How to protect yourself on social networks?

Personal information

The basic idea behind social media and networks is sharing information, photos and other personal details with «friends». However, such details can also be abused by an attacker, for instance for a «social engineering» attack. You should therefore very carefully consider any information you disclose on your profile.

Protect yourself by:

- only ever publishing information about yourself which you would also be happy to share with total strangers in the street.

- limiting access to your published information. (privacy settings)

- only accepting people as «friends» which you also actually know in real life.

- applying a healthy dose of mistrust regarding any messages received from people you don't know.

- not opening any links (documents, pictures, videos, etc.) from unsecure sources, and checking them before clicking on them.

- making absolutely sure that you are using different and strong passwords for your various services.

- using up-to-date software (browser, operating system, anti-virus software, etc.).

Social networks

Social media and networks such as Facebook and Twitter are booming. At first glance, these applications don't seem to pose any immediate threat to e-banking facilities. Due to their widespread use however, they have become very interesting for criminals, too.

Criminals often deliberately place links, abusing social media and networks to act as so-called «virus or malware spreaders» to distribute their malware. These networks could also be potentially used to capture valuable and very personal information about people, which can then be used to target victims for an attack.

Further information: www.ebas.ch/socialmedia