Staying secure on the go

Mobile devices are a big part of our daily lives. While they make it easy to stay connected on the go, mobile devices can be a lucrative playground for cyber criminals to access personal and financial information. Here are a few tips to help you stay secure.

Devices

- Set up passcodes, or leverage touch/face ID.
- Review security and privacy settings, keep software up-to-date, and back up your data.
- Set parental controls on apps and devices.
- Beware of fraudulent texts and emails from seemingly legitimate sources (don't click on links, reply, or enter information; just delete).
- Before returning or disposing of a device, perform a factory reset to delete all data.
- At work, follow usage, storage, transportation, and disposal procedures for company devices.
- If using personal devices for work, follow your company's Bring Your Own Device (BYOD) policies.

Connectivity

- Purchase data and data plans from reputable vendors.
- At home, use a Wireless Protected Access 2 (WPA 2) network and secure, up-to-date network hardware, such as routers.
- Don't perform sensitive tasks or share financial information over public Wi-Fi.
- Replace generic network usernames and passwords given by your provider with your own unique ones.
- For company-bought devices, follow company procedures; you may need to join a Virtual Private Network (VPN).

Apps

- Download apps from official app stores and company websites to prevent downloading fraudulent copycat versions.
- Research apps to check that they encrypt your data for protection, particularly financial, communications, shopping, and smart home apps.
- Manage security and privacy settings.
- Keep app versions up to date; deactivate and delete them if no longer using.
- Consider turning off geo location and other forms of data tracking, like search history.
- Beware of add-ons and links, as they may be malicious or unsecure.
- For work, only use company-approved apps.

Stay secure and vigilant

In 2018, there was an increase in threats against mobile devices from what appear to be threat actors sponsored by nation-states to steal data. Methods include spyware in the form of copycat apps.

Spyware can obtain photos, contacts, and other personal information from your mobile devices to blackmail you, steal your identity, and/or use for wider intelligence-gathering or disruptive activities, such as fraudulent message campaigns.

Source: mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf

UnionBank®

Staying secure while traveling

Traveling poses its own cybersecurity risks. You may be more prone to using public networks or exposed to geopolitical, physical, IT, and cyber environments that are different from the ones at home. Below are a few tips to consider before, during, and after your travels to keep your personal and financial information safe.

Before

- Download your software's most recent versions and security updates.
- Turn off automatic updates and automatic Wi-Fi connectivity to prevent devices from connecting to an open malicious network.
- Bring only necessary devices, along with the correct charging cables, and avoid public charging stations.
- Before traveling abroad, familiarize yourself with cyber risks and physical risks; visit state.gov.
- Lock accounts with strong passwords and enable 2-factor authentication.

During

- If you need to use public Wi-Fi, be aware of the risk; at the very least join a network that is password-protected (i.e., at a business) and not open to any passerby. Use your own data plan, if possible.
- Data can get expensive when traveling abroad. Consider turning off your data plan and using your own hotspot.
- Keep devices on you, locked in the trunk of your vehicle (only during the day), or locked in your suitcase. Always keep your devices in sight at airport checkpoints.
- Be careful with what you do in public on your device and don't overshare information (like your location) on social media.
- Avoid public printers; if you use them, log off and delete your content from the machine. Remember your removable storage devices, such as flash drives and camera memory cards, and keep them in a safe place.

After

- Check if you missed any software updates.
- Revert to your old settings; allow your device(s) to automatically sign in to your home Wi-Fi etc.
- Beware of legitimate-looking fraudulent messages referring to your travels, don't reply or click on links.

While traveling on business

- Know the devices and data that you can transport with you, particularly if traveling abroad.
- Follow your company's procedures and other legal requirements.
- Beware of customized fraudulent emails appearing to come from a legitimate source, such as a supervisor or vendor urgently demanding sensitive information or a money transfer (these are called Business Email Compromise (BEC)). Always verify the source before you act.
- Keep tokens and badges that you may need to access your company's network remotely secure on you.

Learn more at unionbank.com/privacysecurity

UnionBank®

8914862 (11/19)