

Geolocation data do expose you. Social media publications easily feature geolocation data stored by a mobile device. Double-check when your device stores its location and where these data are transmitted. Turn off the GPS function unless you definitely need it at the given moment. Think hard in which situations it makes sense to reveal your whereabouts.

Remember the so-called metadata. For instance, the metadata that your photos contain may include information on the device that you use, its location, or your personal information. Familiarise with what it is that you actually publish on social media in conjunction with your publications.

Timing matters. On a general level, you may say what the day was like yesterday, but you are not allowed to tell about your tasking now or where you are going tomorrow. Do not discuss the past in detail either and refrain from saying anything that is not to be said in public.

Understand what you share and with whom. Familiarise with the equipment and apps that you use. What type of data and information do they collect and where do these data end up? Double-check also privacy settings but remember that all material posted online may always be leaked to an unintended audience. Therefore, think hard before publishing anything.

Don't be an easy target. Sustain INFOSEC. Use strong passwords, change them on regular intervals, and don't use the same password in a number of services. Use dual authorisation. Never click on unfamiliar links. Think what, if anything, should be shared on social media in the first place.

Remember to be critical, in a sound way. While on social media, you can never be sure as to whether your discussion partners are who they claim to be. To be on the safe side, draw a clear line on what can be published online and what cannot, and abide by this on all occasions.

It is not wrong to be too careful. If in doubt whether something can be published, it is always better not to. You are not obliged to use any private social media accounts.

