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 TAN codes - not even system administrators or your boss. A password belongs to you, and you alone!
- being wary when receiving requests by e-mail or telephone. Even e-mails from known senders and telephone calls received from familiar telephone numbers can be fake!

Social engineering attacks 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, Xing, 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.

How can you effectively protect yourself?

Unfortunately, there are no technical measures protecting against any social engineering attacks. Since attackers specifically exploit human characteristics such as helpfulness, insecurity, good faith and basic trust in others, it is very difficult to discover and fend off a social engineering attack.

Generally, the only protection is a "healthy dose of suspicion" towards strangers - but also towards people you (seemingly) know. It is also often helpful to scrutinise the information you disclose about yourself, and who you disclose this to.

In case of suspicion, advise your financial institution

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

- Someone pretends to be an engineer (for instance working for a communication company, an electricity provider, etc.) and tries to gain access to your house or company this way.

- 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).
- At work, you are approached by someone purporting to be an IT employee who pretends having to undertake some maintenance tasks on your computer.
- 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 wide-spread method of snooping on confidential information. This always targets humans. There are no technical protection measures to prevent this. The only measure to take therefore is to apply a healthy dose of suspicion.