

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 4<sup>th</sup> 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.



### 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





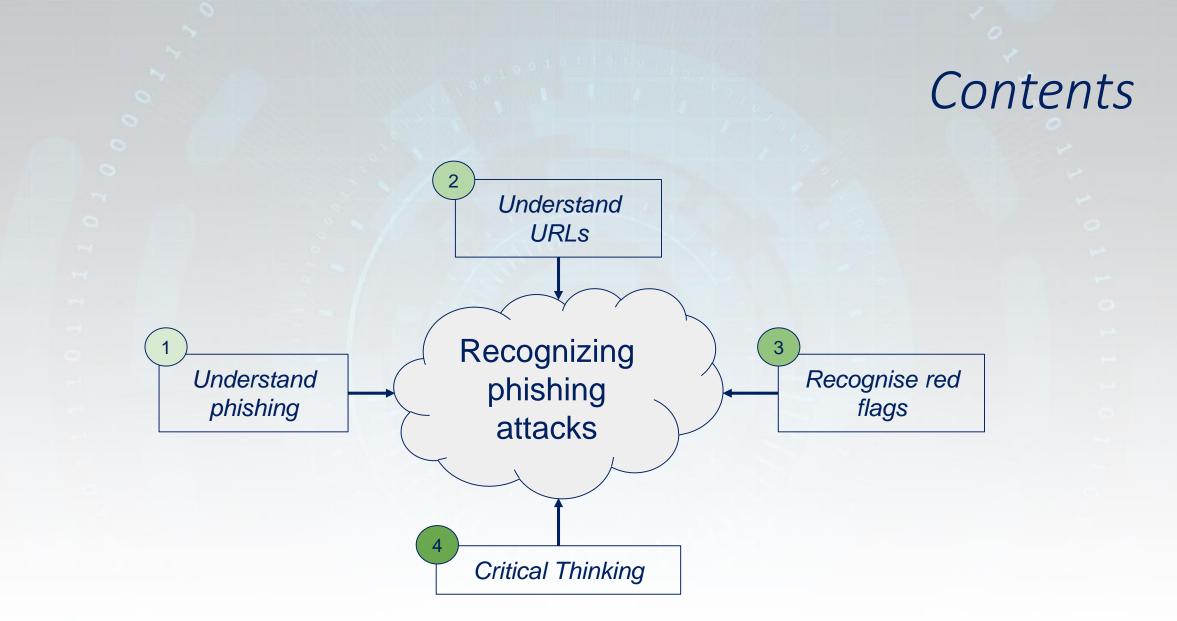
### Student Workload





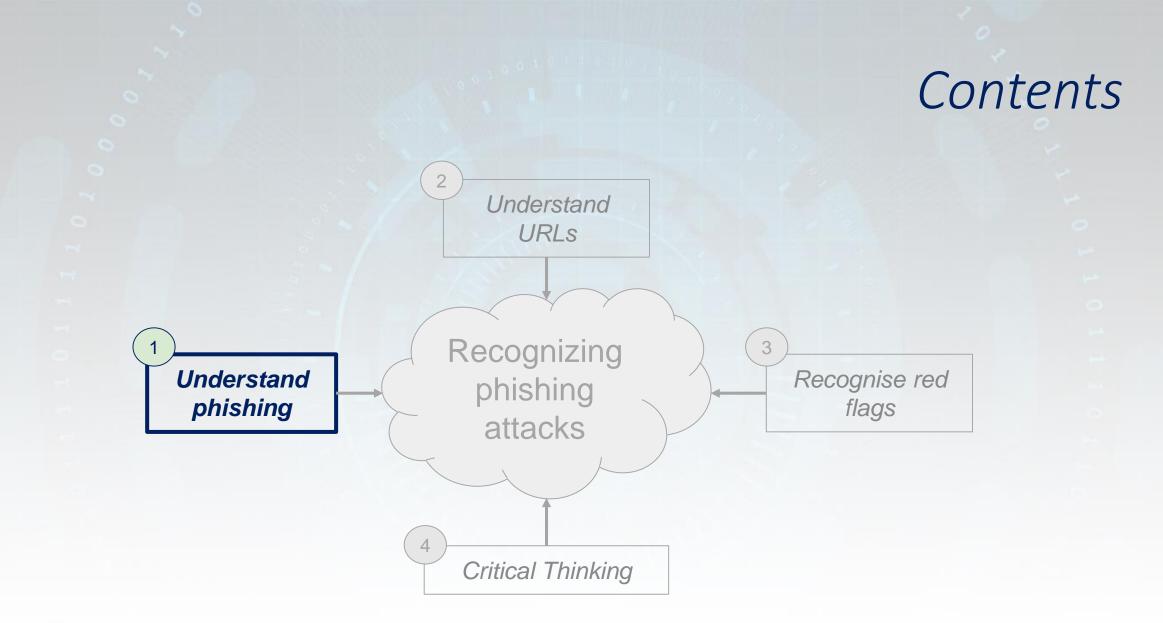
Lecture	2 h
Audio and video material	2 h
Case studies	2 h
Further reading	4 h
Preparation for exam	2 h















#### 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**



#### • Email

- Websites
- Social Media
- Mobile (SMS, voice)
- Any form of communication ...





## 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?

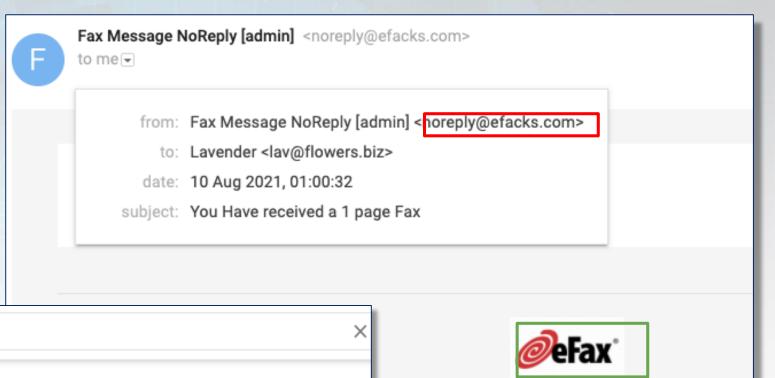






### Message Source

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



https://www.efax.com 👻

efax .com

herPhist

Safeguarding your digital future

Google

#### Fax Online with eFax – The Worlds #1 Best Online Fax Service

eFax iis the global leader in online fax. Send & receive faxes by email. Get a local, toll-free or international fax number. Fax from anywhere our ...

www.eFax.com/en/efax/page/help if you have any questions

Photo by Jigsaw, Google.



#### Message Content

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



 Account Suspended

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

#### Bank America's Most Convenient Bank ®

То

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. <sup>®</sup> are federally registeters service marks of TD Bank, N.A. <sup>©</sup> 2017 TD Bank, N.A. All Rights Reserved.



10

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



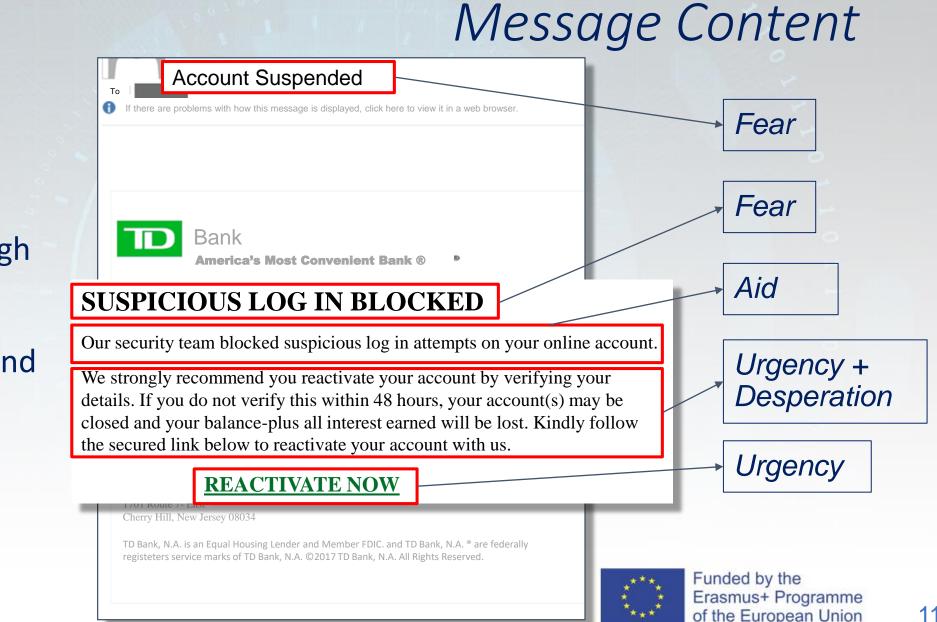


Photo by Sonicwall Phishing Test

## 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



	Luk
L	to n

uke Johnson <luke.json8000@gmail.com> me 🕞

Luke Johnson has shared a link to the following document:





Hi. Here is the doc you asked for. Let me know if you need anything else

Open in Docs

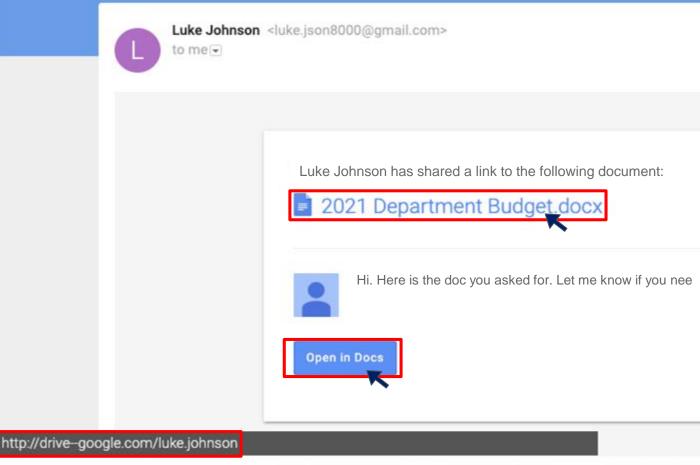
Photo by Jigsaw, Google.



Funded by the Erasmus+ Programme of the European Union

## Hyperlinks/Attachment

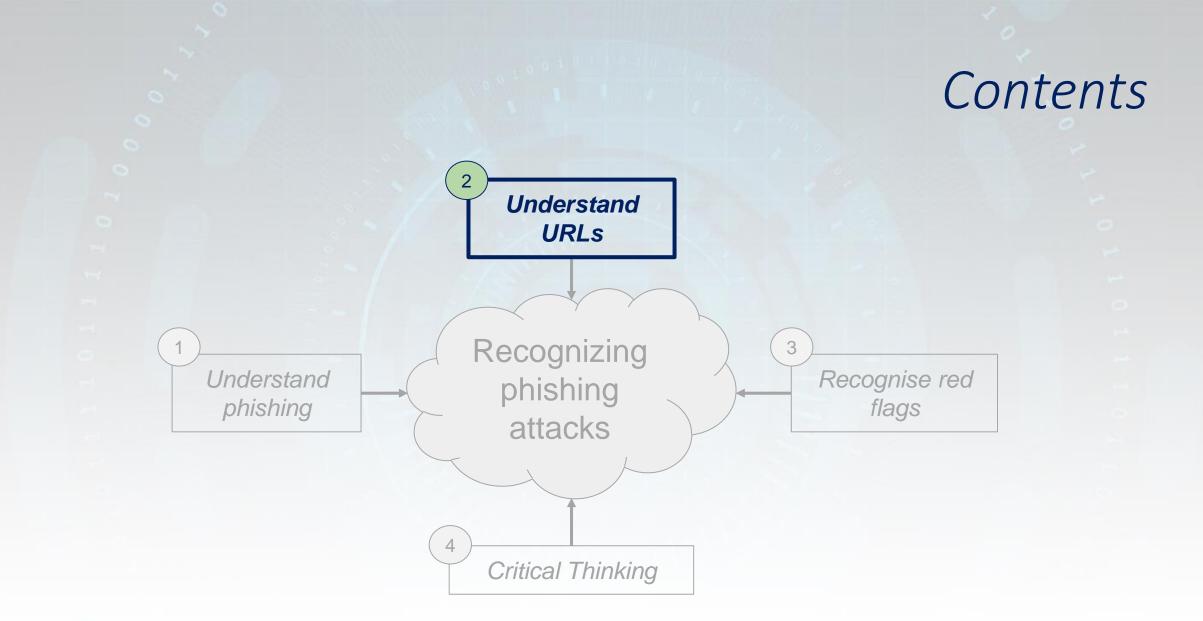
- Mouse over (or hover over) these hyperlinks to reveal its URL.
- The URL shown is the *insecure imitation* of the google drive domain
- http://drive--google.com/luke.johnson



CyberPhish

Photo by Jigsaw, Google.

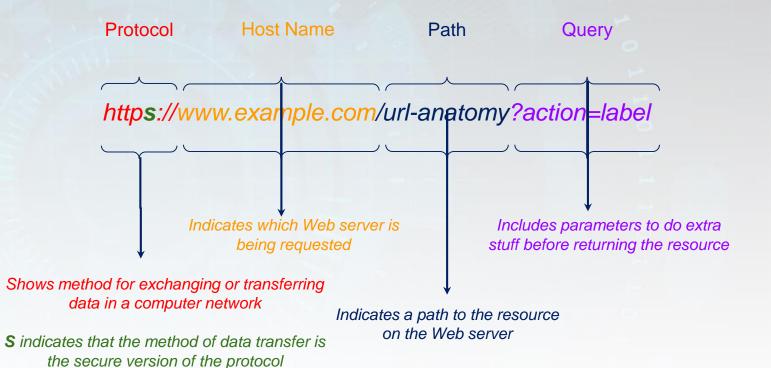








 Uniform Resource Locator (URL) is the address of a given unique resource on the Web.



CyberPhish

https://developer.mozilla.org/en-US/docs/Learn/Common\_questions/What\_is\_a\_URL Protocol, Simple Object Access. "URL." (2007).



Protocol Host Name Path Query https://www.example.com/url-anatomy?action=label Indicates which Web server is being requested Shows method for exchanging or transferring data in a computer network Indicates a path to the resource on the Web server is

*S* indicates that the method of data transfer is the secure version of the protocol

on the Web server



the Web.

Uniform Resource Locator

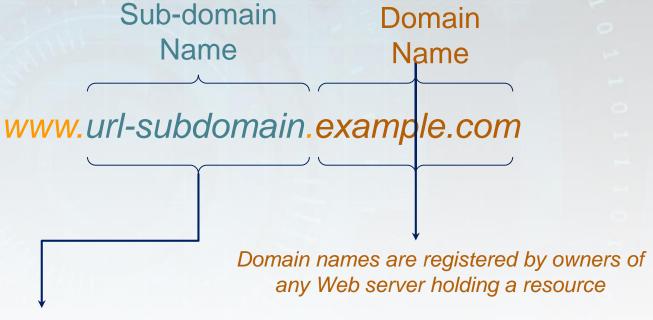
(URL) is the address of a

given unique resource on

https://developer.mozilla.org/en-US/docs/Learn/Common\_questions/What\_is\_a\_URL Protocol, Simple Object Access. "URL." (2007).



 Host name in URL can contain multiple subdomain names



Sub-domain names are tied to the corresponding domain name and indicates a section of the resource accessible through the domain name.



https://developer.mozilla.org/en-US/docs/Learn/Common\_questions/What\_is\_a\_URL Protocol, Simple Object Access. "URL." (2007).



#### Phishing often tries to trick victims with URLs.

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

Protocol	http	0
Host name	amazon.com.mailru382.co	
Path	/packagedelivery/2017Dk25RE3	
Domain name	mailru382.co	
Subdomain item 1	com	
Subdomain item 2	amazon	

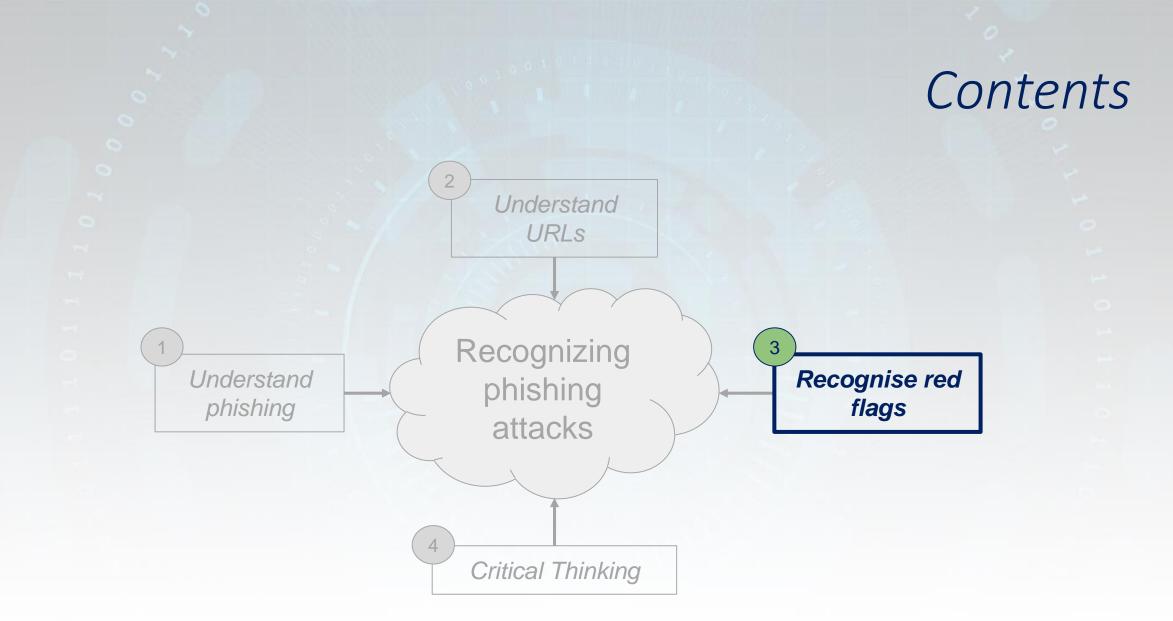




Other tricks with URL	Example	
URL protocol missing its secure protocol indicator.	URL uses <i>http</i> instead of <i>https</i>	
Domain visibly similar a well known domain, but actually different.	google.com misspelled as googgle.com	
Complicated looking domain name to confuse the victim i.e IP address, 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/	











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



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.

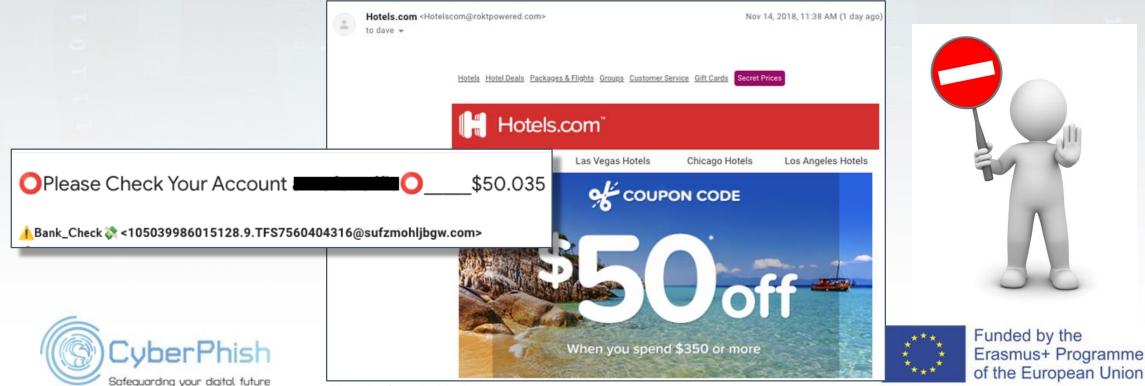


Photo by Stanford Edu.





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



#### 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.







Legitimate

 email sources
 do not have
 issues with
 spelling and
 grammar

From: <a href="mailto:noreply@stanford.edu">noreply@stanford.edu</a> 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.

© 2020 S ecurity Email Verification All Rights Reserved.





Photo by Stanford Edu.



#### Legitimate email sources don't send unsolicited attachments

#### ConeDrive

share a document with you.

Review amendment draft and comment as require.

#### Proposal Draft pdf





Photo by Sonicwall Phishing Test



Send**Transfer**com

Send up to 10GB

Files Sent By:

#### LuisQo@stanford.edu

offer\_\_.pdf

Message: Hallo!! Warning!! Information for students : <u>https://v.ht/stanford</u>

Files Remain Available Until: 3. 4. 2020.

#### Download

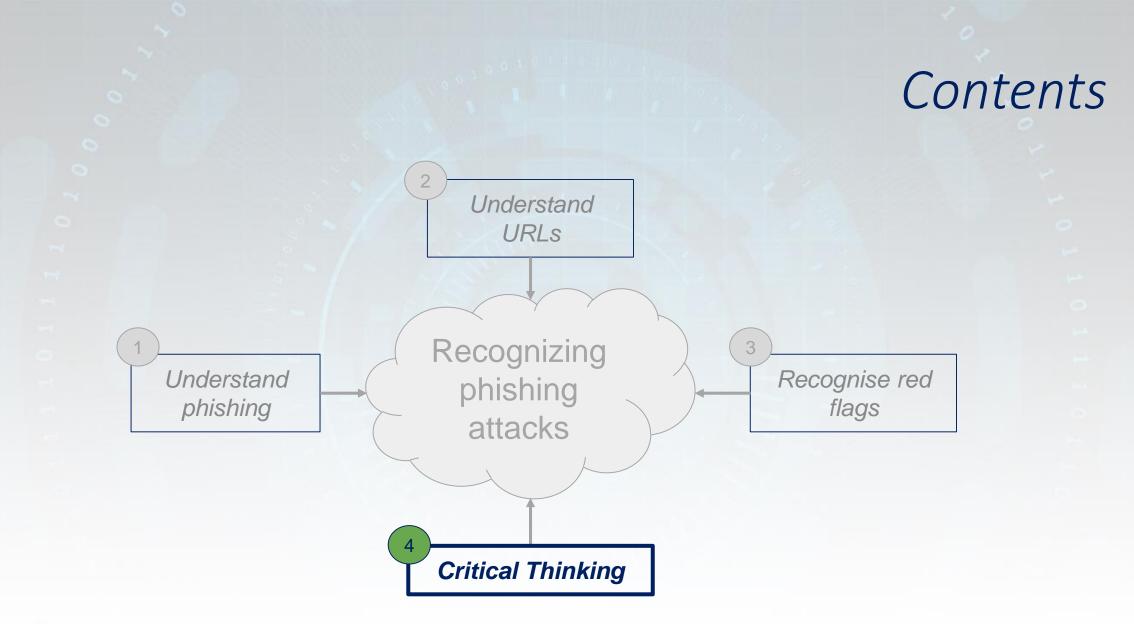
Link:

https://www.sendtransfer.com/download.php?id=c5dbaf14d5be434e5185490412463ec4&email=992554













Phishing detection involves detecting deception.



Spend more time reviewing messages before taking actions Spot check: Does the message check any red flags?









• 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.

	T	TK to me details
	from:	tk867530@gmail.com
	to:	lav@flowers.biz
	date:	10 Aug 2021, 01:37:58
	subject:	I just found a photo of you!
	hey, do	you remember THIS PHOTO!
ttps://drive.google.com.download-photo.sytez.net/AONh1e0hVP		

Photo by Jigsaw, Google.

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





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





Google <no-reply@google.support> to me <



#### Government-backed attackers may be trying too steal your password

There's a chance that this is a false alarm, but we believe that we detected government-backed attackers trying too steal your password. This happens too less than 0.1% of all Gmail users. We can't reveal what tipped us off because the attackers will take noote and change their tactics, but if they are successful at some point they cold access your data or take other actions using your account. To further improve your security, based oon your current settings, we recommend:

#### Change password

https://google.com/amp/tinyurl.com/y7u8ewlr

Photo by Jigsaw, Google.



Google <no-reply@google.support> to mer

02:06

#### Someone has your password

Hi,

Someone just used your password to try to sign in to your Google Account.

#### Information:

Tuesday, 10 August 2021 at 02:06:30 GMT+03:00 Slatina, Romania Firefox browser

Google stopped this sign-in attempt. You should change your password immediately

#### CHANGE PASSWORD

Best, The Mail Team

http://myaccount.google.com-securitysettingpage.ml-security.org/signonoptions



• 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

	Manager Daniel Bridges <daniel_bridges33@gulfslipformpaving.com></daniel_bridges33@gulfslipformpaving.com>
	Information
	August 26, 2013 1:25:12 AM MDT
1.01	dave
Reply-To:	Manager Daniel Bridges <daniel_bridges33@gulfslipformpaving.com></daniel_bridges33@gulfslipformpaving.com>
	USPS.COM
	Notification
	Our courier couldnt make the delivery of parcel to you at 20th August. Print label and show it in the nearest post office.
	Print a Shipping Label NOW
USPS	Copyright 2013 USPS, All Rights Reserved.



Photo by Security Metrics.



#### • Check that you trust app developers before granting account access requests

#### Google

Hi Lavender lav@flowers.biz

Triplt wants to

View your email messages and settings

#### Allow TripIt to do this?

You may review this app's **terms of service** and **privacy policies**. You can remove this or any other app connected to your account in **My Account** 

CANCEL ALLOW

Photo by Jigsaw, Google.

#### Google

Hi Lavender lav@flowers.biz

Triplt wants to

M

View your email messages and settings

#### Allow TripIt to do this?

You may review this app's terms of service and privacy policies. You can remove this or any other app connected to your account in My Account

#### CANCEL

ALLOW

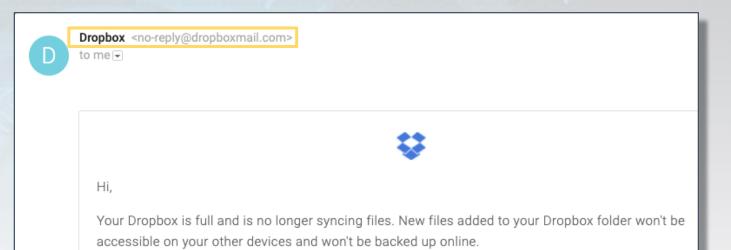
https://www.tripit.com/uhp/userAgreement



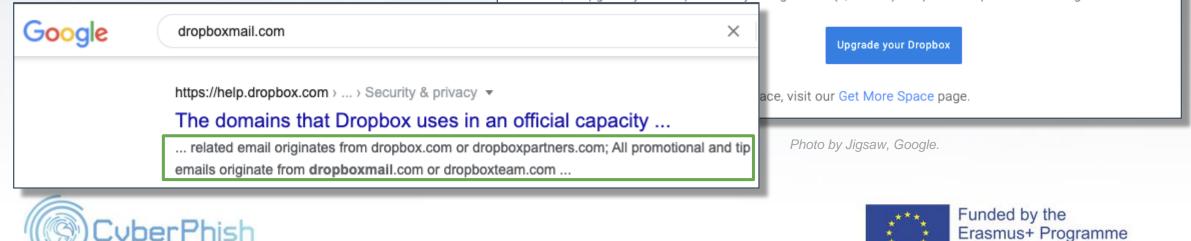


 If you are unsure about a domain, you can use a search engine to find out more information

Safeguarding your digital future



Upgrade your Dropbox today and get 1 TB (1,000 GB) of space and powerful sharing features.



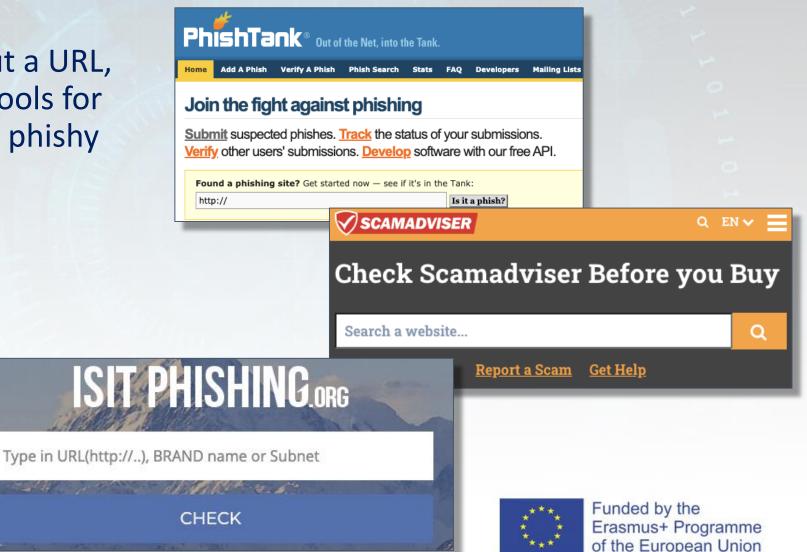
of the European Union

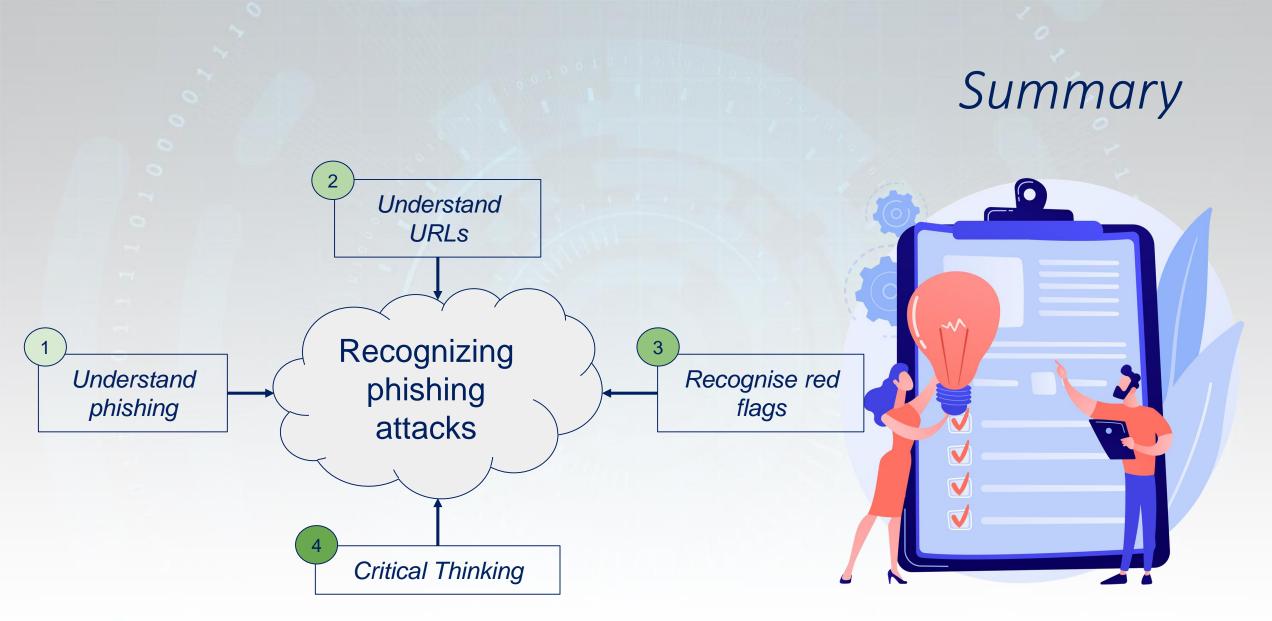
 If you are unsure about a URL, there are free online tools for Looking up potentially phishy URLs

#### Some Examples:

- <u>PhishTank</u>
- <u>CheckPhish</u>
- IsItPhishing
- MalwareURL
- <u>ScamAdviser</u>











### 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





#### 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





### 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



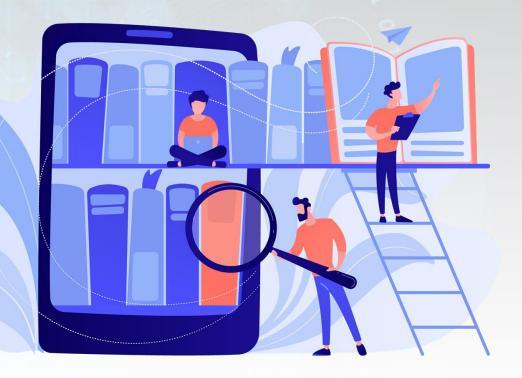


37

#### 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

### Further Reading







### Short Videos

- Phishing email scam anatomy

   https://youtu.be/3gpOM9c6mmA
- Phishing attacks explained
  - o https://youtu.be/Y7zNIEMDml4
  - o https://youtu.be/gqhPkeXMeh0
- Recognising and staying safe from phishing
  - o https://youtu.be/R12\_y2BhKbE







## **Thank you!**





www.cyberphish.eu Project Implementation Period 02 11 2020 – 02 11 2022



CyberPhish Project #CyberPhish



Funded by the Erasmus+ Programme of the European Union

#### 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. <u>https://doi.org/10.1145/3465481.3470029</u>
- 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.
   <u>https://cheapsslsecurity.com/blog/10-phishing-email-examples-you-need-to-see/</u>
- Ellis, D. 7 Ways to Recognize a Phishing Email: Email Phishing Examples. <u>https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email</u>

## Further Reading







### Short Videos

- Phishing email scam anatomy
  - <u>https://youtu.be/3gpOM9c6mmA</u>
- Phishing attacks explained
  - o <u>https://youtu.be/Y7zNIEMDml4</u>
  - o <u>https://youtu.be/gqhPkeXMeh0</u>
- Recognising and staying safe from phishing
  - o <u>https://youtu.be/R12\_y2BhKbE</u>





