SAFETY RECOMMENDATIONS WHEN USING MOBILE APPS

Use caution when downloading apps. Apps can contain malicious software, worms, and viruses. Beware of apps that ask for unnecessary permissions.

Protect your phone from viruses and malicious software, or malware, just like you do for your computer by installing mobile security software.

Avoid storing sensitive information like passwords or a social security number on your mobile device. Confidential company or customer information should never be stored on a personal device and only accessed using the appropriate approved tools. Keep personal information private. Lockdown your privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc. Be wary of requests to connect from people you do not know.

Always log out of apps that have financial information like your bank app or credit card app as soon as you're finished using it.

Update the software for your phone and mobile apps whenever a new version is released, which may contain critical security updates.

Use the passcode lock on your smartphone and other devices. This will make it more difficult for thieves to access your information if your device is lost or stolen. Enable the "Find your device" feature, if available.

Always lock your device when it's not in use or set it to lock automatically after being idle for a set amount of time. For even better security, set your device to erase all data after 10 bad password attempts.

Clear your mobile device before you donate, sell or trade it using specialized software or using the manufacturer's recommended technique. Remove personal information before replacing your phone or tablet. Don't rely on carriers, recycling firms or phone deposit banks to "clean" your device before disposal or resale to third parties. Follow the manufacturer's instructions to remove all personal information from your device before decommissioning it.

Beware of mobile phishing. Avoid opening links and attachments in emails and texts, especially from senders you don't know. And be wary of ads (not from your security provider) claiming that your device is infected. The small screen size of smartphones makes it even harder to spot whether a site is legitimate. If you wish to access a website, type in the address yourself rather than clicking an email link. **Watch out for public Wi-Fi**. Avoid online shopping, banking or other activities that require use of sensitive information when using public Wi-Fi. Use your mobile network whenever possible. Always protect your home wireless network with a password. When connected to public Wi-Fi networks, be cautious about what information you are sending.

Secure your devices: Use strong passwords, passcodes or other features such as touch identification to lock your devices. Passwords should be at least 8 characters in length and a mix of upper and lowercase letters, numbers and special characters. Use different

passwords for every account. Securing your device can help protect your information if your device is lost or stolen.

Shop securely online – Avoid sending payment information or credit card numbers through email. Make sure all personal information transactions are done on a secure site. When shopping online, only use trusted, secure websites. Before providing any personal or financial information, **make sure the address bar changes from an "http" to an "https" address** and includes a padlock logo to the right or left of the browser address bar. The "s" stands for "secure," and if you double-click on the padlock logo, you'll see a digital certificate for the website. When shopping online, use credit cards, not debit cards. This will minimize the damage in the event of a compromised account.

Personal information is like money – Value it. Protect it.: Information about you, such as the games you like to play, what you search for online and where you shop and live, has value – just like money. Be thoughtful about who gets that information and how it's collected through apps and websites.

Own your online presence: Use security and privacy settings on websites and apps to manage what is shared about you and who sees it.

Now you see me, now you don't: Some stores and other locations look for devices with Wi-Fi or Bluetooth turned on to track your movements while you are within range. Disable Wi-Fi and Bluetooth when not in use.

Don't Be A Bragger: Going on your next big vacation? Posting online you're on the other side of the globe is practically a handwritten invitation for trouble. Such personal, up-to-date information like travel plans allows an attacker to combine that information with other knowledge they already have about you to attempt a timely social engineering attack against you over the phone or with email. Instead, try posting photos once you're back.