

TLP:WHITE



NCCIC

Security Tip (ST11-001)

Holiday Traveling with Personal Internet-Enabled Devices

Original release date: December 19, 2011 | Last revised: June 08, 2017

Know the risks

Your smart phone, tablet, or other device is a full-fledged computer. It is susceptible to risks inherent in online transactions. When shopping, banking, or sharing personal information online, take the same precautions with your smart phone or other device that you do with your personal computer — and then some. The mobile nature of these devices means that you should also take precautions for the physical security of your device (see Protecting Portable Devices: Physical Security for more information) and consider the way you are accessing the Internet.

The Internet is at our fingertips with the widespread use of Internet-enabled devices such as smart phones and tablets. When traveling and shopping anytime, and especially during the holidays, consider the wireless network you are using when you complete transactions on your device.

Do not use public Wi-Fi networks

Avoid using open Wi-Fi networks to conduct personal business, bank, or shop online. Open Wi-Fi networks at places such as airports, coffee shops, and other public locations present an opportunity for attackers to intercept sensitive information that you would provide to complete an online transaction.

If you simply must check your bank balance or make an online purchase while you are traveling, turn off your device's Wi-Fi connection and use your mobile device's cellular data Internet connection instead of making the transaction over an unsecure Wi-Fi network.

Turn off Bluetooth when not in use

Bluetooth-enabled accessories can be helpful, such as earpieces for hands-free talking and external keyboards for ease of typing. When these devices are not in use, turn off the Bluetooth setting on your phone. Cyber criminals have the capability to pair with your phone's open Bluetooth connection when you are not using it and steal personal information.

Be cautious when charging

Avoid connecting your mobile device to any computer or charging station that you do not control, such as a charging station at an airport terminal or a shared computer at a library. Connecting a mobile device to a computer using a USB cable can allow software running on that computer to interact with the phone in ways that a user may not anticipate. As a result, a malicious computer could gain access to your sensitive data or install new software.

Don't fall victim to phishing scams

If you are in the shopping mode, an email that appears to be from a legitimate retailer might be difficult to resist. If the deal looks too good to be true, or the link in the email or attachment to the text seems suspicious, do not click on it!

TLP:WHITE

What to do if your accounts are compromised

If you notice that one of your online accounts has been hacked, call the bank, store, or credit card company that owns your account. Reporting fraud in a timely manner helps minimize the impact and lessens your personal liability. You should also change your account passwords for any online services associated with your mobile device using a different computer that you control. If you are the victim of identity theft, additional information is available from <https://www.idtheft.gov/>.

For even more information about keeping your devices safe, read *Cybersecurity for Electronic Devices*.

Author

US-CERT Publications

This product is provided subject to this Notification and this Privacy & Use policy.