training code: BS.IT 00 / ENG DL 1d / EN

Secure Employee – Cyber Awareness lectures for office employees

Purpose of the training

The training is intended to acquaint employees of the organisation with a variety of currently used threats, chiefly socio-technical. Apart from theory and practical examples of possible threats, workshops participants will acquire an ability to increase security for their working environment by using tools such as online scanners, password manager or leakage bases. Trained employees will be able to successfully identify popular types of threats (among others, phishing, spear phishing, scam, clickjacking), react to them and set strong enough securities of their accounts and data (passwords, coding, two-factor authentication). During workshops topics related to popular threats such as false Wi-Fi networks, spying tools, malware (including ransmeware and cryptolckers) will also be discussed. We will also talk about security of mobile devices and good practices of taking care of your own privacy.

Benefits of completing the training

- Raising awareness of threats related to cybercriminals' activity,
- Diminishing the level of risk of theft or phishing of confidential data,
- Diminishing the level of risk of losing continuity of business process'activity,
- Securing iCT's infrastructure,

Expected Listener Preparation

- Basic computer skills

Training Language

- Training: English
- Materials: English

Duration

1 days / 7 hours

Training agenda

1. Social engineering
   - Who is behind it and who benefits from it?
   - What criminals need our data for?
   - Why regular employees of organisation are most often the victims of the cyberattack?
   - What is social engineering and where does its effectiveness and popularity come from ?
   - Methods of Identifying social engineering attacks and methods of avoiding them
   - Consequences of cybercriminals'actions for private persons and organisations
   - How much do our data cost?
2. E-mail security
   - The rules of verifying appendices
   - The rules of verifying links
   - The rules of verifying addressees
   - Does the sender have to be who he or she claims to be?
   - Is it easy to impersonate company's employee?
   - Is it easy to extort huge amounts of money with only one e-mail?
3. Security of Internet browsers
   - What is phishing and how to avoid it?
   - What is typosquating and domainsquating?
   - What are the attacks such as clickjacking, camjacking, likejacking?
   - The rules of verifying information and webstes, as well as URL-s
4. Security of devices and data carriers
   - Data carriers of the unknown origin as a threat
   - Popular social engineering like „per courier", „per pizza"
   - Is USB lamp a data carrier ?

- New devices from IT department
- Secure data erasing

5. Phone attacks
   - Phishing
   - Persuading to do specified actions via phone
   - Is interlocutor who he or she claims to be?
6. Threats related to mobile devices
   - Mobile device security
   - Granting authorisations to applications
   - Smartphone – the best device of surveillance
7. WIFI network threats
   - Free of charge network
   - How the name of network is connected with its security?
   - Is it easy to develop false network which steals data?
8. Password security
   - Are our passwords shared publicly on the Internet?
   - Which of our accounts have already been taken over by hackers?
   - How long does cracking the password take?
   - What is dictionary entry?
   - How to create strong, secure and easy to remember a password?
9. Artificial intelligence serving frauds
   - False identities
   - Using AI to generate the image
   - Using AI to falsify the image
   - Using AI to counterfeit the voice