Safe on Vacation:

Protect Yourself from Digital Fraud

AKB
Asociácia kybernetickej bezpečnosti

Today you can book flights, lodging, car rentals, and tours entirely online. That convenience also attracts cybercriminals. Use the guidance below to stay safe before, during, and after your trip.

Before Your Trip

Holiday Offer Scams

- Be wary of emails or texts advertising unusually cheap vacations.
- Verify that the website is secure (HTTPS with a padlock icon).
- Avoid domains that look suspicious (for example: .xyz, .top, .live).
- Skip any offer that seems too good to be true.

Contests and Giveaways

- Confirm that the organizer clearly lists the rules, contact information, and terms.
- Never enter sensitive data (such as a national ID or Social Security number) unless you fully trust the source.
- Avoid contests that have no official website.

Fake Reservations

- Do not submit personal or payment data through links in unsolicited emails.
- Book through well-known portals, double-check the domain, and read trusted reviews.
- Prefer reservations that include cancellation and refund options.

Reservation Change Phishing

- Ignore emails claiming urgent changes to hotel or airline bookings if they contain links.
- Handle itinerary changes or check-in issues only through the airline's or hotel's official website or app.
- If you get a suspicious payment or confirmation request, contact the provider directly.
- Enter payment details only on verified portals—never through links in emails.

Airport Parking Scams

- Book parking only through official airport pages or well-known parking portals.
- Read reviews and confirm the lot's location on a map.
- Pay through secure, trusted payment gateways.

Paying Online Safely

- Use reputable portals and apps (for example, Apple Pay or Google Pay).
- Never share payment details outside official forms and payment portals.
- Consider virtual payment cards with low spending limits.
- Never share photos of your passport or ID via email or chat.
- Before you pay, confirm the page uses a valid security certificate (HTTPS with a padlock icon).

Out-of-Office (Auto-Reply) Abuse

- Use automatic replies only on your work account.
- Do not set auto-replies for unknown senders.
- Do not mention where you are going or how long you'll be away.
- Avoid sharing personal details in auto-replies—including colleagues' contact information.

During Your Trip

Suspicious Local Service Apps

- Install apps only from official stores (Google Play, App Store).
- Check ratings and reviews before installing.
- In some countries, even official apps may collect personal data—install only what you need.

(Un)Safe Wi-Fi Networks

- Public Wi-Fi can expose your logins and personal data.
- Avoid banking or accessing work email on public Wi-Fi.
- If you must use public Wi-Fi, connect through a VPN.
- Prefer mobile data—arrange a roaming plan before you leave or buy an eSIM when you arrive.
- Turn off automatic connections to networks.

Fraudulent eSIMs

- Buy eSIMs only from official carriers or reputable apps (for example, Airalo or Holafly).
- Do not scan QR codes or follow links from random flyers or open Wi-Fi splash pages.

Sharing on Social Media

- Avoid posting where you are and how long you'll be away while the trip is in progress.
- Share photos and stories after you return.
- Review your privacy settings.
- Arrange for someone to keep an eye on your home (ask a neighbor or family member if you do not have a security system).

Real-Time Location Sharing

- Share your location with a delay and only with people you trust.
- Turn off GPS when you do not need it.
- Tell loved ones in advance how to reach you in an emergency to reduce impersonation risks.

Lost or Stolen Devices

- Do not leave phones, tablets, or laptops unattended.
- Consider smart trackers (for example, Apple AirTag) for luggage or gear.
- Use a PIN and biometric authentication (Face ID, fingerprint).
- Enable device encryption.
- Turn on remote-wipe capabilities.
- Enable a SIM PIN to prevent SIM-swapping.

QR Codes in Tourist Areas

- Avoid scanning random QR codes in public spaces.
- After scanning, verify the URL before you open it.
- Disable automatic link opening after scanning.

Public USB Charging (Juice Jacking)

- Avoid charging from public USB ports.
- Use a wall outlet instead.
- Carry your own power adapter or a USB charging-only cable.

Fake Questionnaires and Surveys

- Provide information only in official hotel or travel-agency surveys.
- Check who is running the survey before you respond.

Phishing and Fake Security Alerts

- Ignore prompts to log in from links in messages (for example, "account locked," "verify credentials," "urgent update").
- Log in only through official websites or apps.
- Turn on two-factor authentication (2FA).

Unsolicited Bluetooth Connections

- Turn off Bluetooth when not in use.
- Do not accept unknown pairing requests.
- Set device visibility to "hidden" or "contacts only."

Unsecured Hotel Computers and Printers

- Do not use public computers to access email, social media, or bank accounts.
- Delete any files you print from your USB drive afterward.
- If you must work, use your own device and a secure connection.

Social Engineering

- Be skeptical of voice or video messages that claim to be from someone you know (deepfakes exist).
- Verify requests through official channels and known phone numbers.
- Never share passwords, login codes, or MFA codes over the phone.
- If someone claims there is an urgent problem (for example, hotel or banking issues), pause and call the official number yourself.
- Avoid making decisions under time pressure—especially where money or logins are involved.

Cyberbullying — An Overlooked Risk

- Limit sharing to trusted people and friends.
- Set your profile to private where possible.
- If targeted, block the abuser and report the content to the platform.
- Keep evidence (screenshots) in case you file a police report.
- For serious harassment, contact the police or a cybersecurity professional.
- Posting photos of children on public profiles is not just unsafe — it creates a serious risk of exploitation. Such content can be targeted and misused by predators. Please respect their privacy and safety. Restrict visibility to close friends and family only.

After Your Trip

Check Your Accounts

- Review your online accounts, social networks, and online banking.
- Check recent logins for email, cloud services, and social networks.
- Look for suspicious activity and act immediately if you find any.
- Review recently used devices and locations (for example, in Google or Facebook settings). Sign out unfamiliar sessions and change your password.
- If you used a public computer during the trip, change any passwords that may have been stored or intercepted.

Check Your Devices and Network

- Update your security software and run a full scan.
- Open your home router's admin page and remove unknown devices. Change the Wi-Fi password if you have doubts.
- Remove unnecessary saved Wi-Fi networks from your phone, tablet, and laptop.
- Uninstall apps you added on the road that you no longer need.

Monitor Your Transactions

- Monitor bank statements regularly and enable payment notifications.
- Report any suspicious transaction to your bank immediately.

General Recommendations

Before You Leave

- Back up photos, contacts, and important files to the cloud or an external drive.
- Download offline maps (for example, Google Maps or Mapy.cz) in case you lose connectivity.
- Save key phone numbers on your device so they're available offline: your country's embassy, local police, and your bank's card-blocking line.
- Scan your passport and ID and store copies securely in case they are lost or stolen.

Protect Your Devices on the Go

- Install updates promptly—keep your system and apps current.
- Use reputable anti-malware software.
- Use a password manager to create and store strong, unique passwords.
- Enable 2FA/MFA wherever available.
- Turn off automatic Wi-Fi connections.
- Hide Bluetooth, AirDrop, and personal hotspot when not needed.
- Avoid public USB chargers; prefer wall outlets or your own adapter.
- Pay securely—prefer virtual cards or Apple Pay/ Google Pay.

If You Become a Victim of a Cyberattack

- Block your payment cards and contact your bank.
- Change passwords for affected services and social networks.
- Report fraud to your bank and report account misuse to the platform.
- Monitor your accounts and statements for unfamiliar charges.
- Preserve evidence—emails, texts, and screenshots can help investigations.
- File a police report as soon as you can.

Final Advice

If you are uncertain, ask an IT professional you trust or consult official sources. Fraudsters rely on people acting under stress. Slow down and verify before you act. Take a moment to verify the situation before reacting — don't let urgency trick you.

www.akb.sk | backoffice@akb.sk | 02 208 67 007