Where your cybersecurity is most vulnerable on the road

Checklist - on vacation

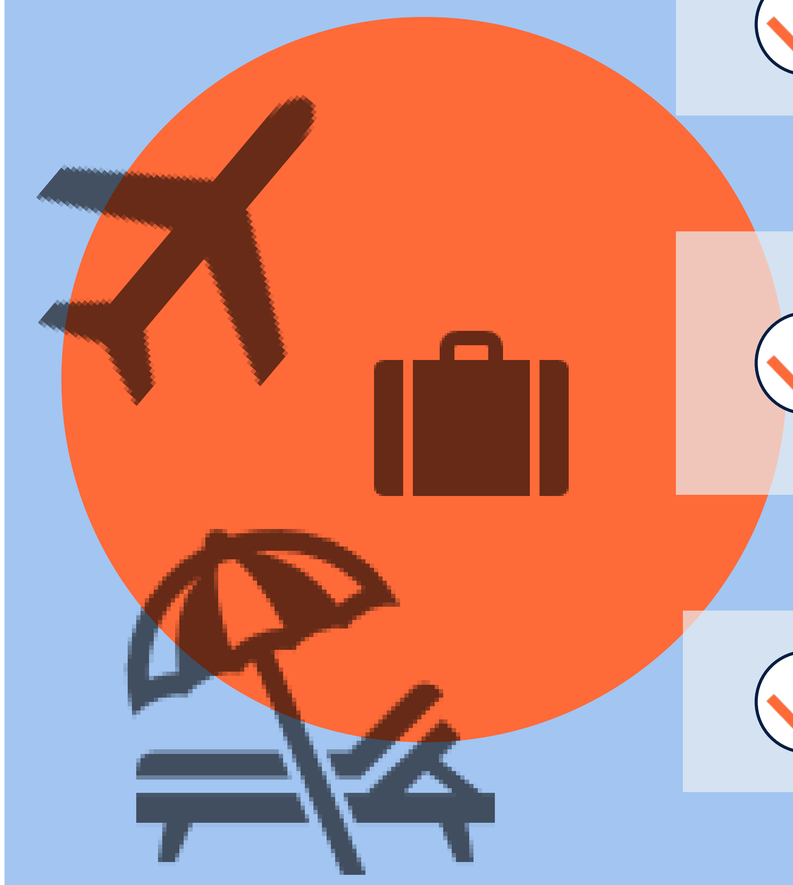
If possible, use the **mobile network for your Internet access** by using your smartphone as a wifi hotspot for your laptop. This **connection is often more secure** than the wifi offered.

When using **public wifi services**, e.g., at airports, train stations, cafés, and hotel lobbies, **pay close attention to correct, legitimate wifi access**. Because this is a common tactic used by cybercriminals to set up supposed wifi hotspots as a "**man in the middle**" in order to spy on data.

Therefore, do **not allow automatic connection** to open networks either.

Use **VPN software** for all wifi connections on the road. This prevents data traffic from being viewed so easily.

If possible, only log in to user accounts where you use **two-factor or multi-factor authentication**.



Do not use public computers to check your emails, social media accounts, etc. This is because **these computers are particularly attractive for cybercriminals** to spy on the access data of many guests and are therefore readily infected with malware.

Only **activate** interfaces such as **bluetooth** if and **for as long as you use them**.

Keep in mind that **publicly posted vacation pictures**, e.g. on Facebook, can tell criminals that you are not at home. Therefore, only **share** current pictures with a **carefully selected circle**.