SKPPSC

Swiss Crime Prevention (SCP)
Haus der Kantone
Speichergasse 6
CH-3001 Bern

www.skppsc.ch

This leaflet was created in co-operation with the **University of Lucerne** and **'eBanking – but secure!'**

www.ebas.ch | www.ebankingbutsecure.ch

Lucerne University of Applied Sciences and Arts

HOCHSCHULE LUZERN

Informatik

FH Zentralschweiz

eBanking but secure!

Autumn 2019

Safe on social media

How to keep your data under control

Your police and Swiss Crime Prevention – an office supported by the cantonal ministries of justice and police.

How it works

- **Social media is open to all**
  Profiles on social media platforms are easy to set up, and can easily be faked.
- **Social media content can spread quickly**
  It is impossible to control who shares what information with whom.
- **Social media loosens inhibitions**
  Communication via smartphone, tablet and computer leads users to write things that they would never say to another person's face.
- **Social media also impacts on reality**
  Insults, lies and threats are always hurtful, and may even have consequences under criminal law – even if they are expressed 'only' on social media platforms.
- **Social media never forgets**
  Once content has been uploaded – whether words, images or sound – it can be accessed via the platform in question even years later.

What you need to know

- **Use your privacy settings**
  Each platform allows you decide what information about your account can be found and read by whom. You should therefore check your privacy settings regularly, and adjust them accordingly.
- **Use a separate, strong password for each platform**
  Never reveal your passwords to anyone else and, where possible, use two-factor authentication. A password manager will help you to create and use a separate password for each platform.
- **Report people or posts**
  If you are being harassed or insulted on a platform or by an individual, report this to the platform operators and block the person concerned. The same applies if you come across problematic content, or notice that other people are being harassed or insulted. The platform operators will review the profile or the content, and may delete it. If the content violates the law (e.g., illegal pornography, sexual harassment, threats, etc.), then please report this to the police.
- **Your personal data is being used**
  Most social media platforms only appear to be free. The real cost is higher, because you are paying with your personal data. There are companies which pay money for that data, so that they can show you personalised advertising, for example. Be aware of what personal data you would like to be passed on, and what information you want to keep confidential.

What you should do

- **Be cautious about disclosing personal information**
  Think about what information you are publishing about yourself, and what people might be able to read about you. Personal information can be used not only for advertising purposes, but also for criminal ones.
- **Be choosy about contact requests**
  Don't accept anyone onto your friends list who you do not actually know in real life. Unknown individuals are often fronts for fraudsters who use social media to identify their victims.
- **Be suspicious if you receive dubious messages and renewed requests from people who are not on your friends list**
  Ask the person – outside the context of the platform – because social media accounts can also be hacked. Criminal hackers use the account for their own purposes, for example by asking people from your friends list for financial support.
- **Don't just click on any and all links**
  Phishing and malware attacks can also be perpetrated via social media platforms. If you are suddenly asked to enter your access data or to download a file, terminate the session immediately.

For further information, visit **www.ebas.ch/socialmedia**