Mobile, Wi-Fi & Travel Security

Bank of America Merrill Lynch

Maintain security while on the go:

As more and more mobile device users work on the go, the potential for cyber-fraud increases. By design mobile devices are secure. However mobile devices, as other computing devices connected to the internet, are not without risk. General user weaknesses, unsecured Wi-Fi, shoulder surfing, as well as misplacing or losing your mobile device, have the potential to make mobile users vulnerable to cyber fraud and device compromise.

What you should know

Cyber fraud is on the rise and criminals are targeting mobile users. Many mobile users do not take adequate security precautions. This lack of security due diligence leaves users vulnerable to possible identity theft and privacy loss.[1]

Top Mobile Schemes

- **Phishing Email or Text** – A fraudulent message addressed to the Mobile user with the intent to deceive user into divulging personal, or sensitive information.
- **Social engineering fraud** – Criminals use tactics to exploit your natural inclination to trust. Messages typically appears to be either from or in support of a friend or family member.
- **Inexpensive Wi-Fi Scam** –Fake hot-spots may show a pop-up window requesting a nominal fee from a credit card. This scam targets the exploitation of credit card users and compromises their data.
- **Shoulder Surfing** –Criminals can troll screens looking for passwords or other sensitive information. An especially common occurrence on mass-transit and in airports.
- **Phone Loss** – Users don't use passwords or implement biometrics at login so a mobile phone can be easily accessed by a person other than the owner of the phone.

Best Practices

Maintaining situational awareness and practicing good device hygiene is key to ensuring a safe mobile computing experience. Utilize the following tips to help keep yourself safe.

Mobile Device Security[2]

- Lock your mobile device with a strong password or use biometric protection.
- Do not access mobile or online banking through third-party applications or sites.
- Download applications only from official app stores. Avoid downloading free apps from unknown sources as they may contain malware.
- Beware of text messages or emails from unfamiliar senders containing links. As this may be a potential phishing scheme.

Wi-Fi Security

- Do not use any wireless network that is unsecured, or does not require a password.
- Do not perform any financial transaction over an unsecured network.
- Update the default password and network name on your home's wireless router.
- Avoid using public Wi-Fi networks to conduct transactions. Many public Wi-Fi networks require a password this however does not necessarily mean that they are secure.

Travel Security[3]

[1] http://blog.securedtouch.com/predictions-for-the-mobile-payment-fraud-landscape-in-2018

[2]https://www.pcworld.com/article/218671/9_ways_to_keep_your_mobile_devices_secure.html

[3] https://insights.travelandtransport.com/travel-and-transport/the-travelers-guide-to-keeping-electronic-devices-secure-at-international-borders

- Use caution when posting your whereabouts on Social Media. Posting location information can make you vulnerable to criminal activity such as burglary.
- Disable remote connectivity and automatic connection to Wi-Fi and Bluetooth. Only connect to Wi-Fi and Bluetooth connections that you trust.
- Always maintain awareness of your surroundings and utilize privacy screens when possible. Shoulder surfers can steal passwords, login ids and other critical information.
- Always back up your device before travel on a secure encrypted network. If your device is compromised wipe the data off of your device and restore from a backup.

Maintain Cyber Awareness

Cybersecurity should not only be limited to the home or office. It is important to practice safe online behavior while on the go. The more someone travels and accesses the public internet, the more cyber risks they face. No one is exempt from cybercrime however practicing good cyber hygiene can reduce your risk and provide you with a productive safe mobile experience.

For more information

For more information about Mobile, Wi-Fi and Travel Security, visit our Fraud Education site through CashPro Assistant at: http://cashprouniversity-dev.bankofamerica.com/cpocms/sites/CashProUniversity/Landing/Fraud/page.htm