BEST PRACTICES FOR MOBILE DEVICE **MANAGEMENT AND PROTECTION**

When it comes to your mobile devices, it's likely they host a plethora of sensitive data, including your financial information, personal communications, and account credentials. If a device was to fall into the wrong hands or be accessed by a malicious actor, the consequences could be devastating. To help keep the data and information you have stored in your mobile devices secure, consider adopting these guiding principles:

1 Protect your passcode

Based on the security structure of some mobile devices, if someone obtains your passcode, they can access your device's password manager, change your account information to lock you out of your device, and even put your stored financial information to use. To best prevent the theft of your phone and passcode, consider taking the following steps:

- Cover your screen when entering your passcode.
- Use a six-digit passcode and make it more complex than 1-2-3-4-5-6.
    - Or implement a password rather than the four- or six-digit passcode.
- Enable Screen Lock, which ensures your phone "goes to sleep" after a minute or two and makes it harder to access.

2 Utilize a third-party password manager

While your device's password manager is more convenient for storing your credentials, using one separate from your device makes it more difficult for attackers to gain access to the comprehensive list of your usernames and passwords. Third-party password managers can also be used both on your phone and with a browser extension on your computer, making it easier to save and supply your passwords across all devices.

3 Enable additional protection

For the applications that allow it, creating a separate PIN number or implementing biometric verification provides an extra layer of security for your high-value information. An application's PIN should be different than your device's passcode.

4 Regularly update and upgrade your devices

By default, most devices are set to automatically receive software updates when plugged in overnight. These updates ensure your device is up to date, receives necessary security patches, and is better protected from the possibility of data theft. If you don't routinely plug in your device overnight, manually installing updates during the day is required. Once your device is no longer eligible to receive software updates or run the newest version of the operating system, it's likely time to replace it with an upgraded model.

Successful Mobile Device Management includes all these characteristics

- ✓ Protect your passcode
- ✓ Utilize a third-party password manager
- ✓ Enable additional protection
- ✓ Regularly update and upgrade your devices
- ✓ Deactivate non-utilized services
- ✓ Refrain from "pluggin in" to public systems
- ✓ Limit applications downloaded to your devices
- ✓ Be cautious and diligent

BEST PRACTICES FOR MOBILE DEVICE **MANAGEMENT AND PROTECTION**

5 Deactivate non-utilized services

For features that aren't regularly utilized, turning them off until you need to use them reduces the size of the attack service of your device. Such features include:

- Bluetooth
- Tap-to-pay
- AirDrop (Apple) or Nearby Share (Android)

6 Refrain from "plugging in" to public systems

When using your device in a public space (such as coffee shops, airports, hotels, etc.) avoid connecting to free Wi-Fi networks and using available charging stations. Instead, use your phone's personal hotspot when possible and bring a portable charger with you to avoid unwittingly allowing malicious actors to breach your device and steal your personal data.

7 Limit applications downloaded to your device

Download applications only if you intend to regularly use them. Over-installing applications just because they're available widens the attack surface of your device, so it's important to be purposeful with what you download. Additionally, review your applications periodically; if you determine you no longer use an app, delete it.

8 Be cautious and diligent

Pay close attention to what you allow when using your devices to prevent vulnerabilities from being introduced. This applies to:

- Permissions requested by applications and websites.
- What your children are doing and/or downloading if you let them use your device.
- Where QR codes originate from and lead to when you scan them.