CPA
Practice Advisor

from reputable companies, and you downloaded them through an app store. They had to be ...

Sep. 02, 2015

Phone in one hand, coffee in the other you check your Facebook, glance at today's news on your CNN app, and view email. Maybe you do a quick check on your bank account balance, or take advantage of an online sale from your favorite store. Then you pull up your Waze app to find the best route to the office.

On your lunch break you play Candy Crush, then check your personal email. Did you count how many times your data was vulnerable? Probably not. These apps are all

from reputable companies, and you downloaded them through an app store. They

complex. In fact, 40% of devices don't even have passwords at all. Finding a balance between complex passcodes and easy access to your phone (and apps) is recommended, but may not be practical.

3. **Coffee, bagel, and a side of free WiFi:** Locations like coffee shops and airports offer free, unsecured WiFi connections allowing an easy pathway for nearby hackers to mine your data. Many consumers use free, unsecured WiFi. One study showed that 50% of devices connect to unsecured WiFi at least once a month in the U.S.1
4. **Installing untrustworthy applications:** Installing an app from a pop-up ad or through a third party site (not a first party application store like Google Play or Apple App Store) increases the risk of malware infecting your device.
5. **Delaying updates:** Waiting to update operating systems or applications increases the risk that your data will be compromised by the vulnerability the application is trying to repair. Sometimes the update released for applications contains better security measures. Same holds true for operating systems; updating when the release has been issued is a recommended best practice.

What does mobile security mean for consumers?

For the first time in history, more than 25% of the global population will use smartphones in 2015, surging to more than one-third of consumers worldwide by 2018.2 The rapid rise of mobile devices translates to the increased use of mobile applications on these devices. Therefore, more and more sensitive and personal data is now being stored on our mobile devices. Mobile devices offer a broad attack surface, attack methods are constantly evolving, and the security solutions that worked for traditional computing (i.e. laptops and workstations) just don't translate to mobile.

Mobile apps are pervasive. They are being created and downloaded at a staggering rate. It is estimated that 179 billion apps will be downloaded in 2015.3 That's a 41%

increase over 2014 download totals. Plus, more than 60,000 new apps are added to

1. Games
2. Shopping
3. Weather
4. Social
5. Transportation

Think about mobile security falling into two buckets for consumers: physical loss/theft and data theft. Often, the data on a lost/stolen mobile device is more valuable than the device itself. You can quickly and easily purchase insurance for a physical loss of your mobile phone, but you have to make smart choices about how you use your mobile device to protect your data.

10 ways to secure your mobile device

Mitigating mobile security risk is critical to protecting yourself. Here are 10 steps you can take to secure your mobile phone, and protect your data:

1. **Know what data is being collected by applications.** According to the FTC, some apps may be able to access your phone and email contacts, call logs, internet data, calendar data, data about the device's location, the device's unique IDs, and information about how you use the app itself.5
2. **Know how your data is being used by applications.** Low data security is (unfortunately) a common problem today. When your device and apps send data without protecting it with encryption, the data can be easily intercepted.
3. **Add a passcode, PIN, or pattern lock.** This helps protect your data from an attacker who gets ahold of your phone, even if the app developer didn't properly secure the data.
4. **Use different passwords for sites and apps.** If you use the same passwords for banking, social media, email, etc., then a hacker only needs to figure out one password to gain access to your identify.

5. **Logout of your applications.** If your application requires a login, ensure that you

gaining access to your account.

8. **Update your operating system and apps when new versions are available.** Operating system updates typically include patches to known security vulnerabilities. Attackers can exploit these vulnerabilities if you do not upgrade your OS.
9. **Avoid unsecured WiFi.** This helps protect against attackers that want to steal your data over networks.
0. **Use an app that provides you visibility into what apps are doing with your data.** The NowSecure Mobile App provides insight into what apps are sharing your data insecurely, what vulnerabilities may be affecting your device, and provides tips to secure yourself. A new version will be coming Fall 2015.

Employing these few steps to securing your mobile phone will lessen the risk that someone can steal your information.

———————

By Andrew Hoog is the co-founder & CEO of NowSecure.

Accounting • Security • Software