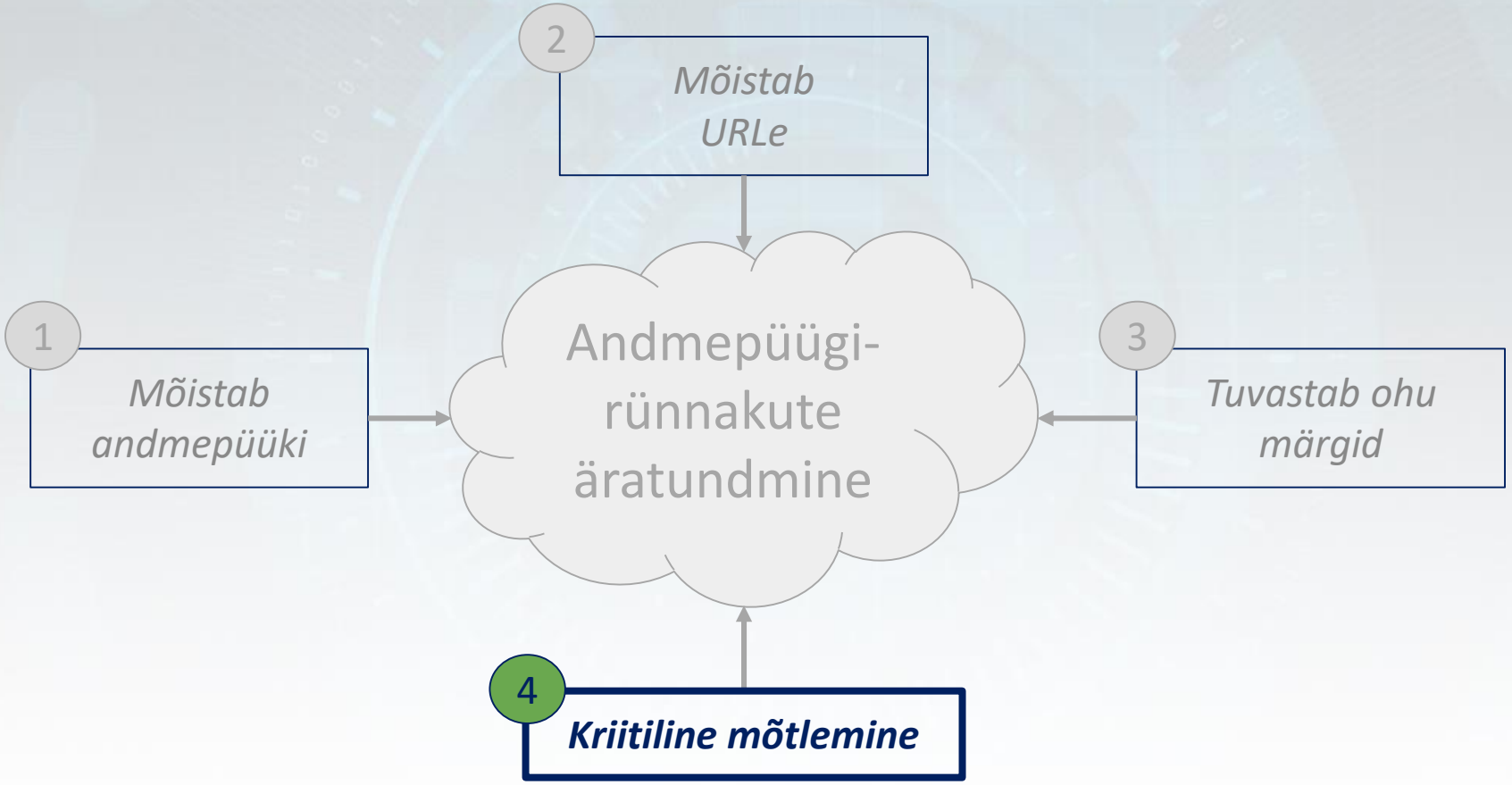


Photo by Stanford Edu.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Loenguteemad



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kriitiline mõtlemine

Andmepüügi tuvastamine hõlmab pettuse tuvastamist.

Enne toimingute tegemist kulutage rohkem aega sõnumite ülevaatamisele

Kontroll: kas sõnum sisaldab ohu märke?

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kriitiline mõtlemine

- Olge eriti ettevaatlik, kui te pole kindel, et teate saatjat.

  Mäletad TK kooliajast ?

- Tuttavus võib luua piisavalt usaldust, et klõpsata pahatahtlikel URL-idel.

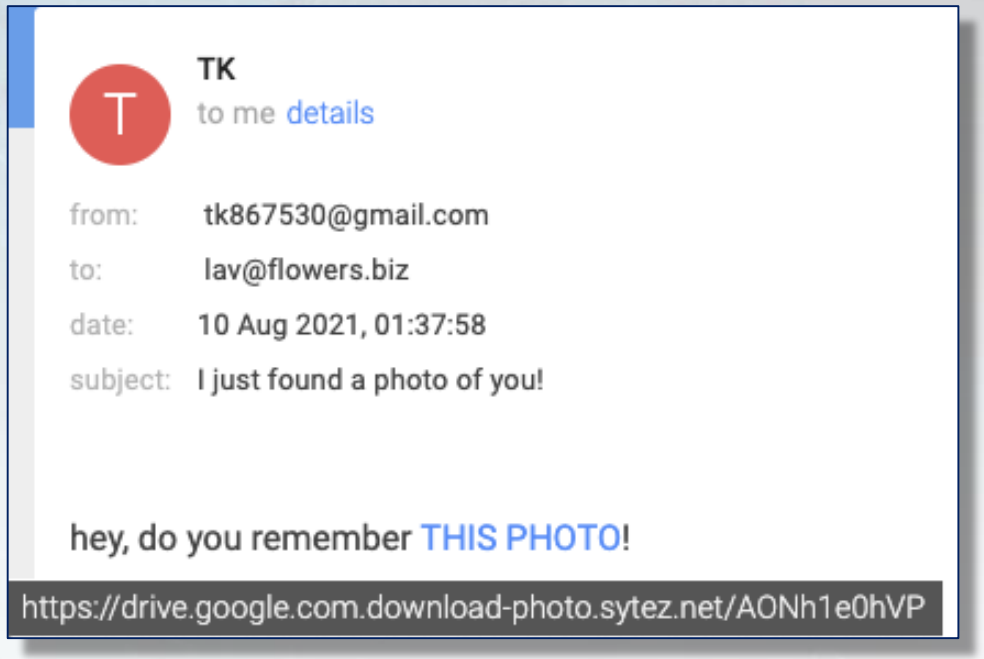


Photo by Jigsaw, Google.

Lisaks on tegelik fotodomeen "sytez.net", mitte Google'i draiv.

Kriitiline mõtlemine

- Vaadake hoolikamalt, kui meilid nõuavad kiireloomulis toiminguid

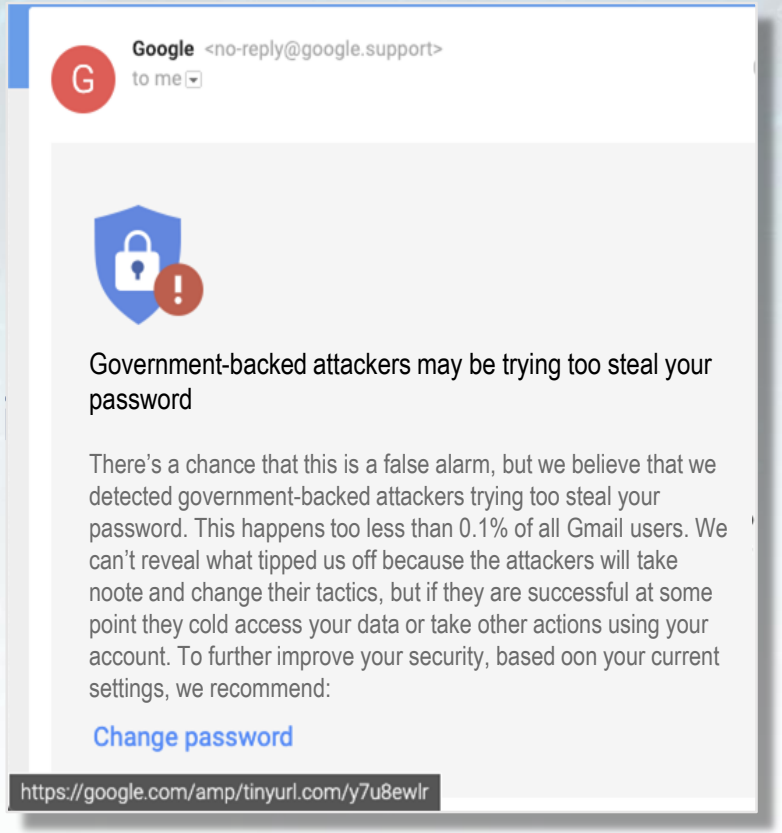
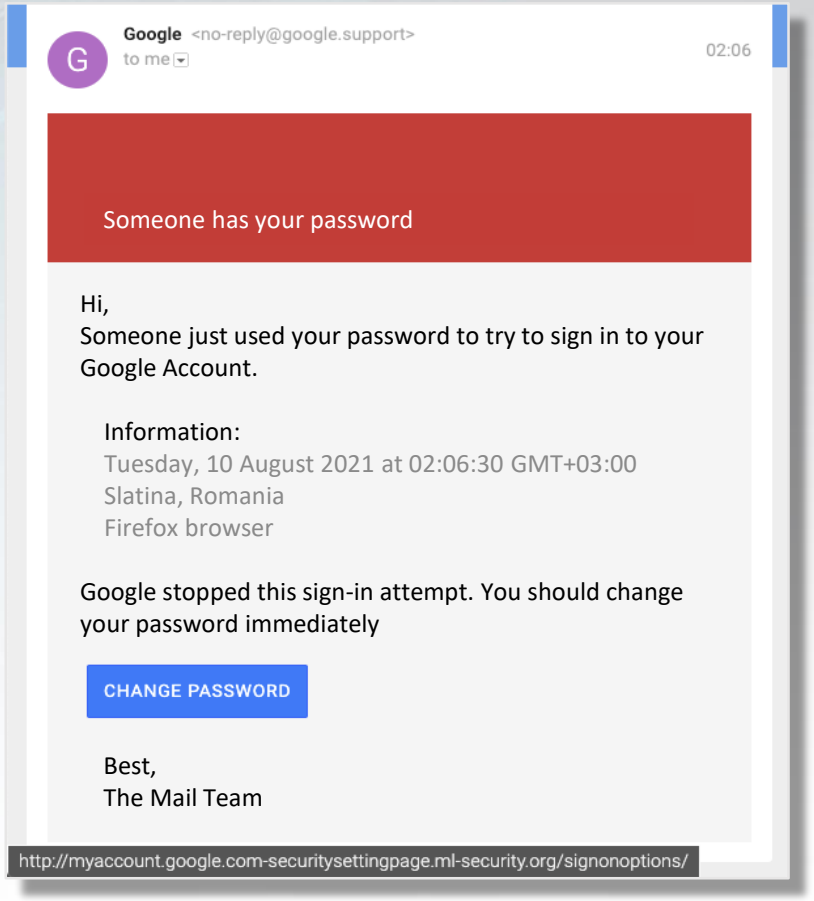


Photo by Jigsaw, Google.



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kriitiline mõtlemine

- Olge teadlik meilidest, mis sunnivad teid välisele veebisaidile minema. Hõljutades kursorit mitte ainult nähtavate linkide, vaid kogu meiliraami kohal, võib näidata peidetud URL-i

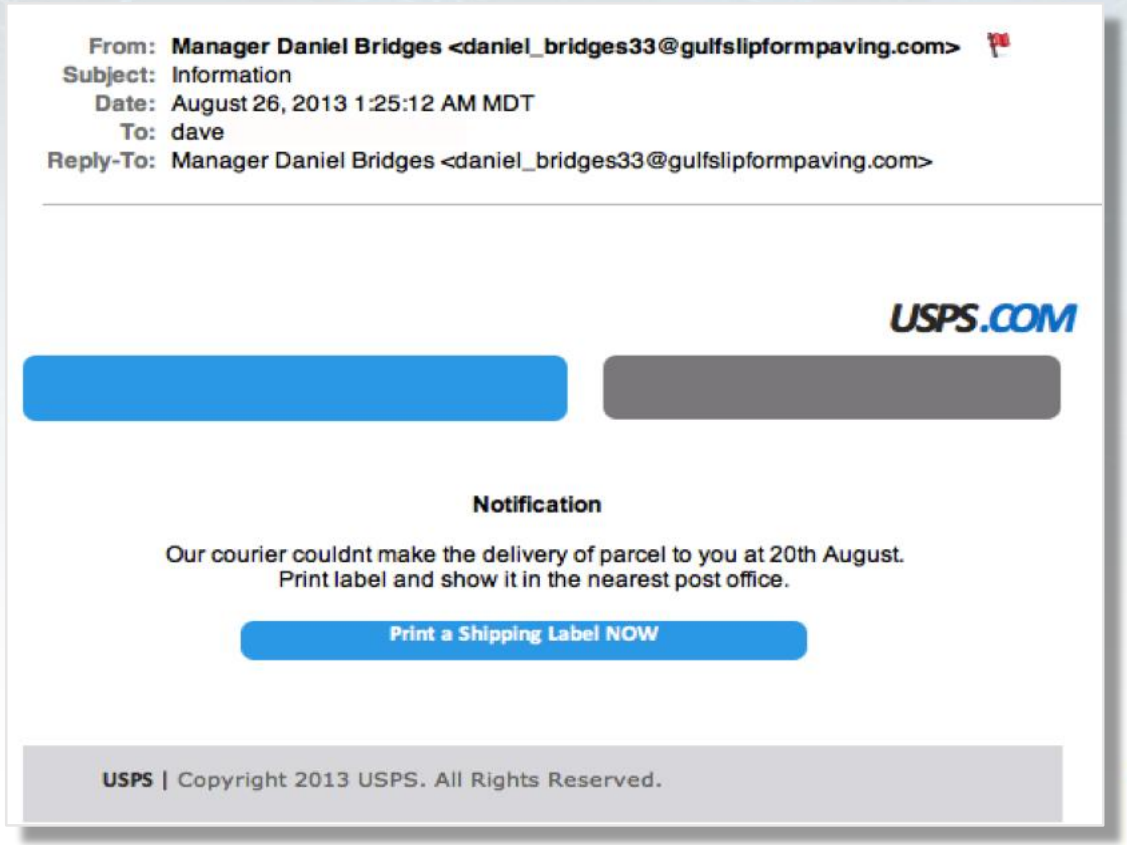


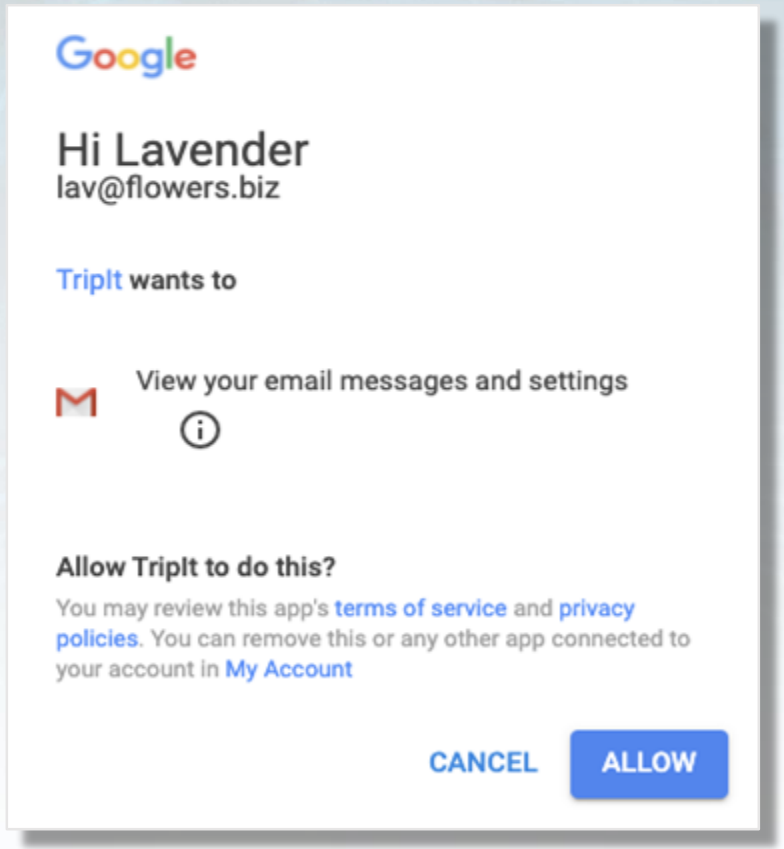
Photo by Security Metrics.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kriitiline mõtlemine

- Enne kontole juurdepääsutaotluste andmist veenduge, et usaldate rakenduste arendajaid



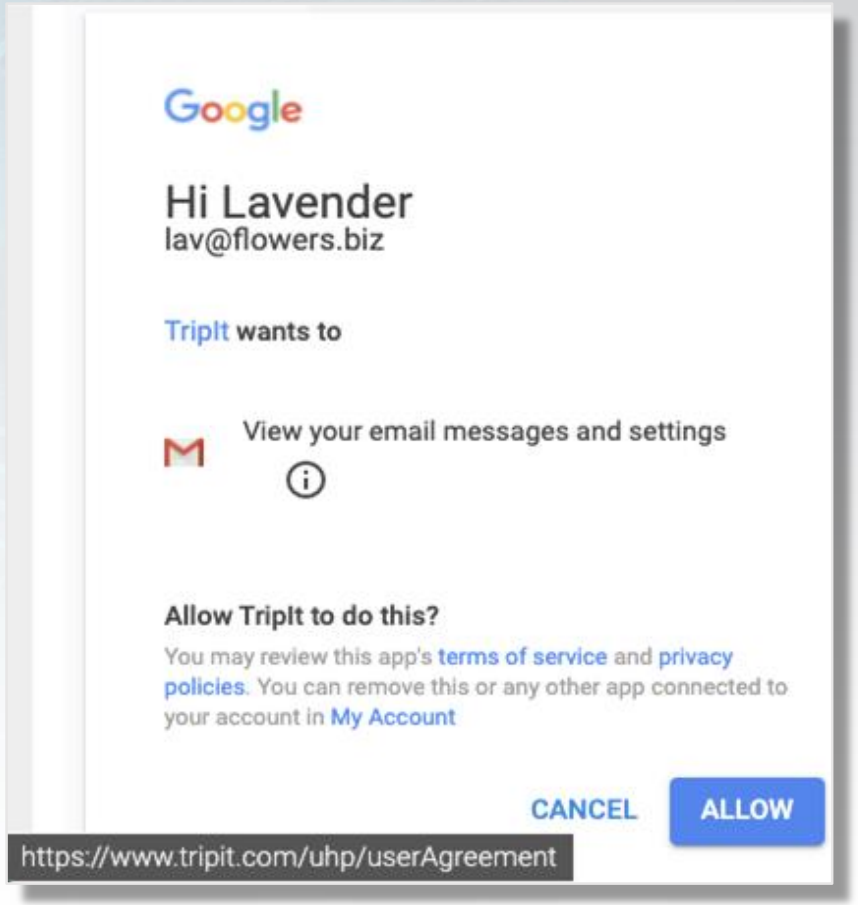


Photo by Jigsaw, Google.

Funded by the Erasmus+ Programme of the European Union

Kriitiline mõtlemine

- Kui te pole domeenis kindel, saate lisateabe saamiseks kasutada otsingumootorit

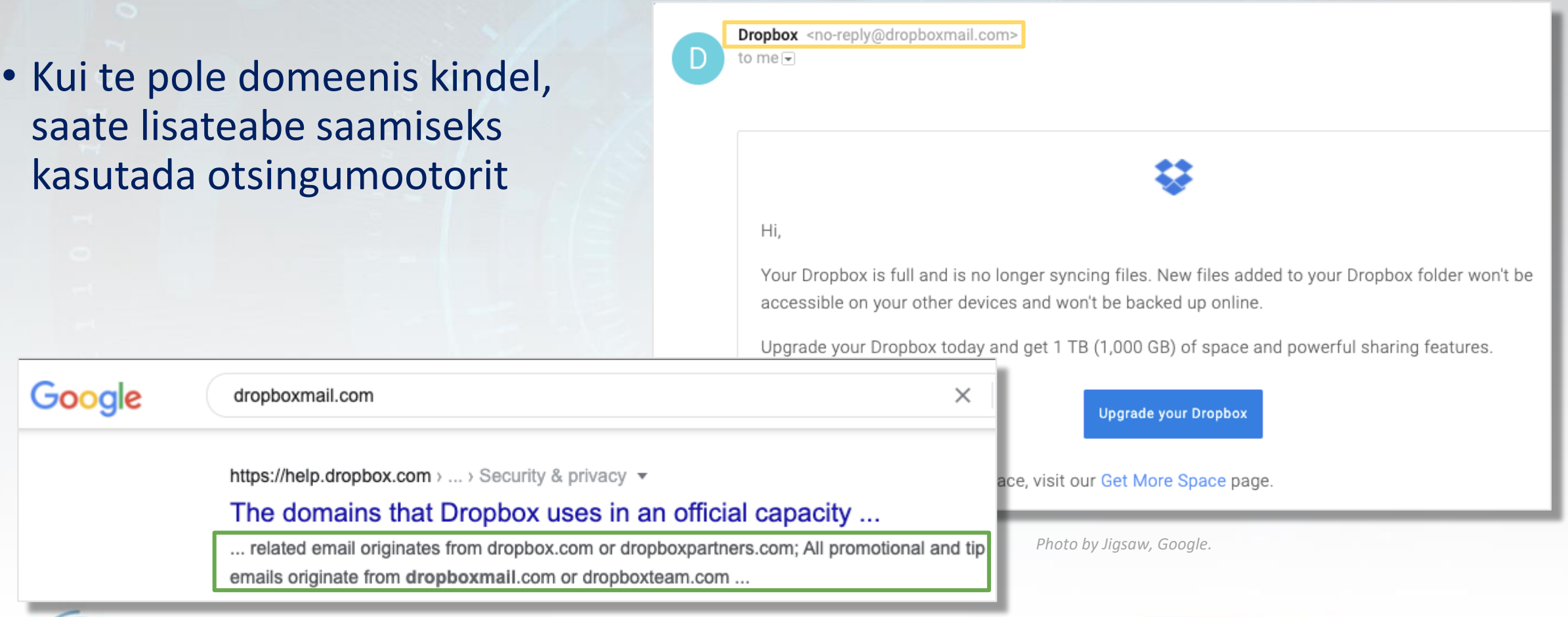


Photo by Jigsaw, Google.

CyberPhish
Safeguarding your digital future

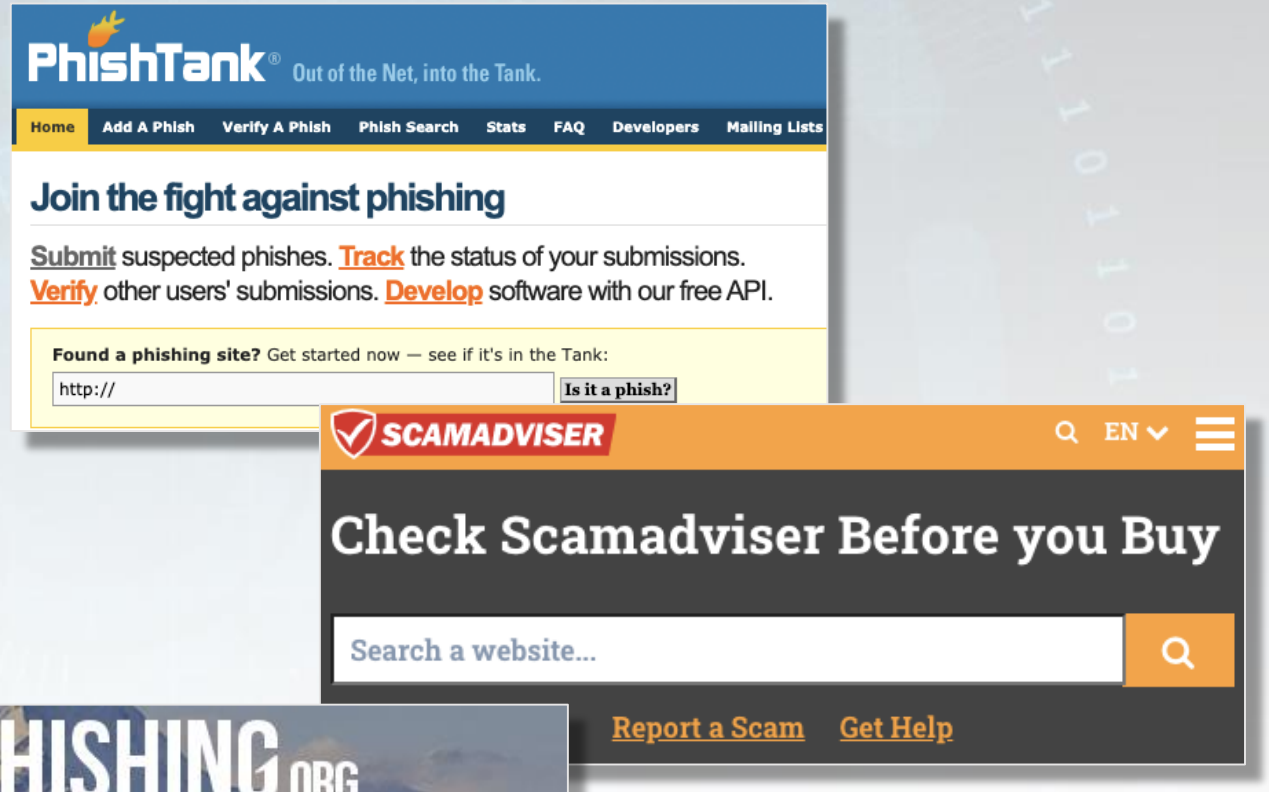
Funded by the Erasmus+ Programme of the European Union

Kriitiline mõtlemine

- Kui te pole URL-i osas kindel, on potentsiaalselt andmepüügiga seotud URL-ide otsimiseks olemas tasuta veebitööriistad

Näited:

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



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kokkuvõte

2 *Mõistab URLe*

1 *Mõistab andmepüüki*

Andmepüügi-rünnakute äratundmine

3 *Tuvastab ohu märgid*

4 *Kriitiline mõtlemine*

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Ülesanne

Kas näete, millised järgmistest on andmepüügi URL-id?

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

Ülesanne

Arutage, millistest muudest ohu märkidest selles loengus ei räägita, mida olete päriselus kogenud või mõnes toodud andmepüügi näidises ära tundnud.

Ülesanne

Minge PhishTanki ja valige hiljuti esitatud andmete hulgast andmepüügianalüüsi näidis:

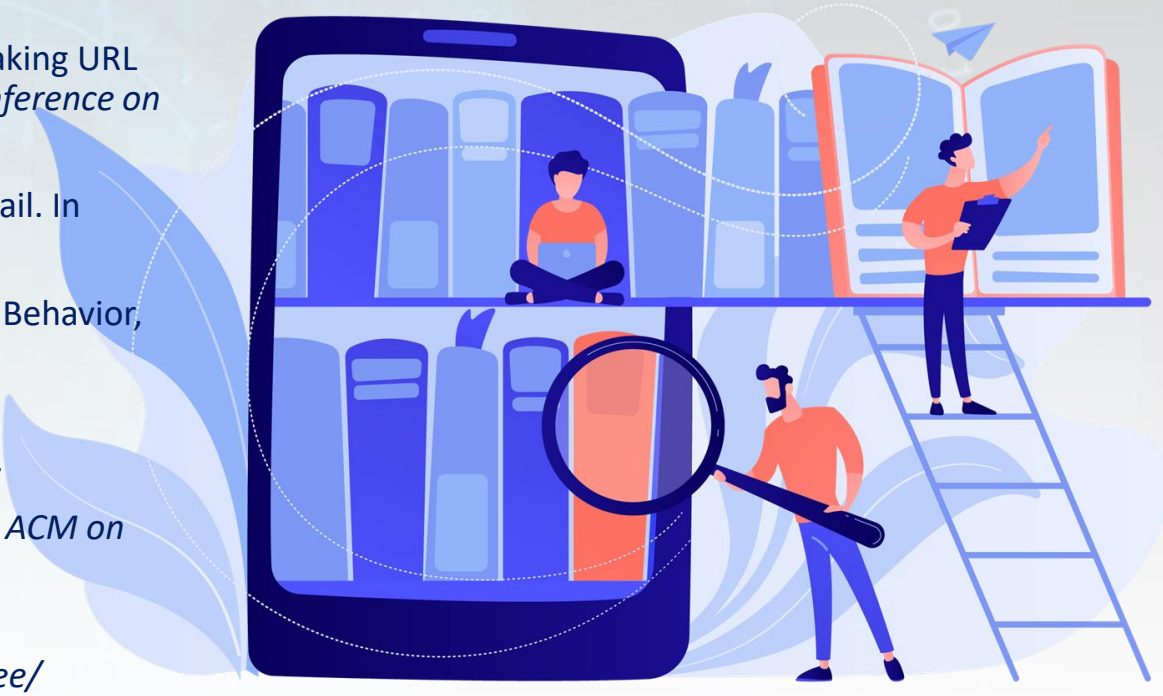
- *Kas saate öelda, kas see on andmepüügi kiri (link) või mitte?*
- *Millised olid andmepüügi näitajad?*
- *Klõpsake "vaata tehnilisi üksikasju". Mida saate sellest õppida?*

https://phishtank.org

Lisalugemine

Selle loengu ettevalmistamisel kasutatud materjal

- **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

Lühivideod

- Phishing email scam anatomy
  - ***https://youtu.be/3gpOM9c6mmA***
- Phishing attacks explained
  - ***https://youtu.be/Y7zNlEMDmI4***
  - ***https://youtu.be/gqhPkeXMeh0***
- Recognising and staying safe from phishing
  - ***https://youtu.be/R12_y2BhKbE***

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Tänan kuulamast