GUIDE

A Guide to Cybersafe Holidays

Publish date09 Jul 2025, Update date: 25 Jul 2025

Just as we turn the key to lock our doors before heading off on holiday, we should also take a moment to lock a few digital doors to safeguard our data. As new technologies emerge and our reliance on digital tools grows – from staying in touch and making payments to navigating unfamiliar places – our digital footprint expands. And when we travel beyond our usual routines, that footprint can become a golden opportunity for cybercriminals to strike while our guard is down.

Staying safe on your travels starts before the trip even begins. To avoid any unwanted surprises during your trip, make sure you follow these guidelines when you plan the trip:

Only book your stay through trusted sites

Book your accommodation, flights, and tours directly with an airline, hotel, or through a reputable booking site, agent, or tour operator. If you're not sure whether the site you found the offer on is a trustworthy company, do a quick online search for recent user reviews to avoid a scam.

Make sure that the flight, train, or accommodation really exists

Once your reservation has been confirmed, and especially if you bought tickets through a third-party website, make sure you visit the official airline or train operator website and enter your booking reference or ticket number to confirm your reservation. You can also search for the flight number in a flight tracking website or reach out to customer service to confirm there are no problems with your reservation. To check whether your accommodation really exists, cross-check the property on Google Maps, look up the property on different travel websites such as Booking or TripAdvisor, and critically consider user reviews on different sites.

Pay via credit card or use a secure payment site

For all of your bookings, always use a credit card or pay through a secure and trusted payment platform. Credit cards offer stronger fraud protection and make it easier to dispute charges if something does go wrong.

Red flags to watch out for:

- You’re asked to pay outside of a secure booking platform, such as by bank transfer or crypto.
- The company or property has no online presence outside one website.
- No confirmation email or booking reference.
- You can’t find any reviews outside of the website where you made the booking, or can only find generic, overly positive ones – with no detailed information.
- The website URL looks suspicious with misspellings of other trustworthy websites.
- You can’t find the booking reference on the official airline or train operator website.
- The company doesn’t respond to calls or emails.
- No match on Google Maps for the booked accommodation, or over-polished photos on the booking site that don’t correspond with the street view on Google Maps.

Tip: If the deal looks too good to be true, it probably is too good to be true.

Ready to go? Follow these safety measures before and during your trip:

Do's

Review the privacy settings of your social media accounts and turn off geolocation.

Make sure your personal information isn't publicly visible. Disabling geolocation helps protect your location data and limits tracking.

Back up your data, keeping both online and offline copies.

Regularly save important files to a secure cloud service and an external drive. This ensures you don't lose data in case of theft, damage, or system failure.

Make sure all your devices are protected with a password, PIN or biometric information.

Strong access controls prevent unauthorised use of your devices and help keep your personal information safe.

Update the software on your devices.

Installing updates ensures you have the latest security patches, protecting your devices from known vulnerabilities.

Review the data stored on your devices

You may be required to provide access to them when entering certain countries. Take only the minimum necessary or encrypt the data!

Shield the keypad on an ATM to protect your PIN

Use your hand or body to cover the keypad while entering your PIN to prevent hidden cameras or prying eyes from seeing it. If you spot anything unusual on the machine, don't use it.

Don'ts

Announce the dates of your trip on social media

Sharing travel plans publicly can alert criminals that your home or belongings may be unattended.

Trust public charging kiosks

Cybercriminals can modify public USB ports to install malware or steal data from your device.

Pair your phone to the computer system in a rented car

Even if it seems convenient, you may be leaving more data behind than you intended, such as your contacts, messages, and call logs, for others to access later.

Use public WiFi

Unsecured networks are easy targets for hackers. If necessary, use a VPN to add a layer of protection. Anyone can set up a wireless hotspot. If you must, use a VPN.

Access online banking or save any credentials in the browsers of public computers.

These systems may have spyware or keyloggers, putting your sensitive data at serious risk.

Leave your cards or devices unattended.

Even a brief moment is enough for theft or tampering. Always keep your belongings with you or securely locked away.

Heading back home? Don’t forget to:

Take the time to review your bank activity - check for any suspicious transactions you can’t recall making.

Delete any and all holiday-specific apps that you no longer need.

Back up your new data – you wouldn’t want to lose all the memories from your trip!

Do you suspect one of your devices or accounts may have been compromised? Better safe than sorry - change your password as soon as possible.

Tags

Crime areas:

Cyber-attacks • Forgery of money and means of payment • Fraud against payment systems

Keywords:

Public Awareness & Prevention

Document type:

How-to guide

Type:

Public awareness and prevention

Entities:

European Cybercrime Centre (EC3)