Where your cybersecurity is most vulnerable on the road

Checklist - before vacation

- **Update all the devices** you want to take with you to the latest version. This applies to **operating systems, programs and apps**. Activate automatic updates to maintain this status on the road.
- Install an **access lock** on all devices via **password, code, fingerprin**t or similar.
- Create **backups** of all devices that you keep safe at home. As a tip, follow the 3-2-1 backup rule.
- Implement **two-factor or multi-factor authentication** for sensitive accounts. For example, for email accounts, social media accounts, etc. Make sure to **authenticate every time** you log in, instead of enabling options like "Trust this device".
- Optimize the **password setting** of all accounts you might access on the road. Use a **secure, unique password for each account**.
- If possible, **delete work-related data from the devices**. Alternatively, **encrypt** them. Also **encrypt important digital documents** such as airline tickets or scans of your vaccination certificate. Instructions for the Microsoft Windows and Mac OS X operating systems can be found, for example, at the German Federal Office for Information Security (BSI).

- Install and test **VPN software** that you can use for all **wifi connections while on vacation**. Several Perseus-recommended providers offer free versions or 1-month usage periods - perfect for vacation. Refer to our Homepage for more information: www.perseus.de/produkt/marktplatz
- If you don't already know, find out how to use your **smartphone as a wifi hotspot** for your laptop.
- If there is particularly sensitive data on your devices or you want to be on the safe side: **Set up the ability to remotely wipe your devices**.