



NEWSLETTER

INFORMATION

SECURITY

v5

Websites and social media are the source of many kinds of information. But it is also a source for cyber criminals to approach you. The use of social media has become part of our daily lives. Social media and other websites can be mined for sensitive information.

Be aware: What goes on the Internet stays on the Internet!

Websites

Never visit websites that you don't trust, and don't click on links provided by unknown or untrusted sources. Never enter personal data in a pop-up window. By providing such data you will increase the chance of identity theft.

Social Media

Employees on social media should be aware that their postings could have effects on the company / personally. Personal information gathered from social media can be misused for example via social engineering. In that case someone pretends to be someone else, for example through a targeted (spear) phishing mail, by telephone, but also via WhatsApp or other communication platforms.

Do:

- Choose strong passwords and change when it is suspected to be leaked.
- Keep personal and work accounts separate.
- Use different passwords for personal and work accounts.
- When in doubt, always verify via another communication method (when someone request by mail, verify by calling the phone number you know).

Don't:

- Post sensitive technological or business information.
- Post personal information (e.g. birth date, address, etc.).
- Click on suspicious links.
- Talk / discuss about your company, this can have a negative impact on the company.

Remember – "If you're not paying for the product" (e.g. Facebook) - "you are the product!"



Social Media



Still have questions?

Please contact

<mailto:a.boei@tkh-airportsolutions.com>