UNITED STATES DEPARTMENT OF STATE

OSAC

BUREAU OF DIPLOMATIC SECURITY

Cybersecurity Basics

Traveler Toolkit; Cyber

4/27/2018

As technical and physical cyber defenses become more robust and effective, individuals have become the increasingly weak link in the security chain. This weakness is exploited by malicious actors through threats like phishing. No matter the technology that a company installs, a data breach or ransomware attack is only one click away. The following tips describe and offer advice regarding common cyber security issues that are non-technical in nature, and are particularly relevant to individuals traveling abroad. These actionable steps can help individuals mitigate risks from a number of online threats. While individuals may suffer from cyber fatigue, cyber threats are only going to increase and a single mistake can lead to a security incident. Therefore, repetition of these precautionary measures is essential to maintaining your security.

Keep privacy settings on: Use privacy settings to maximize your online privacy, especially on social media platforms. In addition, you should disable unnecessary location services. Malicious actors can exploit any personal information they find online.

Use strong passwords: Use long passwords with a mix of characters, as weak passwords undermine other security measures. Do not write down passwords, share them, or repeat them across multiple sites, and be sure to update passwords periodically. A password management system can help you generate strong passwords and store them securely. Avoid using password recovery questions with answers that are easy to guess or could be found in a social media profile.

Encrypt your data: Use encryption to protect data stored on your devices and for communication. Consider the use of a virtual private network (VPN), which can protect online activity by shielding information on public networks from malicious activity.

UNITED STATES DEPARTMENT OF STATE
OSAC
BUREAU OF DIPLOMATIC SECURITY

Only use secure Wi-Fi: Free Wi-Fi may be convenient, but it is not secure. You have no control over the legitimacy or security of public Wi-Fi; therefore, limit connections to public internet, including at hotels, cafes, and airports, and use a VPN if possible. Disable any internet auto-connect features on your devices and delete old Wi-Fi networks.

Never leave devices unattended: The physical security of your devices is as important as the technical security. If you are away from your devices, even for a moment, whether a computer, phone, or external drive, use lock screens and passwords to protect them. Be vigilant in maintaining the physical integrity and security of your devices.

Don't plug in to your computer: Malware is easily spread through USBs, smartphones, and external drives when plugged into a device. Avoid plugging unknown external devices into your computer, and run a virus scan when you do plug something in. As external devices can carry malware, do not accept any electronic devices as gifts.

Careful with what you click: Scams can be carried out by phone, text, social media message, or email. To mitigate phishing risks, limit the amount of personal information you share. The information you share publicly can potentially help malicious actors access more valuable data. Scrutinize incoming messages, including using anti-virus software to scan attachments, and hover over links with the cursor to verify the URLs. Do not click on anything that you don't recognize or that looks suspicious in any way.

Disable Bluetooth and Wi-Fi: Malefactors can see what networks you connect to, spoof them, and trick you into connecting to a compromised network later. Therefore, keep your devices "hidden" so they are not discoverable to nearby Bluetooth users, and do not access or transmit sensitive data from a public network.

Enable 2-Factor Authentication (2FA): 2FA adds an additional layer of security to your password, which should not be considered 100% reliable as a lone security measure. Passwords can be compromised in data breaches or guessed using powerful computers. 2FA

requires an extra step whenever you log in from a new device, which reduces the ability to hack into a system using a password alone.

Use the right software: Ensure that all individuals in your network are using legitimate software with the latest security updates. Install a trusted anti-virus program and keep software, mobile operating systems, and apps up to date to maximize cyber defense effectiveness. Routinely back up data, as you may need to erase and reinstall your system if you are the victim of a security breach.

Further Information

For additional information on this report or any other questions on cyber threats and information security, private-sector organizations are encouraged to contact OSAC's Analyst for Cyber Threats & Information Security.