

Cyber security training

The purpose of the training is to introduce different cyber-attack methods. By knowing these an organization can prevent serious threats, such as taking over an e-mail address, stealing personal data and trade secrets, or even taking control of the entire organization's infrastructure and business.

❖ **Fraudulent e-mails (phishing/spoofing)**

- ⦿ The e-mail implies that it comes from an important person in the company
- ⦿ The e-mail implies that there is a problem with the user's account, and in order to solve it they should log into the account

❖ **Password attacks**

- ⦿ Password spray
- ⦿ Password dictionary attack
- ⦿ Most used passwords
- ⦿ Password recommendations
- ⦿ Password leaks, haveibeenpwned
- ⦿ Fake e-mail examples

❖ **Spyware and adware**

- ⦿ Various software programs that collect information from the user's computer, monitor the activity of the user, and log everything that is written (e.g., passwords). Annoying ads that, when clicked on, take to a fraudulent page.

❖ **Public Wi-Fi without password**

- ⦿ As strange computers can connect to a public Wi-Fi accessible without password, that may be used for malicious purposes.
- ⦿ A hacker creates a Wi-Fi with the name of a company. A user connects to the Wi-Fi in good faith, but the network redirects the user to a fake network.

❖ **Spam**

- ⦿ Product or service ad/newsletter
- ⦿ Malicious e-mails

🔦 Social Engineering

- ⦿ Art of manipulating people to give access to a hacker voluntarily.
- ⦿ Thereby, advantage is taken of the person's:
 - laziness
 - lack of attention
 - excessive trust (someone pretends to be an IT person)
 - enthusiasm (they promise X if you do Y NOW)
 - sincere wish to help
 - trust (they believe they are following the order of a superior)
- ⦿ Old, discarded equipment that have not been cleaned up – contain data and accesses.
- ⦿ Listening or observing the entry of password.

🔦 Security solutions

- ⦿ PIN instead of password
- ⦿ Multi-factor authentication (MFA)
- ⦿ Passwordless login
- ⦿ Bitlocker
- ⦿ Microsoft Defender for Office365 instead of ATP

Time of training: agreed with the customer

Trainer: Tarmo Kumar/ Mairo Juss

Duration of training: 2 hours

Place of training: online

Number of participants: up to 20 people in one group or as agreed with the customer

Investments:

Setup of service and report of results: €600