Are you cyber secure?

We show you which cyberrisks your firm is exposed to – and how you can protect yourself against them.

The Internet and use of email is increasingly a playground for malicious and fraudulent activity. Cyber criminals are sourcing valuable information from online activity and using this to blackmail companies, or to steal money from foreign accounts. Often, these criminals will bypass technical measures, preferring to expose weaknesses in human behavior to gain access to systems and information. In this paper, we explore current cyber risks and explain how to deal with them.

What do I have to know about cyberrisks? What are the dangers?

With certain attacks, cyber criminals can get in and out the network in a matter of hours, if not minutes.

Statistics show that the number of successful cyber-attacks continues to rise. Companies of all sizes are affected. Technical measures are the basis of every defense against cyberrisks – firewalls, antivirus software and similar, constantly updated to the state of the art. But increasingly, cyber criminals exploit nontechnical vulnerabilities, gaining access to corporate networks by targeting employees. Hence the “people factor” becomes a significant weak point. Various methods of attack are used, the most important:

- **Social Engineering:** Cyber criminals try to influence employees to reveal confidential information – often on the telephone. The attackers use publicly available information (for example from the Facebook profile of the targeted person) to get confidential business information or user data.

- **Phishing:** Cyber criminals use fake websites or e-mails to gain access to confidential information such as user names or passwords. With this stolen identity, the criminal can then manipulate data or trigger asset transfers.

- **CEO Scam:** Employees are prompted via e-mails from a seemingly legitimate senior manager to arrange cash transfers. An important part of the CEO scam is the reference to urgency and secrecy. Cyber criminals also often use fake telephone numbers to allay possible doubts.

- **Malicious software (malware):** Attackers use malware to achieve various objectives. The three most common are:
  - Access to a protected system
    (Examples: Trojan horse, backdoor)
  - Access to confidential information
    (keyloggers, spyware)
  - Deleting or encrypting data
    (virus, ransomware)

Ransomware attacks are rising. With this type of attack, the data on an affected device is encrypted and thus becomes unusable. The criminals demand a ransom in return for decryption. As in conventional blackmail, there is no guarantee that the data will be decrypted after the ransom gets paid and that the data will once again be accessible.

Trojan horses are also used frequently. This is a kind of malware that is sent as an e-mail attachment, often in the form of a Word or Excel file. When the attachment is opened, the malicious software is installed on the computer. The attacker will thus gain remote access to the server and can download confidential data or transfer money.
**How can I protect myself and my company against cyber risks?**

Vigilance is the best form of protection against Internet criminals. If you and your employees adhere to the following tips you will be able to avert a lot of harm.

- Never click on a link in an email and do not open any attachments if you do not know the sender and/or you have any doubt about the authenticity of the sender.

- Under no circumstances should you disable security mechanisms (e.g. a macro-blocker). If you are asked to do so when opening a file immediately notify your company’s security officer or system administrator.

- Never reply to e-mails from unknown people and/or unexpected senders. By answering, you indicate to potential attackers that the email address is in use, at which point they might continue their attacks.

- Do not respond to emails that either promise you material benefits (“You have won!”), try to get you to take ill-considered actions by implying urgency (“Act now!”) or try to frighten you (“Your account will be blocked!”).

- Check any link in emails before clicking on them: If you move the cursor over the link you will see the referred web address. Does it match the displayed text? Pay attention to the way it is written; in the case of URLs with several words separated by dots, the term immediately before the suffix (.ch, .com, .net) is the key factor.

- Be suspicious if content and style of an email do not match the (alleged) sender. A respectable company will not send you emails in poor English with lots of spelling mistakes.

- Be very cautious with personal information on publicly accessible platforms such as Facebook or Twitter.

Have you received an email which seems suspicious to you and which is associated with UBS – for example as the alleged sender? Please submit the email via this [form](#). Please ensure that this email contains no personal data such as account details.

**Where can I find more information about current cyber risks?**

Government agencies provide information on their websites, including the current risk situation, and offer guidance to protect yourself against the most common cyber risks.

**MELANI – Melde- und Analysetelle Informations- sicherung des Bundes** (Swiss Federal Reporting and Analysis Center for Information Security). On this website you will find a summary of current risks, tips for your protection and further information. The website is aimed at SMEs and private individuals in Switzerland. melani.admin.ch

**Europol** – this English site contains valuable guidance to protect yourself against identity theft, card fraud, malware and much more. europol.europa.eu > Media Corner > Crime Prevention

**ENISA** – The European Union Agency for Network and Information Security. On this English page you will find a wide range of content on the theme of cyber risks. enisa.europa.eu/topics

ubs.com/safety