Published on *University of Colorado* (https://www.cu.edu)

Stay Cybersecure While Traveling: Avoid Public USB Charging Risks [1]

Both the FBI and TSA have issued warnings against plugging phones or devices directly into public USB charging ports, especially in airports. Cybercriminals can exploit these seemingly convenient charging stations to access your device while it charges. Once connected, they may be able to steal personal data, install malicious software, or even gain remote control of your device.

Public USB charging stations are also commonly found in train stations, hotel lobbies and shopping malls — and pose similar risks.

Safer charging options while traveling

- **Use your own charger and electrical outlet.** Bring a wall charger and plug it into a standard electrical outlet. This eliminates the data transfer risk posed by public USB ports.
- **Use a USB data blocker.** This small device acts as a physical barrier between your phone and a public USB port, allowing only power to flow through, blocking any data transfer. Simply plug the blocker into the port and connect your charging cable to it. Visit FBIJohn [2]

to learn more about the types of data blockers.

USB-C Blocker

- **Carry a portable power bank.** A fully charged power bank is a safe and convenient way to recharge devices on the go—no public ports required.

Additional cybersecurity tips for travelers

- **Enable multi-factor authentication (MFA).** MFA adds an extra layer of security by requiring a second step to verify your identity, such as a code sent to your phone. Enable MFA on all critical accounts, especially email, banking and work applications. Read more about MFA [3].
- **Be cautious about public Wi-Fi.** Public networks (e.g., in airports, hotels) are notoriously insecure. Avoid logging into sensitive accounts while connected to them. If you must use public Wi-Fi, always connect through a VPN. This helps protect your data from being intercepted by cybercriminals.
- **Keep software and apps up to date.** Software updates often include essential security patches. Set your devices to update automatically or check for updates.
- **Be mindful of what you share online.** Avoid posting travel details—like hotel names, flight times, or real-time location—while you're away. Cybercriminals can use this information to target you or your property while you're traveling.
- **Protect your family's devices.** Families often travel with multiple devices, including those used by children. Set parental controls and educate kids on the dangers of oversharing online. Make sure all family devices have up-to-date software and basic security settings enabled. Read Keep Your Family Secure Online [4] to learn more.

A little preparation goes a long way when it comes to cybersecurity on the road. By following these best practices, you can help protect your data, and your peace of mind, while traveling.

Groups audience:
Office of Information Security

Links
[1] https://www.cu.edu/security/stay-cybersecure-while-traveling-avoid-public-usb-charging-risks
[2] https://fbijohn.com/what-is-a-usb-data-blocker/ [3] https://www.cu.edu/security/multi-factor-authentication-added-protection-cybercrime [4] https://www.cu.edu/security/keep-family-secure-online