SECURING KEY ACCOUNTS AND DEVICES

Mobile Devices

That smartphone in your pocket – or your tablet or laptop – contains significant information about you and your friends and family, including contact numbers, photos and locations. Your mobile devices need to be protected. Take the following security precautions and enjoy the conveniences of technology with peace of mind while you are on the go.

Keep a Clean Machine

- **Keep security software current on all devices that connect to the internet**: Having the most up-to-date mobile security software, web browser, operating system and apps is the best defense against viruses, malware and other online threats.
- **Delete when done:** Many of us download apps for specific purposes, such as planning vacations, and no longer need them afterwards, or we may have previously downloaded apps that are longer useful or interesting to us. It's a good security practice to delete all apps you no longer use.

Protect Your Personal Information

- **Secure your devices:** Use strong passwords, passcodes or other features such as touch identification to lock your devices. Securing your device can help protect your information if your device is lost or stolen and keep prying eyes out.
- **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 WiFi or Bluetooth turned on to track your movements while you are within range. Disable WiFi and Bluetooth when not in use.

Connect with Care

- **Get savvy about WiFi hotspots:** Public wireless networks and hotspots are not secure, which means that anyone could potentially see what you are doing on your laptop or smartphone while you are connected to them. Limit what you do on public WiFi, and avoid logging in to key accounts like email and financial services. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection.
- **When in doubt, don't respond:** Fraudulent text messages, calls and voicemails are on the rise. Just as with email, mobile requests for personal data or immediate action are almost always scams.

Find more information at https://www.staysafeonline.org