



Funded by the
Erasmus+ Programme
of the European Union

Cyber-Attacks: Social Engineering and Phishing

Case Studies

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.



Learning Goals



Explain different types of Phishing attacks and learn to recognise them

Student Workload



Lecture	1,5 h
Audio and video material	0,5 h
Case studies	4,5 h
Further reading	0,5 h
Preparation for exam	2 h

Contents

- Bank of Valletta
- Cyprus Post Office
- Smart-ID
- Personal Data Leaks
- Emotet Malware
- Phishing Attack Simulation

Contents

- **Bank of Valletta**
- Cyprus Post Office
- Smart-ID
- Personal Data Leaks
- Emotet Malware
- Phishing Attack Simulation

Discuss how security risks can harm the infrastructure and affect the people's life

Case Description

The Bank of Valletta had been hacked, and hackers have deposited 13 million euros to foreign accounts. To focus on the cause, the bank has shut down the work of ATMs, messaging systems, mobile banking services and branches. As a result, many people were caught without money for a few hours or even a few days. The people were left stranded and couldn't buy day-to-day goods



This Photo by Unknown Author is licensed under CC BY-NC

Case Description

- Money was deposited to foreign accounts
- The bank had traced the fraudulent transactions and was being reversed
- Attack had been originated overseas
- Bank was working closely with international police to nullify the attack
- HSBC, stated that their services were operating smoothly
- Payments to four countries were blocked
- Hackers tried sending funds to UK, US, Czech, and Hong Kong, bank alerted the prime minister and started the reverse transactions
- MFSA keeping an eye out
- Shop owners were in the dark due to no services

Questions for Discussion



- What could you learn from this attack?
In terms of
 - *protected assets*
 - *security risk*
 - *risk impact*
- How would you have acted?
 - *As bank's customer*
 - *As bank official/manager*
 - *As system administrators*

Questions for Discussion



- What could have prevented the following situations?
 - *Security risk happening*
 - *Crisis after the security event*
- If you were the bank's manager:
 - *How would you have calmed the situation?*
 - *How would you recover the lost money and the bank's reputation?*

Contents

- Bank of Valletta
- **Cyprus Post Office**
- Smart-ID
- Personal Data Leaks
- Emotet Malware
- Phishing Attack Simulation

Discuss principles of persuasion and potential action to decrease impact of phishing attacks

Case Description

- Cyprus post office is a strategic organisation operating under the Cyprus government. Most people in Cyprus use postal services, especially parcel delivery (online shopping) – a service that has seen a tremendous increase since the COVID-19 pandemic started
- This is not the first-time scammers have targeted/used the Cyprus post office as subject to their scam. Before this, in 2018, scammers have sent the text messages from various sources, including Facebook messages, to people claiming that the Cyprus Post have selected subscribers for a chance to win a high-tech phone. The messages intended to mislead users in many ways, including theft of personal details, access to personal electronic accounts and online services, and information on online banking details

Case Description

The message scam in 2018:



Συγχαρητήρια! Είστε ένας από τους 10 τυχερούς πελάτες που επιλέξαμε και τους δίνουμε την ευκαιρία να κερδίσουν ένα Samsung Galaxy S10.

The message scam in 2021:

Cyprus Post [stagesprgrss-ftp@stagesprogress.com]
YOUR PACKAGE WILL BE AT YOUR HOME SOON.

Tracking Code is : HL1487158H1A

Hello,

We regret to inform you that your package has been stopped at the last step, please make a payment of 1.99 EUR so that you will receive it by the end of next week.

PAY

At this time we thank you for your trust.

Sincerely, the Post Cyprus team

The Cyprus Post warned that fake messages asking for payment of custom duties are being sent to the public by email

Case Description

Cyprus Post [stagesprgrss-ftp@stagesprogress.com]

YOUR PACKAGE WILL BE AT YOUR HOME SOON.

Tracking Code is : HL1487158H1A

Hello,

We regret to inform you that your package has been stopped at the last step, please make a payment of 1.99 EUR so that you will receive it by the end of next week.

PAY

At this time we thank you for your trust.

Sincerely, the **Post Cyprus** team

Questions for Discussion



- What principles of persuasion could be identified in the *Cyprus Post Office* case?
- Why should *Cyprus Post Office* case be considered as a phishing attack?
- Why do scammers pretend to be from the “*known*” public authorities and/or organisations?
- How should the “*known*” public authorities and/or organisations themselves respond to the scams?

Contents

- Bank of Valletta
- Cyprus Post Office
- **Smart-ID**
- Personal Data Leaks
- Emotet Malware
- Phishing Attack Simulation

*Discuss how threat agents
uses the modern
authentication techniques to
harm protected assets*

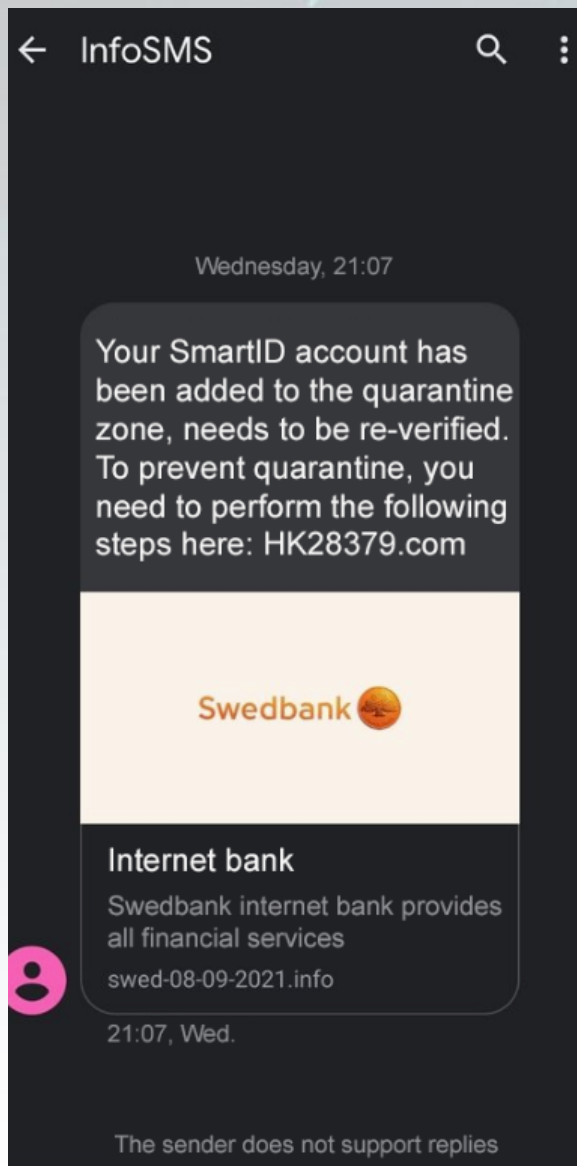
Case Description

Smart-ID is the easiest, safest and fastest way to authenticate yourself online, register in e-services and sign documents. Smart-ID enables the person to enter the Internet or mobile bank and other e-services securely and conveniently with your preferred smart device. Smart-ID is not related to SIM cards or mobile operators; only Internet access is needed.



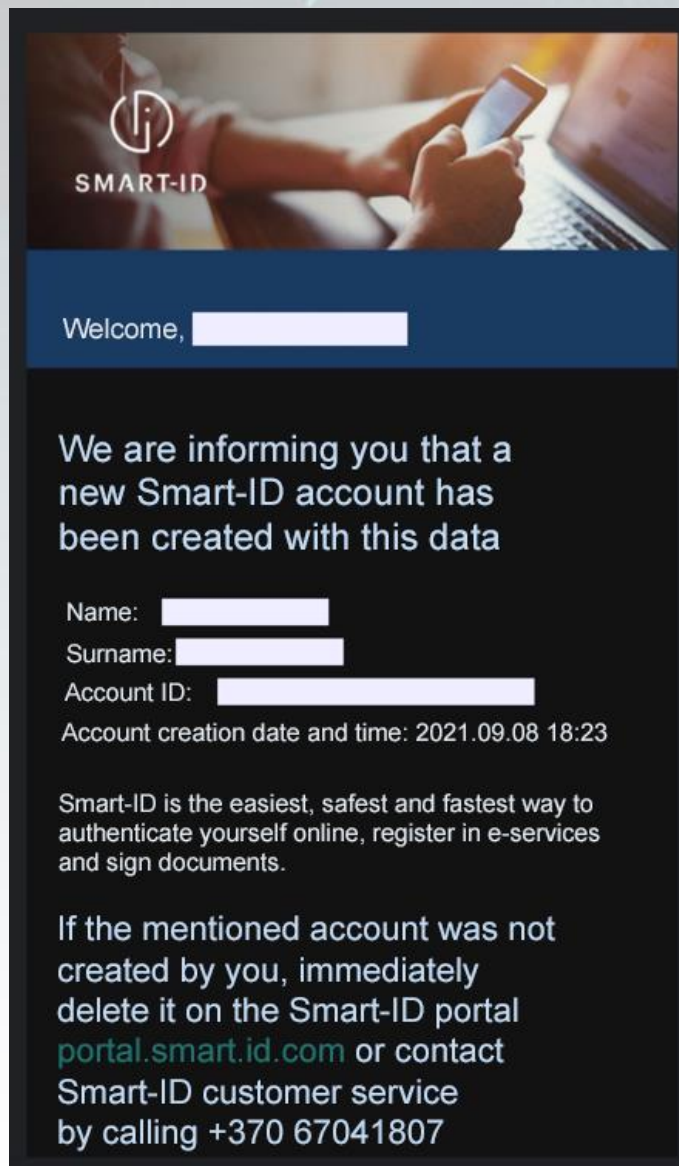
<https://www.smart-id.com>

Case Description



In September 2021, scammers have been sending SMS messages to the Lithuanian citizens with various content aimed at just one thing: drawing citizens' attention to the alleged security of their funds, personal Smart-ID or online banking accounts. The messages ask to click on the active internet link and provide personal login details to neutralise the risk.

Case Description



If the victim clicks on the link, the fake website opens, where the user has to provide personal information or “activate“ the account.

Questions for Discussion



- How safe authentication tools, like Smart-ID, could be used to steal citizens' money?
- What actions should be done after getting such an SMS?
- What are red flags indicating the phishing SMS?
- What actions should you do if you are hacked?
- Is it possible to recover the lost money?
- What lessons could be learnt in this situation?

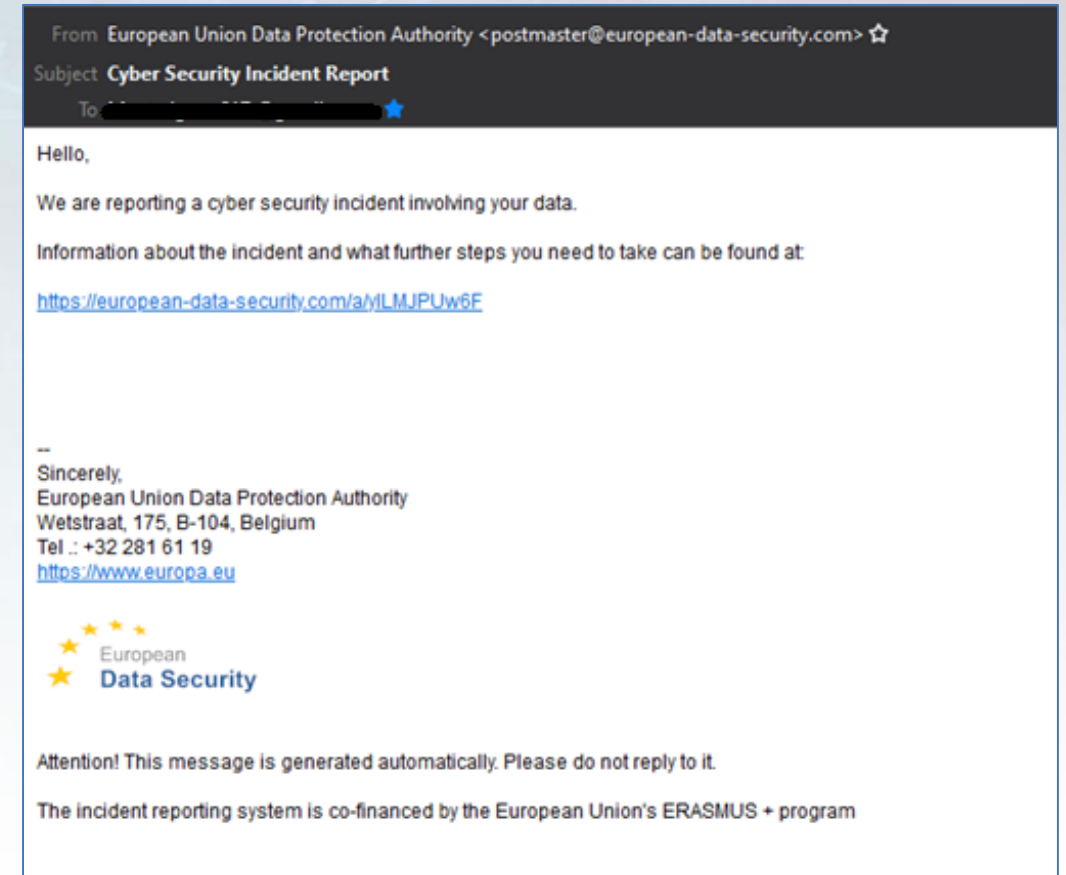
Contents

- Bank of Valletta
- Cyprus Post Office
- Smart-ID
- **Personal Data Leaks**
- Emotet Malware
- Phishing Attack Simulation

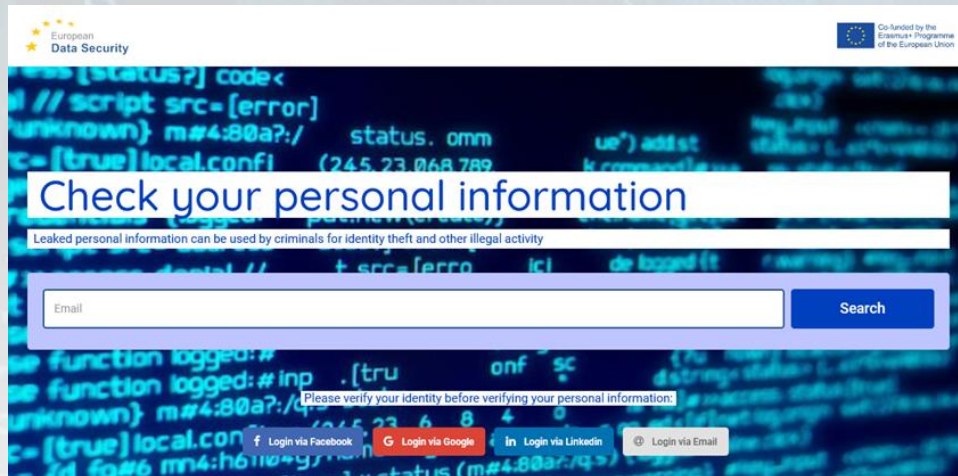
Discuss how to recognise falsified emails offering various services from untrusted organizations

Personal Data Leaks Case Description

Within three weeks during spring 2021 in Lithuania, at least four large thefts of personal data were made public. These events caused massive media attention and a lot of discussions. The scammers have exploited the situation and sent falsified letters. In these letters, the recipients were encouraged to join the not existing organisation's web page and check if their personal data were exposed



Personal Data Leaks Case Description



European Data Security

Co-funded by the Erasmus+ Programme of the European Union


Check your personal information

Leaked personal information can be used by criminals for identity theft and other illegal activity


Please verify your identity before verifying your personal information:

Login via Facebook Login via Google Login via LinkedIn Login via Email


Data leak incidents



Eksptarai: „CityBee“ duomenų nutekėjimo skandalo buvo galima išvengti
2021 kovo mėn. 8d. | 15min.lt



Dar vienas kibernetinis įsilaužimas: nutekinti „Orakulo“ klientų duomenys
2021 vasario mėn. 12d. | kaunas.kasvyksta.lt

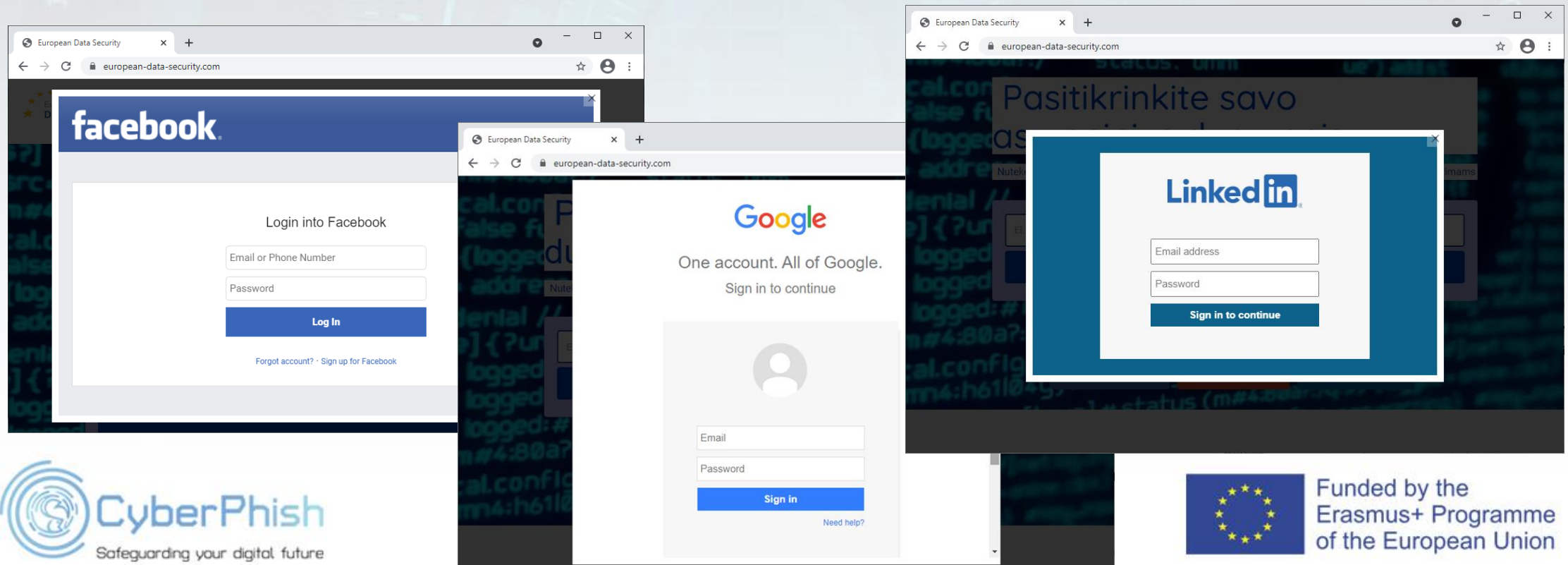


Panašu, kad „DarniPora.lt“ taip pat prarado itin jautrius 400 tūkst. vartotojų duomenis
2021 vasario mėn. 19d. | 15min.lt


If the victim of attack pressed the link, they were directed to the webpage of the non-existing organization. On this page, the victim was requested to log into one of the social networks


Personal Data Leaks Case Description

When the victim selected one of the accounts, the fake join windows were opened. The information (e.g., login details – *login name* and *password*) entered into these windows was stolen



The image shows a browser window displaying a phishing website titled "European Data Security" at the URL "european-data-security.com". The website features three overlapping login windows for Facebook, Google, and LinkedIn. Each window contains fields for email/phone number and password, along with a "Log In" or "Sign in to continue" button. The background of the website is dark with green binary code and text.

 CyberPhish
Safeguarding your digital future

 Funded by the
Erasmus+ Programme
of the European Union

Questions for Discussion



- What to do if your account login data was compromised ?
- What to do when you received such email ?
- What are red flags indicating about phishing email, login forms?
- What lessons did you learn from this situation ?

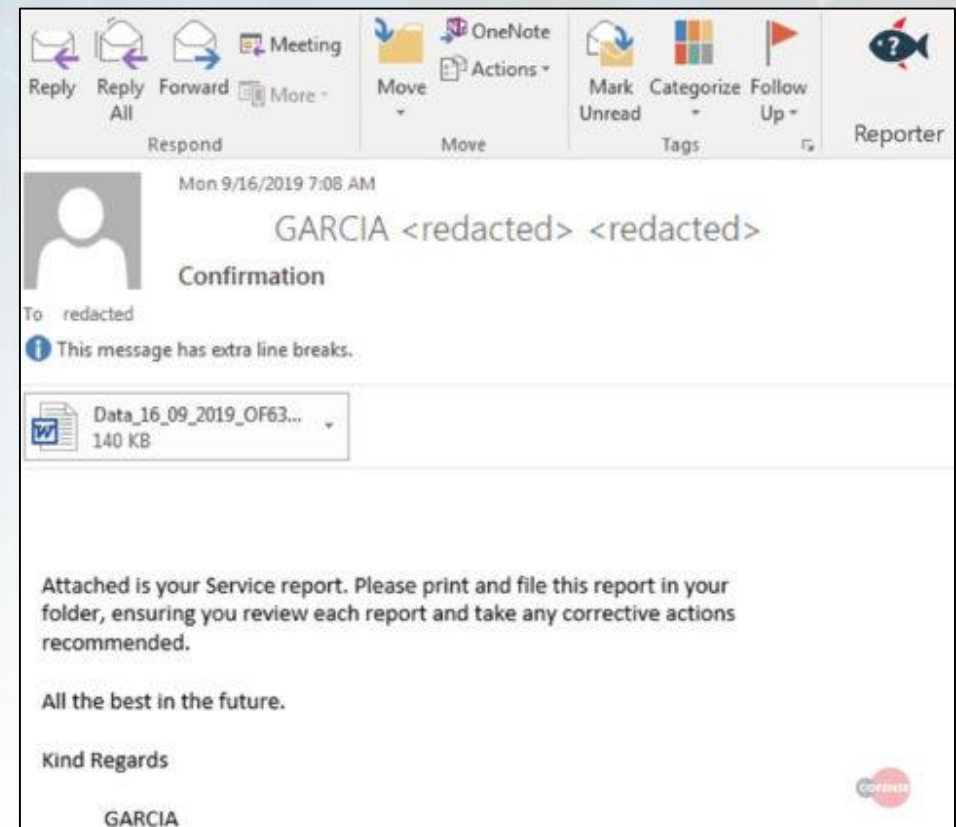
Contents

- Bank of Valletta
- Cyprus Post Office
- Smart-ID
- Personal Data Leaks
- **Emotet Malware**
- Phishing Attack Simulation

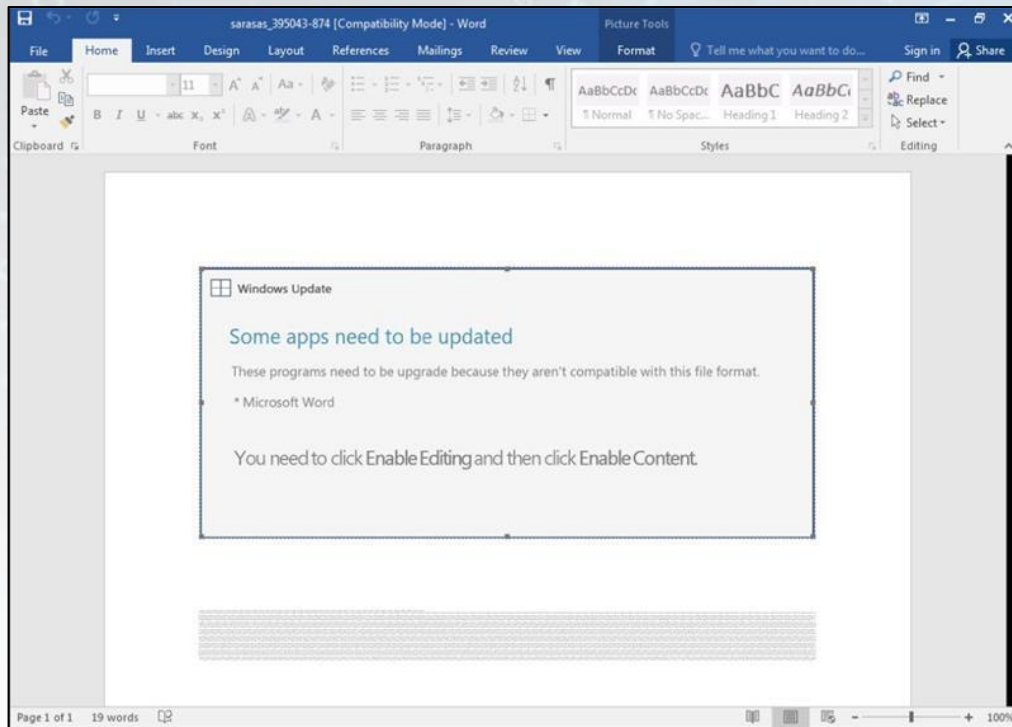
Discuss the impact of potentially malicious emails received from the trusted senders

Emotet Malware Case Description

- Malicious spam (malspam) pushing **Emotet** malware is the most common email-based threat. It uses a "thread hijacking" technique that utilizes legitimate messages stolen from infected computers' email clients. This malspam spoofs a legitimate user and impersonates a reply to the stolen email. Thread hijacked malspam is sent to addresses from the original message



Case Description



This technique is more effective than less sophisticated methods, which many people have now learned to spot. The approach is more successful at convincing potential victims to click on an attached file or click on a link to download a malicious Word document with macros designed to infect a user with Emotet

Questions for Discussion



- How could a person to double check the if the email is coming from a legitimate source even if it looks like a reply to a conversation?
- Is a person supposed to receive files like these on the day-to-day work?
- Does one need any anti-malware software even if he or she (*thinks that he/she*) never surfs strange websites or uses the device only for the work-related activities?
- Should a person open the attachment, if the email looks important and related to the work activities, but attachments looks suspicious?

Contents

- Bank of Valletta
- Cyprus Post Office
- Smart-ID
- Personal Data Leaks
- Emotet Malware
- **Phishing Attack Simulation**

Discuss the impact of phishing attacks to organisation

Phishing Attack Simulation Case Description



A telecommunication company decided to run a controlled simulation to explore how their employees are aware of phishing attacks. The simulation was carried out in the early hours of the day. The phishing email was sent on the 17th of March 2021, at 8:26 am. The purpose of selecting the time was to get the employees off-guard as that will be one of the first emails received for the day. The phishing email content required a security update, which contained a link stated to be the path to updating credentials (when the link is clicked, it redirects the user to the staging website built using the domain name bought)

Phishing Attack Simulation Case Description

Simulation Results

- The simulation targeted approximately **250** employees.
- In total, **179** link clicks were observed from the company's network, and **40** clicks were observed from outside the company's network.
- **Three** people reported about the phishing attack. The other **four** called to get a confirmation if the email was legitimate. **Two** employees called to complain about the not-working link.

Day	Number of clicks from company's network	Number of clicks from external network
1	161	>30
2	18	>10
Total	179	>40

Phishing Attack Simulation Case Description

Victims' profiles

- **Member of financial team**
 - *Received a few minutes after the phishing email was sent*
 - *Respondent asked to correct link*
 - *Access to client data, payment processes/data, accounting data*
- **Head of unit**
 - *Access to data of different type*
 - *Potential harm to organisation's reputation*
- **Non-engineering team member**
 - *Access to colleagues data in the same unit*
 - *Opens gate for future attacks*
- **Member of engineering unit from different region**
 - *Access to data in the regional unit*
 - *Potential harm to services in the region*
- **Member of engineering unit**
 - *Access to organisation's intranet*

Phishing Attack Simulation

Questions for Discussion



- Define the phishing attack
 - *What is a profile of the phisher?*
 - *What is the phishing attack method?*
 - *What is the vulnerability?*
 - *What is the impact?*
- What are the red flags indicating that the email is the phishing attack?
- What is the impact of this phishing attack to the considered company?
- How to raise phishing awareness in the considered company?

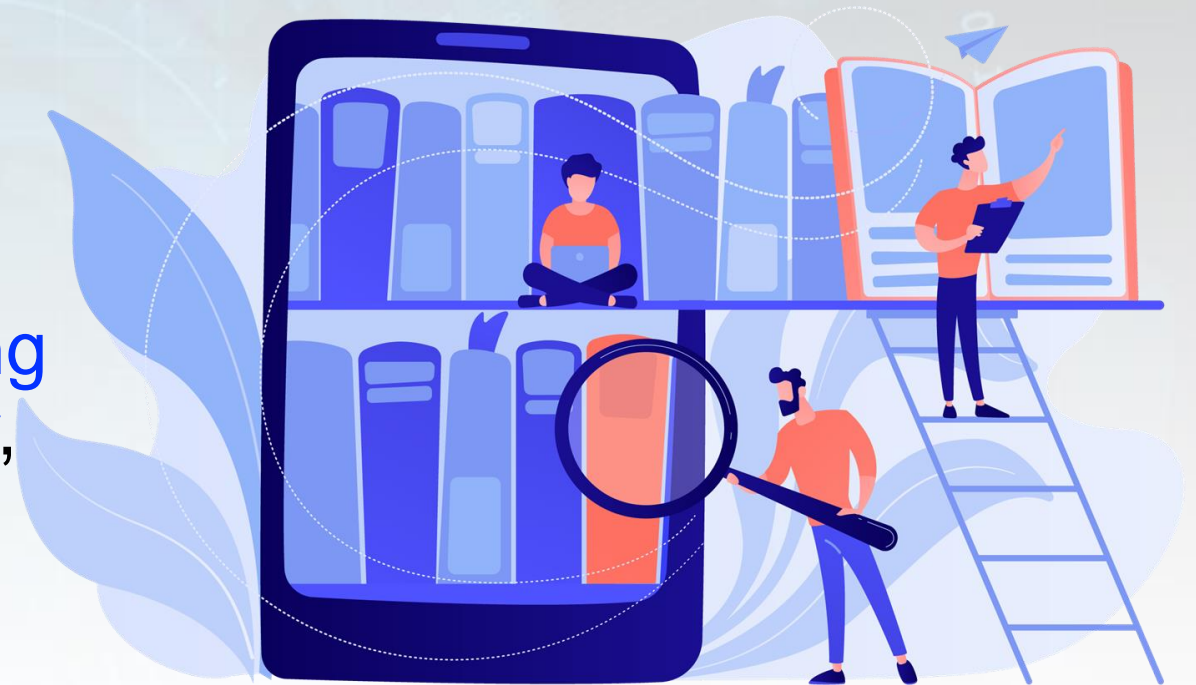
Summary

- How security risks harm the infrastructure and affect the people's life
- Principles of persuasion and action to decrease impact of phishing attack
- How threat agents uses the modern authentication techniques to harm protected assets
- How to recognise falsified emails offering various services from untrusted organisations
- Impact of malicious emails received from the trusted senders
- Impact of phishing attacks to organisation



Further Reading

- **Kevin D. Mitnick and William L. Simon (2002):**
The Art of Deception, Controlling the Human Element of Security,
Willey Publishing, Inc.



Short Videos

- Bank Security Breach
<https://youtu.be/kkc3nkCXUk0>
- Cyber Attack on Banks and Post Office
<https://youtu.be/yB3N9U6V3c4>
- Smart-ID Registration with ID-card
<https://youtu.be/m9t4PY0DROM>
- Emotet - the Evolution of Malware
<https://youtu.be/CkwKTBifXJg>
- Phishing Attack Simulator
<https://youtu.be/hh25C0cdop0>



Thank you!

