Cyber Security Awareness Training

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

Version 1.6

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
- Email
- Passwords
- Two-factor authentication
- Wi-Fi / VPN
- Backups

Motivation

- Hacker attacks (e.g. ransomware) 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
- Bank account details
- User names/passwords
- Financial reports
- Hardware and software used in the organization

- Social security number
- Birth date, Birth place, Mother's name (are often used as authenticator to recover a password)
- Email addresses (are often used for authentication e.g. in company networks)
- etc.

Social engineering

- Definition: Methods that attackers use to elicit confidence and by this get sensitive information from employees/users, often using pressure and trying to elicit sympathy (Phishing)
- Especially receptionists need to be careful when receiving calls or welcoming a so called "printer repair technician" on the campus
- Examples:
  - if a bank transfer ordered by the supposed boss is not made immediately, high reminder costs are threatened
  - an attacker prunes 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
    - attacker send an email asking users to urgently contact customer support under the mentioned number (number is not the one of the mentioned company but one controlled by the attacker) - Callback Phishing

Security on the Internet

- Browsers and email 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 of the website or email poor? Are the images of bad quality?
- 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.uk or https://company.de instead of https://company.com
    - Example: https://facebk.com instead of https://facebook.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 (93.235.136.159) 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 (and unexpected email attachments) 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 an email

- When using selling platforms only communicate with others over the official contact application of the platform
    - If a potential buyer is contacting you via messenger then be cautious
    - Don't allow others to pressure you but instead abort contact if in doubt

- If you receive an email with a suspicious attachment from a friend/colleague, call the sender before opening the attachment to check if the email 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!

Email

- Many email programs only show the name of the sender but not the complete email address
- Forged Emails: Attackers make an email seem valid although it is a fake/scam
- Verify the domain: only service@paypal.com is valid, customerservicepaypal@gmail.com not
  - Be aware that the second email address doesn't get filtered out by mail servers and spam filters and therefore is interesting for attackers

- Don't use the same email account for everything, separate work from personal
- Use separate account when shopping online
    - Many vendors add buyers automatically to mailing lists, therefore account will receive lots of mails over time
    - If account receives too much spam then it can be closed and replaced by a new one
    - -> Personal account stays cleaner from undesired emails

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:
  - Avoid Leetspeak (replacing of characters by similar looking symbols and numbers, e.g. @ for "a" or 3 for "e")
  - 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
  - Do not reuse passwords
  - Be aware that passwords that are easy to remember for you are also easy to guess by an attacker

- 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
    - Words that can be found in a dictionary or citations from famous books, movies etc.

- 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 or HPI Identity Leak Checker 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: KeepassXC and Bitwarden
    - Browser extensions increase convenience by automatically filling in login fields
- Many commercial providers also offer free variants/plans
    - However, if an attacker hacks the provider's servers, 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 it protects effectively against abuse
- Activate where possible

- Avoid tokens that are sent via SMS to your phone, better use tokens that change every few seconds and are generated by an app
- If possible store QR code/setup code in password manager in order to not being locked out of services if cell phone gets lost

Wi-Fi

- Hackers can easily set up their own Wi-Fi with the same name as the original one (e.g. Library- or train-Wi-Fi)
  - avoid public, unencrypted Wi-Fis
  - use only encrypted Wi-Fi and/or VPN instead
  - Preferably use cable connections instead of Wi-Fi

VPN

- VPNs don't make a connection "more secure" as today most connections are already encrypted using SSL/TLS
- VPN is useful
  - if you want to hide from your internet provider which sites you visit
  - if you want to hide to a webpage from which country you are coming (and e.g. want to activate content that would not be available without VPN)

- Commercial VPN providers promise to encrypt user data and therefore not being able to access and decrypt it, although this is difficult to verify
- Avoid "free" VPN providers

Data protection

- Think about what types of data you have in your work or private place and consider how you protect it if it is lost, stolen or in position of somebody unfriendly
- Computers: Although you need to log in in order to use, its data can be read if its disc is connected to another computer or an USB-Stick with a second operating system is connected
- Better encrypt them with tools like BitLocker, VeraCrypt on Windows, FileVault on Mac and LUKS on Linux
- The same applies to hard discs and USB-sticks: Once connected to a computer, data can be read from them if they are not encrypted

Cloud-based/online Storage

- Many cloud providers encrypt your data on their servers - but they have the master key and can therefore encrypt and read your data
- Better watch for providers that offer Zero-knowledge storage
    - This means that data is encrypted locally on your machine before being transmitted to a cloud provider
    - Nobody else but you can read the data
- Alternatively encrypt files locally with tools like Cryptomator and BoxCryptor before sending them e.g. to Dropbox

Backups

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

General information

- You can never be 100% "secure" from attacks, you can only manage and mitigate against the risks that you are being faced with
- Regularly review if what you've been doing yesterday is still useful and secure today and tomorrow

- With products that you can use for free, you are often the product yourself
  - Providers use customer data and sell it to advertising partners
  - Freeware might be spyware sending sensitive information from your computer to the developer's servers
  - Sometimes it is better to pay for a product and thus limit data collection
- Only install software that is necessary and only download it from reliable sources

- Always keep operating system and software up to date
- Keep virus scanner up to date
- Be aware that suites that promise to do "all" stuff related to security for you have their limits
- Do not connect unknown USB sticks that you have found e.g. in the parking lot to a computer
    - Programs can start independently, unnoticed and without user action
    - Attackers can use these methods specifically to penetrate a network