Funded by the Erasmus+ Programme of the European Union

Overview of Understanding and Handling Cyber-Attacks

Recognising Phishing Attacks

Case Studies Analysis of Phishing Attacks and Techniques

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 different phishing attacks resulting effects of the attacks and how to recognise and handle these phishing attacks

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Student workload

Lecture	3 h
Audio and video material	3 h
Case studies	3 h
Further reading	6 h
Preparation for exam	3 h

Funded by the Erasmus+ Programme of the European Union

Contents

- What are phishing attacks and risks?
- Case studies analysis of phishing attacks
  - What are phishing threats and risks in each case?
  - How to recognise and handle these phishing risks?

Funded by the
Erasmus+ Programme
of the European Union

What is a Phishing Attack?

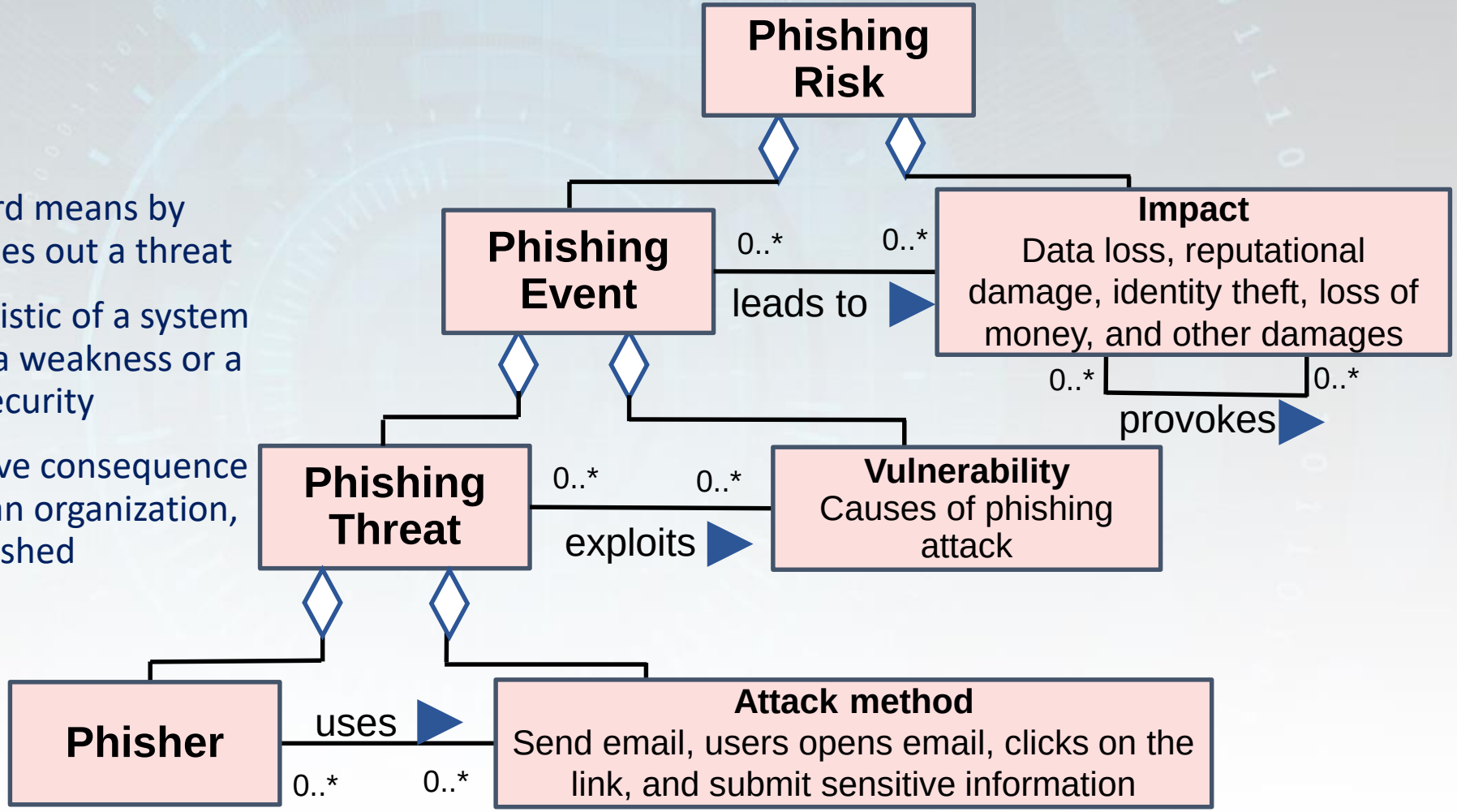
Phishing is *a social engineering scam that can result in data loss, reputational damage, identity theft, the loss of money, and many other damages to peoples and organisations. A phishing scam usually starts with an email trying to gain the potential victim's trust and convince them to take the attacker's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

[Abroshan, 2021]

Funded by the
Erasmus+ Programme
of the European Union

What is a Phishing Risk?

- **Attack method** – standard means by which a threat agent carries out a threat
- **Vulnerability** – characteristic of a system asset that can constitute a weakness or a flaw in terms of system security
- **Impact** - potential negative consequence that may harm assets or an organization, when a threat is accomplished

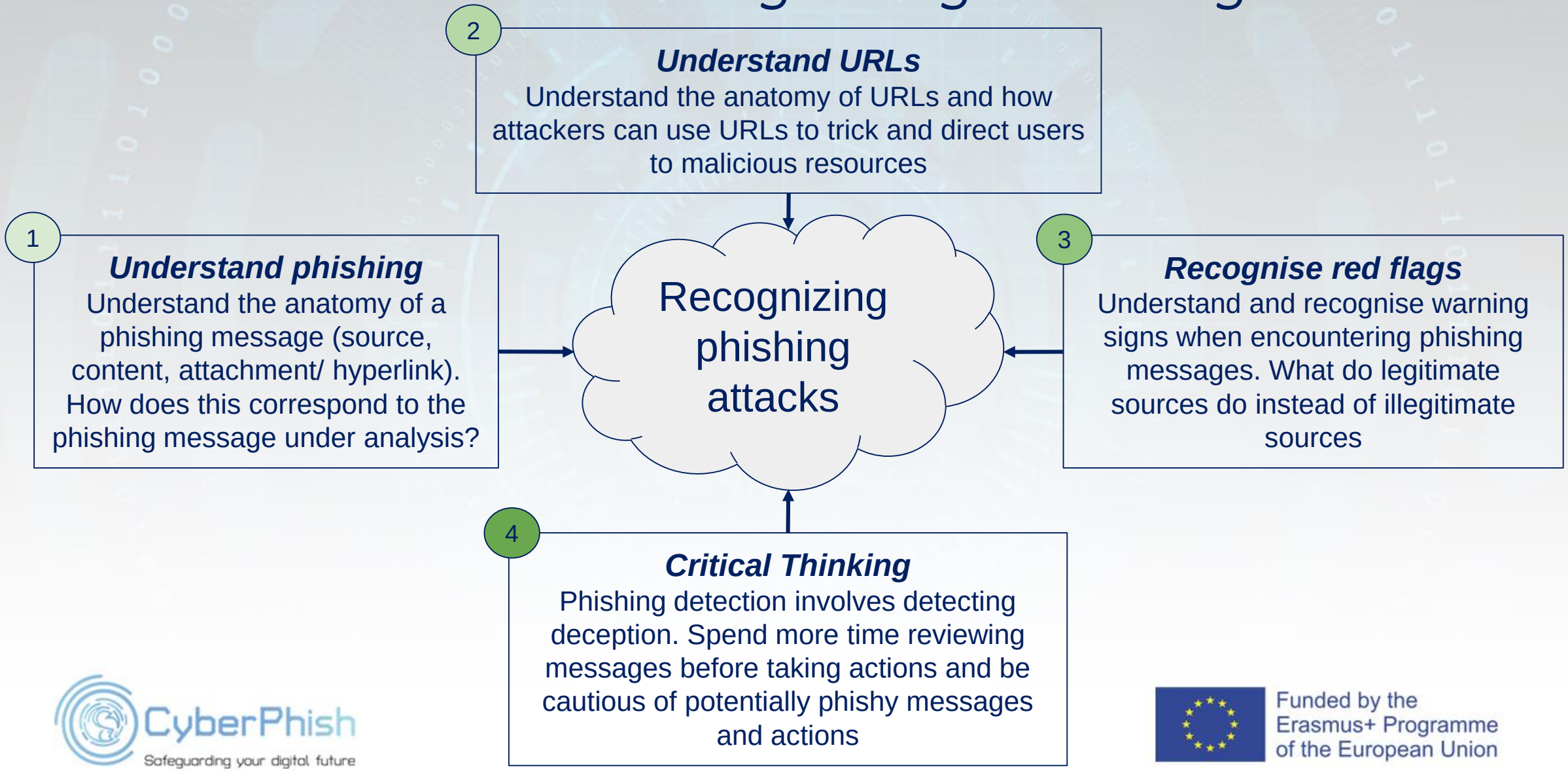


[Dubois at al., 2010]

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Recognising Phishing Attacks



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Case Studies

Selected Cases

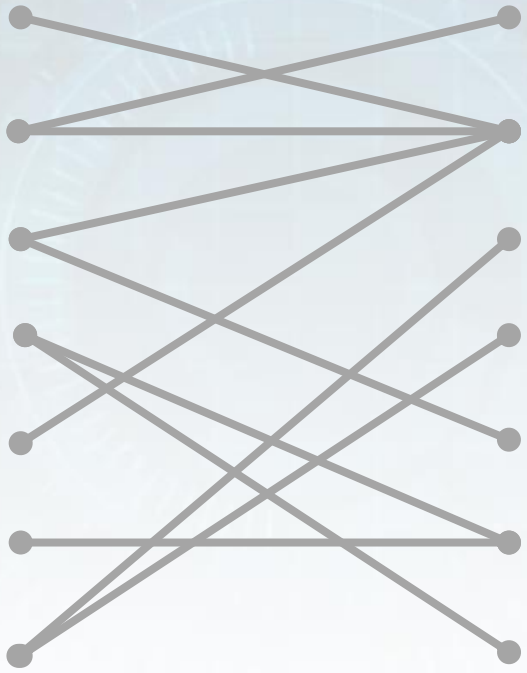
- COVID-related Attacks
- GDPR-related Attacks
- Tech Support Attacks
- Cryptocurrency Scams
- Extortion Scams
- Advance Fee Scams
- Social Media Scams

Funded by the
Erasmus+ Programme
of the European Union

Case Studies

Selected Cases

- COVID-related Attacks
- GDPR-related Attacks
- Tech Support Attacks
- Cryptocurrency Scams
- Extortion Scams
- Advance Fee Scams
- Social Media Scams



- GDPR-related Attacks
- Emails
- Instant Messaging
- Social Networks
- Websites
- Lottery Scams
- SMS

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

COVID-related Attacks

- During COVID-19 we noticed an uptick on pandemic-related scams through emails and SMS like fake Centers of Disease Control and Prevention (CDC) or health organisations' notifications, about vaccine coverage, where you can get vaccine, vaccine statistics, status of employees vaccination etc
- Prevalent attacks include COVID health advice email scams

Funded by the Erasmus+ Programme of the European Union

Risk Analysis

COVID phishing risk

to get
nancial
loggers,

Phish
thre

Phisher

uses

0..*

Singapore Specialist : Corona Virus Safety Measures

DT

Tuesday, 28 January 2020 at 03:51

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

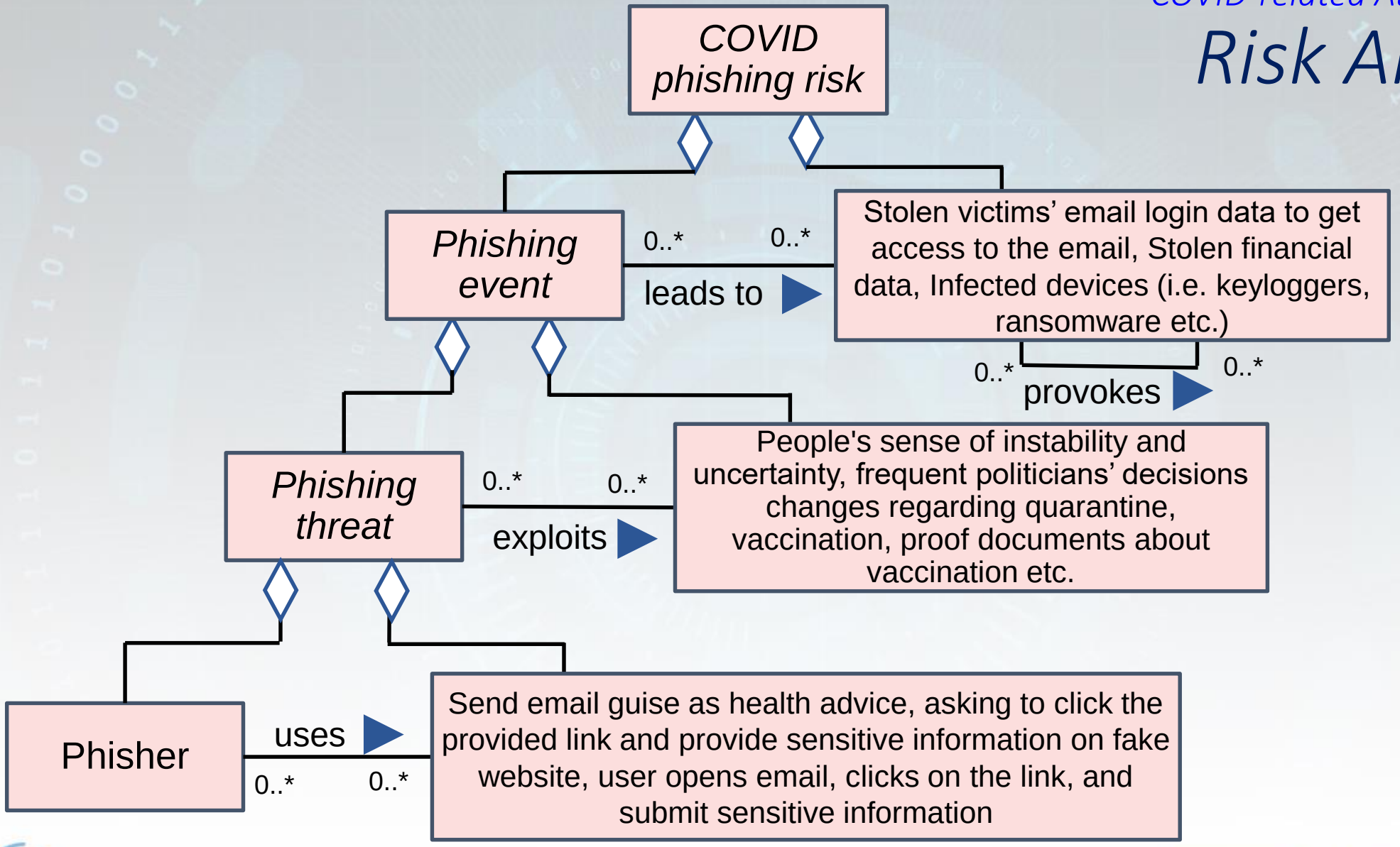
Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards
Dr
Specialist wuhan-virus-advisory

Coronavirus Phishing Email (Source: Wired)

Funded by the Erasmus+ Programme of the European Union

Risk Analysis



Coronavirus Phishing Email (Source: Wired)

Risk Recognition

2. Understand URLs
2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the content

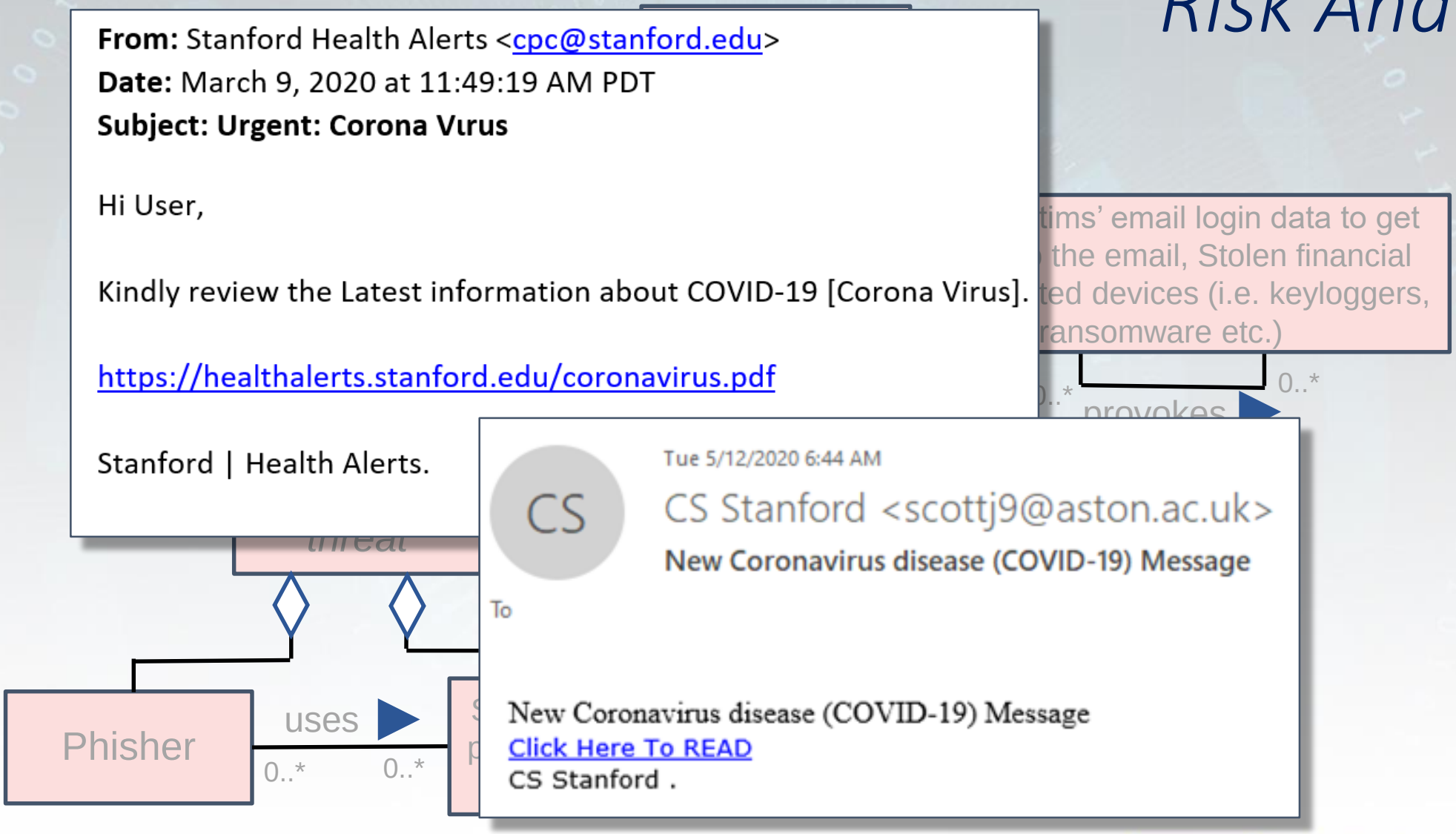
1. Understand Phishing
Phishing source: Email
Phishing message anatomy:
a. Who is the message is from? *[Redacted]*
b. What is the message content?
Coronavirus safety measures
c. Are there hyperlinks/attachments? *Yes*

3. Recognising Red Flags
3.1 Credible COVID information sources do not send unsolicited emails
3.2 Legitimate emails usually call you by your name (i.e, not "*Sir*")
3.3 Legitimate emails do not have issues with spelling and grammar i.e "*Symptoms Common Symptoms*"

4. Critical Thinking
4.1 Check that email is from a credible and expected source
4.2 Be cautious of hyperlinks/attachments; they may link to a malicious resource
4.3 Be cautious when emails requests actions with a sense of urgency/fear
4.4 Use a search engine to find out more information on email contents, before trusting the message
4.5 Look up potentially phishy URLs using free phishing detection tools
4.6 Delete the email you were sent if reasonably certain it is a phishing

Funded by the
Erasmus+ Programme
of the European Union

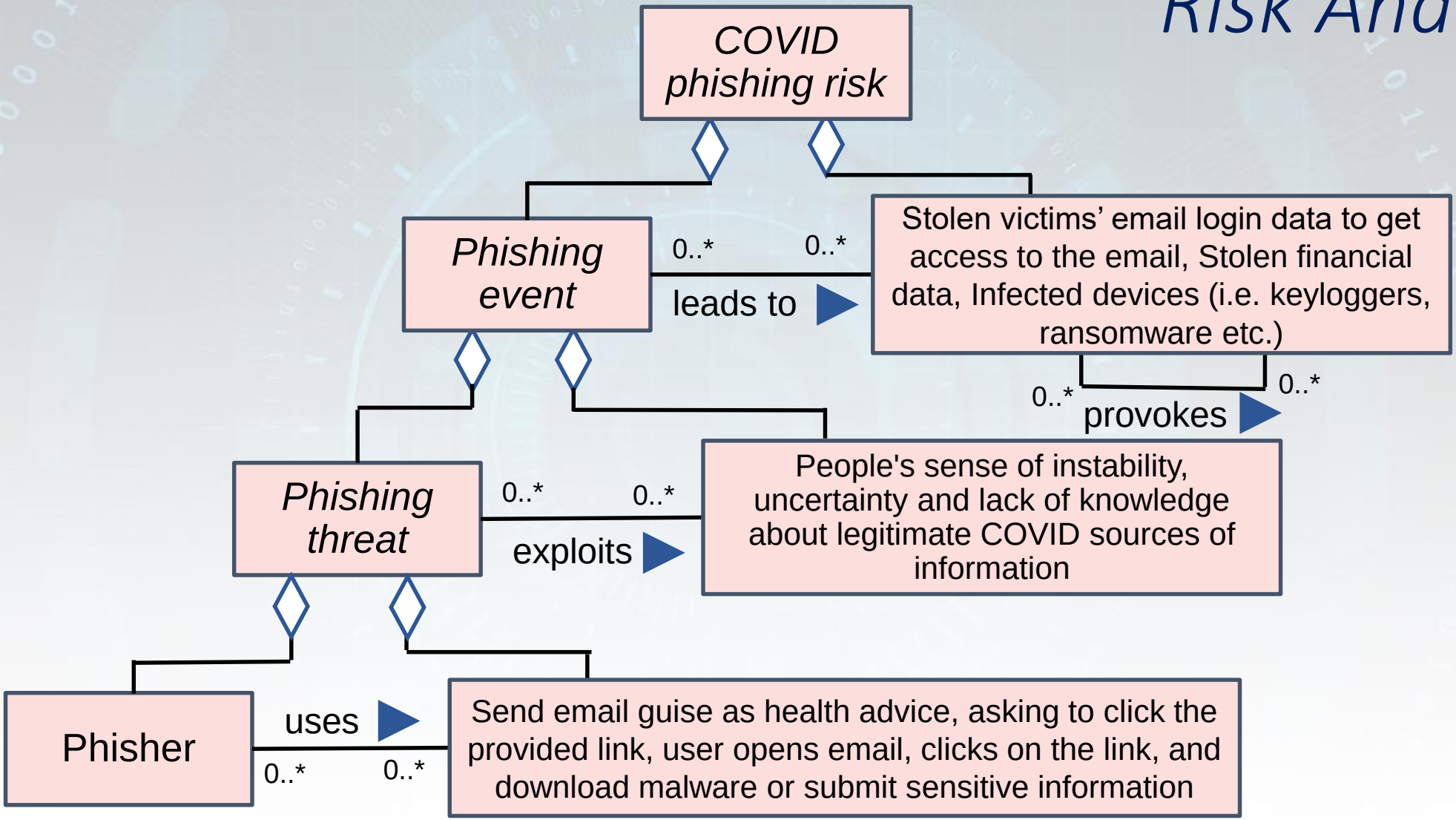
Risk Analysis



Coronavirus Phishing Email (Source: Stanford.edu, Stanford.edu)

Funded by the Erasmus+ Programme of the European Union

Risk Analysis



Coronavirus Phishing Email (Source: Stanford.edu, Stanford.edu)

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

2. Understand URLs
2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious

1. Understand Phishing
Phishing source: Email
Phishing message anatomy:
a. Who is the message is from?
cpc@stanford.edu, scottj9@aston.ac.uk
b. What is the message content? *Coronavirus*
c. Are there hyperlinks/attachments? *Yes*

3. Recognising Red Flags
3.1 Credible COVID information sources do not send unsolicited emails
3.2 Legitimate emails usually call you by your name
3.3 Legitimate emails are professional and have a uniform template format

4. Critical Thinking
4.1 Check that email is from a credible and expected source
4.2 Be cautious of hyperlinks/attachments; they may link to a malicious resource
4.3 Use a search engine to find out more information on email contents, before trusting the message
4.4 Look up potentially phishy URLs using free phishing detection tools
4.5 Delete the email you were sent if reasonably certain it is a phishing

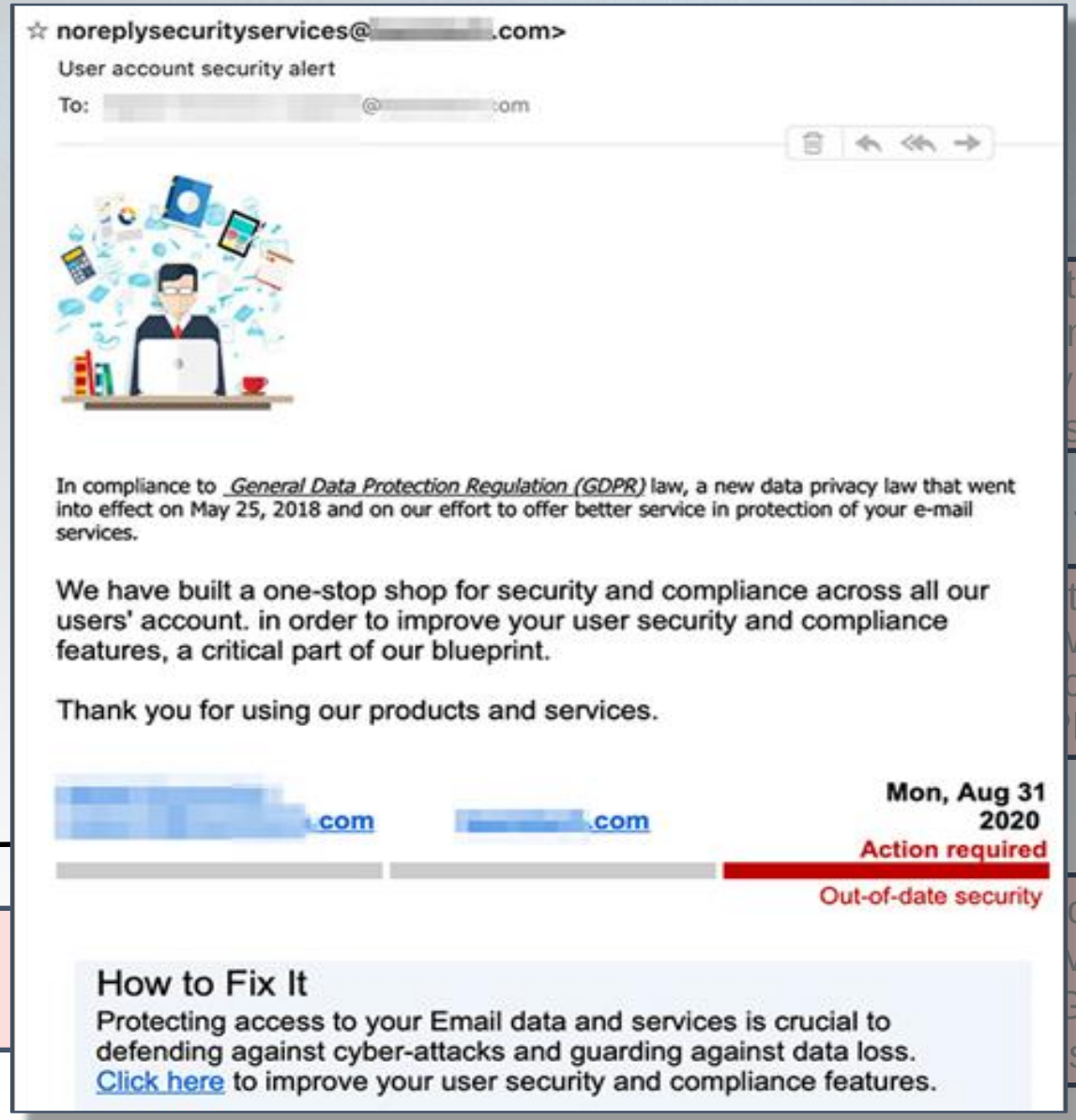
Funded by the Erasmus+ Programme of the European Union

GDPR-related Attacks

- Many GDPR related phishing attacks occurs in 2018, as all companies and organisations were mandated to implement GDPR in their organisations
- Attacker tactics can include sending
  - *fake emails in pretence of a company helping with GDPR activities, to steal information*
  - *fake emails in pretence of companies providing information on data policy changes to customer*

Funded by the Erasmus+ Programme of the European Union

Risk Analysis



tims' email login data to get
mail. Sensitive data could be
ictim' email or stolen contacts
sed for further cyber attacks

0..*

.* provokes

t trained about GDPR,
w violations
cause of timeline for
R compliance

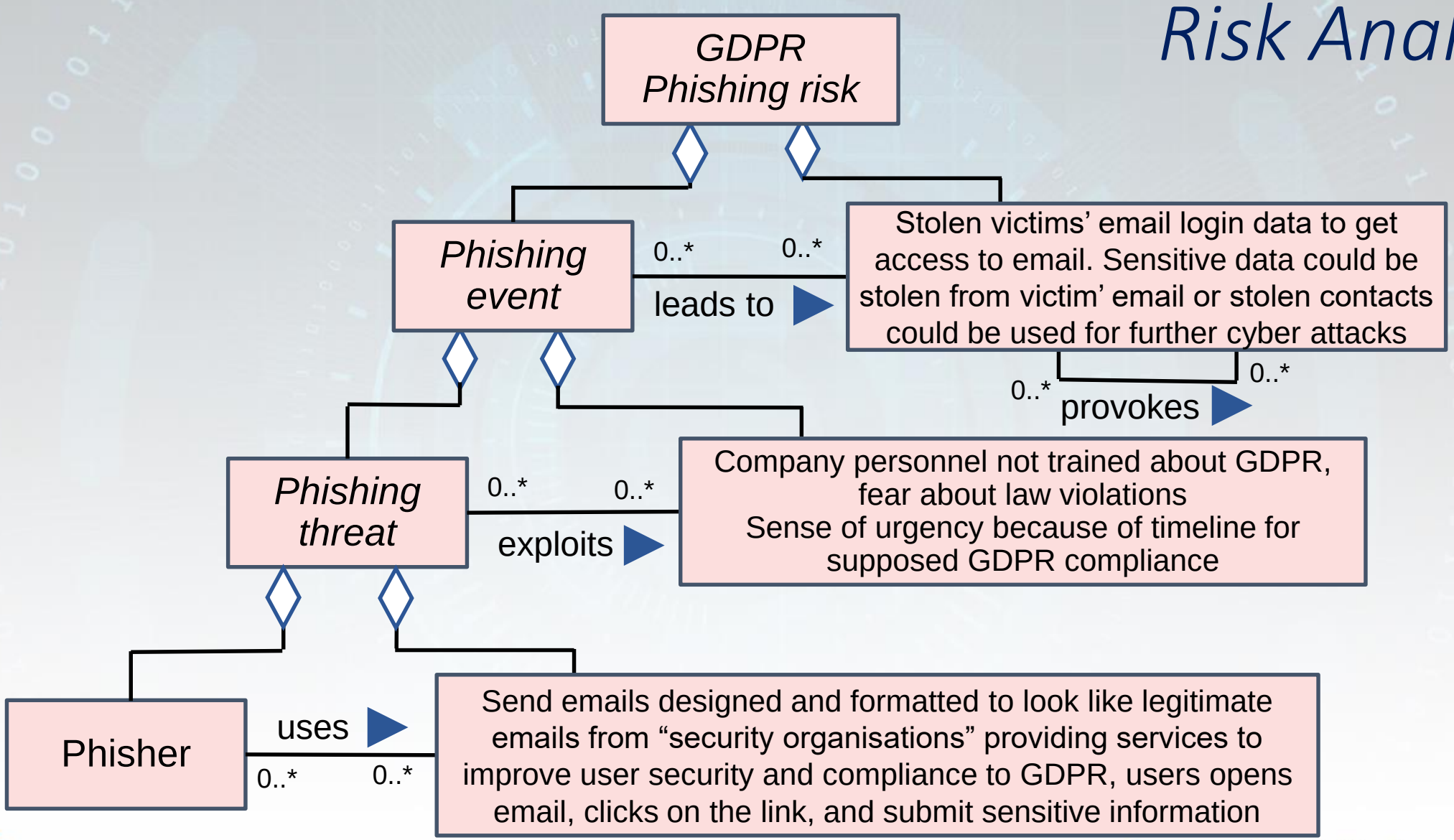
Phisher

ook like legitimate
viding services to
GDPR, users opens
sitive information

GDPR Phishing Email (Source: Databreachtoday)

Funded by the Erasmus+ Programme of the European Union

Risk Analysis



GDPR Phishing Email (Source: Databreachtoday)

Risk Recognition

2. Understand URLs
2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the content

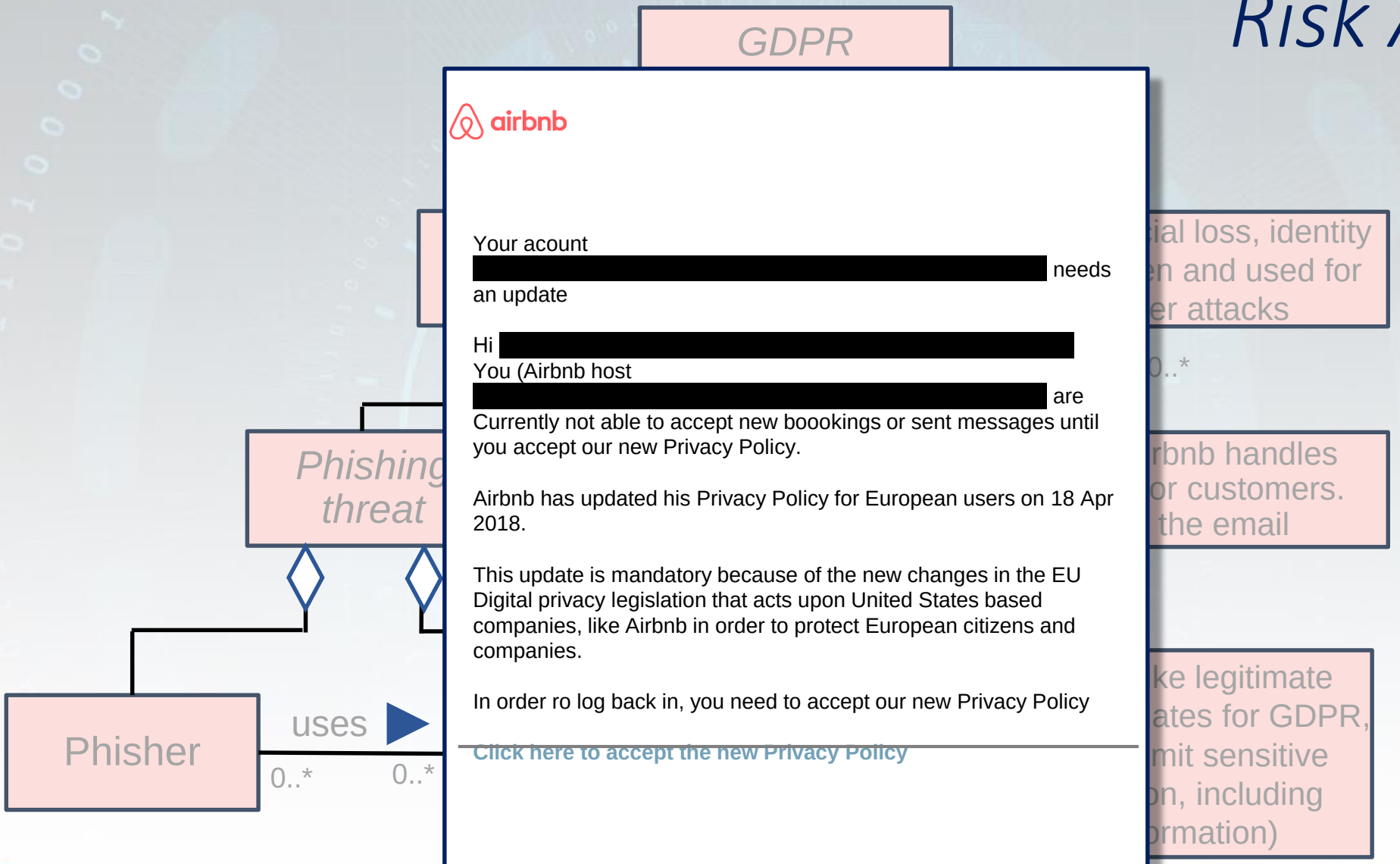
1. Understand Phishing
Phishing source: Email
Phishing message anatomy:
a. Who is the message is from? *noreplysecurityservices*
b. What is the message content? *Account security alert*
c. Are there hyperlinks/attachments? *Yes*

3. Recognising Red Flags
3.1 Legitimate email messages do not have conflicting contents eg "*GDPR*" vs "*Out of date security*"
3.2 Legitimate service emails are professional and have a uniform format

4. Critical Thinking
4.1 Check that email is from a credible and expected source
4.2 Be cautious of hyperlinks/attachments; they may link to a malicious resource
4.3 Be cautious when emails requests actions with a sense of urgency/fear
4.4 Use a search engine to find out more information on the organisation providing the supposed service
4.5 Look up potentially phishy URLs using free phishing detection tools
4.6 Delete the email you were sent if reasonably certain it is a phishing

Funded by the Erasmus+ Programme of the European Union

Risk Analysis

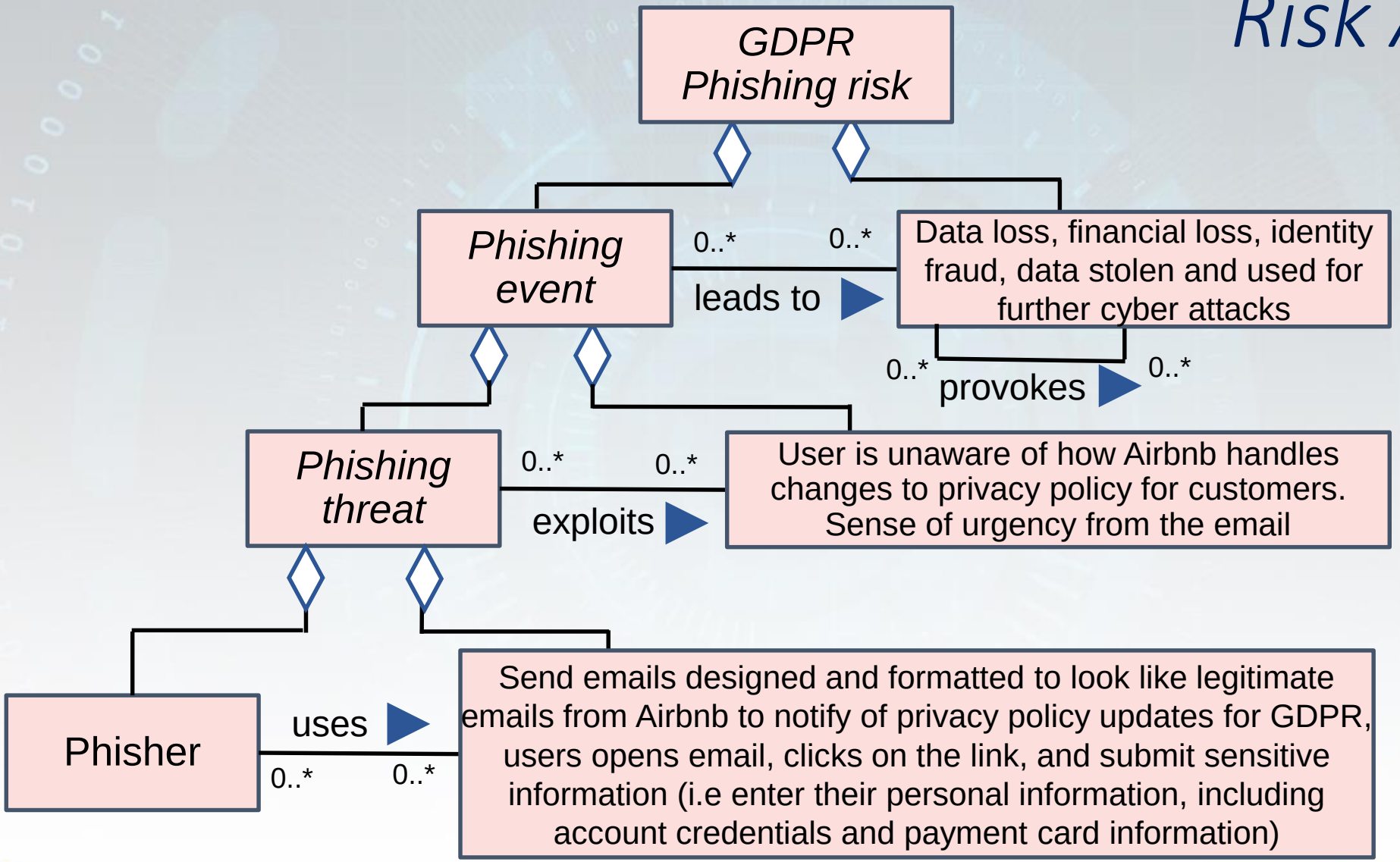


GDPR Phishing Email (Source: Securityaffairs)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Risk Analysis



GDPR Phishing Email (Source: Securityaffairs)

Risk Recognition

2. Understand URLs
2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the message content

1. Understand Phishing
Phishing source: Email
Phishing message anatomy:
a. What is the message content? *GDPR update for account*
b. Are there hyperlinks/attachments? *Yes*

3. Recognising Red Flags
3.1 Legitimate companies handle privacy policy agreements directly on the website or application
3.2 GDPR notifications sent by companies to its customers don't ask for users' credentials

4. Critical Thinking
4.1 Check that email is from a credible and expected source
4.2 Be cautious of hyperlinks/attachments; they may link to a malicious resource
4.3 Check the sender's email address for discrepancies that are indicators of fraud (see Airbnb list)
4.4 Check more information of the email content on the official Airbnb website
4.5 Look up potentially phishy URLs using free phishing detection tools
4.6 Delete the email you were sent if reasonably certain it is a phishing

Funded by the Erasmus+ Programme of the European Union

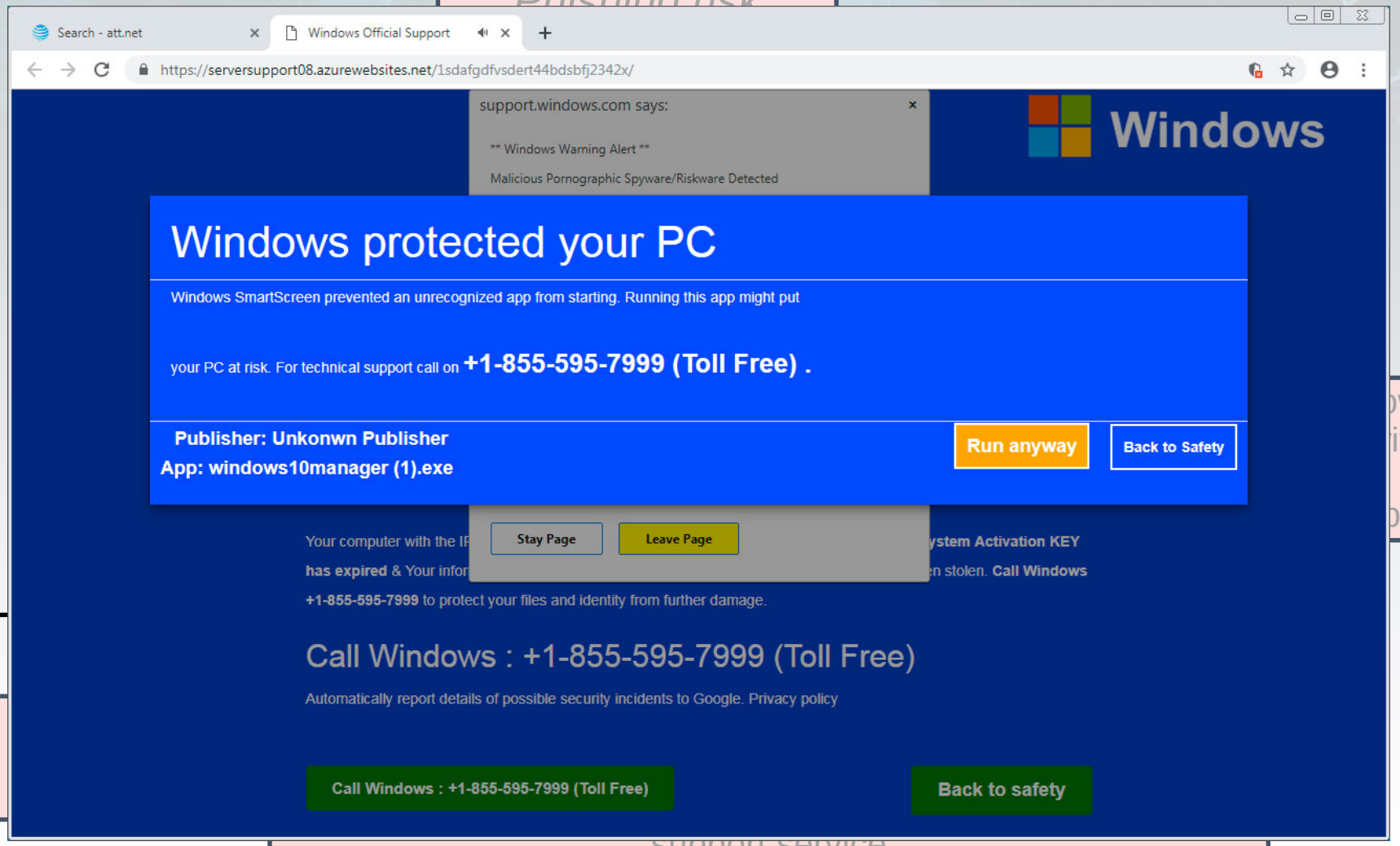
Tech-Supported Attacks

- In technical support scams, a scammer claims to offer a legitimate technical support service and may use different tactics to get victims attention including cold calls, website pop-ups, email messages, and SMS
- Most popular tactics used, include
  - *website pop-ups warning user about a computer virus*
  - *technical services email scams*

Funded by the
Erasmus+ Programme
of the European Union

Risk Analysis

Tech support
Phishing risk



ows
ith
puter

Phisher

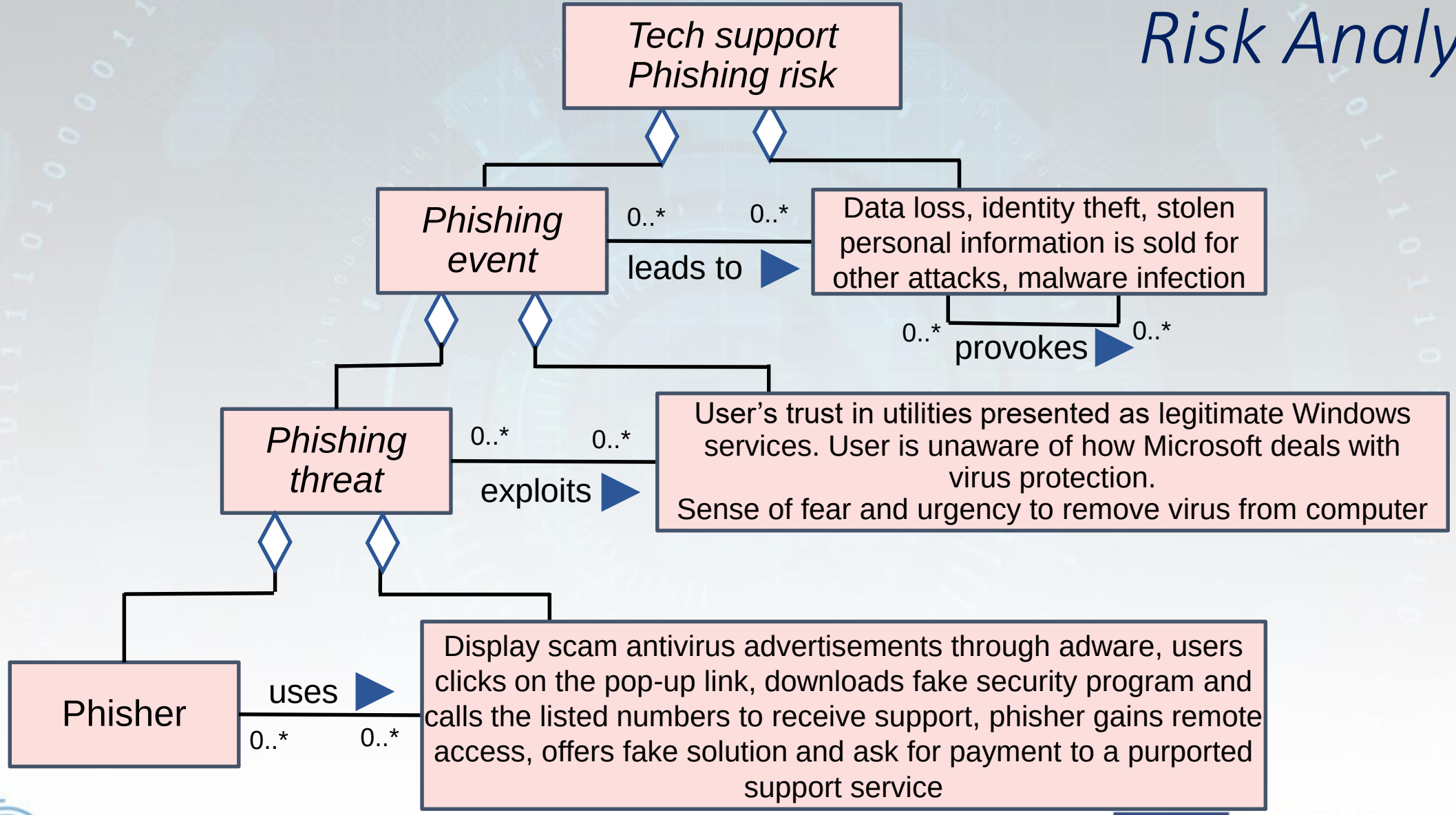
support service

Tech Support Phishing Email (Source: Bleepingcomputer)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Risk Analysis



CyberPhish
Safeguarding your digital future

Tech Support Phishing Email (Source: Bleepingcomputer)

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

2. Understand URLs
2.1 Do not click on any pop-up call to action buttons or links

1. Understand Phishing
Phishing source: Website
Phishing message anatomy:
a. Who is the message is from? *Pop-up*
b. What is the message content?
Antivirus protection
c. Are there call to action prompts? *Yes*

Recognizing phishing attacks

3. Recognising Red Flags
3.1 Legitimate Windows protection will be handled by local Windows Defender and not on a website
3.2 Microsoft does not send unsolicited pop-ups on websites
3.3 You cannot call "*Windows*" on a phone number

4. Critical Thinking
4.1 Be cautious of all unexpected pop-ups on websites, do not click on unexpected pop-ups and block pop-ups where possible
4.2 Be cautious when pop-ups requests actions with a sense of urgency/fear
4.3 Never give an account password or login information for "verification" over the phone or in an email
4.4 Close the website generating the suspicious pop-up

Funded by the Erasmus+ Programme of the European Union

Risk Analysis

Tech support

Amazon.com - Your Cancellation 173-222723-2163799

order-update@amazon.com
Today, 5:27 AM
You

Reply

This message was identified as spam. We'll delete it after 10 days. It's not spam

Your order has been successfully canceled.
For your reference, here's a summary of your order:

You just canceled order 173-222723-2163799 placed on June 26, 2017.

Status: CANCELED

1 of The Optometry.
By: Phaedon Wallace

Sold by: Amazon.com LLC

Sources Network Performance Memory Application Security Audits

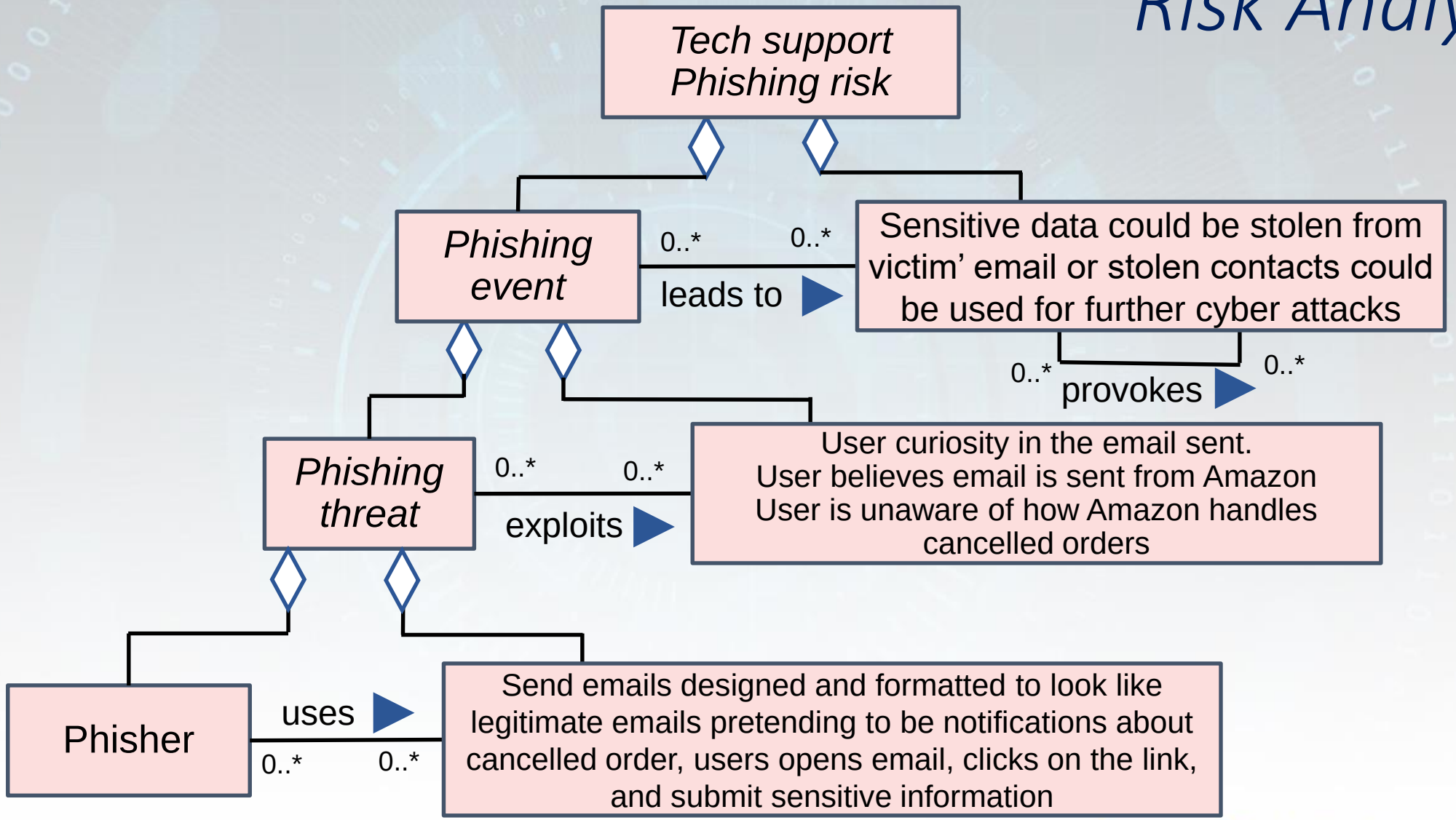
173-222723-2163799

Tech Support Phishing Email (Source: vk-intel)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Risk Analysis



Tech Support Phishing Email (Source: vk-intel)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

2. Understand URLs

2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the content

1. Understand Phishing

Phishing source: Email
Phishing message anatomy:
a. Who is the message is from? "*order-update@amazon.com*"
b. What is the message content? *Cancelled Amazon order*
c. Are there hyperlinks/attachments? *Yes*

3. Recognising Red Flags

3.1 Legitimate emails from Amazon call you by your name
3.2 Legitimate service emails are professional and have a uniform format.
3.3 Note that the URL path links to "**http://www.cuinavo.com/maritime.php**" and not an Amazon resource
3.4 Amazon sends order cancellation email from "*order-update@amazon.com*" a legitimate Amazon email, but the email format is not professional. Message email is likely spoofed

4. Critical Thinking

4.1 Check that email is from a credible and expected source
4.2 Even if it looks legitimate, go to your actual account on the company's legitimate website eg "*amazon.com*", to verify any concerns
4.3 Be cautious as these email scam types can take advantage of your sense of curiosity and greed
4.4 Look up potentially phishy URLs using free phishing detection tools
4.5 Only give an account password or login information for "verification" on secure parts of legitimate websites
4.6 Delete the email you were sent if reasonably certain it is a phishing

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

1. Understand Phishing

Phishing source: Email

Phishing message anatomy:

a. Who is the message is from? "*order-update@amazon.com*"

b. What is the message content? *Cancelled Amazon order*

c. Are there hyperlinks/attachments? *Yes*

2. Understand URLs

2.1 Do not click on any attachments or links

2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious

2.3 Be cautious if the URL path does not matc

3. Recognising Red Flags

3.1 Legitimate emails from Amazon call you by your name

3.2 Legitimate service emails are professional and have a uniform format.

3.3 Note that the URL path links to "**http://www.cuinavo.com/maritime.php**" and not an Amazon resource

3.4 Amazon sends order cancellation email from "*order-update@amazon.com*" a legitimate Amazon email, but the email format is not professional. Message email is likely spoofed

4. Critical Thinking

4.1 Check that email is from a credible and expected source

4.2 Even if it looks legitimate, go to your actual account on the company's legitimate website eg "*amazon.com*", to verify any concerns

4.3 Be cautious as these email scam types can take advantage of your sense of curiosity and greed

4.4 Look up potentially phishy URLs using free phishing detection tools

4.5 Only give an account password or login information for "verification" on secure parts of legitimate websites

4.6 Delete the email you were sent if reasonably certain it is a phishing

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

2. Understand URLs
2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the content

1. Understand Phishing
Phishing source: Email
Phishing message anatomy:
a. Who is the message is from? "*order-update@amazon.com*"
b. What is the message content? *Cancelled Am*
c. A

3. Recognising Red Flags
3.1 Legitimate emails from Amazon call you by your name
3.2 Legitimate service emails are professional and have a uniform format.
3.3 Note that the URL path links to "**http://www.cuinavo.com/maritime.php**" and not an Amazon resource
3.4 Amazon sends order cancellation email from "*order-update@amazon.com*" a legitimate Amazon email, but the email format is

4. Critical Thinking
4.1 Check that email is from a credible and expected source
4.2 Even if it looks legitimate, go to your actual account on the company's legitimate website eg "*amazon.com*", to verify any concerns
4.3 Be cautious as these email scam types can take advantage of your sense of curiosity and greed
4.4 Look up potentially phishy URLs using free phishing detection tools
4.5 Only give an account password or login information for "verification" on secure parts of legitimate websites
4.6 Delete the email you were sent if reasonably certain it is a phishing

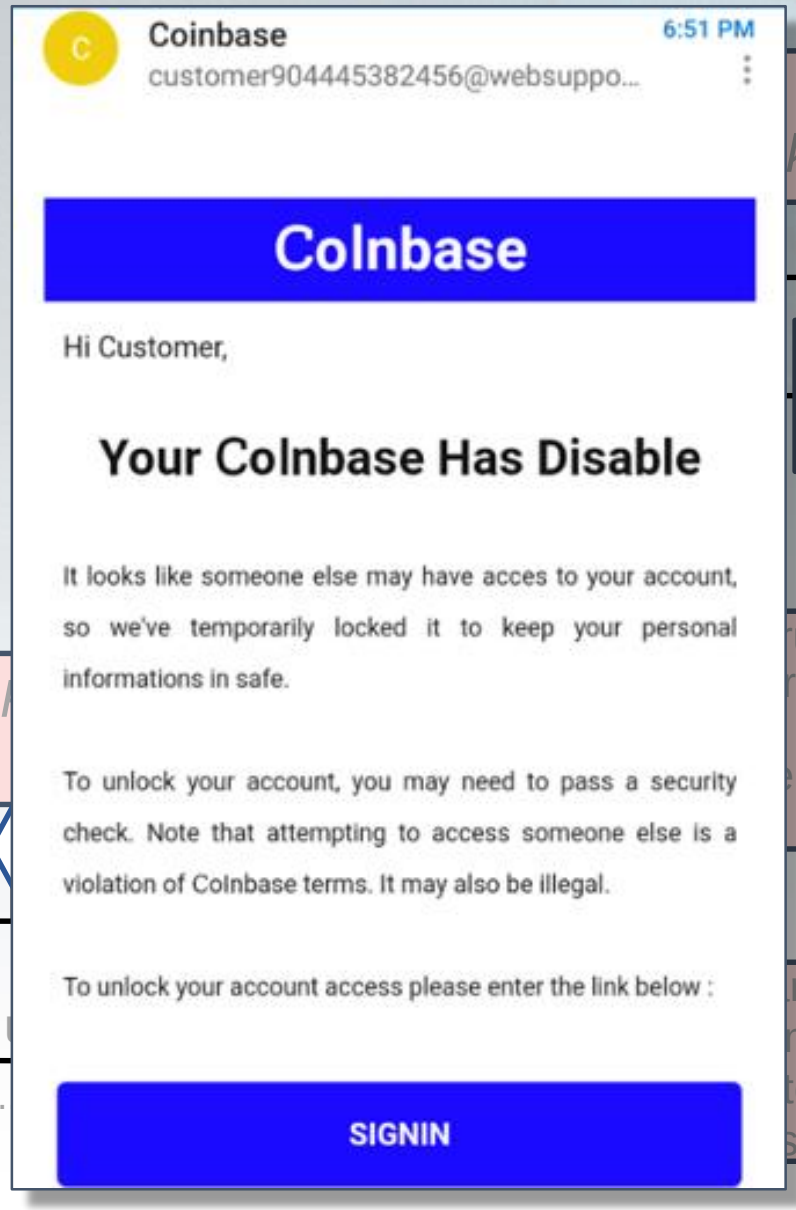
Funded by the Erasmus+ Programme of the European Union

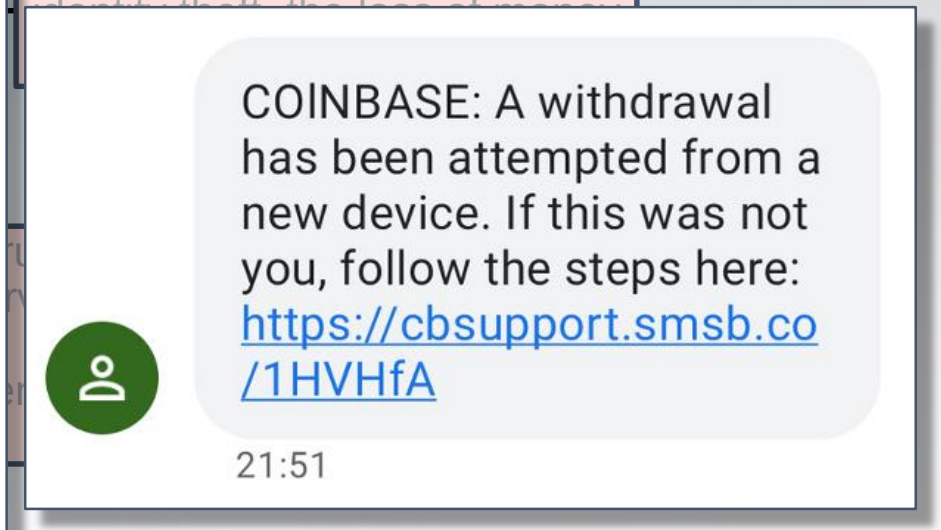
Cryptocurrency Scams

- As Bitcoin and other cryptocurrencies surged in price and popularity, hackers and cybercriminals became more interested in stealing it
- Attackers can use phishing to impersonate representatives from popular cryptocurrency exchanges like Binance, Huobi Global, or Coinbase

Funded by the
Erasmus+ Programme
of the European Union

Risk Analysis





Data loss, reputational damage,

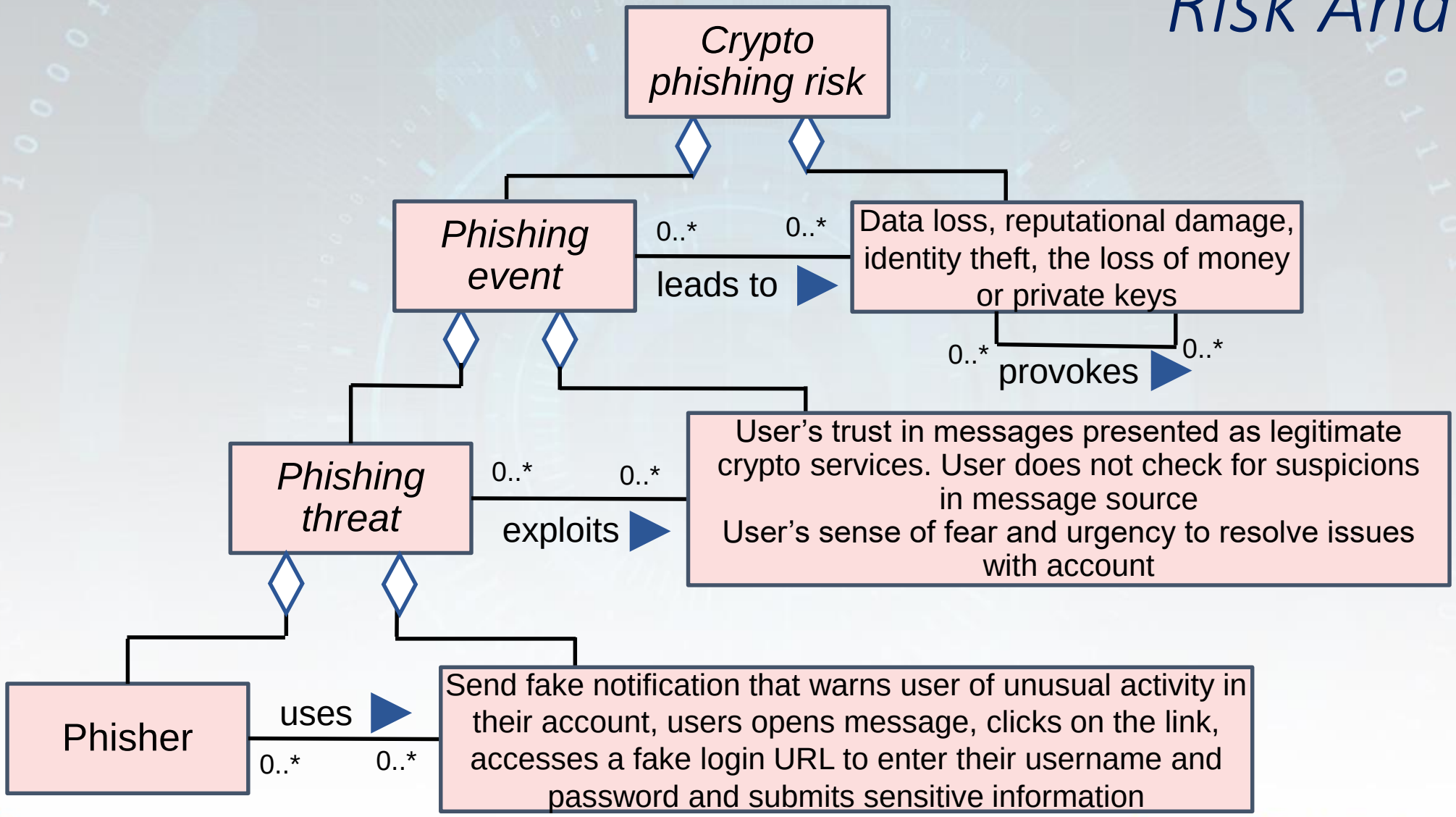
rns user of unusual activity in message, clicks on the link, to enter their username and s sensitive information

Phisher

Cryptocurrency phishing email. Source: Reddit
Cryptocurrency phishing text message. Source: Reddit

Funded by the Erasmus+ Programme of the European Union

Risk Analysis



Cryptocurrency phishing email. Source: Reddit
Cryptocurrency phishing text message. Source: Reddit

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

2. Understand URLs

2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the content

1. Understand Phishing

Phishing source: Email, SMS
Phishing message anatomy:
a. Who is the message is from? "*...@websupport.com*", *SMS Phone number*
b. What is the message content? *Account disable notification, Withdrawal notice*
c. Are there hyperlinks/attachments? Yes

3. Recognising Red Flags

3.1 Messages from legitimate apps call you by your name
3.2 Legitimate messages are professional and well formatted
3.3 Legitimate messages do not contain typos i.e using "*CoInbase*" instead of "*Coinbase*", "*Your CoInbase Has Disable*", or "*SIGNIN*"
3.4 Legitimate email domain for Coinbase is "*...@coinbase.com*" not "*...@websupport.com*"

4. Critical Thinking

4.1 Double-check the sender's address, legitimate emails from Coinbase should have email addresses ending in *.coinbase.com*
4.2 Reach out directly to Coinbase customer support for problems with your account or a payment
4.3 Be cautious as these scam types take advantage of your fear and urgency
4.4 Cross check security information on the legitimate service website
4.5 Never click links/attachments from unknown sources, check suspicious URLs using free phishing detection tools
4.6 Only give an account password or login information for "verification" on secure parts of legitimate websites
4.7 Delete the email you were sent if reasonably certain it is a phishing

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

2. Understand URLs

2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the content

1. Understand Phishing

Phishing source: Email, SMS
Phishing message anatomy:
a. Who is the message is from?
"*...@websupport.com*", *SMS Phone number*
b. What is the message content? *Account disable notification, Withdrawal notice*
c. Are there hyperlinks/attachments? Yes

3. Recognising Red Flags

3.1 Messages from legitimate apps call you by your name
3.2 Legitimate messages are professional and well formatted
3.3 Legitimate messages do not contain typos i.e using "*CoInbase*" instead of "*Coinbase*", "*Your CoInbase Has Disable*", or "*SIGNIN*"
3.4 Legitimate email domain for Coinbase is "*...@coinbase.com*" not "*...@websupport.com*"

4. Critical Thinking

4.1 Double-check the sender's address, legitimate emails from Coinbase should have email addresses ending in *.coinbase.com*
4.2 Reach out directly to Coinbase customer support for problems with your account or a payment
4.3 Be cautious as these scam types take advantage of your fear and urgency
4.4 Cross check security information on the legitimate service website
4.5 Never click links/attachments from unknown sources, check suspicious URLs using free phishing detection tools
4.6 Only give an account password or login information for "verification" on secure parts of legitimate websites
4.7 Delete the email you were sent if reasonably certain it is a phishing

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

2. Understand URLs
2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the content

1. Understand Ph
Phishing source: Email, SMS
Phishing message anatomy:
a. Who is the message is from? "*...@websupport.com*", *SMS Phone number*
b. What is the message content? *Account disable notific*
c. Are

3. Recognising Red Flags
3.1 Messages from legitimate apps call you by your name
3.2 Legitimate messages are professional and well formatted
3.3 Legitimate messages do not contain typos i.e using "*CoInbase*" instead of "*Coinbase*", "*Your CoInbase Has Disable*", or "*SIGNIN*"

4. Critical Thinking
4.1 Double-check the sender's address, legitimate emails from Coinbase should have email addresses ending in *.coinbase.com*
4.2 Reach out directly to Coinbase customer support for problems with your account or a payment
4.3 Be cautious as these scam types take advantage of your fear and urgency
4.4 Cross check security information on the legitimate service website
4.5 Never click links/attachments from unknown sources, check suspicious URLs using free phishing detection tools
4.6 Only give an account password or login information for "verification" on secure parts of legitimate websites
4.7 Delete the email you were sent if reasonably certain it is a phishing

Funded by the Erasmus+ Programme of the European Union

Extortion Scams

- Extortion scams are unfortunately making a comeback where fraudsters and hackers can access data from breaches and make an "*I Know Your Password*" threat to victims
- Attackers can also claim to have accessed your computer and its camera, obtained sexually explicit video or images of you and may even get you to pay by Bitcoin

Funded by the Erasmus+ Programme of the European Union

Risk Analysis

Extortion

From: Beitris Englert <hbeleonoretvi@outlook.com>
Date: July 12, 2018

Subject:

It seems that, xxxxxxxxx, is your password. You may not know me and you are probably wondering why you are getting this e mail, right?

actually, I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. after that, my software program obtained all of your contacts from your Messenger, FB, as well as email.

What did I do?

I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

exactly what should you do?

Well, in my opinion, $2900 is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address: 1KiCTVUq5A9BPwoFC8S965tsbtqcWr8bty
(It is cAsE sensitive, so copy and paste it)

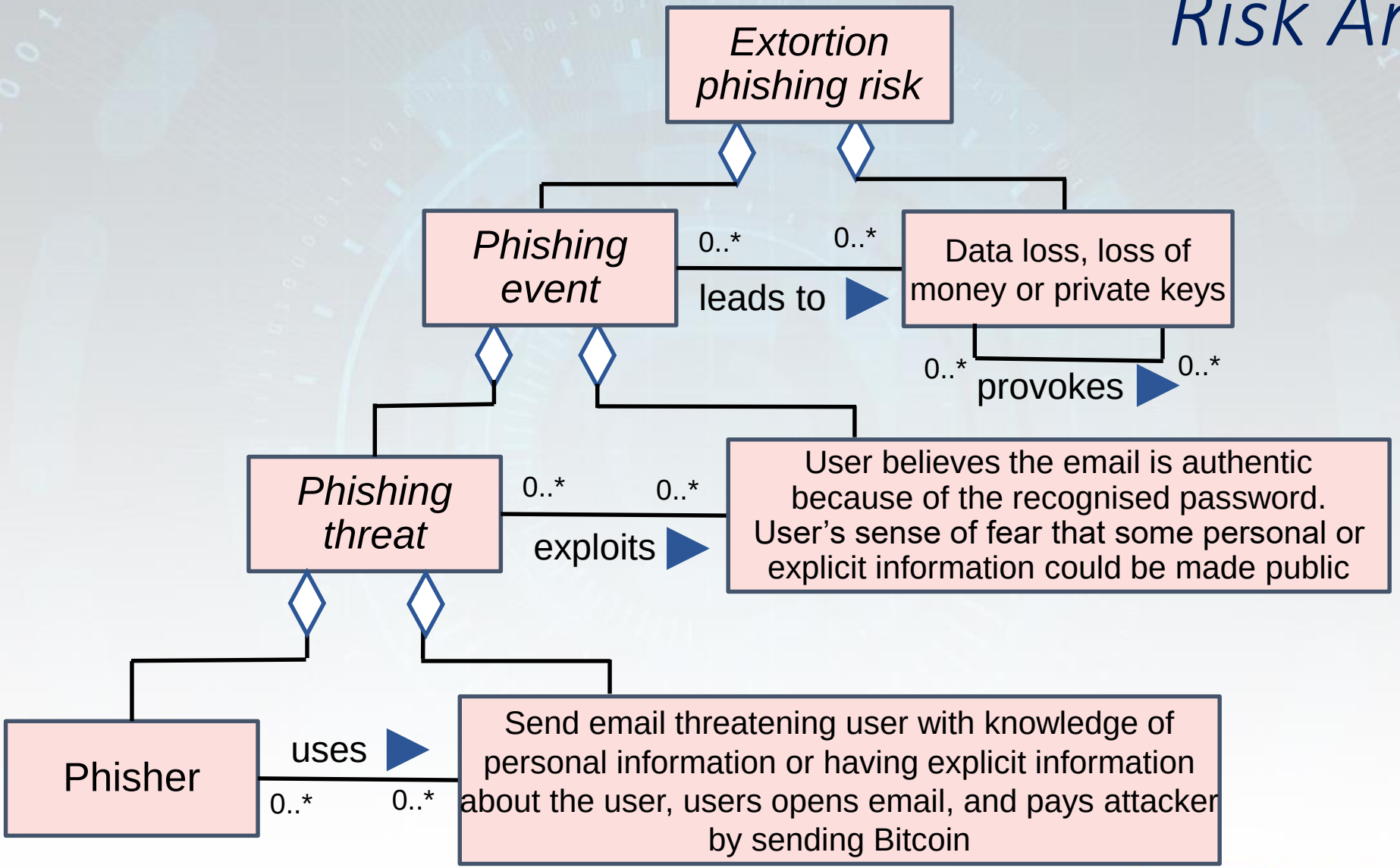
ntic
word.
sonal or
public

Phisher

Extortion Phishing Email (Source: MailOnline)

Funded by the Erasmus+ Programme of the European Union

Risk Analysis



Extortion Phishing Email (Source: MailOnline)

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

2. Understand URLs
2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the content

1. Understand Phishing
Phishing source: Email
Phishing message anatomy:
a. Who is the message is from?
"*...@outlook.com*"
b. What is the message content? *Sex extortion*
c. Are there hyperlinks/attachments? *Yes*

3. Recognising Red Flags
3.1 In most cases, the emails are empty threats and not because the user was hacked
3.2 The attacker may have obtained sensitive information from a data breach, leak or publicly available on the internet

4. Critical Thinking
4.1 Be cautious as these email scam types can take advantage of your fear and shame
4.2 Check if your email has been compromised at websites i.e *haveibeenpwned.com* or *dehashed.com*
4.3 If the password is still in use, it is important to secure these accounts
4.4 Delete the email you were sent if reasonably certain it is a phishing

Funded by the Erasmus+ Programme of the European Union

Advance Fee Scams

- Advance fee scams are still potent during the COVID pandemic, as people have fallen on hard times. These phishing attacks occur when a criminal abroad is offering a share in a large sum of money for helping them transfer the money out of their country
- To do this, they'll request your banking information or ask you to pay the fees, charges or taxes

Funded by the Erasmus+ Programme of the European Union

Risk Analysis

[SPAM]ATN International Credit Settlement
Central Bank of Nigeria [printer@brandmelloon.co.uk]
Sent: Sat 10/13/2012 5:20 AM
To: dave@d

Central Bank of Nigeria.
ATM International Credit Settlement,
Directorate of International Payment.

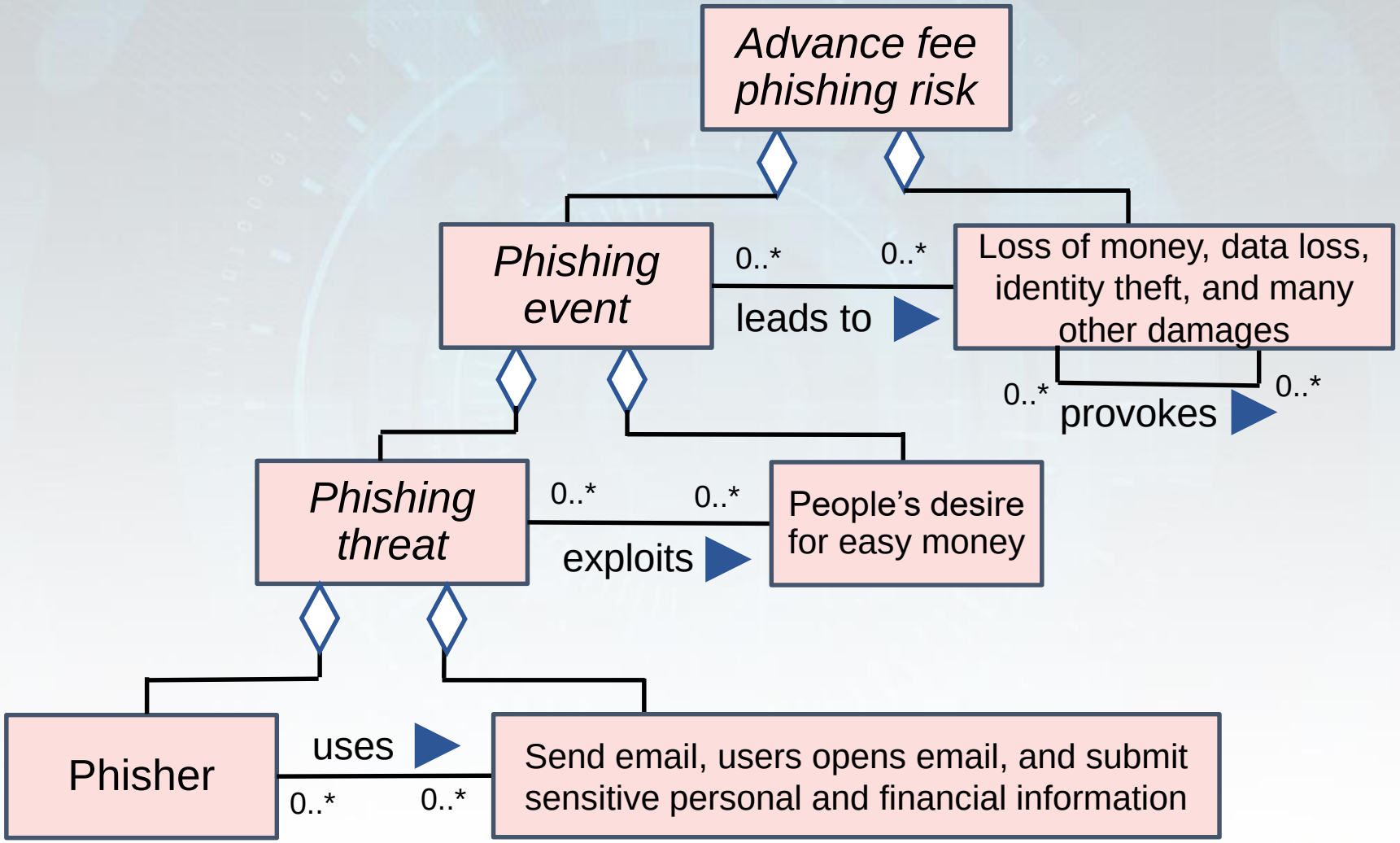
This is to officially notiify yoou about your Fund that was supposed to be rendered to you via numeroous ways i.e. Coourier Companies, Western Union Money Transfer and Banks. Due to this lost of Funds oof yours which was suppose to be given to you but failed to. So in this case, a beneficial meeting was held on the 25th of August 2012 at the World Bank iin Switzerland, which top officials and Central Bank Governors froom different countries in the world were present at the meeting. Which they discussed on how your Fund can be giiven to you withoout any loss at this time, which yoou have to stop any further communication with any other person(s) or office(s) to avoid any hitches in receiving your ATM payment.

In conclusion at the meeting., The President of World Bank Mr. Jim Yong Kim has strictly authorized 6 Banks in the World to deliver all Funds through courier companies. Your Fund which is truly $3.5 Million USD (Three Million, Five Hundred Thousand United States of America Dollars) to all beneficiaries in various countries in the world as an ATM MASTER CARD. Below are the authorized Banks;

Daiwa Bank R/Osaka/Japan.
Caja De Madrid/Madrid/Spain.
Lloyds Bank R /London/England.
Central Bank of Nigeria/Lagos/Nigeria.
Banco di Santo Spirito/Rome/Italy.
Bank of New York Mellon Corp/New York/USA.

Extortion Phishing Email (Source: Massmoola)

Risk Analysis



Extortion Phishing Email (Source: Massmoola)

Risk Recognition

2. Understand URLs
2.1 Do not follow on any instructions in the email message

1. Understand Phishing
Phishing source: Email
Phishing message anatomy:
a. Who is the message is from? *Central Bank of Nigeria*
b. What is the message content? *Credit settlement*
c. Are there hyperlinks/attachments? *No*

Recognizing phishing attacks

3. Recognising Red Flags
3.1 If someone is offering you free money, it's usually too good to be true
3.2 Legitimate service emails from banks are professional, have a uniform template format, and do not send unsolicited emails

4. Critical Thinking
4.1 Never give banking information to someone you've never met
4.2 Be cautious as these email scam types can take advantage of your sense of curiosity and greed
4.3 Delete the email you were sent if reasonably certain it is a phishing

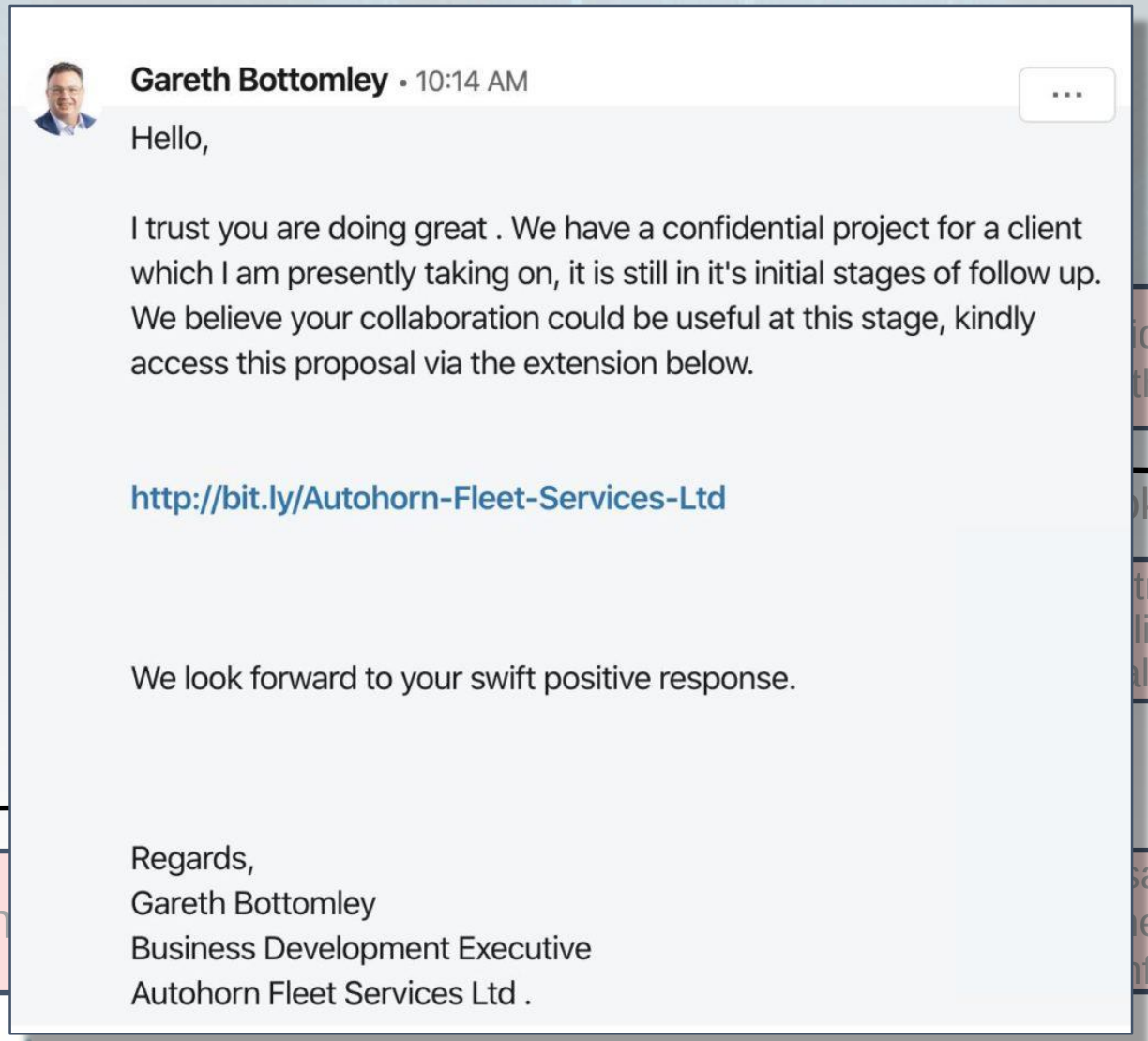
Funded by the Erasmus+ Programme of the European Union

Social Media Scams

- Here, attackers use social media sites such as Facebook, LinkedIn or Twitter, to trick users into clicking on malicious links or revealing personal information
- Attackers can also find a wealth of information about potential victims on social media to launch a targeted attack

Funded by the
Erasmus+ Programme
of the European Union

Risk Analysis



Gareth Bottomley • 10:14 AM

Hello,

I trust you are doing great . We have a confidential project for a client which I am presently taking on, it is still in it's initial stages of follow up. We believe your collaboration could be useful at this stage, kindly access this proposal via the extension below.

http://bit.ly/Autohorn-Fleet-Services-Ltd

We look forward to your swift positive response.

Regards,
Gareth Bottomley
Business Development Executive
Autohorn Fleet Services Ltd .

dentity theft,
ther damages

0..*

okes

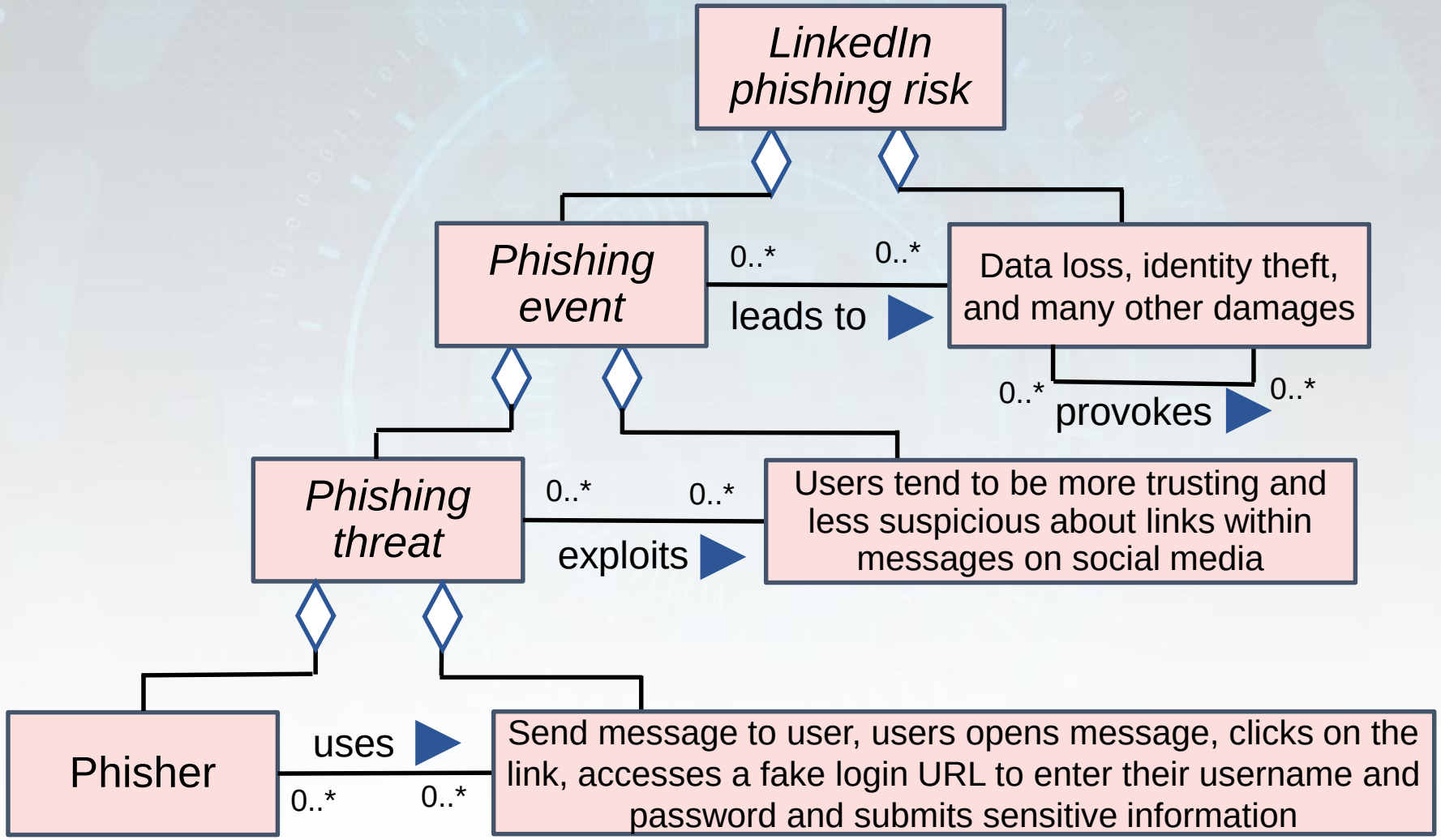
trusting and
links within
l media

Phish

sage, clicks on the
eir username and
nformation

Extortion Phishing Email (Source: LinkedInTraining)

Risk Analysis



Extortion Phishing Email (Source: LinkedInTraining)

Risk Recognition

2. Understand URLs
2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious

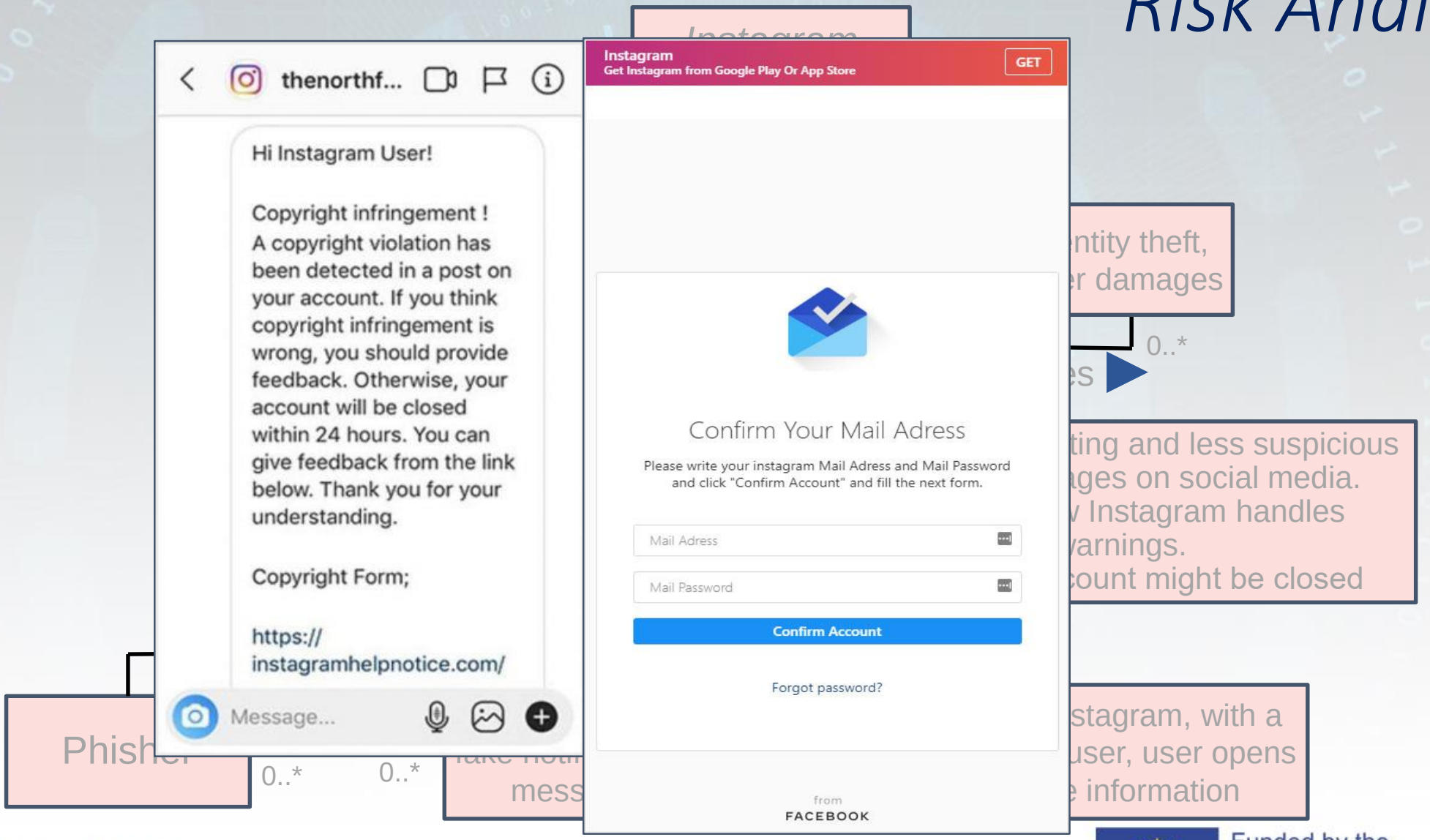
1. Understand Phishing
Phishing source: Direct message
Phishing message anatomy:
a. Who is the message is from? *LinkedIn User*
b. What is the message content? *Collaboration proposal*
c. Are there hyperlinks/attachments? *Yes*

3. Recognising Red Flags
3.1 If someone unknown is offering collaboration, it's likely suspicious
3.2 Attackers use URL shortening services like "*bit.ly*" to shorten and hide phishing links

4. Critical Thinking
4.1 Only give an account password or login information for "verification" on secure parts of legitimate websites
4.2 Even if it seems like the message is from someone you trust, there's a chance that their account has been compromised
4.3 Always use enhanced privacy settings on social media
4.4 Do not click on suspicious links in DMs, check suspicious URLs using free phishing detection tools
4.5 Never accept LinkedIn connection requests from someone you're not familiar with
4.6 Be careful about sharing too much personal information on social media
4.7 Unfollow/Block suspicious accounts and delete the message you were sent if reasonably certain it is a phishing

Funded by the Erasmus+ Programme of the European Union

Risk Analysis

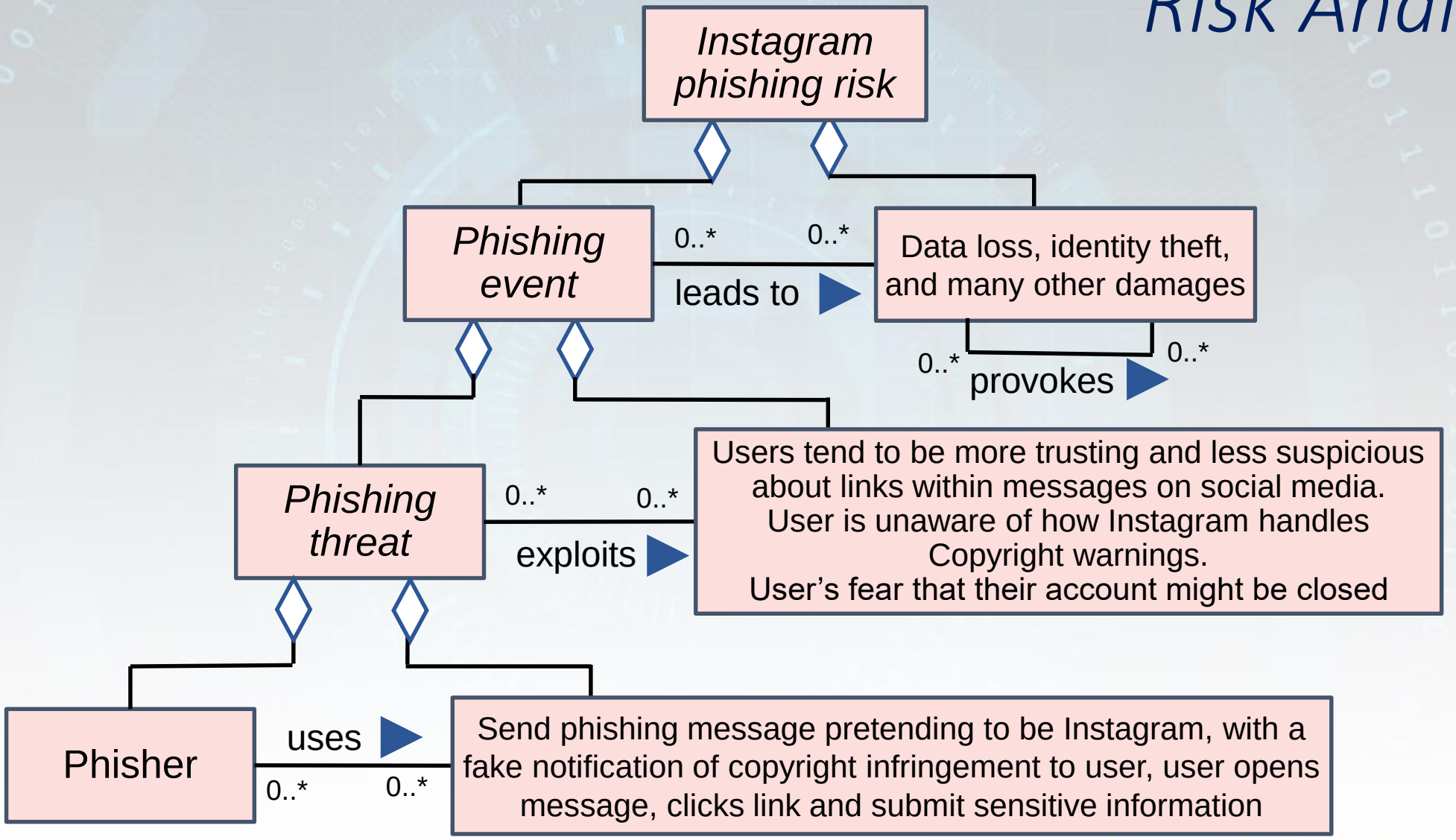


Social Media Phishing Email (Source: Hackread)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Risk Analysis



Social Media Phishing Email
(Source: Hackread)

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

2. Understand URLs

2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the platform domain

1. Understand Phishing

Phishing source: Direct message
Phishing message anatomy:
a. Who is the message is from? *Instagram User*
b. What is the message content? *Copyright infringement claim*
c. Are there hyperlinks/attachments? *Yes*

3. Recognising Red Flags

3.1 Legitimate copyright claim notifications will be send personally by Instagram
3.2 Instagram will always use the name registered to your account to address you
3.3 The link provided should match the platform domain i.e "*instagram.com*" not "*instagram**helpnotice**.com*"

4. Critical Thinking

4.1 Only give an account password or login information for "verification" on secure parts of legitimate websites
4.2 Even if it seems like the message is from someone you trust, there's a chance that their account has been compromised
4.3 Always use enhanced privacy settings on social media
4.4 Do not click on suspicious links in DMs, check suspicious URLs using free phishing detection tools
4.5 Be careful when messaging users that you're not familiar with, and that you do not follow
4.6 Unfollow/Block suspicious accounts and delete the message you were sent if reasonably certain it is a phishing

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

2. Understand URLs
2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the platform domain

1. Understand Phishing
Phishing source: Direct message
Phishing message anatomy:
a. Who is the message is from? *Instagram User*
b. What is the message content? *Copyright infringement claim*
c. Are there hyperlinks/attachments? *Yes*

3. Recognising Red Flags
3.1 Legitimate copyright claim notifications will be send personally by Instagram
3.2 Instagram will always use the name registered to your account to address you
3.3 The link provided should match the platform domain i.e "*instagram.com*" not "*instagram**helpnotice**.com*"

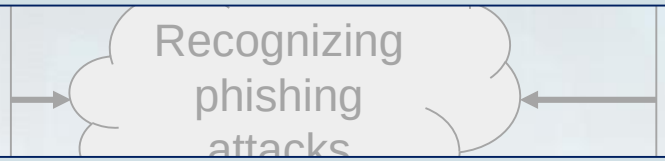
4. Critical Thinking
4.1 Only give an account password or login information for "verification" on secure parts of legitimate websites
4.2 Even if it seems like the message is from someone you trust, there's a chance that their account has been compromised
4.3 Always use enhanced privacy settings on social media
4.4 Do not click on suspicious links in DMs, check suspicious URLs using free phishing detection tools
4.5 Be careful when messaging users that you're not familiar with, and that you do not follow
4.6 Unfollow/Block suspicious accounts and delete the message you were sent if reasonably certain it is a phishing

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

2. Understand URLs
2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the platform domain

1. Understand Phi
Phishing source: Direct message
Phishing message anatomy:
a. Who is the message is from? *Instagram User*
b. What is the message content? *Copyright infringe*
c. Are th



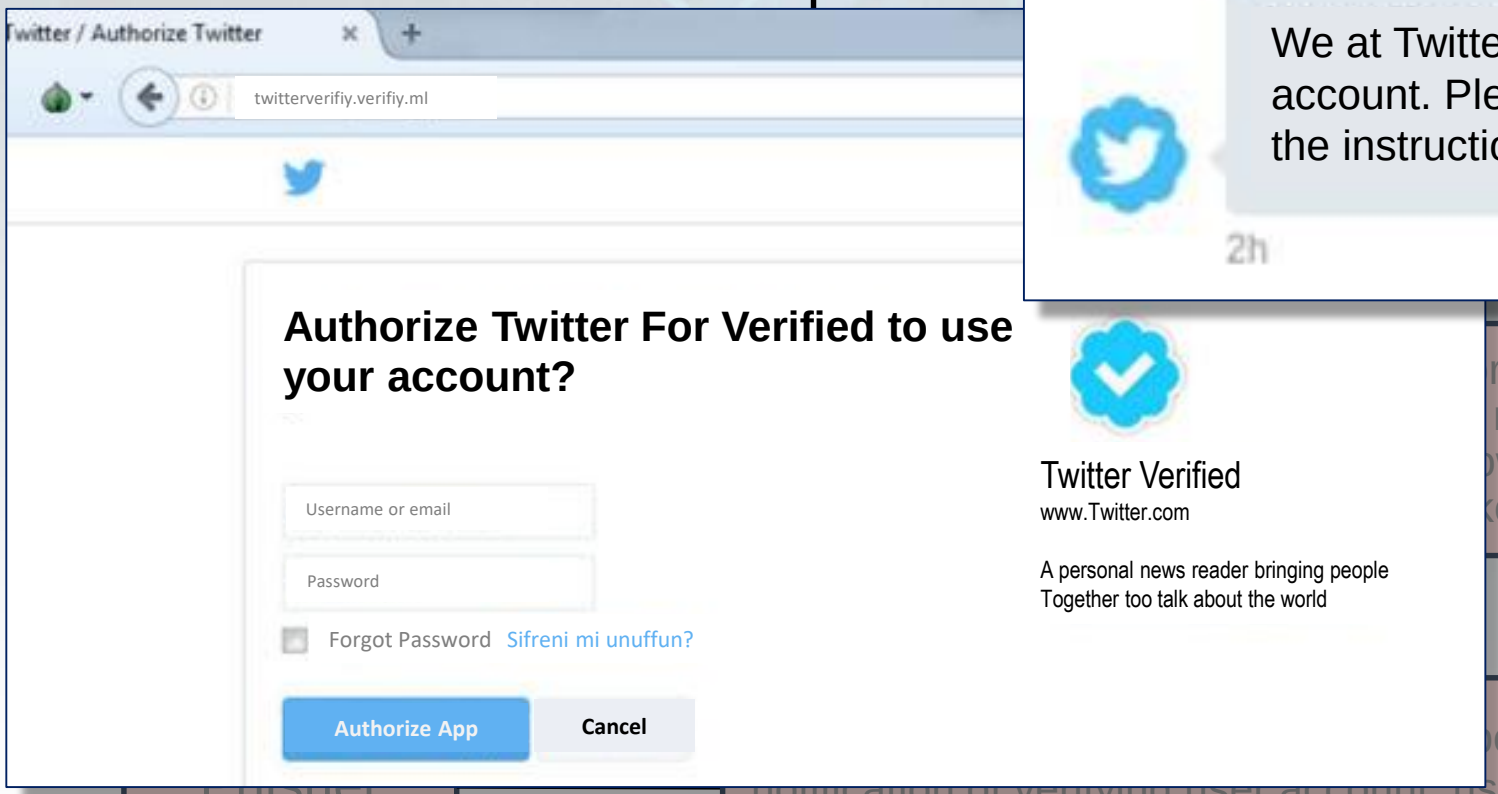
3.1 Legitimate copyright claim notifications will be send personally by Instagram
3.2 Instagram will always use the name registered to your account to address you

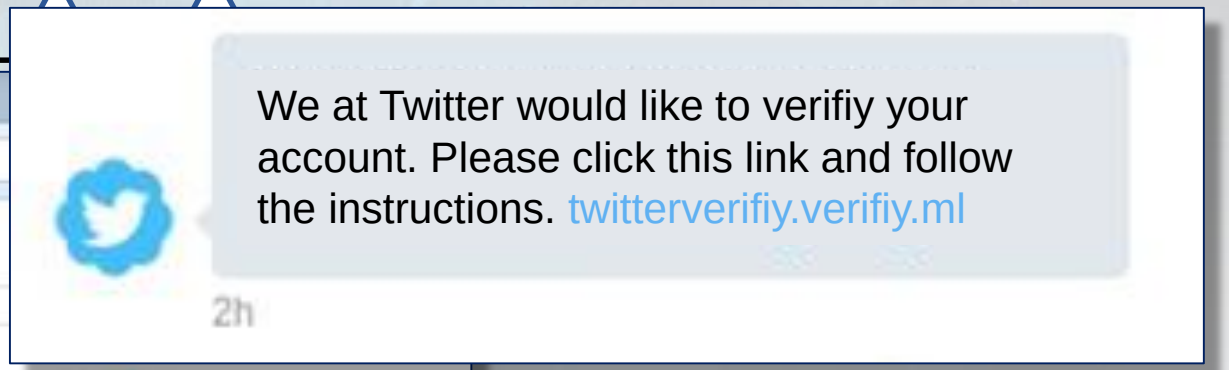
4. Critical Thinking
4.1 Only give an account password or login information for “verification” on secure parts of legitimate websites
4.2 Even if it seems like the message is from someone you trust, there’s a chance that their account has been compromised
4.3 Always use enhanced privacy settings on social media
4.4 Do not click on suspicious links in DMs, check suspicious URLs using free phishing detection tools
4.5 Be careful when messaging users that you’re not familiar with, and that you do not follow
4.6 Unfollow/Block suspicious accounts and delete the message you were sent if reasonably certain it is a phishing

Funded by the Erasmus+ Programme of the European Union

Risk Analysis

Twitter phishing risk





re trusting and less suspicious about
messages on social media.
w twitter handles account verification.
e verification status on Twitter

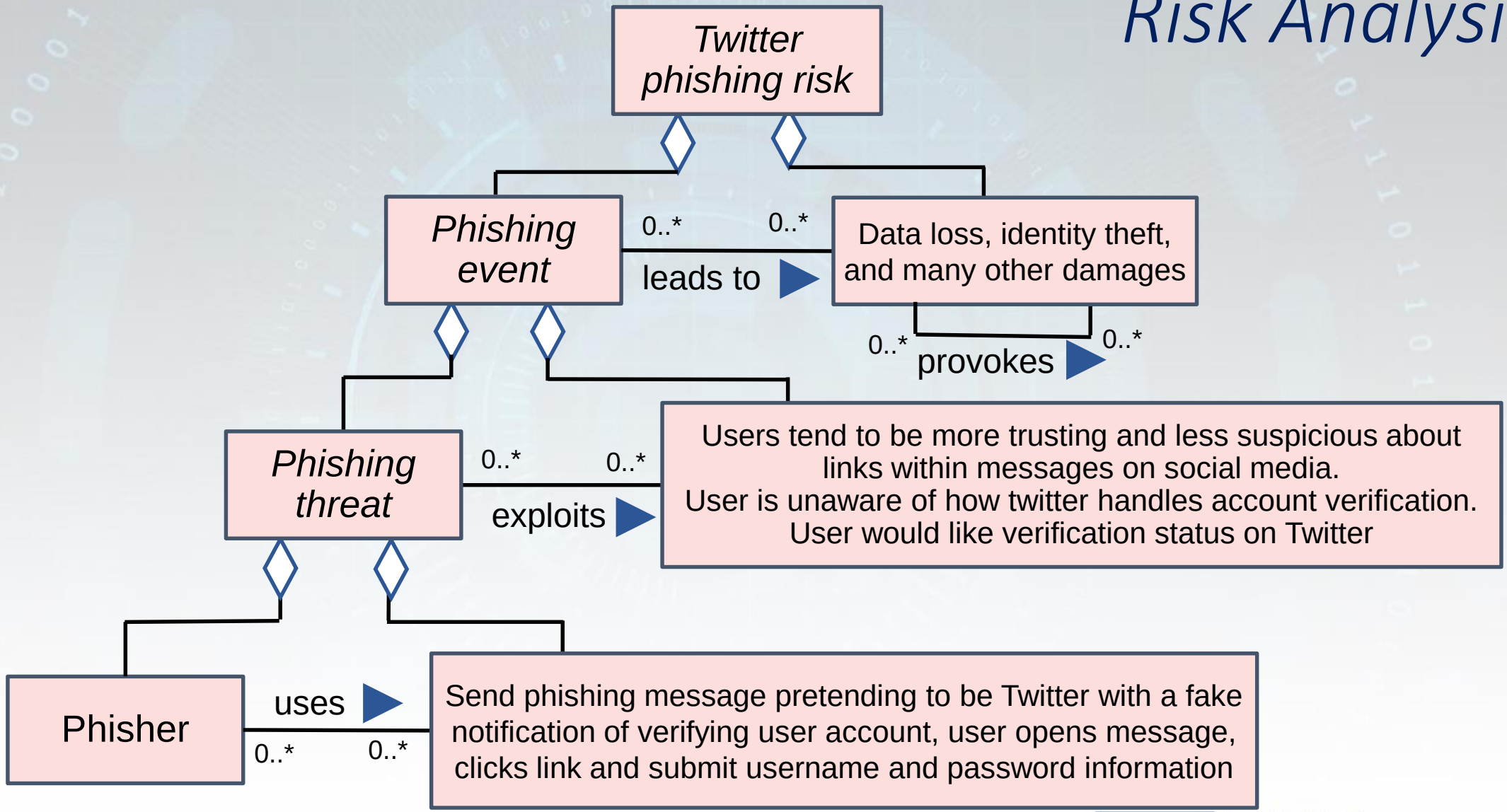
e Twitter with a fake
er opens message,
clicks link and submit username and password information

0..*

0..*

Social Media Phishing Email (Source: Malwarebytes)

Risk Analysis



Social Media Phishing Email (Source: Malwarebytes)

Funded by the Erasmus+ Programme of the European Union

Risk Recognition

2. Understand URLs
2.1 Do not click on any attachments or links
2.2 Hover over the attachment to reveal the URL and analyse to determine if malicious
2.3 Be cautious if the URL path does not match the platform domain

1. Understand Phishing
Phishing source: Direct message
Phishing message anatomy:
a. Who is the message is from? *Twitter User*
b. What is the message content? *Account verification claim*
c. Are there hyperlinks/attachments? *Yes*

3. Recognising Red Flags
3.1 Legitimate twitter verification process is handled by a request process to Twitter (not the other way around)
3.2 Twitter will always use the name registered to your account to address you
3.3 The link provided should match the platform domain i.e "*twitter.com*" not "***twitterverifiy.verifiy.ml***"

4. Critical Thinking
4.1 *Only give an account password or login information for "verification" on secure parts of legitimate websites eg "twitter.com*
4.2 *Even if it seems like the message is from someone you trust, there's a chance that their account has been compromised*
4.3 *Always use enhanced privacy settings on social media*
4.4 *Do not click on suspicious links in DMs, check suspicious URLs using free phishing detection tools*
4.5 *Be careful when messaging users that you're not familiar with, and that you do not follow*
4.6 *Unfollow/Block suspicious accounts and delete the message you were sent if reasonably certain it is a phishing*

Funded by the Erasmus+ Programme of the European Union

Summary

- Phishing case studies
- Risk analysis of highlighted phishing attacks and scams
- Recognising these phishing attacks to prevent the resulting phishing risks

Funded by the Erasmus+ Programme of the European Union

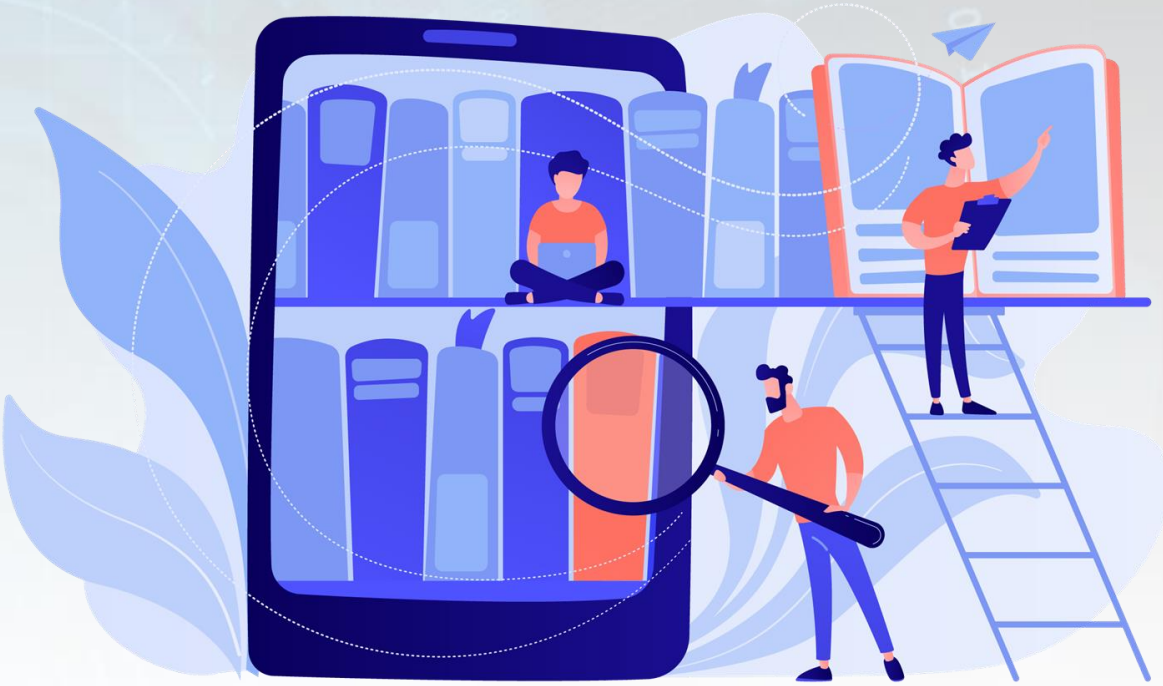
Assignment

- Discuss 3 phishing attacks, not mentioned, that you think are prevalent today
- Build a risk analysis for these phishing scams highlighting the attack methods, vulnerabilities, and phishing events that form the phishing risk
- Discuss how you can recognise these scams and prevent the resulting phishing risks

Funded by the Erasmus+ Programme of the European Union

Further Reading

- **Dubois E., Heymans P., Mayer N., Matulevičius R.** (2010) A Systematic Approach to Define the Domain of Information System Security Risk Management. *Intentional Perspectives on Information Systems Engineering 2010: 289-306*
- **Abroshan H.** (2021)**:** Root Causes of Falling Victim to Phishing – The Effects of Human Behavior, Emotions, and Demographics., *PhD thesis*, Ghent University.
- **Althobaiti, K., Meng, N., & Vaniea, K.** (2021). 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). Anatomy of a Phishing Email. In CEAS.
- **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). Anatomy of a Phishing Email. In CEAS.



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Short Videos

- Phishing email scam anatomy
  - ***https://youtu.be/3gpOM9c6mmA***
- Some phishing attack examples
  - ***https://youtu.be/lpGfxIAQhSo***
  - ***https://youtu.be/pGEAZdp0MAI***
- 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!

Short Videos

- Phishing email scam anatomy
  - ***https://youtu.be/3gpOM9c6mmA***
- Some phishing attack examples
  - ***https://youtu.be/lpGfxIAQhSo***
  - ***https://youtu.be/pGEAZdp0MAI***
- 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