Social engineering

To obtain confidential information, criminals often abuse the good faith, helpfulness or insecurity of their victims. Whether this involves fictitious telephone calls, fake policemen or phishing - the target of social engineering attacks is always a human being. The best protection is a "healthy dose of suspicion".

Protect yourself against social engineering attacks by...

- disclosing as little information about yourself as possible. On social networks in particular, you should only ever divulge information very sparingly.
- never letting anybody else know your passwords or codes – such as card PINs or online banking credentials. Access data and PIN codes belong to you and you alone!
- being wary when receiving requests by e-mail or telephone – especially if pressure is exerted on you. Even e-mails from known senders and telephone calls received from familiar telephone numbers can be fake!

Social engineering attacks often aim at eliciting personal or confidential information (for instance access data, passwords, etc.) from you, to then use them illicitly.

As a first step, criminals try to collect as much information about their victim as possible. That's because with this information, it is easier to mislead them. This for instance allows fraudsters to then pretend to be someone you know.

And the ideal means to obtain information is the Internet. Social networks (https://www.ebas.ch/en/social-media-and-networks/) in particular, such as Facebook, LinkedIn, Instagram, etc., contain very many personal details. Based on such data, attackers can then specifically address someone. Thanks to the information collected, they then seem trustworthy.

Generally, the only protection is to maintain a healthy dose of suspicion towards strangers – but also towards people you (seemingly) know. It is also a good idea to think carefully about the information you disclose about yourself, and who you disclose it to.

In case of suspicion, end the conversation

If you are contacted unexpectedly or if anything seems suspicious in general, do not disclose any further information and end the conversation. If anything seems suspicious with regard to your e-banking, don't divulge anything, and advise your financial institution as soon as you can. The coordinates can be found here (https://www.ebas.ch/en/partners/) .

Social engineering examples

- You receive an e-mail asking you to click on a link and then log in, or to disclose some personal details.
- Someone calls you on the telephone and would like to ask you certain questions for a survey (for instance as to how much you earn, about security measures on your computer, etc.).
- An attacker fakes the e-mail sender address and this way pretends to be someone else you know (potentially with an attachment containing malware).

- You receive an email from your boss asking you to make an urgent payment.
- At work, you are approached by someone purporting to be an IT employee who pretends having to undertake some maintenance tasks on your computer.
- Someone pretends to be an engineer (for instance working for a communication company, an electricity provider, etc.) and tries to gain access to your computer, house or company this way.
- Some social engineering attacks even involve people specifically applying for a vacancy in a company to then proceed to steal specific information.

Social engineering is a method used by attackers to try and obtain sensitive information or trigger a certain response in people by applying psychological tricks to manipulate them. The fraudsters' techniques include pressure, deceit and specifically exploiting people's trust in others. This manipulation often goes unnoticed and can basically affect anyone. That's why it's so important to stay vigilant and to protect your personal data.