CERT.PL >_
NASK

https://incydent.cert.pl / cert@cert.pl

Guidelines for secure usage of social media and e-mail

- **Do not use your personal** e-mail and social media for business matters
- **Do not use your personal devices** (computers and phones) for work
- **Do not use company-issued devices** for personal matters
  (especially to read your personal e-mail), do not allow family members or other third-party access to these devices

- When logging into online accounts always **verify the domain name** visible in the address bar. A domain name is a part of the address between *https://* and the first subsequent / character
- **Ignore any other requests to provide your login credentials,** even if the message looks official, and especially if it requires immediate action and threatens account deactivation
- Report all suspicious messages incoming to your business e-mail to the administrators in your organization
- You can inquire **CERT Polska** about any suspicious e-mails you receive on your personal account (https://incydent.cert.pl / cert@cert.pl)
- Be especially cautious of messages:
  - containing attachments, especially password-protected archives and Office documents
  - requiring immediate action

- **Use long password** (at least 14 characters long)
- A good way to create a long, memorable password is to **come up with a phrase** consisting of several words, e.g. 3RedScootersDrinkSmoothies
- Avoid creating passwords containing **publicly accessible or easily guessable personal information** (e.g. containing your name, birthdate, etc.)
- Change your password only **when it might have been compromised.** There is no need to change it periodically
- **Do not reuse passwords** (especially for your e-mail, online banking and other sensitive services)
  - **Use password managers.** The ones built into your browser or available on your mobile phone are secure and easy to use

- **Use two factor authentication** (2FA) where possible
  - Two factor authentication for your **e-mail and social media** is a must
  - If your current e-mail provider doesn't support 2FA - change it
  - The best method for a second factor authentication and the only one resistant to phishing is **hardware U2F token** (eg. YubiKey)

- **Verify your contact information** provided in your e-mail and social media accounts. Valid backup contact information greatly increases chances of recovering lost or hacked accounts
- If you suspect that your account has been hacked, **change your password,** check the **login history,** and **terminate all active sessions**

- Regularly **update all software,** including the operating system. Install updates immediately when they become available
- Use an **up-to-date antivirus** software
- VPN software **does not** protect against phishing and malware

- Use **end-to-end encrypted** messengers for sensitive or private conversations
- Use the **"disappearing messages"** when available - the attackers cannot steal what does not exist anymore