AICPA Private Companies Practice Section

# Protecting your mobile devices

## October 2018 edition of PCPS *IT Corner with Roman*

Roman H. Kepczyk, CPA, CITP, CGMA

The use of mobile devices such as smartphones and tablets have become a standard operating practice for most CPAs who use them to access critical firm information and resources when they are away from the office. Unfortunately, many firms take a non-standard approach to allowing these devices to connect to the firm's resources which could inadvertently put the firm's information and network at risk. The solution is to develop a comprehensive mobile device policy and mandate adherence to security best practices. Below are considerations for protecting your mobile devices.

- **Mandate strong passcodes/access:** Mobile device passwords and passcodes should be unique avoiding home addresses, birthdays, and other easy to guess numbers that a thief could find out by searching through the user's online profile.
- **Don't share access:** Users shouldn't give others access to their mobile device and should change the code after the firm's IT support personnel do any maintenance (which they should automatically mandate if they access the device).
- **Utilize screen locks:** Screen locks should be setup and configured to wipe the information on the device after a set number of failed attempts (usually 5-7). The screen should also automatically lock when not used for a short period of time (i.e. 1 or 2 minutes) requiring the user to re-enter the code or a biometric equivalent (fingerprint scan or face scan).
- **Report theft or loss of device:** Users must contact their IT department immediately to remotely wipe the mobile device if it is lost or stolen (or contact their mobile service carrier if the firm is not responsible for maintaining the device).
- **Turn off geotagging:** A surprising number of applications include the GPS coordinates with photos, texts, or social media usage which can tag your location with amazing accuracy. These geotags can be nefariously used to identify when the user is away from home on vacation or at a confidential client meeting (providing the exact office address).
- **Keep firmware/applications current:** Make sure the smartphone is set to automatically update the latest versions and patches of the device's operating system (i.e. Android, Mac iOS) as well as the applications utilized (including a firm recommended antimalware program). It is also important to educate users that when they are prompted to run any update that includes a security patch that they do so as soon as possible.
- **Encrypt data:** Users should be shown how to verify that data encryption is turned on their mobile device. While most current smartphones have this feature automatically setup, older legacy smartphones did not mandate this, so users should be shown how to update the operating system and turn on encryption.
- **Automatically sync/backup device:** Smartphones can be dropped and broken, lost or stolen so it is imperative that the data on it is protected and the best way is to automatically back it up via the Internet. Be sure that the standards for the backup system follow the firm's standards on encryption and passwords.

- **Don't share Personally Identifiable Information (PII):** It goes without saying but users need to be reminded not to send texts or emails with any confidential client or personal information such as bank accounts, passwords, or social security numbers including information captured in photographs or attachments.
- **Avoid Wi-Fi for sensitive transactions:** Personnel should be trained to utilize the smartphone's mobile hot spot rather than Wi-Fi for accessing firm data securely, doing online banking, or shopping where the user's bank account or credit card information may be entered, and always verify being on a secure connection when entering any sensitive information (https: or shttp: should be in the website address header). User's should also disable Bluetooth and not select auto-connect to Wi-Fi which minimizes the risk of accessing malicious connections to the Internet.
- **Use reputable application stores:** Personnel should only download applications from authorized providers such as Google Play for Android or the Apple App Store for iPhone programs. This minimizes the risk of downloading clone applications that provide free versions of popular applications but can be rife with ransomware that will make your data inaccessible or malware that captures your login name and password as well as monitor all your activities.
- **Review applications before installing:** Be sure to search (Google) comments and ratings on applications before installing them on a mobile device. This may tip users to hidden pitfalls as well as help the user better understand what the application does and what the vendor does with the information.
- **Don't allow "Jailbroken" or "Rooted" phones:** Jailbreaking is a term to describe Apple iPhones (rooting describes Android devices) that have been modified to work on different carriers or to add features not allowed by carriers. Rooting and Jailbreaking overrides the security features within the operating system of the smartphone, compromising the device and usually voids the warranty so they should never be allowed.

Mobile devices are an important addition to a CPA's arsenal of business tools and applications and will become increasingly important as the profession continues to become more global and mobile. It is the responsibility of all users to make sure these tools are securely and properly utilized.

*Roman H. Kepczyk, CPA, CITP, CGMA is the Director of Firm Consulting for Xcentric, a division of Right Networks and works exclusively with CPA firms to implement today's leading best practices and technologies incorporating Lean Six Sigma methodologies to optimize firm production workflows. Roman is also the author of "Quantum of Paperless: A Partner's Guide to Accounting Firm Optimization" which is available at Amazon.com and to members of the PCPS.*