Staying Cyber Safe While Traveling Outside of Your Network

April 20, 2017

The FBI reported over $1 billion in victim losses from cyber-crime in 2016. Knowing criminal infiltration tactics and practicing methods to avoid potential breaches can help to achieve safe, secure device usage, even when traveling. When outside of personal or business networks, internet-enabled devices are especially at risk, yet there are precautions that can be taken and a few items to keep in mind that can inspire better decision-making when traveling.

Unsecure Wi-Fi: Cyber criminals can access devices connected to public wireless networks. Safer options include making sure that your devices don't automatically connect to networks and visiting only encrypted sites (those that begin with "https://"), or accessing sensitive materials through a device's cellular data internet

connection instead of an unknown Wi-Fi network, as one might find at a coffee shop or public transit station.

Multi-factor authentication: While it is good practice to lock devices with strong passcodes, enabling multi-factor (or two-factor) authentication for online accounts provides stronger security. This kind of verification requires additional forms of identification (such as responding to questions, physical tokens, or biometric authentication) to access data rather than a single password. Two factor authentication protects by requiring more than one piece of evidence authenticating a user's identity in order to gain access. Traditionally, this requires something tangible the user has (such as a debit card) and something that the user knows (the pin needed to access funds).

Encryption: Encryption helps protect sensitive information by adding an additional level of security to a device. Only a person with the correct encryption key can access encrypted data, preventing unauthorized users from obtaining information on a lost or stolen device.

Backing up data: Before traveling, backing up important data ensures that it will not be lost if a device is lost, stolen or compromised. Options include cloud storage or local backups to an external drive. For additional security, cloud service providers also use encryption.

Shoulder surfing: Despite the levels of encryption and protection on an internet-enabled device, criminals can easily steal information by "shoulder surfing," or looking over the shoulder of individuals conducting business or accessing personal information on their device.

Social media: Clicking on third-party applications through social media can bring threats onto a device. Additionally, enabling location sharing or posting travel information or photos to social media may alert criminals seeking to target personal property. Practicing caution while using social media can protect both digital and personal assets.

Traveling outside of personal or business networks requires taking additional precautions and security measures. For more information on staying cyber safe,

contact your Anchin relationship partner or Anthony Bracco, Partner and Leader of Anchin's Litigation, Forensic and Valuation Services Group, at 212.840.3456 or info@anchin.com.