



AWARENESS OF PHISHING SCENARIO

Name Of The Presenter: Vasileios Fotis

Month Year: Nov 2020

PHISHING DEFINITION

Definition

- Acquisition of confidential data
- Persuade to provide sensitive data
- Access account information and results in:
 - identity theft
 - financial loss
- Uses Social Engineering

It is a Cybercrime

Social engineering

➤ What is it?

Exploiting the generally trusting nature of people

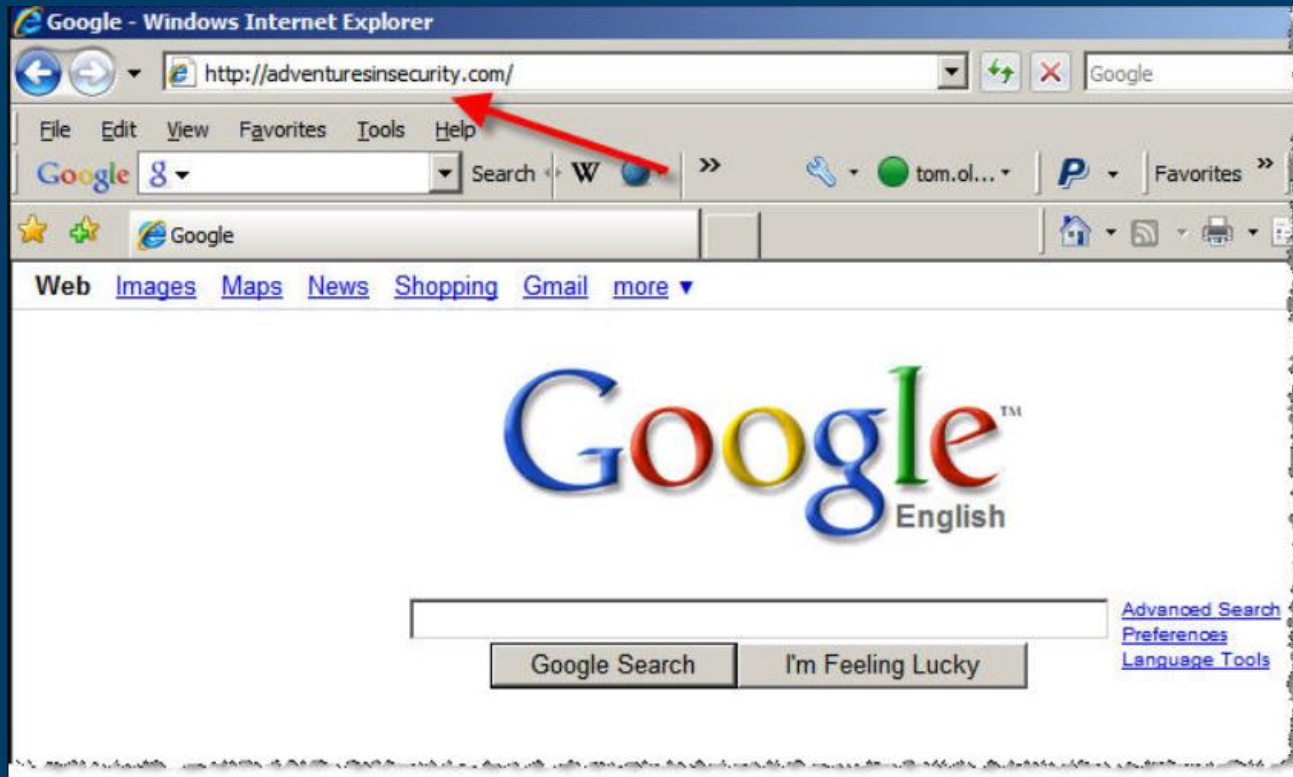
Offline

- Vishing
- Pharming
- Communication Spoofing
- Tailgating
- Dumpster diving
- Shoulder surfing

Online

- Bulk phishing (aka phishing)
- Spear phishing
- Whale phishing (whaling)

Social engineering



Social engineering



Social engineering



Social engineering



Social engineering



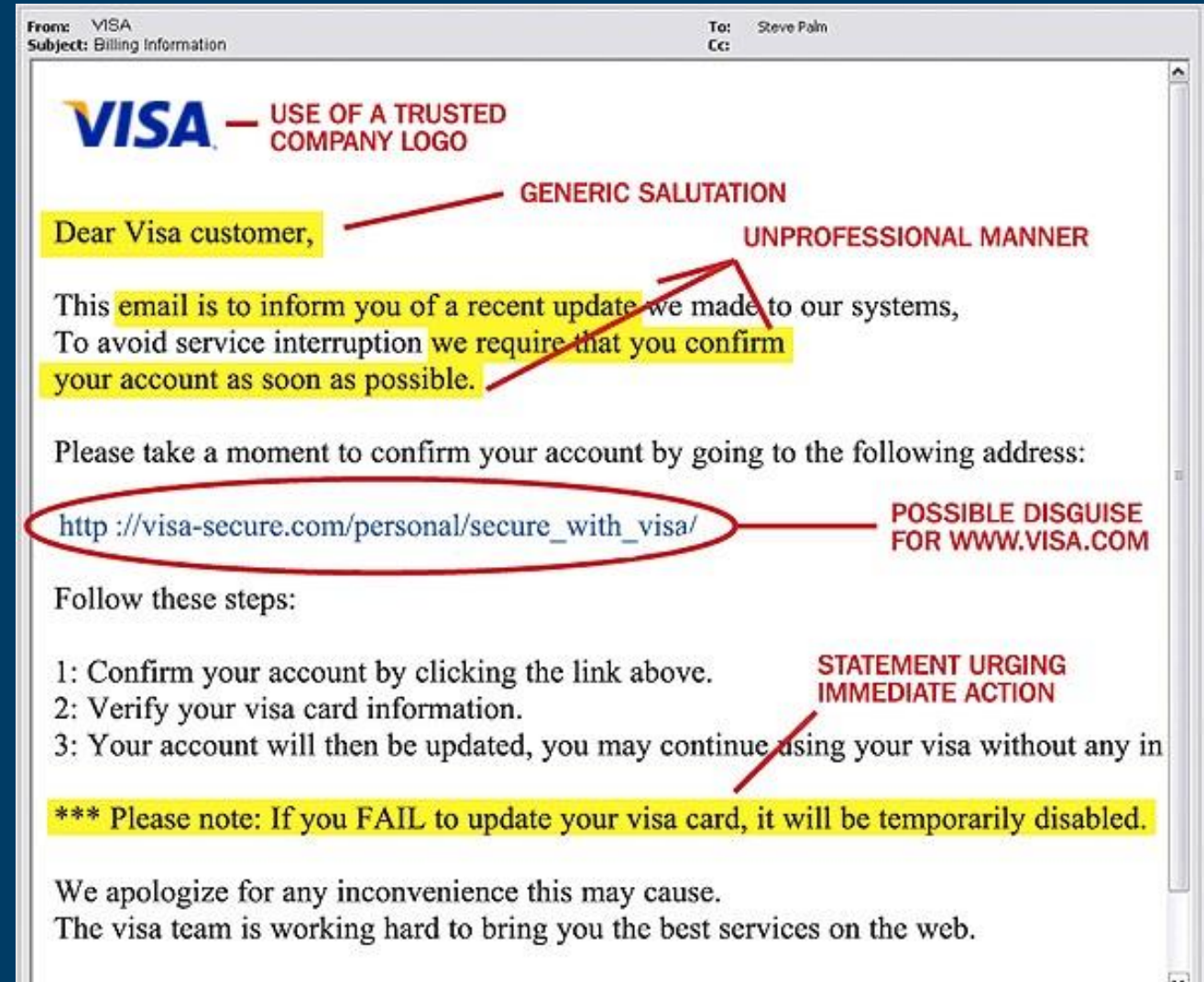
Social engineering



Categories of phishing

Bulk phishing (aka Phishing)

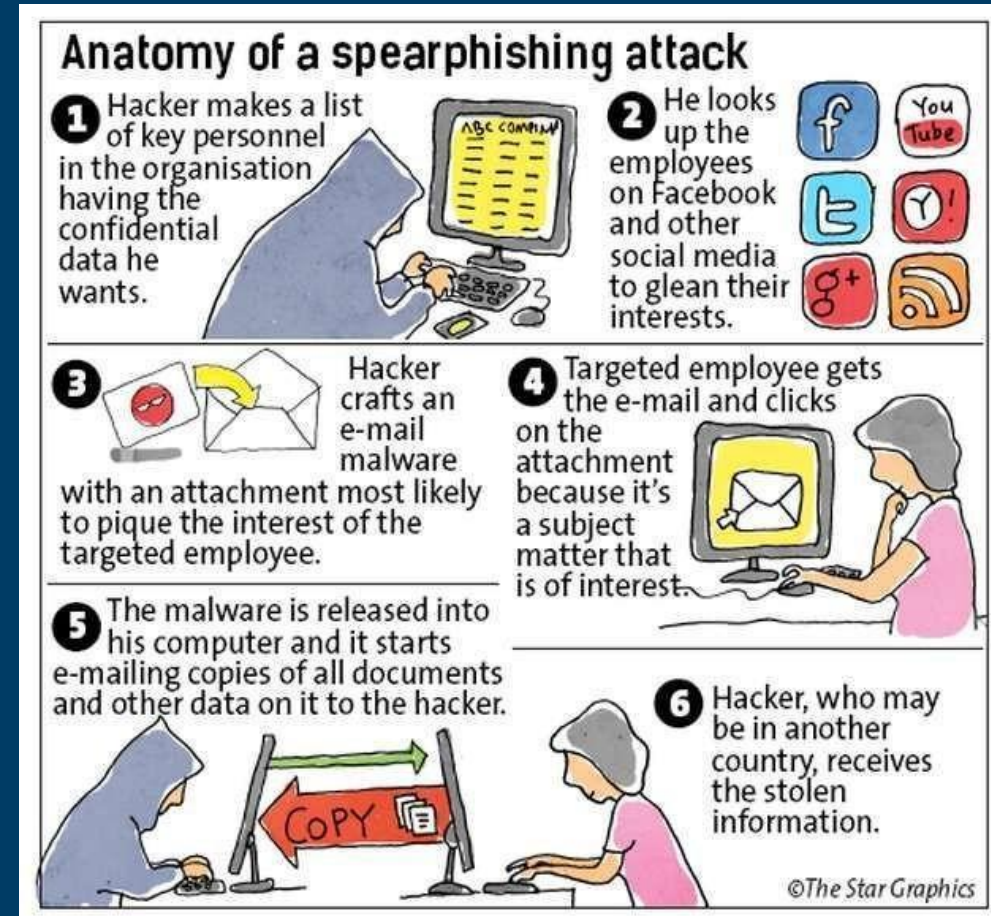
- Sending emails purporting to be from reputable sources
- General attack: it is like spam email, sent to a large pool of people



Categories of phishing

Spear Phishing

- sending emails ostensibly from a known or trusted sender to targeted individuals
- Specific Attack: sent from a person who we know in order to make the email more trustful



Categories of phishing

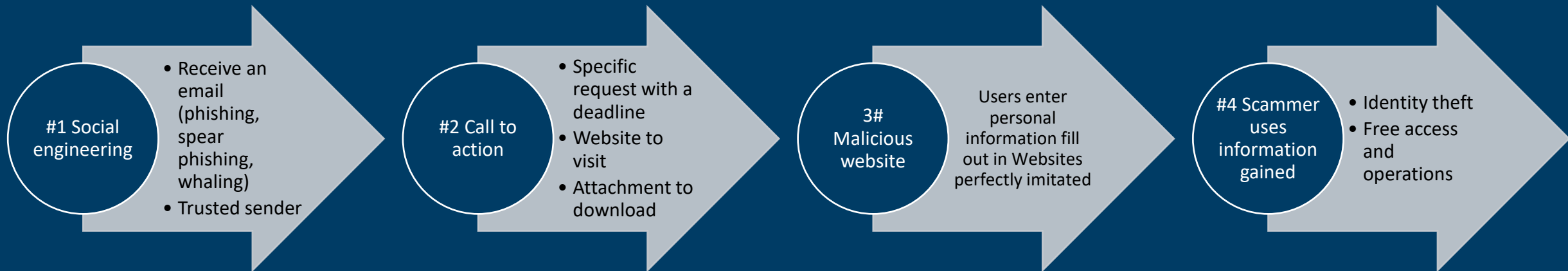
Whale phishing (Whaling)

- Sending email to wealthy, powerful, or prominent individuals.
- Specific Attack: addressed to people by whom it is possible take greater advantages because of their hierarchy position




PHISHING ATTACK KILL CHAIN

Main stages of the phishing attack



Importance of social engineering in a phishing attack

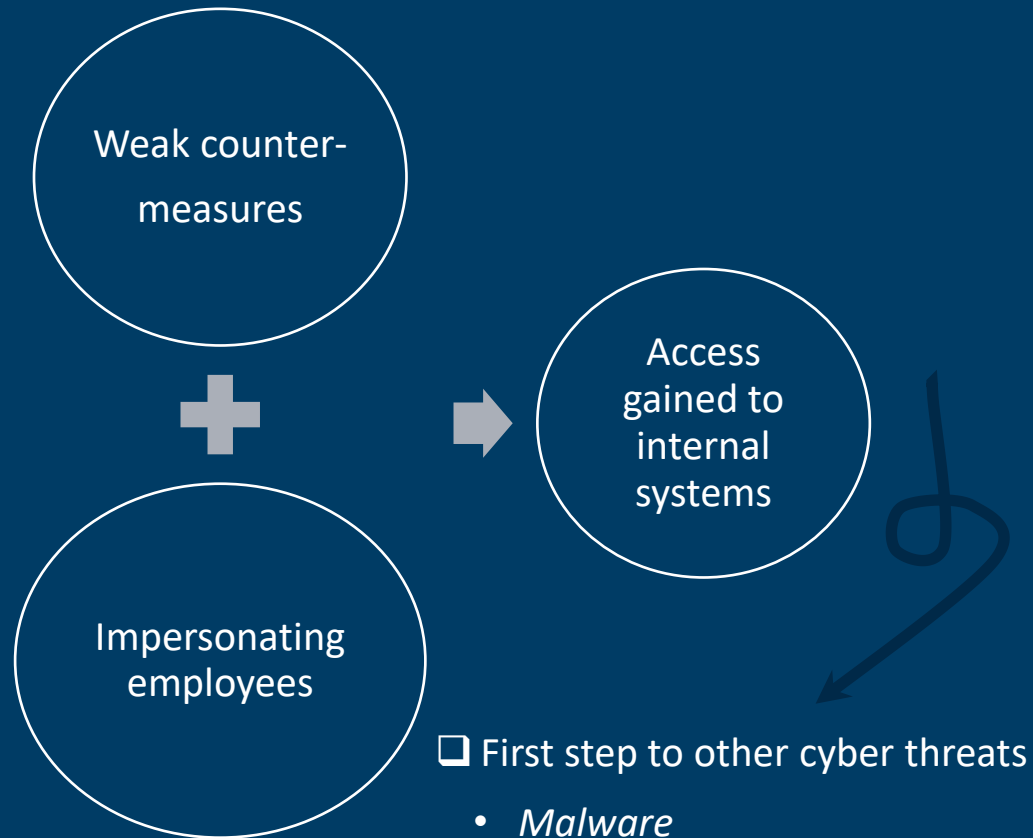
- Enhance effectiveness of the attack itself by undertaking advantage from
 - ✓ *human weak behaviours*
 - ✓ *habits*
 - ✓ *believes*



Humans are **more likely to comply** with a request under certain circumstances

*PHISHING IS STILL
SO POPULAR*

Who is using phishing and the need to use it



□ First step to other cyber threats

- *Malware*
- *Botnet*
- *Spam*
- *Information leakage*
- *Data breaches*



SCAMMERS

person who commits fraud

Phishing increasingly threat

- Employees have not enough awareness
 - > Attacks based on social engineering
 - > Only one person necessary to have a successful attack
- Sophisticated and targeted attacks
 - Harder to detect

Human are and they will be
the weakest link in cybersecurity

Latest statistics (2019-2020)

- Business processes are targeted
 - ❑ 76% of businesses have reported being a victim of a phishing attack
 - ❑ 33% of breaches included social attacks
 - ❑ 29% of breaches involved use of stolen credentials (Symantec)
 - ❑ 94% of malware was delivered via email (Verizon Data)

Human are and they will be
the weakest link in cybersecurity

Latest Phishing Trends

- Criminals use COVID19 phishing emails.

WHO reported that at the beginning of the pandemic everyone got spoofed

- Hackers hiding behind file sharing services: phishing emails impersonating **Microsoft *SharePoint*** and ***OneDrive***.

Anti-fog, anti-PM2.5, anti-poll, anti-dust, trend, anti-road violence mask



○ Coronavirus Mask <Contact@accutrelyaccept.top>

○ it@gazstroy.com

Wednesday, March 11, 2020 at 2:15 PM

[Show Details](#)

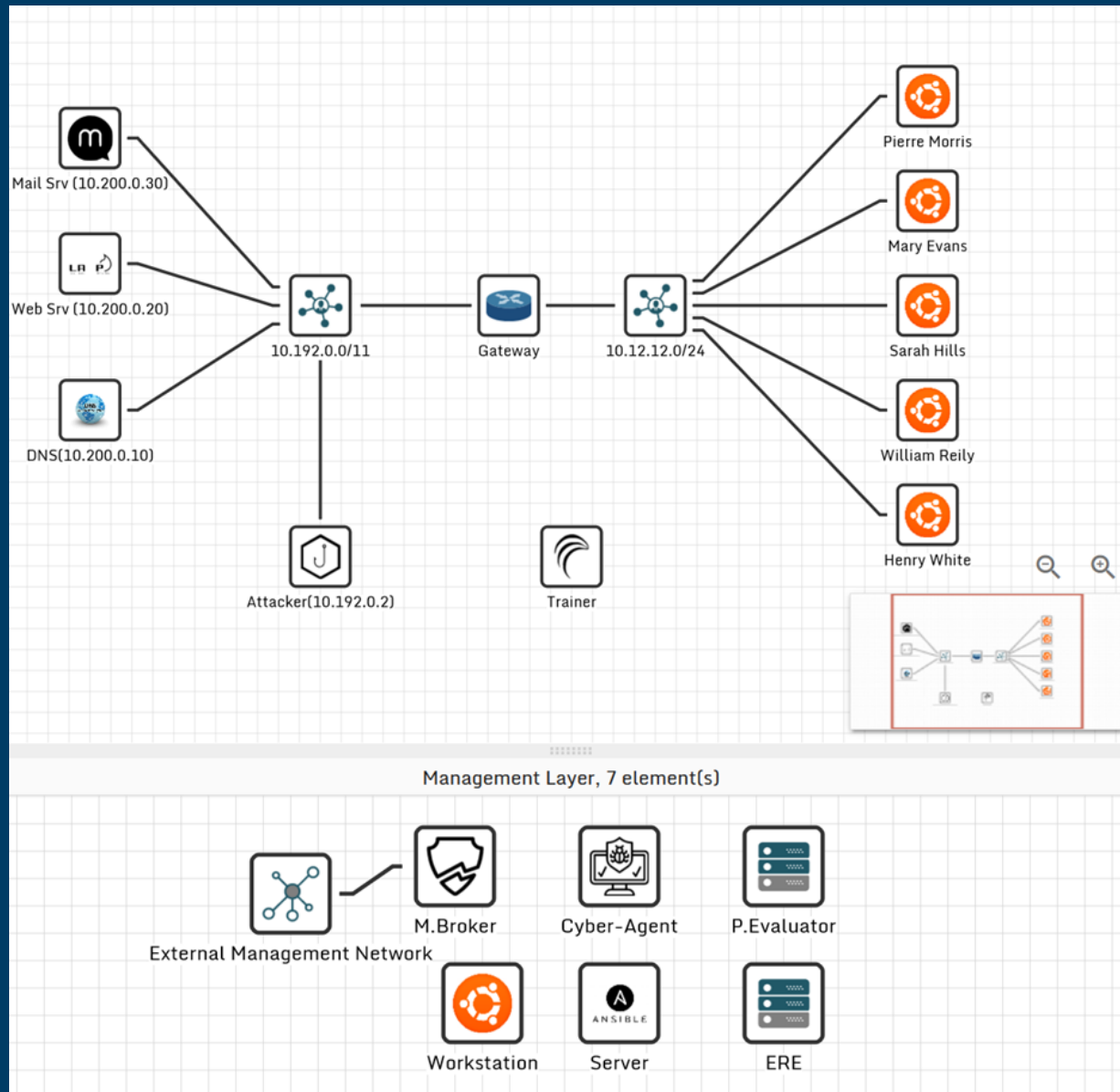


Discover the Highly Effective Anti-Pollution Clean Air Breathing Mask

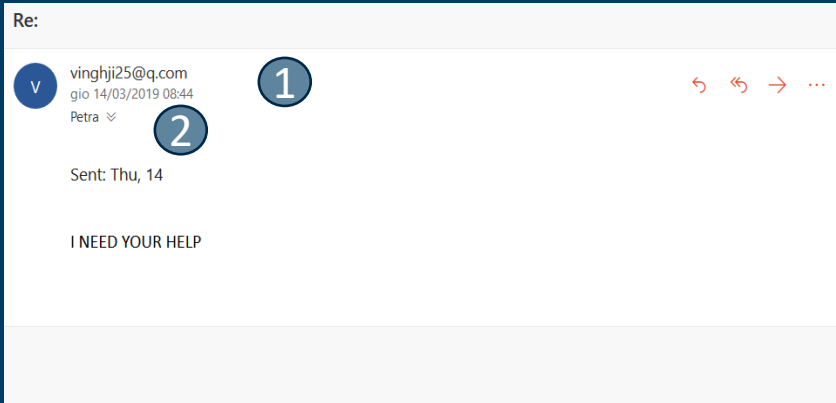


CYBERWISER HANDS- ON SCENARIO

Phishing attack exercise

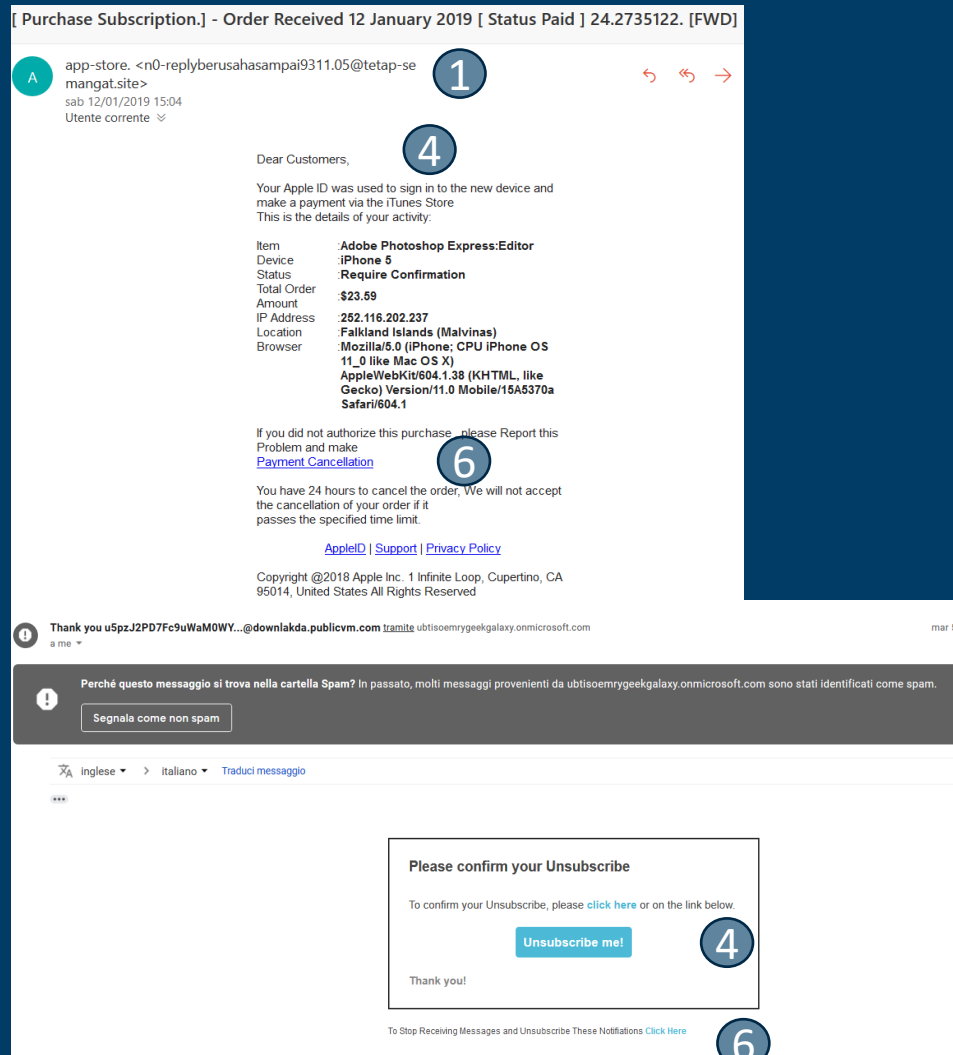


User actions to identify Phishing indicators



1. Verify the sender's address
2. Verify the recipient's address
3. Hover over the link
4. Don't trust a company you don't do business with
5. Notice grammatical error
6. Don't click on any links
7. Don't open any attachments

Identify Phishing indicators



1. Verify the sender's address
2. Verify the recipient's address
3. Hover over the link
4. Don't trust a company you don't do business with
5. Notice grammatical error
6. Don't click on any links
7. Don't open any attachments

Identify Phishing indicators

https://www.google.com/#btnl=axiikue57jc35cru0ss09ld33h5924y417k3vyl4q1e255yjdj8fz11qwff2a862hi8yvjl0l7ye8vf7n6my8pag857i2nl4a31r5t80alx1mvbl51407s1dc3sf5q7i02576447k66iw2pv6rh8mps5fml4wx4fenmo1fk99x42a9bs3384roa9iw39th12pep081970g6p87sl35u60c489f48c67136of4t254uxa06629g802gea54846f63uk71cbu0kf5l46hmdzjm7c0z22i956gs0j6j5yz0cxbj978z1i20t0m153w7keubw78mjewg554207bsn199862k23711ts79o3j2j9fw70495l0603np8rjz2q0980hie5n909l22hy2buv3o7t3w881llmwe1o10zr4fmdfn327k6558289i82z09ntyg99669538t2eb9rx9v68aqz2l0762sy4cdjg7d7v3ew17trbwp4khe2c04c78021w859a2v1lp4kxz4no5vfk996lp6ei4405fq4fy4mov243wu8fw5n0xla14z1mncvsh6p0g28o788v7wm6ip867f96rax9a5f9gp0l5946021w66m0325yl3m769vtem7tg&q=sgjjhcmoca

BB Becky Berrington <lmchavez@student.sisd.net>
gio 06/09/2018 23:12
andremigliore@gmail.com ✕

Good afternoon, andremigliore.

«We are upset, but Your application not took into account...»

From this website You NEVER such a notice DO NOT DISPLAY ③

⑥

FROM this website You will accept only joyful messages. For example, like these ones:

- accrued funds prepared by for cashing out

⑤

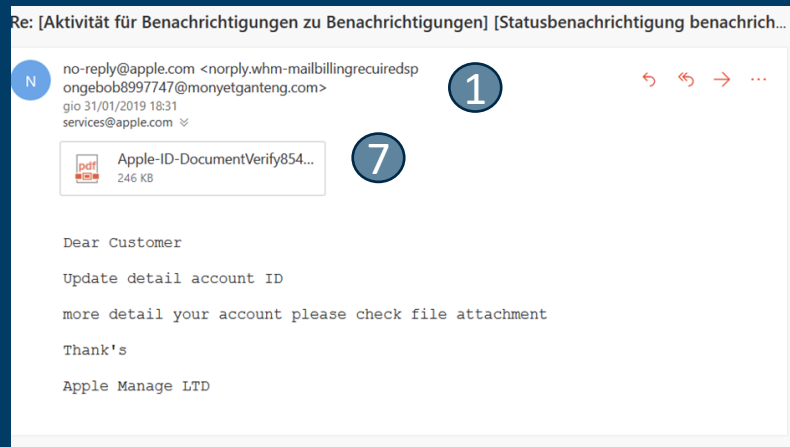
Your notification will come already after a couple of hours. So – everyday.

Becky Berrington

Your personal colleague

1. Verify the sender's address
2. Verify the recipient's address
3. Hover over the link
4. Don't trust a company you don't do business with
5. Notice grammatical error
6. Don't click on any links
7. Don't open any attachments

Identify Phishing indicators



1. Verify the sender's address
2. Verify the recipient's address
3. Hover over the link
4. Don't trust a company you don't do business with
5. Notice grammatical error
6. Don't click on any links
7. Don't open any attachments


User actions evaluation on handling an email

- **Open** an email: +1
- **Open** a **link** or an **attachment** in a **legitimate** email: +1
- **Report** a **malicious** email to the SOC: +1
- **Delete** of a **malicious** email: +1
- **Open** a **link** or an **attachment** in a **malicious** email: -1
- **Report** a **legitimate** email to the SOC: -1
- **Delete** of a **legitimate** email: -1

User Performance evaluation tool

Flags x +

10.254.0.5:9000/user1

 **CYBERWISER.eu**
Cyber Range & Capacity Building in Cybersecurity

Performance Evaluator

Evaluation Pierre Morris Mary Evans Sarah Hills William Reilly Henry White

8 Right Actions 4 Wrong Actions Your current score is: 0.5 out of 5

Name	Open	Clicked	Reported	Deleted
IT1_PHISHING	False	False	False	False
IT2_PHISHING	True	True	False	False
IT3_PHISHING	False	False	False	False
IT4_PHISHING	True	False	False	False
OT1_PHISHING	False	False	False	False

Economic Risk evaluation

Qualitative		
Quantitative		
Indicators		
Info		
Risk Status Quantitative		
Overall risk status:		
Typical Loss: 91,173.40 EUR		
Worst Case: 268,625.18 EUR		
Events: 5.452		
Threat:	WRP11: Phishing	Typical Loss: 91,173.40 EUR ▼
Risk WRP11-R1:	Hacker gains access to confidential company data A1: Confidentiality	Typical Loss: 308.49 EUR ▼
Target Machine	10.200.0.20	Typical Loss: 308.49 EUR ▼
Risk WRP11-R2:	Employee loses access to company data A2: Availability	Typical Loss: 90,848.82 EUR ▼
Risk WRP11-R3:	SOC is occupied with non-malicious emails A3: Functionality	Typical Loss: 16.09 EUR ▼

Phishing attack exercise

- Identify **phishing indicators** in an email.
- **Distinguish** phishing from legitimate emails.
- Understand the **right actions** to be taken when receiving a phishing email.
- Understand the importance of having **training** on **cyber risks** topics.

Exercise presentation

