Social media and networks

Social media like Facebook, Instagram or YouTube are booming. At first glance, these don't seem to pose any immediate threat to e-banking. However, due to their widespread and often carefree use, they are also of interest to criminals.

Protect yourself by...

- only ever posting information you would also be happy to disclose to a complete stranger in the street, too.
- limiting access to the information you post (privacy settings).
- only accepting people as "friends" who you actually know in some other way (for instance, personally).
- applying a "healthy dose of suspicion" whenever you receive messages from people you don't know.
- not clicking on any links originating from unknown sources, and checking documents, pictures, videos etc. first before you open them.
- using different and strong passwords for different services.
- using up-to-date software (browser, operating system, anti-virus, etc.).

Hackers just love social media

Social media are frequently used by criminals as so-called "virus spreaders" for systematically placing links aimed at distributing malware.

These networks also allow them to gain insight into personal information about people, which can then be used for a targeted attack in a next step.

Personal information

You use social media to share photos and personal details with "friends". Such information though can also be abused by attackers, for instance for a "social engineering" (https://www.ebas.ch/en/social-engineering/) attack.

You should therefore consider very carefully what kind of information you disclose in your profile: Only ever post personal data which you would be happy to pass on to a complete stranger in the street as well.

A "healthy" dose of suspicion should generally be applied when using these networks. You should only ever accept friendship requests from people who you know either personally or through some other channel.

Files such as documents, pictures, videos etc. should always be checked with your antivirus software first. And this no matter whether they originate from a trustworthy or non-trustworthy source.

Posts and interactions

Please be aware that it is not just personal data published by you, but also all your posts and interactions such as likes, shares etc. which are analysed by service providers and then aggregated into a (potentially unfavourable or even plain incorrect) user profile, which they may for instance then sell on for advertising pur-

poses. These profiles they generate spread rapidly across further social networks, survive for several years and are difficult to erase, or cannot be deleted at all.

For social networks, you should therefore remember the following: Don't just communicate cautiously, but also think about what you post!

Links

One click on a link leading to a malicious website is enough to infect your device with malware (Drive-By Download (https://www.ebas.ch/en/drive-by-download/)). You should therefore think hard about whether you would really like to see the contents before opening any link, and whether this came from a trustworthy source.

Under www.getlinkinfo.com (http://www.getlinkinfo.com) you can check shortened link addresses (see Further information (#moreInfo)).

It is also vital that browser, operating system and antivirus software in particular plus all other software are always kept up-to-date ("Step 3 - prevent" (https://www.ebas.ch/en/3-preventing-with-software-updates/)).

Log-in and password

Requirements concerning a good password (https://www.ebas.ch/en/4-protecting-online-access/) also apply to social media and networks. It is absolutely necessary to treat access data confidentially.

It is also important to use different passwords for different services, too. **Never use the same password for your social media and networks as for your e-banking facility.**

To better protect your social accounts, you should also use two-factor authentification (https://www.ebas.ch/en/4-protecting-online-access/) of your respective service providers, if at all possible.

Data protection

In connection with social media and their use, great emphasis is also placed on protecting your personal information. Information and tips as to appropriate behaviour can be found on the Federal Data Protection and Information Commissioner (FDPIC) (https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/datenschutz.html) website (in German).

Recommended settings

Social media offer many configuration options. Our checklists are meant to assist you in establishing secure Facebook (https://www.ebas.ch/en/facebook-settings/), Twitter (https://www.ebas.ch/en/twitter-settings/), Instagram (https://www.ebas.ch/en/instagram-settings/) and LinkedIn (https://www.ebas.ch/en/linkedin-settings/) configurations.

Social media only seemingly have nothing to do with e-banking security, since fraudsters are not choosy as to the source of information they can tap.

It only takes a few effective measures to use these new media without having to worry about it.

Info sheet: *Download (PDF) (https://www.ebas.ch/wp-content/uploads/2020/01/socialmediaSKP_en.pdf)*

Further information for all those interested

Some social media limit the maximum length of posts published. Twitter for instance only allows 280 characters per message. To enable you to also post longer links, there are certain websites offering a service to shorten such links. For instance,

“https://www.ebas.ch/de/ihrsicherheitsbeitrag/erweiterter-schutz/114-socialengineering”

is transformed into

“http://bit.ly/P4u765”.

From this shortened address, you can no longer establish directly where this link will actually lead. This can be exploited by criminals to use shortened links pointing to infected websites.

Before clicking any shortened link, you should therefore check the original address first. You can for instance check where shortened link addresses lead on www.getlinkinfo.com (https://www.getlinkinfo.com). In addition to the original address, you will also be provided with further information on the website involved.