How to: Be secure on the move with social media

Safely benefit from the new communication mediums

What are the risks?

- From disclosure of confidential company information to criminal relevance, e.g., with financial reporting data or privacy breaches.
- Infringement of copyright and intellectual property.
- Social engineering attacks, which often occur when using social media.
- Links to fraudulent websites and the dissemination of viruses via social media.
- Publication of "false" contributions in your name which may damage your reputation.

Do not publish company confidential data in social media

All information classified as "Internal", "Confidential" or "Strictly Confidential“ does not belong in public social media. Only use information classified as either “Public” or "Unrestricted".

Be alert with links that you receive via social media.

Criminals use social networks more frequently to access information and to disseminate computer viruses. Before opening an attachment, contact the sender if you didn’t expect to receive something. To avoid risks, navigate to links via another route. This applies to all services.

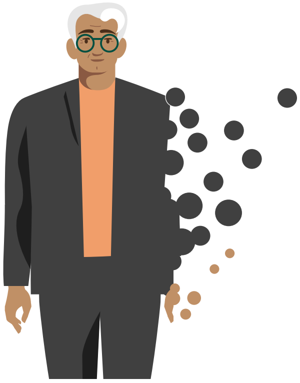
Think before you post - what’s added on the internet, stays.

Even though it may feel rewarding, it may not be a good idea to post something online when you’re emotional. Also, when you’re completing a profile for an online account, only provide necessary information.

More to keep in mind when using social media

If it’s free – you are the product

Generally, there is no fee for social media sites. You do not pay with money but with the rights to the use of the information that you add. Social media is notably used for advertising purposes and marketing, and therefore for the information you enter. This requires sensitivity to the data you’re sharing on social media and its data protection requirements. Consider precisely which information and personal data you divulge on the platform.



Identity theft and the dissemination of falsehoods

Your digital identity is the sum of all activities and information you enter online that can be tracked back to you. It is your digital footprint. Social engineering and other forms of cybercrime may try to use your digital identity in order to access sensible and secured information. Employees are not always the "final victims“; instead, they are often instrumentalized as tools for further, more dangerous attacks.

Configure your privacy settings restrictively

Make the privacy settings of each platform that you use confidential and select the appropriate settings to protect access to your data/information. Determine who really needs to have access to your personal data and an overview of your activities online? To protect your privacy, it is often sufficient to offer access only to your direct contacts.

Further Information

Check to see if your organization has further guidance on using social media.

Request further training on the secure use of social media for yourself and your team.