«Social Engineering» Information and Prevention

What do Social Engineering attacks look like?

- Someone pretends to be an engineer (i.e. working for a telecommunications company, 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 enter a log-in, or to disclose personal information (phishing).
- Someone calls you and pretends to run a survey to obtain sensitive information (e.g. your income, your security measures etc.).
- Someone arrives at your place of work masquerading as an IT person, and pretends he needs to undertake some maintenance on your PC.

All these attacks have the one aim of eliciting personal or confidential information from you (e.g. log-in data, passwords etc.) to then use them for illicit purposes.

Social Engineering

Social Engineering is a common method to capture confidential information, and the attack is always aimed at human beings. Frequently, someone's good faith and helpfulness , but also their insecurity are abused to obtain confidential information. Anything from a fake telephone call to people pretending to be someone else to phishing attacks is possible.

Generally, only a «healthy» dose of suspicion can help. It is also sometimes helpful to check what information you are divulging about yourself, and to whom.

Protect yourself:

- Divulge as little personal information about yourself as possible. In particular, be very economical with information on social networking sites such as Facebook, Xing etc.
- You should categorically NEVER divulge your passwords to another person, not even a system administrator or your boss. A password belongs to you, and to you ALONE!
- Be suspect of e-mail queries. Even e-mails with known sender addresses (friends) can be fake.

In case of doubt, let your finance institute know

In case you think anything looks suspicious about your e-banking, don't divulge anything, and let your finance institute know immediately. You will find their details under http://www.ebankingbutsecure.ch.

Further information: www.ebas.ch/socialengineering

«eBanking – but secure!» is offering helpful security hints for e-banking users

eBanking but secure!

You will find further practical information on measures and approaches required to ensure that e-banking applications are used securely under **www.ebankingbutsecure.ch**. The use of this website is free.

Hochschule Luzern – Informatik
Campus Zug-Rotkreuz, Suurstoffi 41b
CH-6343 Rotkreuz