

03.07.2026

What to consider when taking mobile devices on your summer holiday?

Holidays mean relaxation, spontaneous bookings, navigation, sharing pictures or just quickly doing your e-banking – with many of these things directly handled via smartphones or tablets now. And that is exactly why cyber-criminals particularly target mobile devices during the holiday season.

If you act carelessly while out and about, you risk losing your data, having your accounts hacked or suffering financial losses. You can however significantly reduce these risks with just a few simple measures.

Before your trip: Prepare your devices

Before leaving, you should check and prepare your mobile devices:

- Install the latest security updates for your operating system and apps.
- Remove any unused apps or old user accounts.
- Create an up-to-date back-up of your data and photos.
- Activate your screen lock with a PIN, finger print or your face recognition feature.
- Activate functions like “Find my” or “Find my device”.
- Save vital telephone numbers separately.
- Depending on your holiday destination, it is advisable to use a simple second mobile phone with only the basic functions you need and to leave your main private phone at home.

It is especially when travelling that a lost or stolen smartphone can quickly become a problem, in particular if it contains saved payment data, e-mails or access data.

Be wary of public WiFi networks:

Free Wifi offered by hotels, airports or cafés is handy, but frequently not secured. Cyber criminals can try to read your data when you access them or to offer fake hotspots.

You should therefore remember the following:

- Use your mobile data wherever possible.
- Only connect to official hotel or restaurant WiFi.
- Avoid sensitive activities such as e-banking via public networks.
- Deactivate automatic WiFi connections.

A VPN (Virtual Private Network) can offer additional protection but is no substitute for careful behaviour.

Holiday time is high season for phishing

During the summer holidays, faked messages all around travel, bookings or parcel deliveries will start piling in. Par-

ticularly popular:

- faked booking confirmations
- purported problems with your credit cards
- text or WhatsApp messages on purported flight changes
- faked messages from hotels or tour operators

Don't just click on any old ink without thinking, and don't open any suspicious attachments. Always closely check senders and websites.

Careful with USB charging stations

Public USB charging stations at airports or in railway stations could well be manipulated. There is a risk that data are scanned or malware is installed ("juice jacking").

The safer option:

- your own charger
- a standard socket
- a power bank

After your trip: Carry out checks

After your holiday, it is recommended to run some quick security checks:

- Review your account and credit card movements.
- Remove any travel apps or user accounts you no longer need.
- Change your passwords for important accounts if you used any public networks.
- Check all active devices and log-ins for your key online services.

Further tips on how to securely use your mobile device during your travels can be found here: <https://www.ebas.ch/en/holidays-trips/> (<https://www.ebas.ch/en/holidays-trips/>)