WHAT’S ON YOUR SMARTPHONE OR TABLET?

When you look at your mobile device, do you see a computer in your pocket? One that may connect automatically to unsecure wireless, while it contains banking information, credit card numbers, contact information, and other sensitive data? Do you additionally use it for work purposes, and possibly have sensitive emails stored on it?

Cybersecurity experts agree that smartphones and tablets are the new “weak spot in the battle against cyber-criminals” (Bloomberg Technology, January 2015).

Help is on the way

Our office is committed to providing the best and latest mobile device security awareness information to UA faculty, staff and students. Read on to learn about threats, and what you can do to protect your information and devices.
Your Device is a Target

Having your smartphone or tablet lost or stolen is inconvenient, but losing it can be the least of your worries. The information contained on your device is far more valuable than the device – both to you, and to the bad guys.

Consider the following:
- 5.2 million smartphones were lost or stolen in the U.S. in 2014. (Consumer Reports)
- #1 of IT’s weakest security links are perceived as mobile devices, followed by social media. (CyberEdge Group)
- 25% of all mobile devices encounter a threat each month. (Skycure)

Why are Hackers Targeting Mobile Devices?

According to the Pew Research Center, nearly two-thirds of Americans are now smartphone owners. For many, this is their primary entry to the online world. Increased use of smartphones and tablets, coupled with the owners’ lack of awareness of the risks involved in using these devices, has created a target-rich environment for the bad guys.

While the news is full of grim accounts of how these portable “computers” in our pockets have become a hackers’ playground, becoming aware of the risks and how to mitigate them will take you far in protecting your information.

UA Information Security’s Tips to Mobile Device Security

Over the next two months, we will outline what you can do to secure your devices, and protect your identity, privacy, and the University’s data (if you use your device for University business). Here are our top 5 tips:

1. LOCK IT with a PIN, password, or pattern
   - While there are many ways to keep your data safe from virtual attacks, none of those measures help if someone can physically grab your device and access your data. Even if you leave your device for a moment, be sure that it is locked, as it can take very little time for someone to copy your data. Lock it up, just as you would your house, car, or other valuable items.

2. Install security software
   - Not just computers need security software! Hackers target tablets and smartphones as well. Installing security software goes a long way to protecting your information. This applies to all brands (including Apple!).

3. Manage your apps
   - Download: Make sure to only download Apps from trusted sources. Those sources try to ensure that no malicious apps can be downloaded.
   - Update: Always update your apps. These updates often fix vulnerabilities found since the last patch. This goes double for your operating system (OS)!
   - Uninstall: If you don’t use an app, uninstall it!

4. Use a "find your phone" tool
   - Not only can these tools help you find your missing phone, they can also help make sure your data is secure. Make sure to use one that has a data wipe tool to ensure your privacy and security, should your device become compromised.

5. Backup -- and backup again
   - Backing up your device regularly can protect you from the unexpected. Back up twice, to an external drive and to an offsite location such as an online backup, to protect against fire, burglary, or water damage.

Check back next month for more tips on securing your devices, or go to our Mobile Device Security page!