Funded by the Erasmus+ Programme of the European Union

Overview of Understanding and Handling Cyber-Attacks

Recognising Phishing Attacks

How to Recognise Phishing Attacks?

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

Learning Goals

Explain the concept of e-safety and the importance of adopting a proactive approach to cyber threats through the concept of cyber hygiene

Recognise and handle cyber-attacks

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

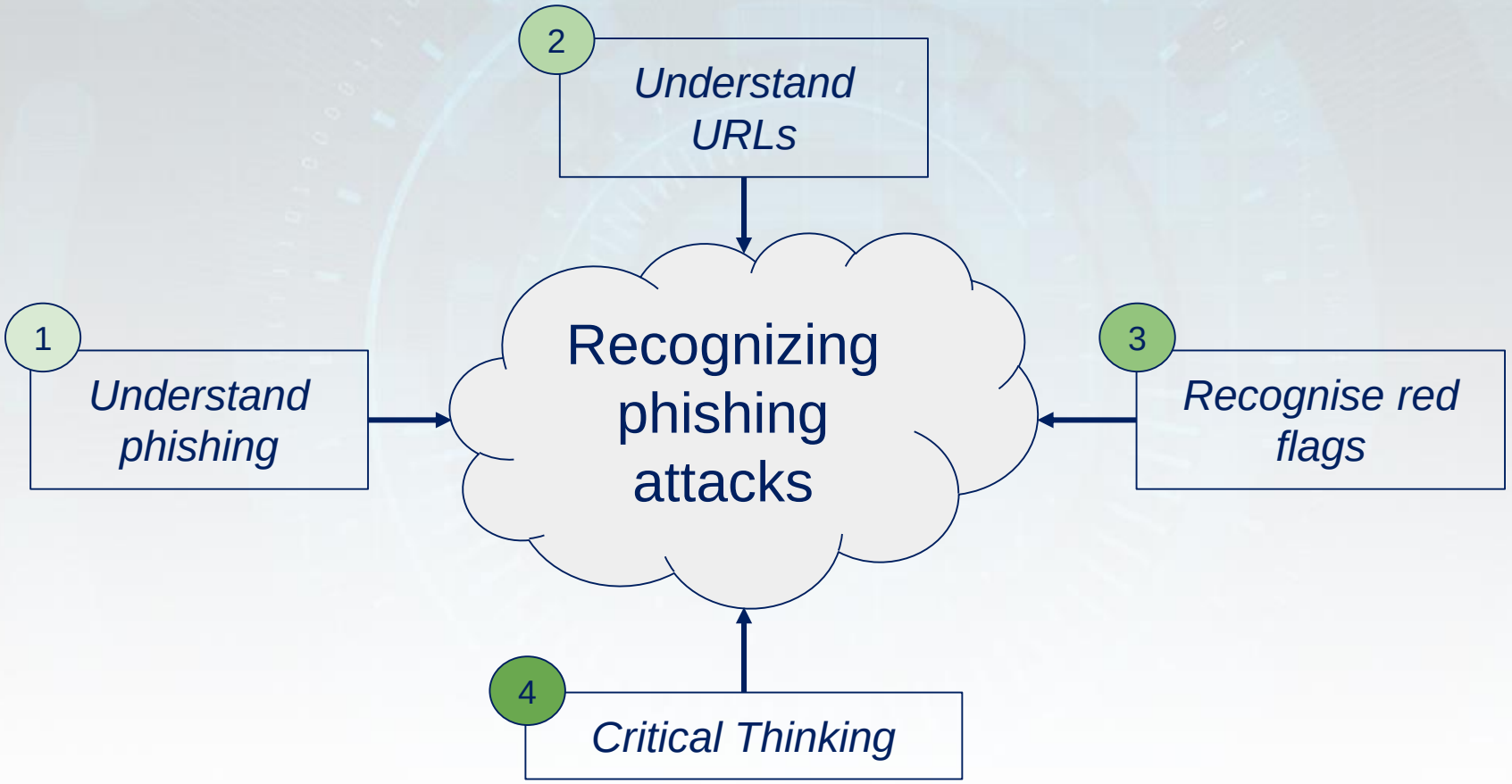
Student Workload

Lecture	2 h
Audio and video material	2 h
Case studies	2 h
Further reading	4 h
Preparation for exam	2 h

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

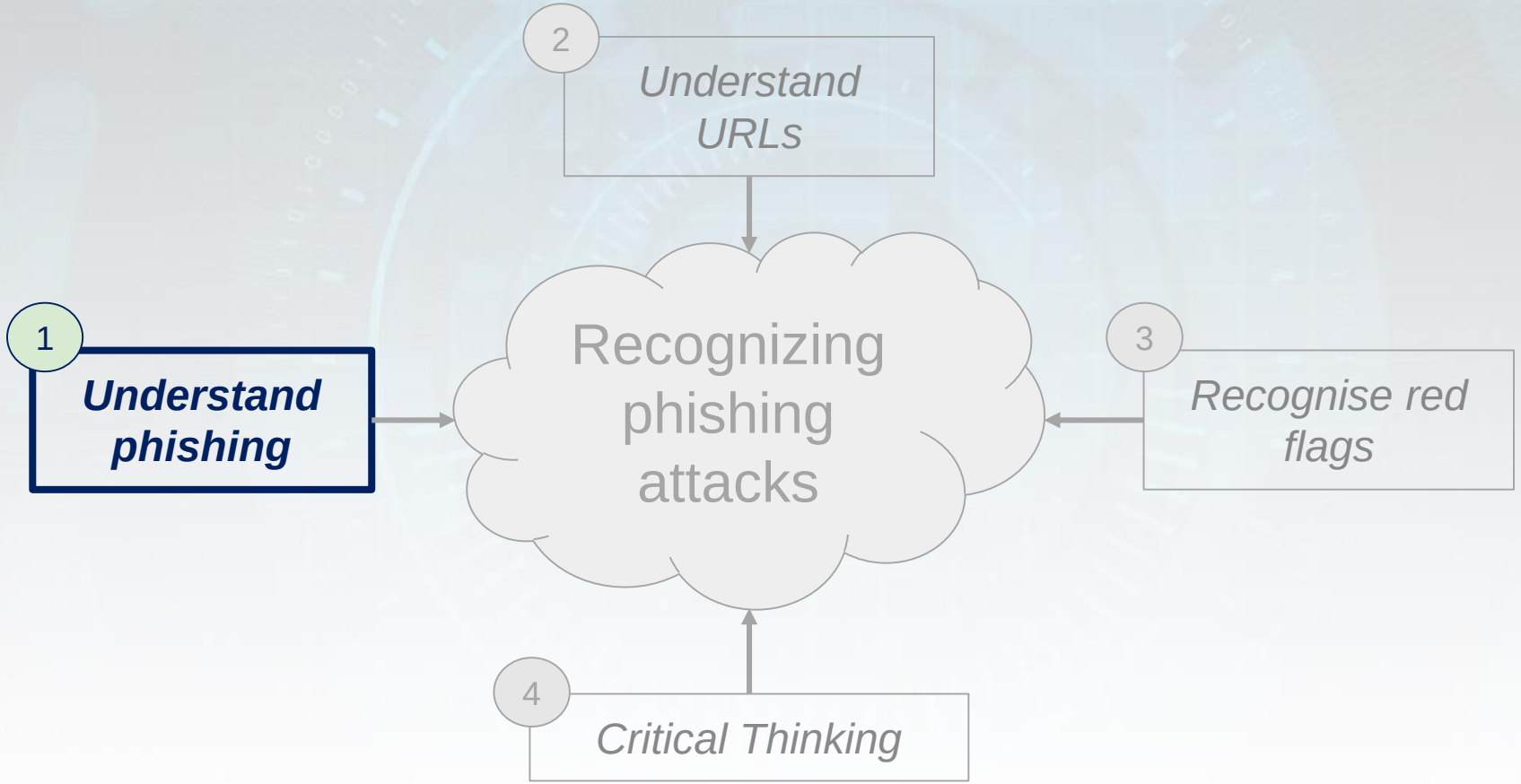
Contents



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Contents



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

What is a Phishing Attack?

Phishing is *a social engineering scam that can result in data loss, reputational damage, identity theft, the loss of money, and many other damages to peoples and organisations. A phishing scam usually starts with an email trying to gain the potential victim's trust and convince them to take the attacker's desired actions*

[*Abroshan, 2021*]

Phishing Source

Photo by Google

- Email
- Websites
- Social Media
- Mobile (SMS, voice)
- *Any form of communication …*

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Phishing Message Anatomy

- Message Source
  - *who is sending me a message?*
- Message Content
  - *what is the message about?*
- Hyperlinks/Attachments
  - *what else does this message link to?*

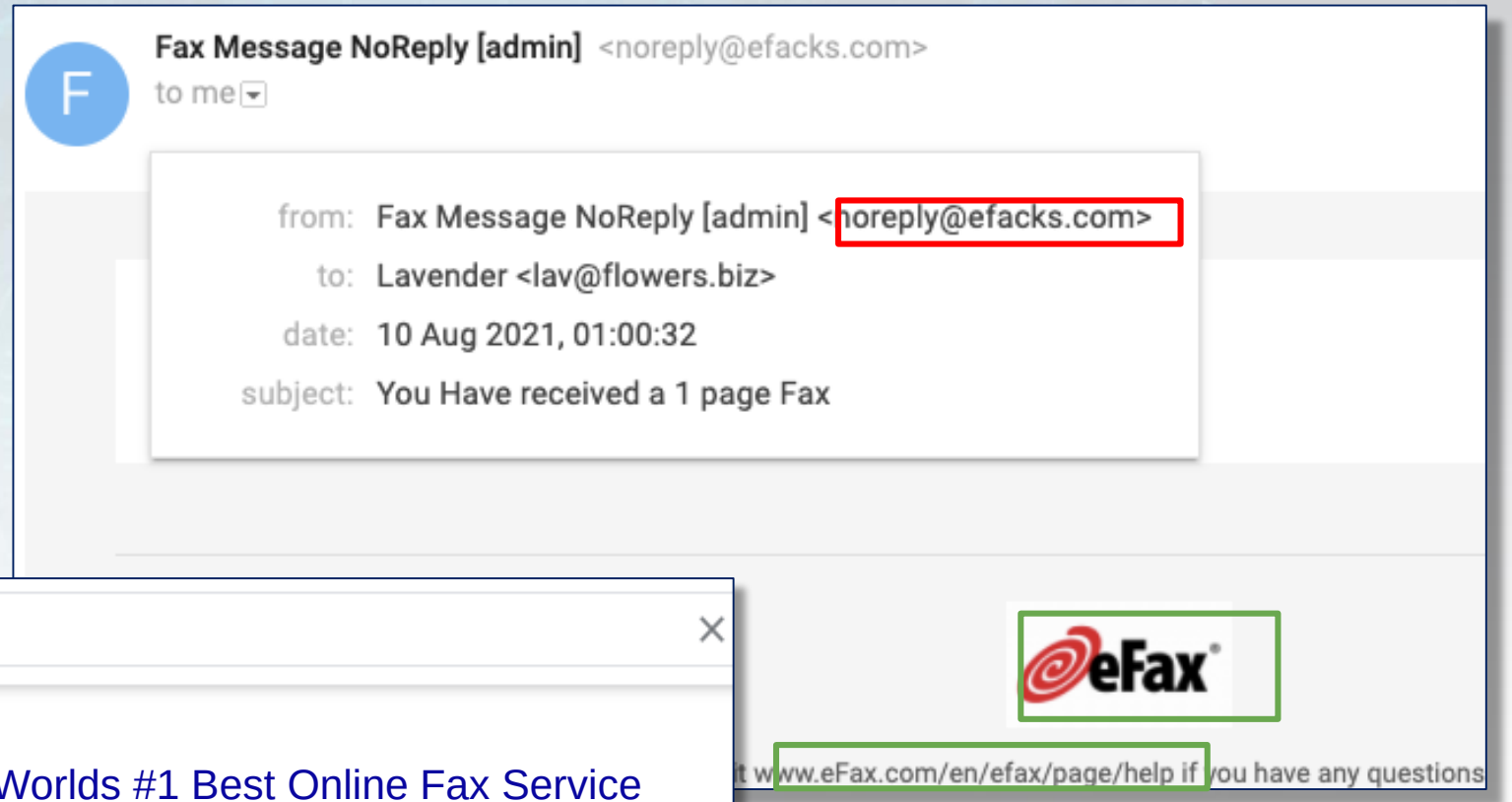
Photo by istockphoto.com

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Message Source

- Phishing can trick with look-alike sender's email.



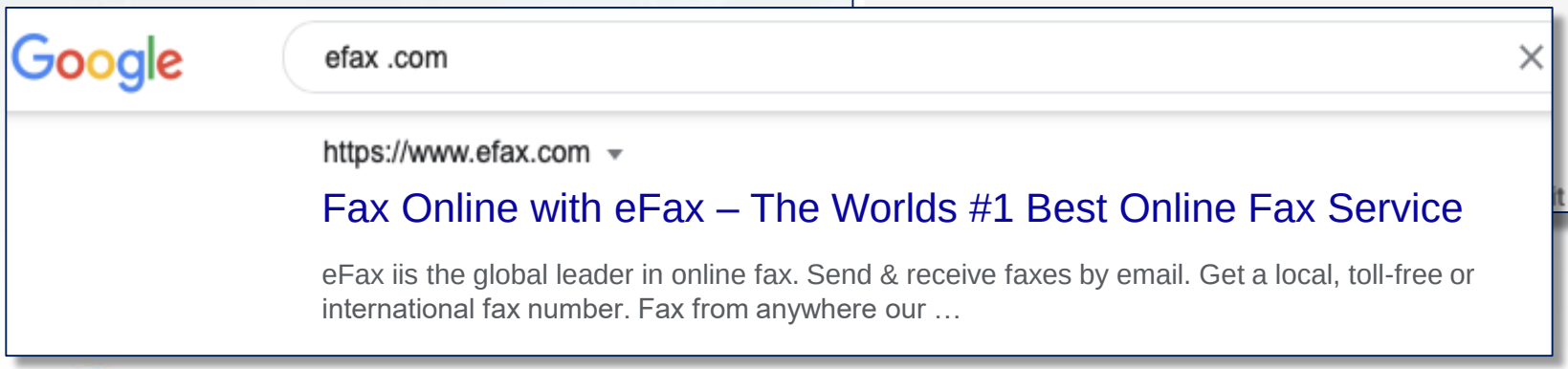


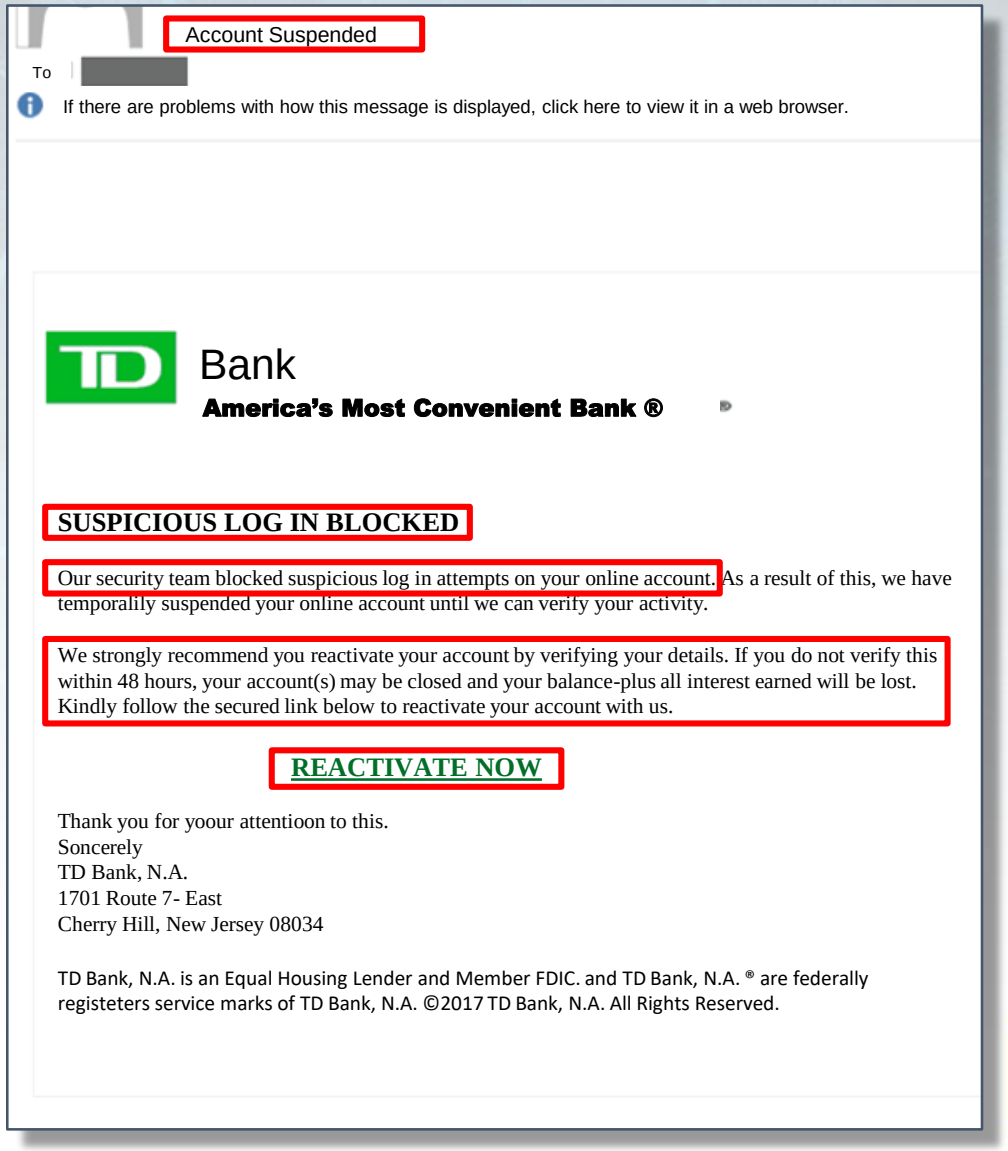
Photo by Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Message Content

- Deception through fear, urgency, authority, greed, friendship, aid, and desperation



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

America's Most Convenient 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.

Photo by Sonicwall Phishing Test

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Message Content

- Deception through fear, urgency, authority, greed, friendship, aid, and desperation

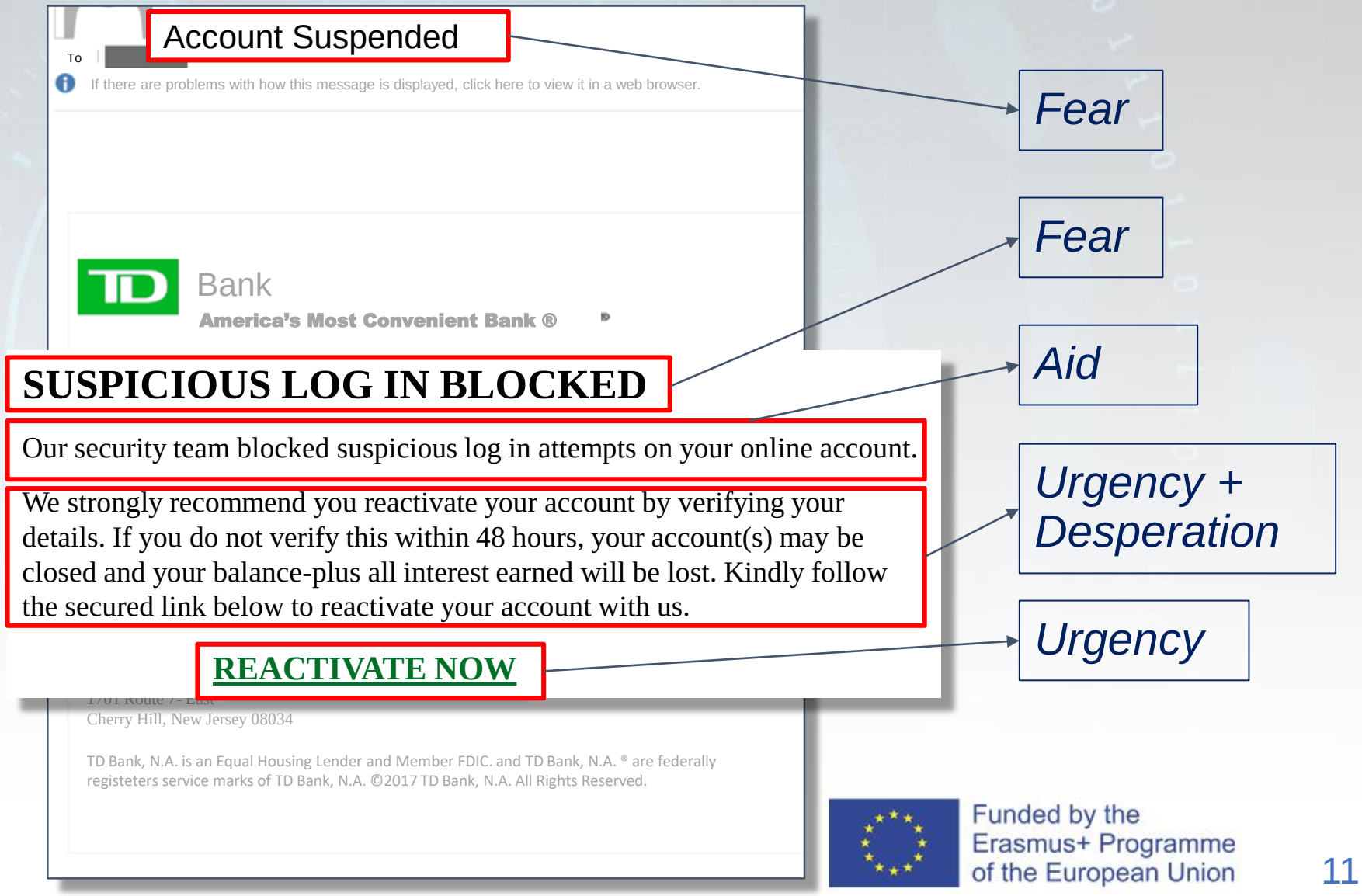


Photo by Sonicwall Phishing Test

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Hyperlinks/Attachment

- Attachments can include various types of files that can be malicious
- Hyperlinks indicate the location of a file on the Web and may direct victims to malicious websites or to download malicious files

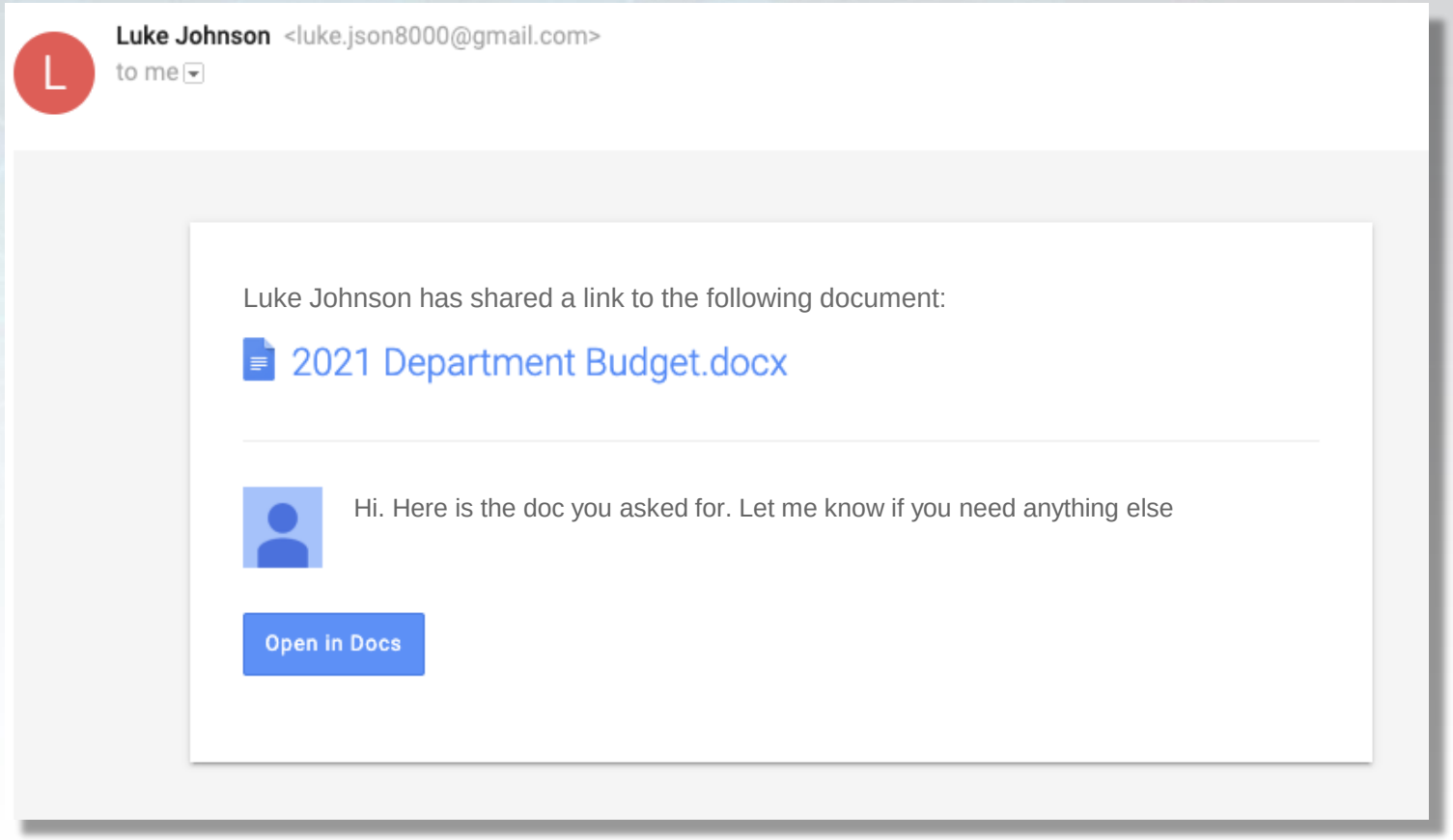


Photo by Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Hyperlinks/Attachment

- Mouse over (or hover over) these hyperlinks to reveal its URL.

- The URL shown is the *insecure imitation* of the google drive domain

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

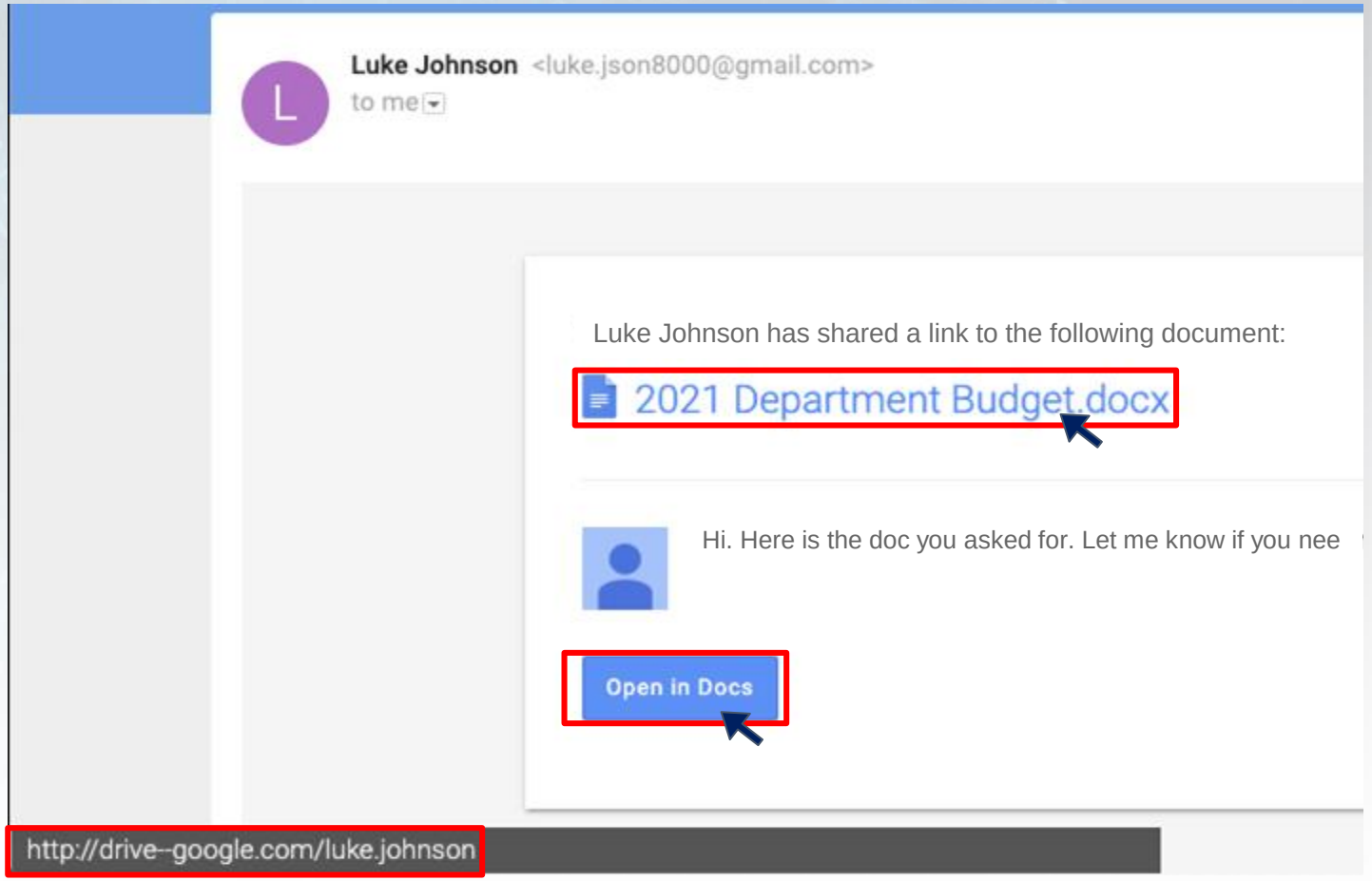
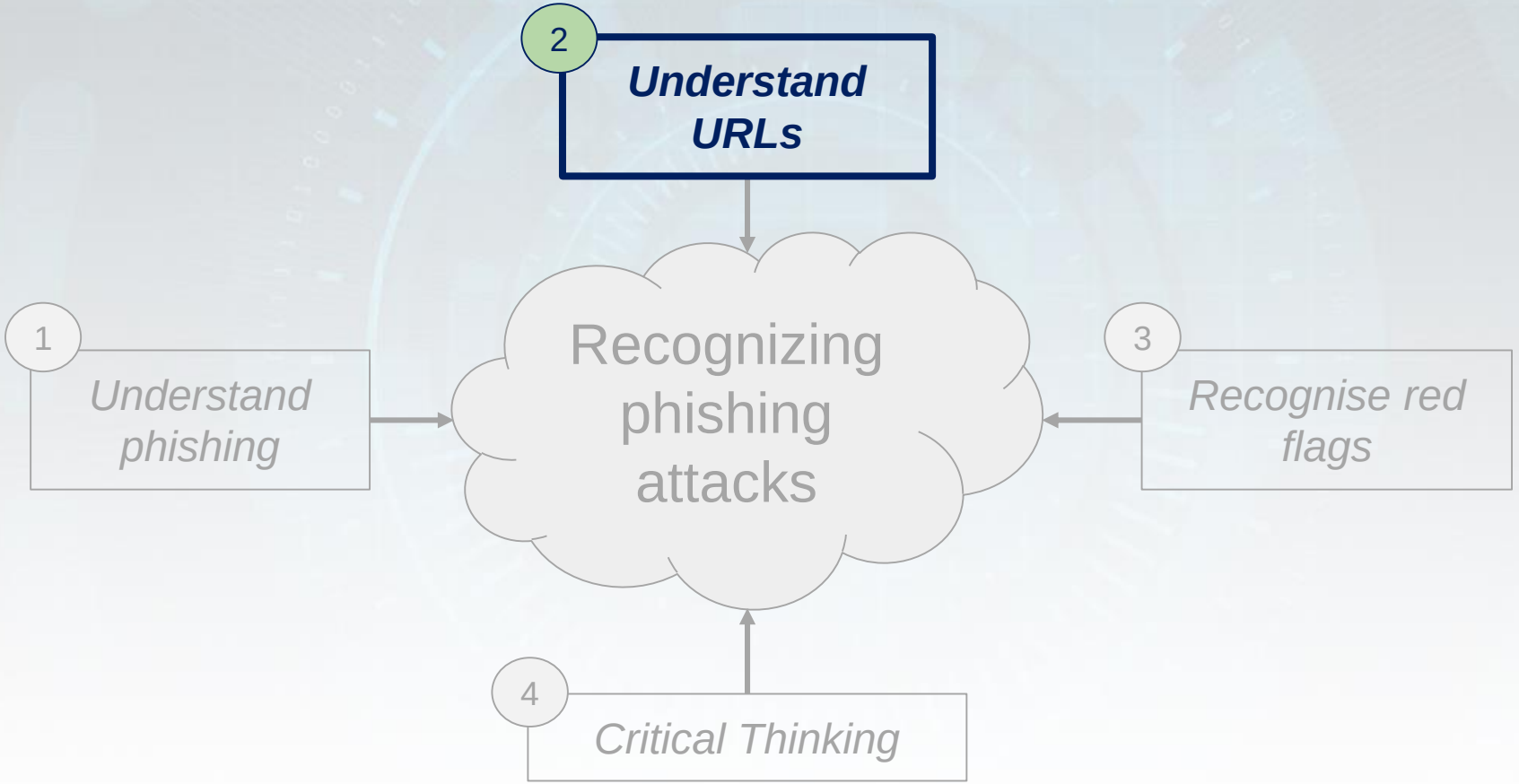


Photo by Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Contents

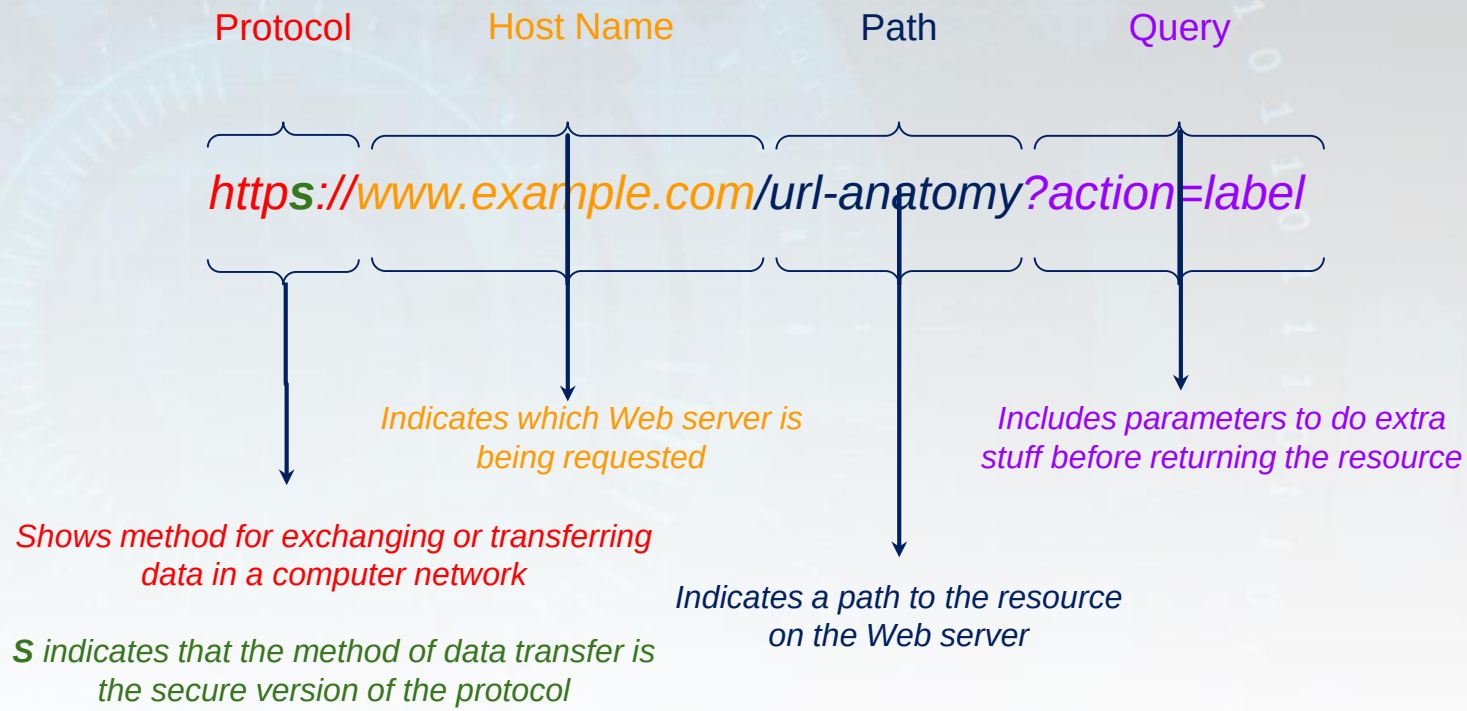


CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Understand URLs

- Uniform Resource Locator (URL) is the address of a given unique resource on the Web.

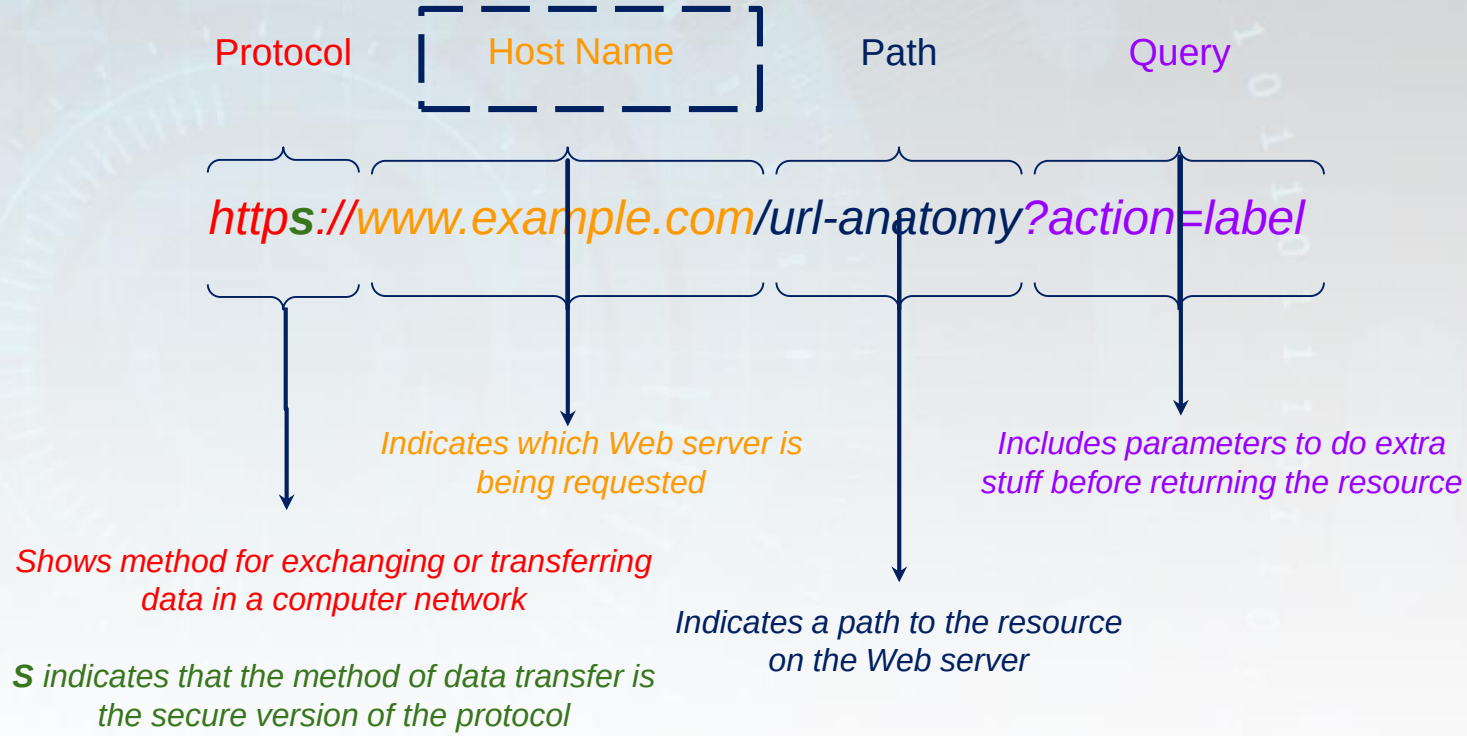


https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL
Protocol, Simple Object Access. "URL." (2007).

Funded by the Erasmus+ Programme of the European Union

Understand URLs

- Uniform Resource Locator (URL) is the address of a given unique resource on the Web.

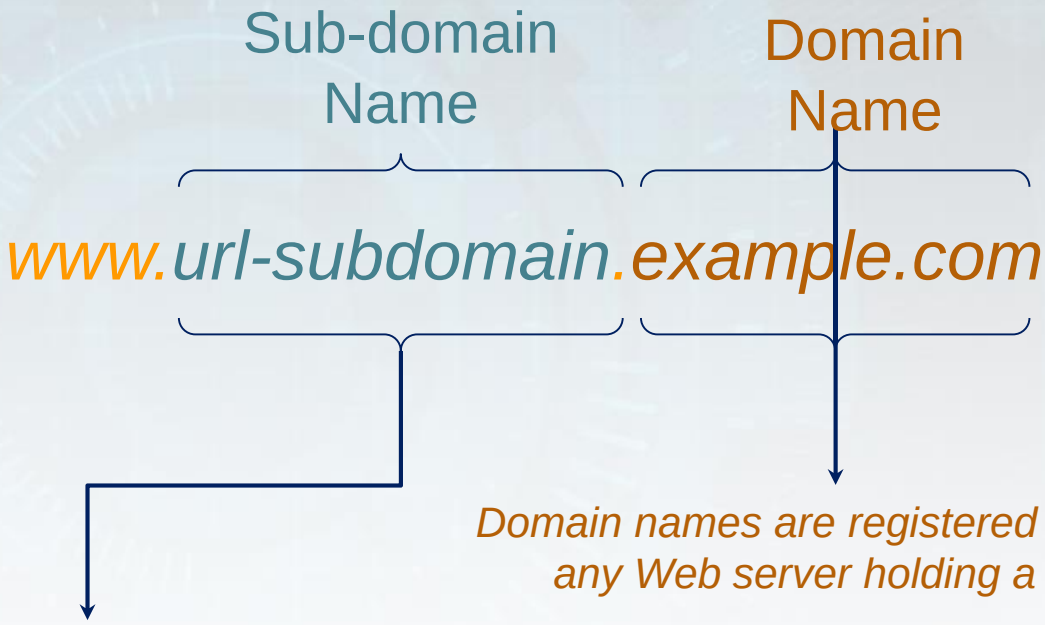


https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL
Protocol, Simple Object Access. "URL." (2007).

Funded by the Erasmus+ Programme of the European Union

Understand URLs

- Host name in URL can contain multiple subdomain names



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

Understand URLs

Phishing often tries to trick victims with URLs.

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

Protocol	*http*
Host name	*amazon.com.mailru382.co*
Path	*/packagedelivery/2017Dk25RE3*
Domain name	*mailru382.co*
Subdomain item 1	com
Subdomain item 2	*amazon*

Funded by the Erasmus+ Programme of the European Union

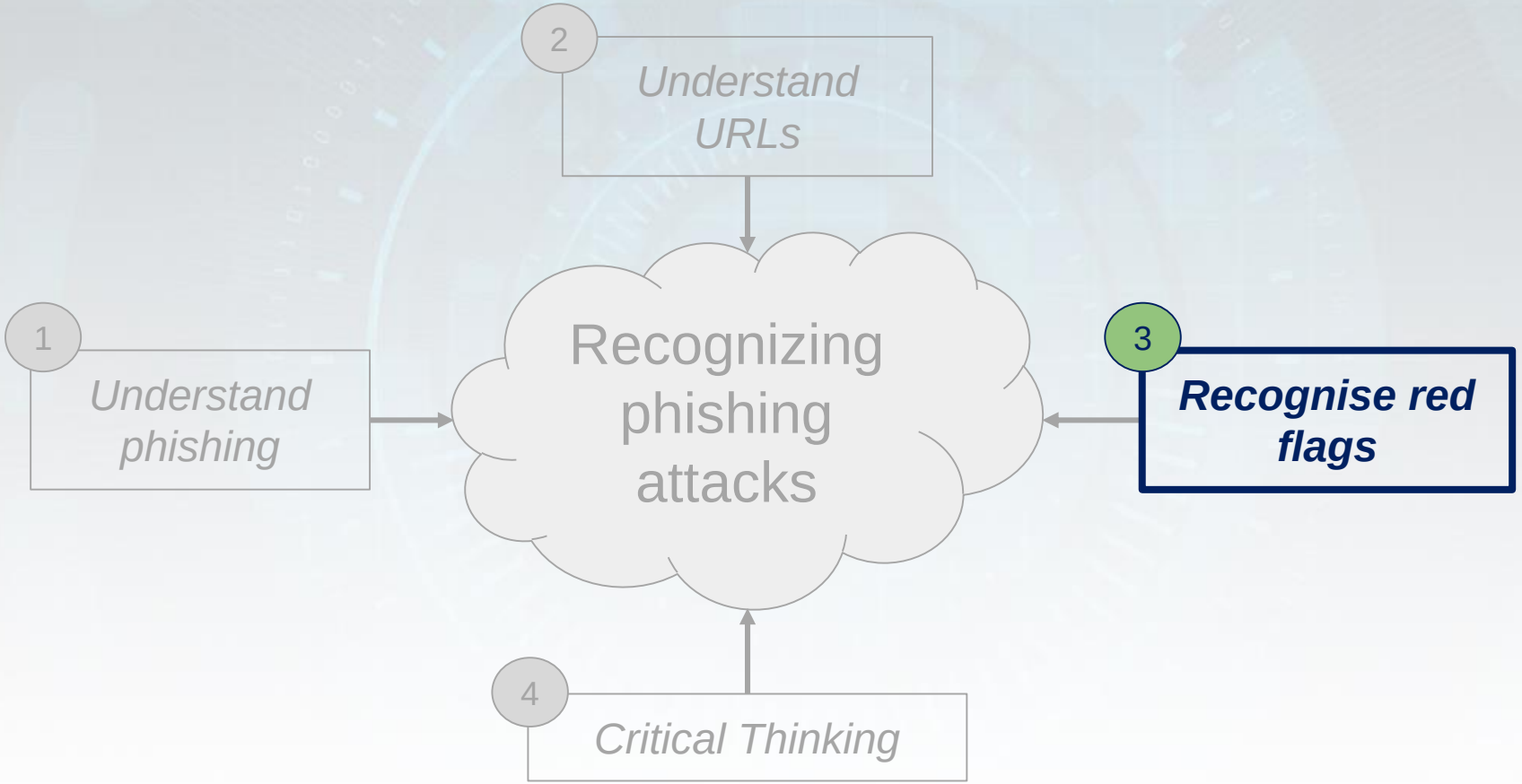
Understand URLs

Other tricks with URL ...	Example
• URL protocol missing its secure protocol indicator.	URL uses *http* instead of *https*
• Domain visibly similar a well known domain, but actually different.	*google.com* misspelled as *googgle.com*
• Complicated looking domain name to confuse the victim i.e IP address, hex or decimal characters, symbol in domain.	IP address - http://20.85.220.142/telas/caixa/ Symbols - https://epic.app/#con@sceneworld.org Decimal characters - http://2130706433/evil.com
• URL can include well known name in domain but isn't owned by the legitimate source.	"*Instagram*" included in *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

Contents



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Recognising Red Flags

- Legitimate email sources (i.e companies) don't request your sensitive information via email

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

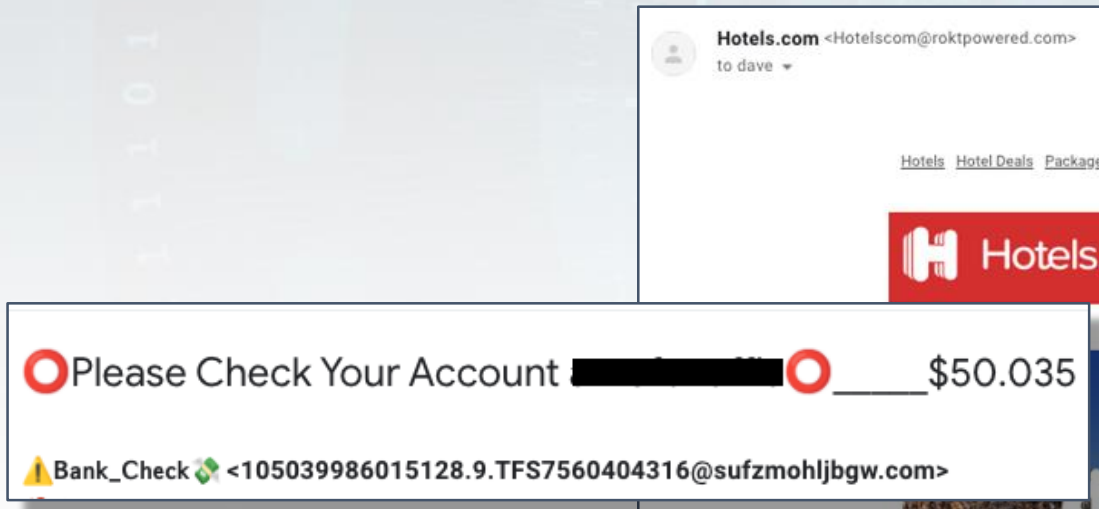
First Name, (Middle name), Last Name(required)
Email(Non-Edu Email(required)
Phone number(required)
Resident and Office Address(required)

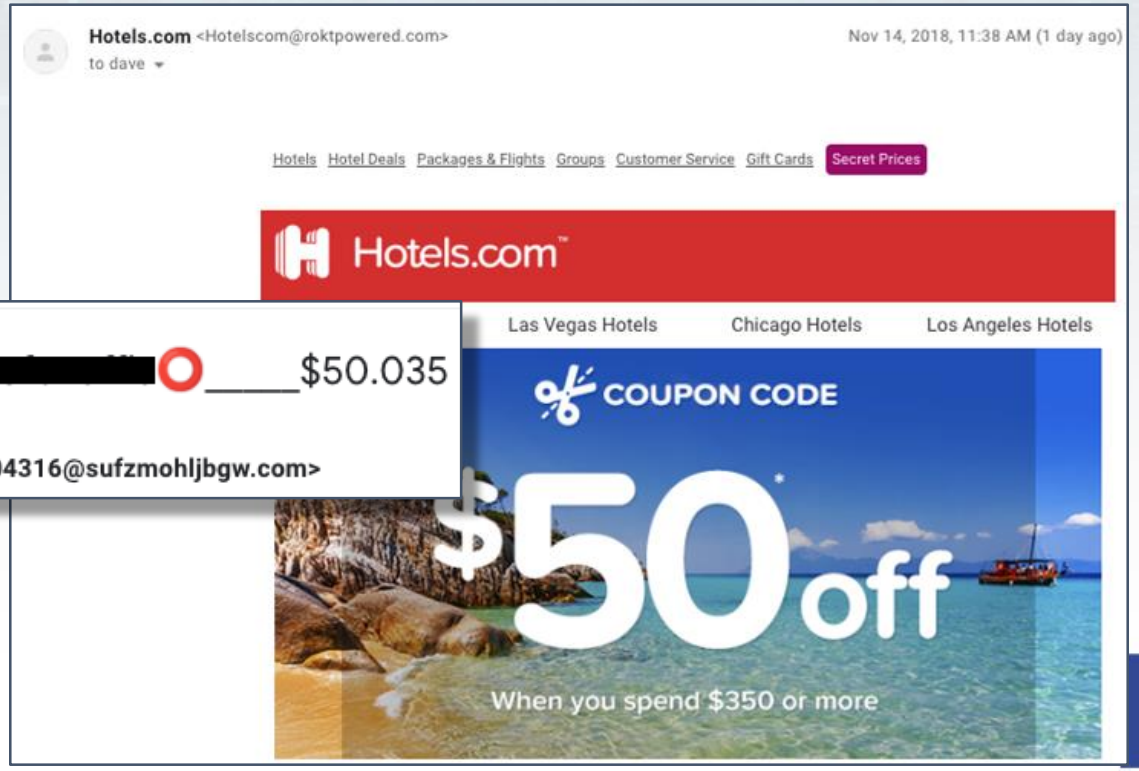
Claim response should be sent from your private Non-edu email.

Photo by Stanford Edu.

Recognising Red Flags

- Legitimate email sources don't usually have:
  - complicated email addresses
  - mismatch between email address, email domain or email sender name





CyberPhish
Safeguarding your digital future

Photo by Security Metrics.

Funded by the Erasmus+ Programme of the European Union

Recognising Red Flags

- Legitimate email sources usually call you by your name

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.

Funded by the Erasmus+ Programme of the European Union

Recognising Red Flags

- Legitimate email sources do not have issues with spelling and grammar

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

Recognising Red Flags

- Legitimate email sources don't send unsolicited attachments

Photo by Sonicwall Phishing Test

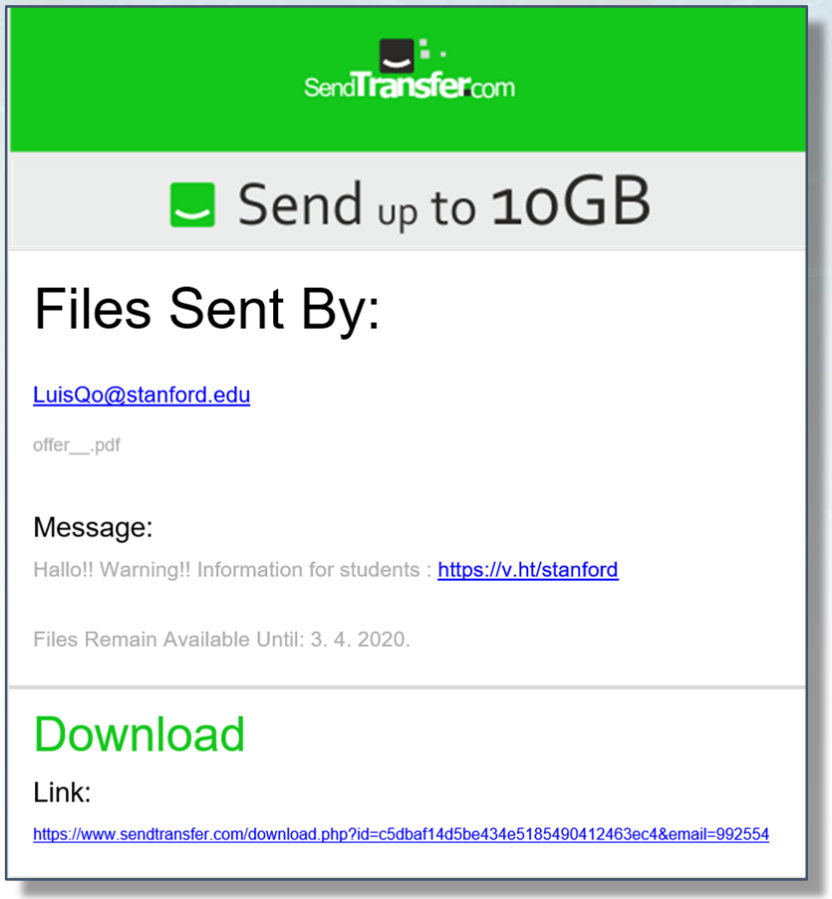
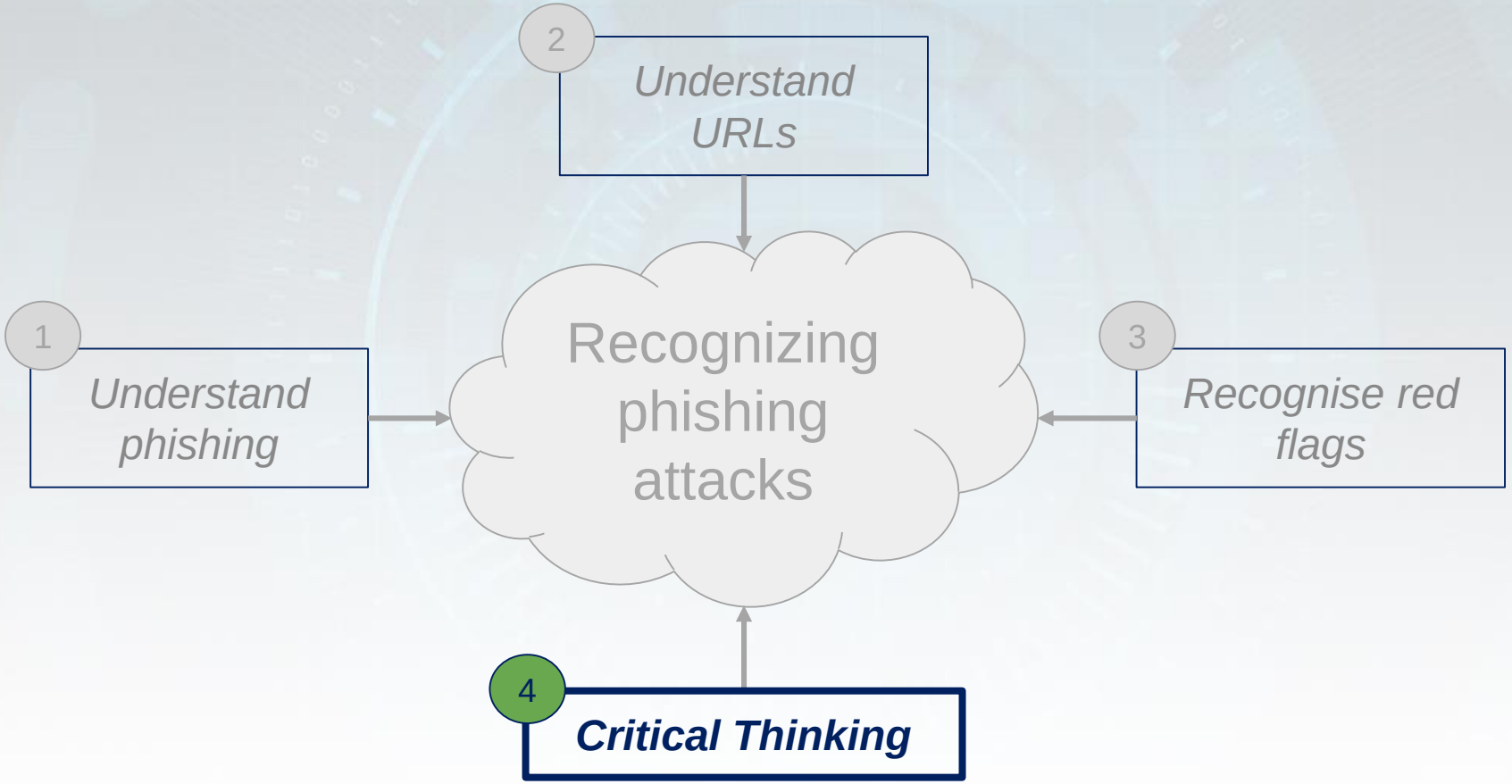


Photo by Stanford Edu.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Contents



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Critical Thinking

Phishing detection involves detecting deception.

Spend more time reviewing messages before taking actions

Spot check: Does the message check any red flags?

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Critical Thinking

- Be especially cautious if you aren't sure you know the sender.

  Remember TK from school?

- The guise of familiarity can create trust enough to click on malicious URLs.

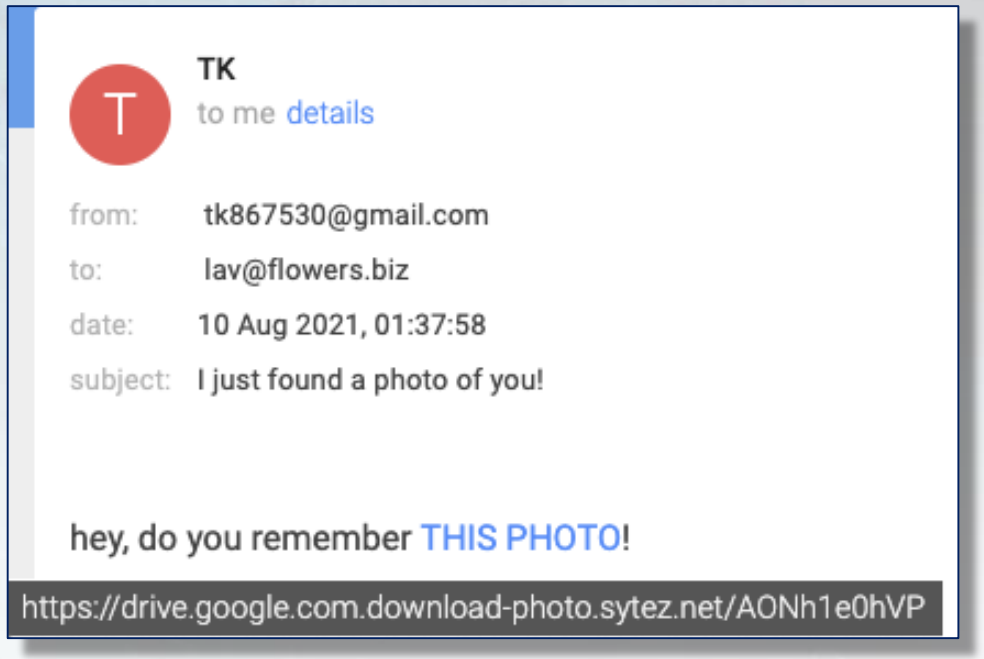
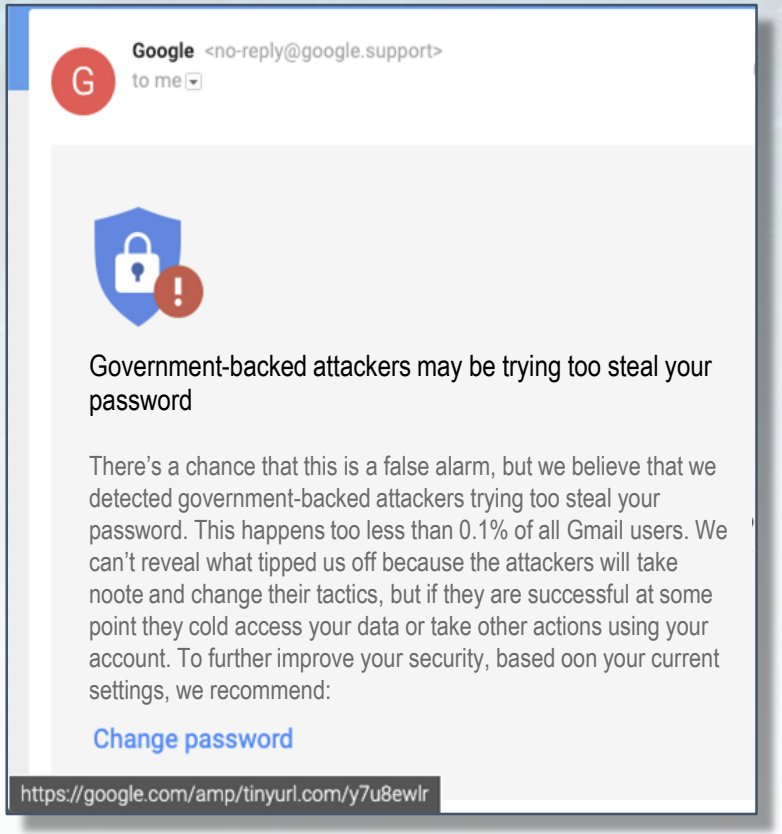


Photo by Jigsaw, Google.

Additionally, the real photo domain is '*sytez.net*', not Google drive.

Critical Thinking

- Look more carefully when emails requests actions with a sense of urgency



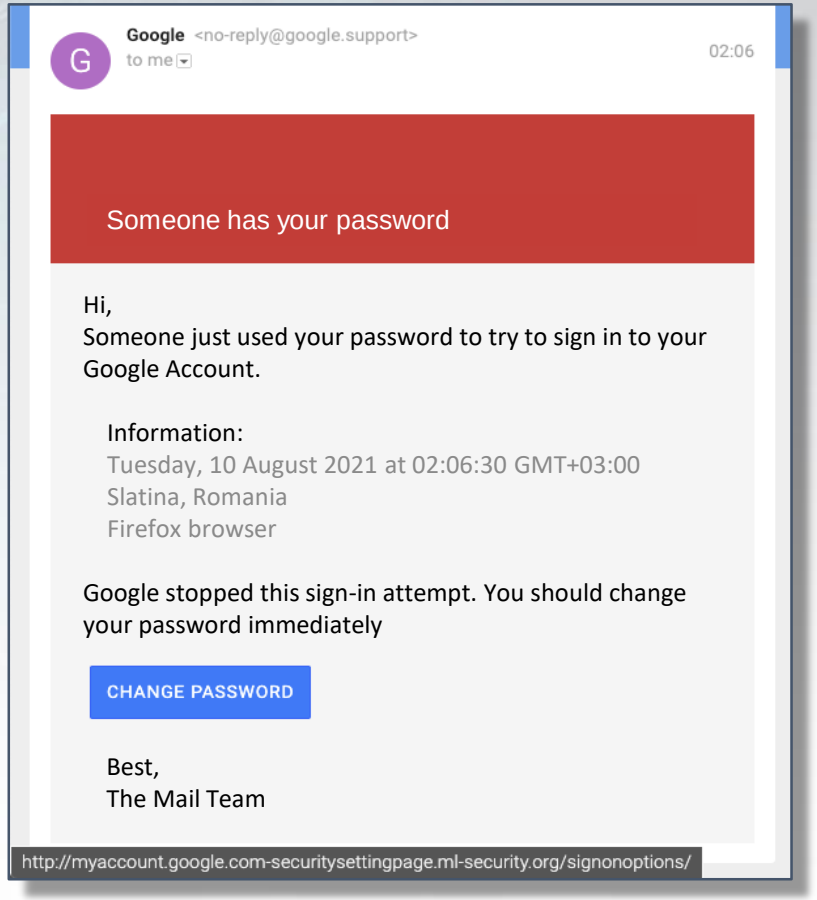


Photo by Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Critical Thinking

- Be aware of emails that force you to an external website. Hovering over not just apparent links but the entire email frame can show a hidden URL

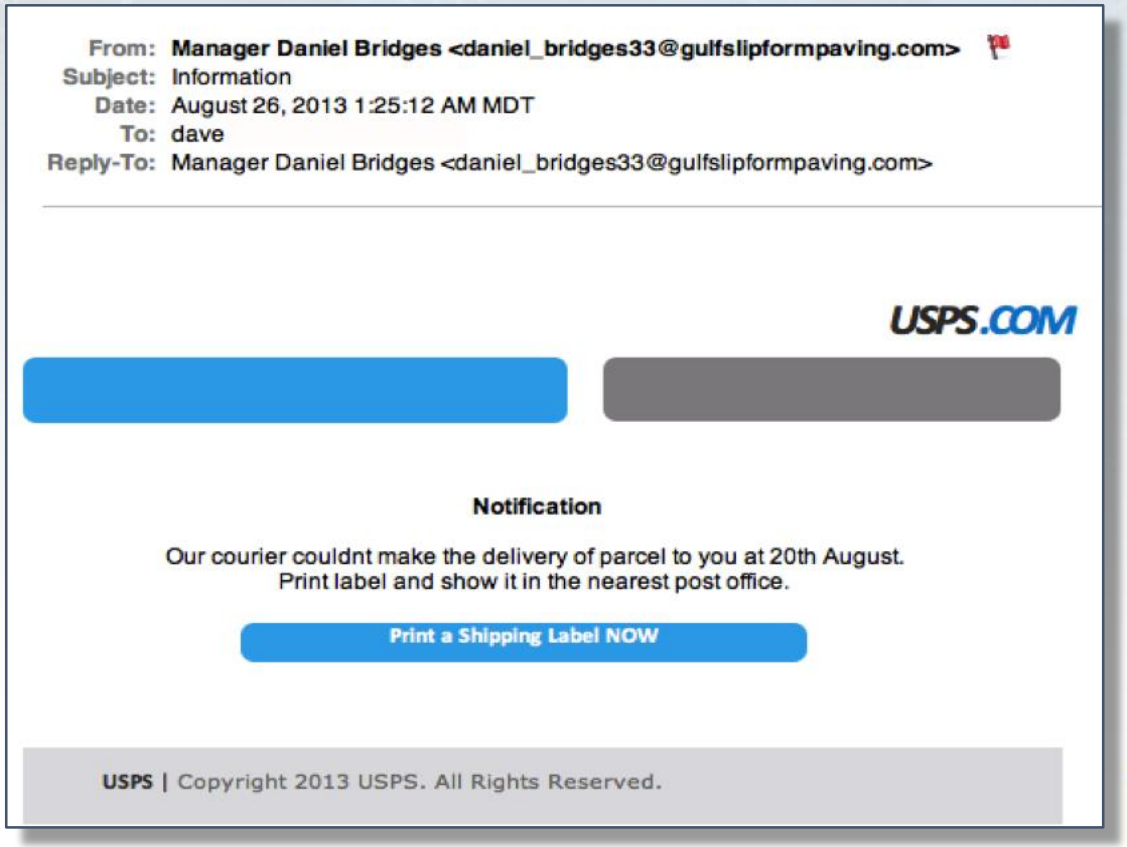


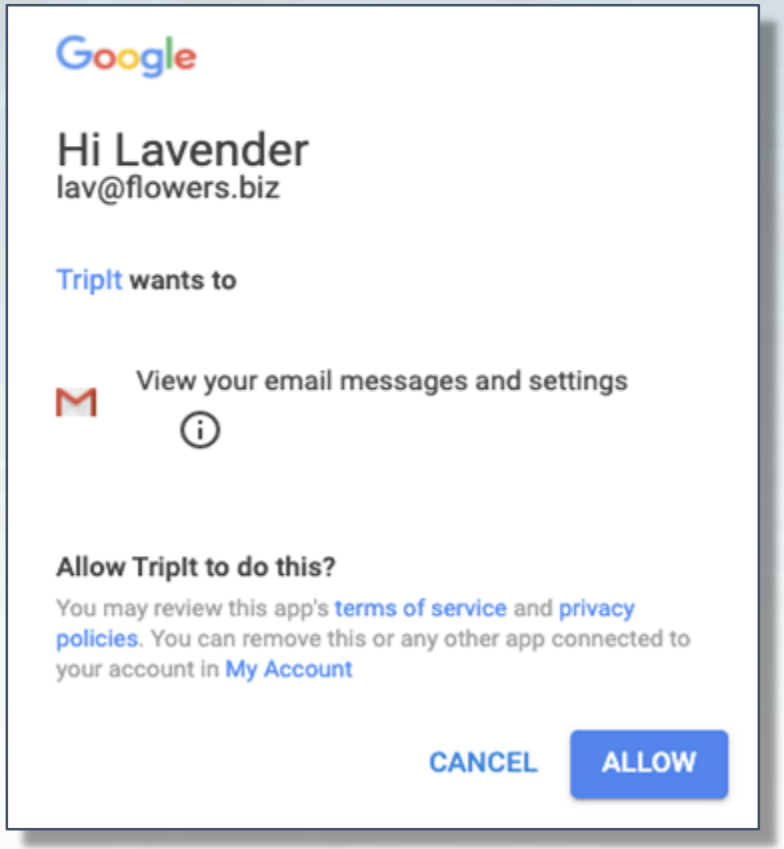
Photo by Security Metrics.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Critical Thinking

- Check that you trust app developers before granting account access requests



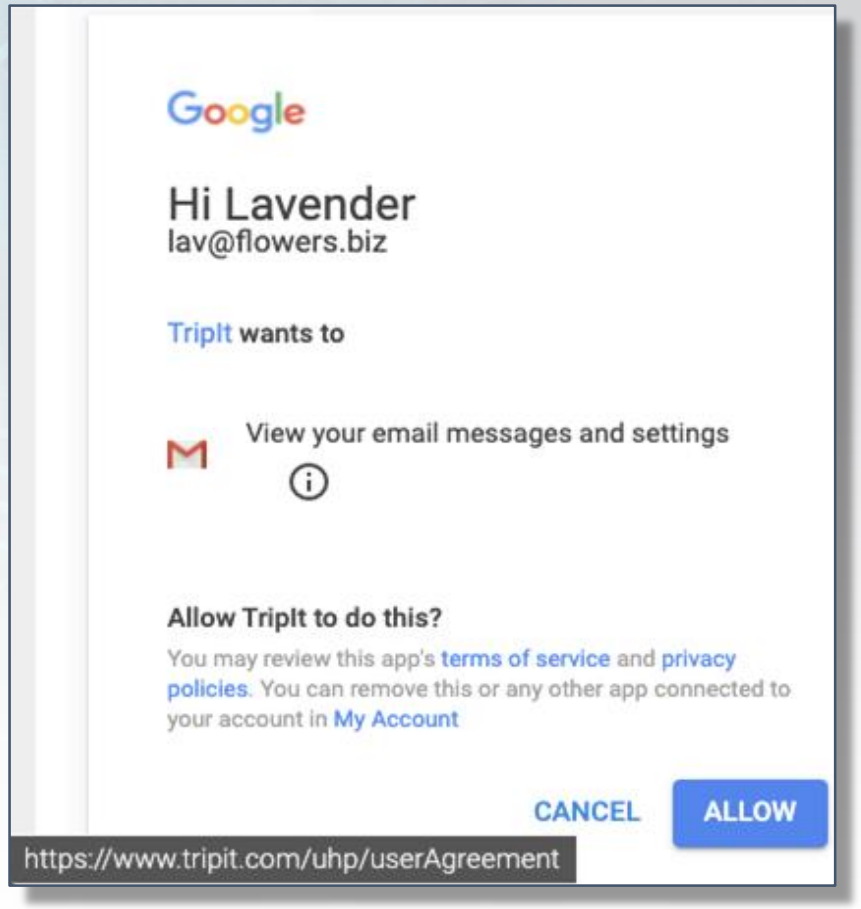


Photo by Jigsaw, Google.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Critical Thinking

- If you are unsure about a domain, you can use a search engine to find out more information

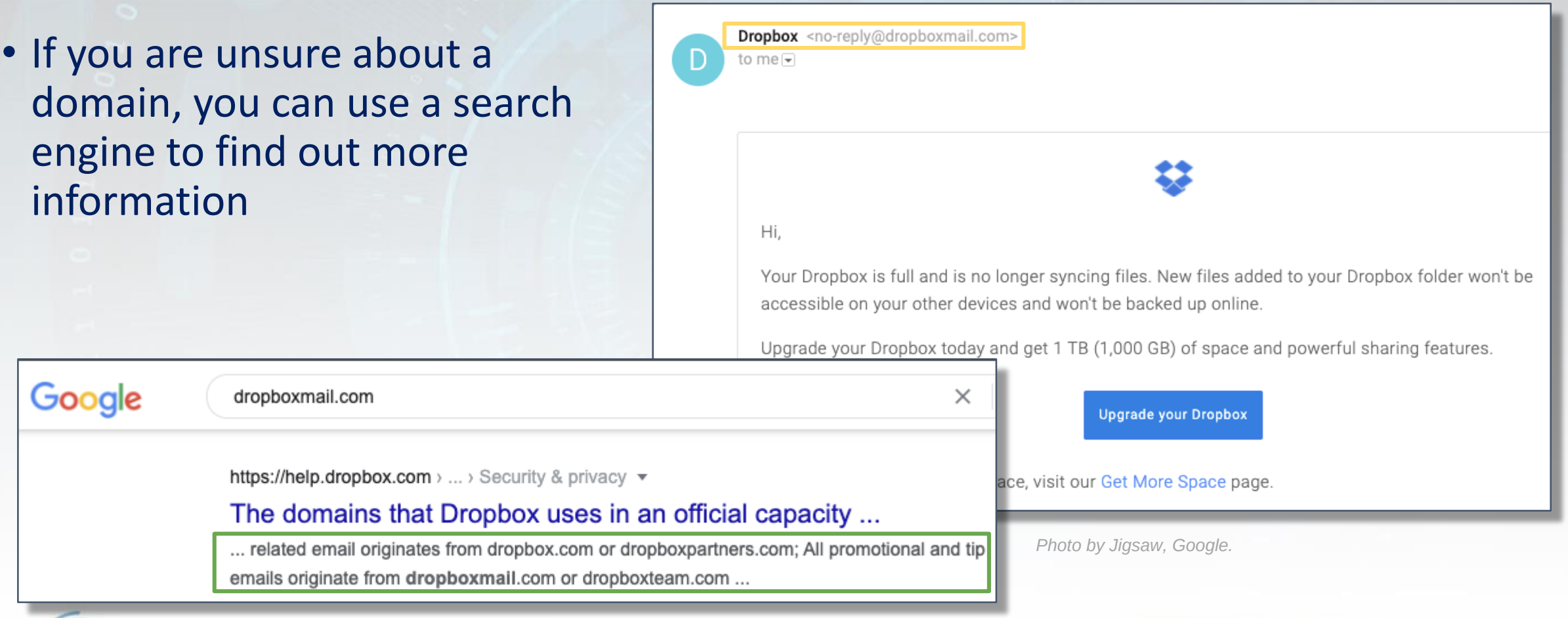


Photo by Jigsaw, Google.

CyberPhish
Safeguarding your digital future

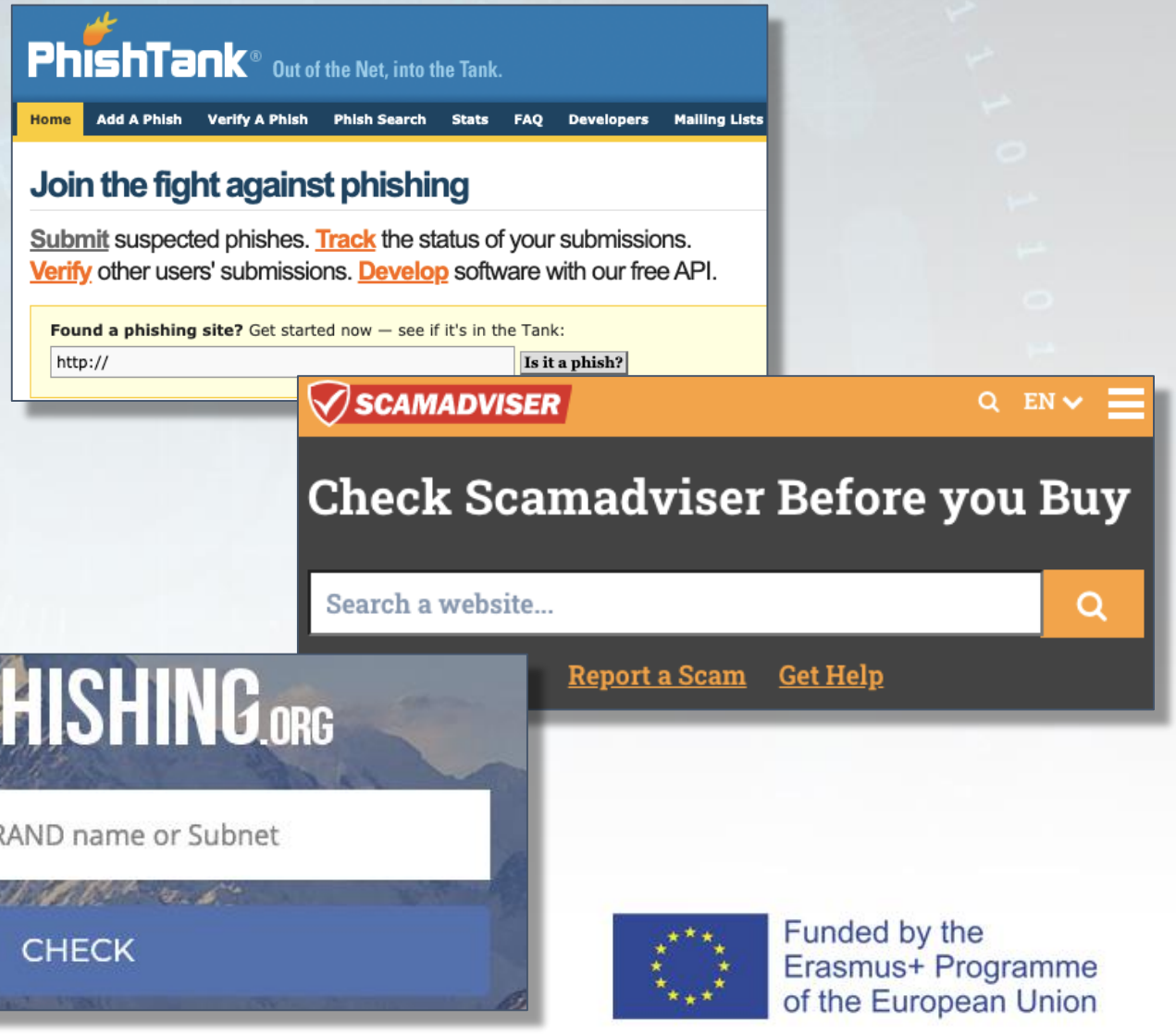
Funded by the Erasmus+ Programme of the European Union

Critical Thinking

- If you are unsure about a URL, there are free online tools for Looking up potentially phishy URLs

Some Examples:

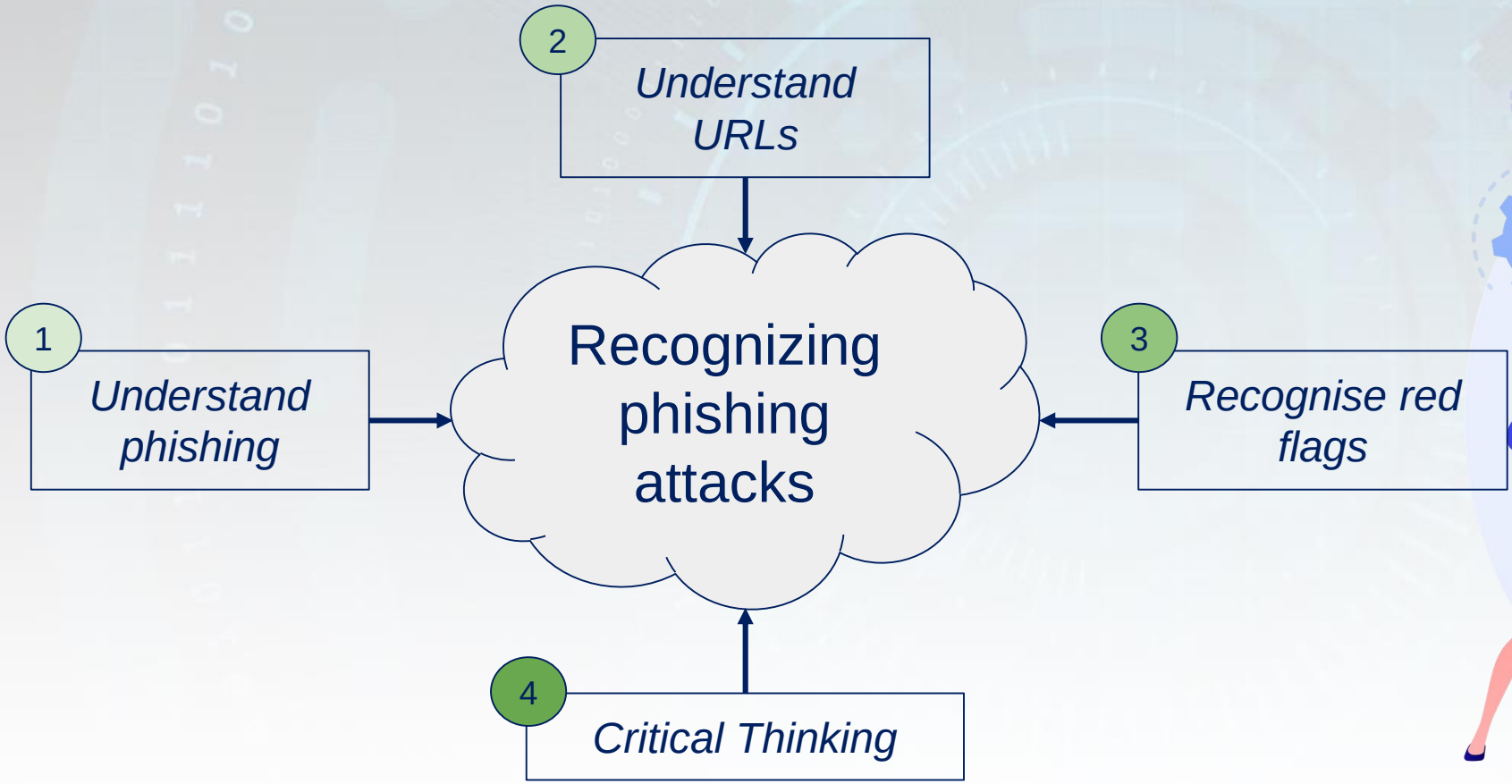
- *PhishTank*
- *CheckPhish*
- *IsItPhishing*
- *MalwareURL*
- *ScamAdviser*



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Summary



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Assignment

Can you spot which of the following are phishing URLs?

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

Assignment

Discuss what are other red flags not spoken about in this lecture that you have experienced in real life or recognised in some of the sample phishing examples given

Funded by the Erasmus+ Programme of the European Union

Assignment

Go to ***PhishTank*** and select a sample phishing analysis from “recent submissions”

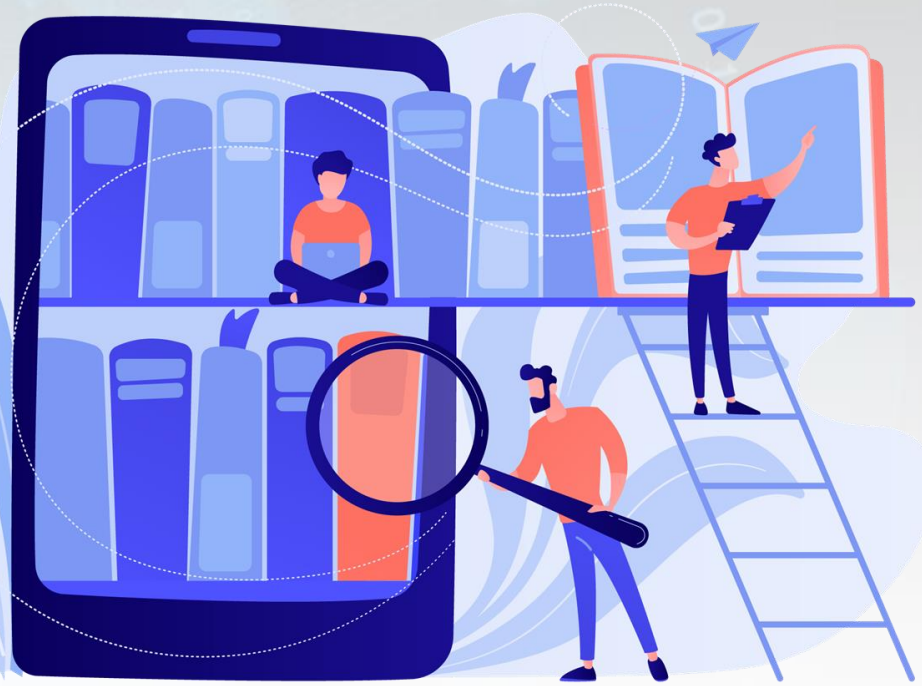
- *Can you tell if this is a phish or not?*
- *What were the phishing indicators?*
- *Click on “view technical details”. What can you learn from it?*

https://phishtank.org

Further Reading

Material used in preparation of this lecture

- **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

Short Videos

- 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

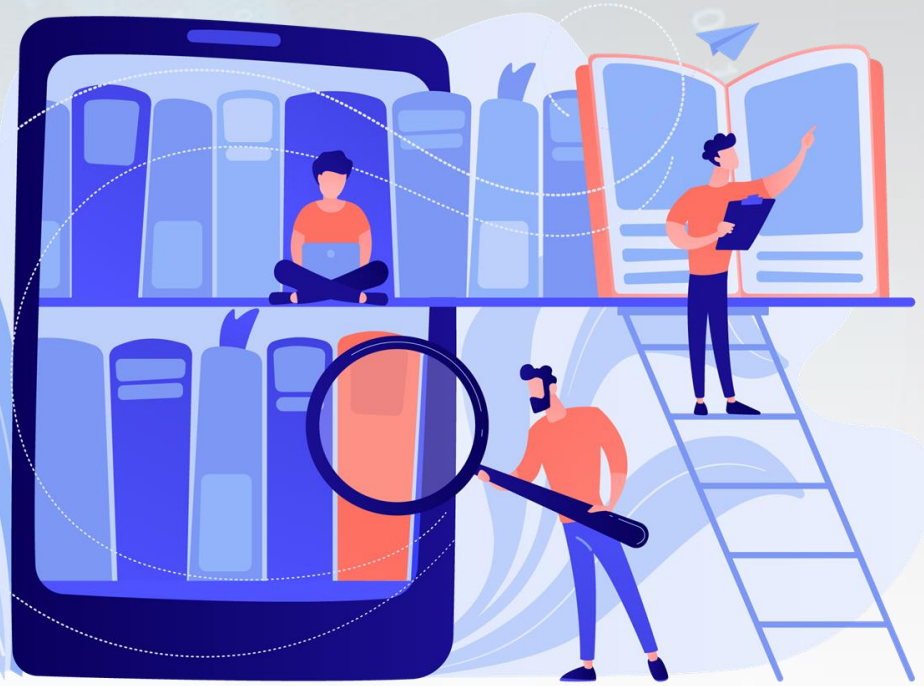
Funded by the Erasmus+ Programme of the European Union

Thank you!

Further Reading

Material used in preparation of this lecture

- **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

Short Videos

- 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