Cyber Security Awareness Training

Created by https://security-companion.net/

Version 1.1

About this training

- Released under open source license (Creative Commons Zero v1.0 Universal)
  -> Training is freely available
  -> use, changes and duplication is allowed
- Current version can be downloaded here

Overview

- Motivation
- Social Engineering
- Security on the Internet
- Passwords
- Two-factor authentication
- Backups
- General information

Motivation

- Hacker attacks on companies and organizations have increased significantly lately
- All technical safeguards are useless if the people who operate them bypass security measures consciously or unconsciously
- Employees of an organization are often the weakest link in the chain.
- This presentation is intended to equip employees for the future and to raise security awareness.

Data worth protecting

- Addresses of external or internal contacts
- Account details
- User names/passwords
- Financial reports
- Hardware used in the organization
- etc.

Social engineering

- Methods attackers use to elicit sensitive information from employees, often using pressure and trying to elicit sympathy
- Examples:
  - if a bank transfer ordered by the supposed boss is not made immediately, high reminder costs are threatened
  - The attacker prones to be a new colleague and asks for help by submitting passwords during a phone call.

- further examples:
    - Attackers pretend to be technical support, e.g. from Microsoft, and claim that they need to solve a problem on a computer.
    - attacker pretends to be a grandson and claims to be in (financial) need

Security on the Internet

- Browsers and e-mail clients are directly exposed to the Internet -> always keep them up to date in order to being protected against new attacks as good as possible
- Before clicking a link from email, chat app, SMS etc. always check the following:
  - Did I expect this link?
    - Link from a parcel delivery service although no parcel is expected
    - Link from a bank but I have no account from this bank

- Do I know the URL (= link address)?
- Is the translation poor?
- Is there really no letter changed in the URL? https://amazon.com and https://amaz0n.com are completely different.
- Am I on the official site or does the last part of the domain belong to another country? .ru, .uk, .cn etc.?
  - Example: https://company.com.mx or https://company.de instead of https://company.com

- Before clicking on a link, point to it with the mouse (on tablets long press on it) and check its correctness in the status bar.
    - Is an IP address (192.168.178.1) visible instead of an URL?
- Check shortened links with services such as https://urlex.org/ or https://unshorten.me/ (they display the whole link).

- When visiting unknown pages, check them critically and if in doubt, cancel the visit.
- Does the design look strange or is it missing completely?
- Websites can be checked for viruses with https://virustotal.com
- It is more secure to enter the address of a website directly in the browser instead of clicking on the link in the e-mail.

- If you receive an e-mail with a suspicious attachment from a friend/colleague, call the sender before opening the attachment to check if the e-mail is legitimate.
- Look for the lock in the browser bar 🔒
  - Attention: The lock only means that the connection between browser and client is encrypted.
  - A lock does not automatically mean that the site is secure or not operated by an attacker.

- Never install software that is advertised in a browser pop-up.
- Do not log into email accounts or online banking on public computers (hotel lobby, library etc.) as attackers can record data.
- Never activate macros in Microsoft Word, Excel etc. with suspicious attachments!

Passwords

- Attackers have long password lists with millions of passwords at their disposal. They try these on login pages until they succeed
- Examples of bad passwords:
  - P@ssw0rd
  - summer2021
  - secret1
  - abc123

- Minimum requirements for passwords:
    - Use at least 12 characters with a combination of upper, lower case letters, numbers and special characters.
    - The longer a password the more difficult it is to crack it
    - Do not reuse passwords

- Avoid the following words in passwords as attackers can easily research them:
  - Name of pet or children, middle name
  - Birthday, address
  - Words related to the employer (building name etc.)
  - Current year

- Better use the first letters of a sentence
    - Example: IltepwS55: I like to eat pizza with Salami 55.
- Never store passwords directly in plain text on the hard disk or attach them to the screen with a piece of paper.
- Use haveibeenpwned.com to check if your email address/password combination has been part of a data leak.

Password manager

- Digital safe for all user-password combinations
    - passwords are stored encrypted on hard disk and secured by a master password
- Synchronization between multiple devices possible
- Often offer the possibility to generate randomly generated passwords

- Free open source variants: KeepassX and Bitwarden
  - Browser extensions increase convenience by automatically filling in login fields
- Many commercial providers also offer free variants
  - However, if an attacker hacks the providers server's your own passwords also might get stolen and eventually being published on darknet

Two-factor authentication

- Secure logins with a second factor in addition to the username/password combination.
    - Example: chronological sequence of digits on the cell phone (token that changes every few seconds)
    - Only with the token a login is possible and therefore protects effectively against abuse
- Always activate where possible!
- Possibly store QR code/setup code in password manager in order not to be locked out of services if cell phone gets lost

WiFi

- Hackers can easily set up their own WiFi with the same name as the original one (e.g. Library-WiFi).
    - avoid public, unencrypted WiFis
    - use only encrypted WiFi and/or VPN instead
- Commercial VPN providers promise to encrypt the user data and therefore not to be able to access and uncrypt it. But it is difficult to verify this

Data protection

- With products that you can use for free, you are often the product yourself
    - Providers use customer data and sell it to advertising partners
    - Sometimes it is better to pay for a product and thus limit data collection

Backups

- Make regular backups of important data, e.g. via NAS or USB stick
- Keep several versions, e.g. according to the scheme grandfather, father, child
- Only backups that are not connected to a computer or network (offline backups) protect against encryption by Trojans or similar.
- Regularly practice restoring data in order to being prepared in case of an emergency

General information

- Always keep operating system and software up to date
- Keep virus scanner up to date
- Do not connect unknown USB sticks that you have found eg. in the parking lot to a computer
    - Programs can start independently, unnoticed and without user action
    - Attackers use these methods specifically to penetrate a network.