INFOSEC

ADVISORY BULLETIN

Third Quarter 2017

Mobile Device Security

Tablets and smartphones have become the tools we use to enable our ever-increasing technology-laden personal and professional lives. These devices are mobile and very easy to use and give us the choice of countless numbers of apps to make us more available to communicate and productive. These devices and apps also open us up to more potential security weaknesses and ways in which to get hacked. In addition to shopping at legitimate websites, you want to ensure your computer or mobile device is secure. Cyber criminals will try to infect your devices so they can harvest your bank accounts, credit card information and passwords. Take the following steps to keep your devices secured:

If you have children in your house, consider having two devices: one for your children and one for adults. Kids are curious and interactive with technology. As a result, they are more likely to infect their own device. By using a separate computer or tablet just for online banking and shopping, you reduce the chance of becoming infected. If separate devices are not an option, you may want to consider separate accounts on the shared computer and ensure your children do not have administrative privileges.

Only connect to wireless networks you manage, such as your home network or networks you trust when making financial transactions. Public Wi-Fi networks available at your local coffee shop may be great for reading the news, but not for accessing your bank account.

Obtaining Mobile Apps

The first step is making sure you always download mobile applications from a safe, trusted source. Remember, just about anyone can create a mobile app, so you have to be careful where you get them. Cyber criminals have honed their skills at creating and distributing infected mobile apps that appear to be legitimate. If you install one of these infected apps, criminals can take control of your mobile device to read your emails, listen to your conversations and harvest your contacts. By downloading apps from only well-known, trusted sources, you reduce the chance of installing an infected app. What you may not realize is the brand of mobile device you use determines your options.

AMERICAN LAND TITLE ASSOCIATION
1800 M ST NW, SUITE 300S
WASHINGTON, DC 20036
P. 202.296.3671 | F. 202.223.5843
WWW,ALTA,ORG | SERVICE@ALTA.ORG

For Apple devices, such as an iPad or iPhone, you can only download mobile apps from a managed environment: the Apple App Store. The advantage is Apple does a security check of both the mobile apps and their authors. While Apple cannot catch all the bad guys or all the infected mobile apps, this managed environment helps to dramatically reduce the risk of installing an infected app. In addition, if Apple finds an app in its store that it believes is infected, it will quickly remove the mobile app. Windows Phone and Android mobile devices use different approaches than Apple. Android gives you more flexibility by being able to download a mobile app from anywhere on the Internet. However, with this flexibility comes more responsibility. You have to be more careful about what mobile apps you download and install, as not all of them are reviewed. Google's app store is called Google play, which is similar to Apple. The mobile apps you download from Google Play have had some basic checks. As such, we recommend you download your mobile apps for Android devices only from Google Play. Avoid downloading Android mobile apps from other websites, as anyone, including cyber criminals, can easily create and distribute malicious mobile apps and trick you into infecting your mobile device. As an additional protection, consider installing anti-virus on your mobile device.

To reduce your risk even more, avoid apps that are brand new, that few people have downloaded or that have very few positive comments. The longer an app has been available or the more positive comments it has, the more likely that app can be trusted. In addition, install only the apps you need and use. Ask yourself, "Do I really need this app?" Not only does each app potentially bring new vulnerabilities, but also new privacy issues. If you stop using an app, remove it from your mobile device. (You can always add it back later if you find you need it.)

Finally, you may be tempted to jailbreak or root your mobile device. This is the process of hacking into it and installing unapproved apps or changing existing, built-in functionality. We highly recommend against jailbreaking or rooting, as it not only bypasses or eliminates many of the security controls built into your mobile device, but often also voids warranties and support contracts.

Permissions

Once you have installed a mobile app from a trusted source, the next step is making sure it is safely configured and protecting your privacy. Installing and/or configuring mobile apps often require that you grant certain permissions. Always think before authorizing any access, "Does your app really need those permissions to do its stated job?" For example, some apps use geo-location services. If you allow an app to always know your location, you may be allowing the creator of that app to track your movements; perhaps they can even sell that information to others. If you do not wish to grant the permissions an app is requesting, shop around for another app that meets your requirements. Remember, you have lots of choices out there. Apple devices allow some permissions to be changed in Settings or at runtime, such as access to geo-location information. Windows and Android mobile devices are different. They present you with an all-or-nothing approach. If you do not grant all of the specified permissions, you can't install the app.

Updating Apps

Mobile apps, just like your computer and mobile device operating system, must be updated in order to remain current. Criminals are constantly searching for and finding weaknesses in apps. They then develop attacks to exploit these weaknesses. The developers that created your app also create and release updates to fix these weaknesses and protect your devices. The more often you check for and install updates, the better. Most platforms allow you to configure your system to update mobile apps automatically. We recommend this setting. If this is not possible, we recommend you check at least

every two weeks for updates to your mobile apps. However, when your apps are updated, always make sure you verify any new permissions they might require.

Your Computer/Mobile Device

In addition to shopping at legitimate websites, you want to ensure your computer or mobile device is secure. Cyber criminals will try to infect your devices so they can harvest your bank accounts, credit card information and passwords. Take the following steps to keep your devices secured:

If you have children in your house, consider having two devices: one for your kids and one for the adults. Kids are curious and interactive with technology. As a result, they are more likely to infect their own device. By using a separate computer or tablet just for online transactions, such as online banking and shopping, you reduce the chance of becoming infected. If separate devices are not an option, then have separate accounts on the shared computer and ensure your kids do not have administrative privileges.

Only connect to wireless networks you manage, such as your home network, or networks you know you can trust when making financial transactions. Using public Wi-Fi networks, such as at your local coffee shop, may be great for reading the news, but not for accessing your bank account.

Educating Kids

The number one thing you can do to protect kids is to talk to them. Know what your kids are doing online and educate them about today's risks and what they should do to protect themselves.

Safety at Home: Even with great mobility, home is where safe, online behaviors start. The younger you start talking to them, and they to you, the better. Hold regular conversations about online safety issues, even going so far as to show them actual negative events that have taken place. If you don't know what your kids are doing, simply ask. Play the clueless parent and ask them to show you what the latest technologies are and how they use them. Kids love the idea of being the teacher and will open up. For example, perhaps they are on Instagram. Ask them to show you how Instagram works; have them set up an account for you and have you follow them. Not only are you learning and monitoring what your kids are doing, you are making it that much easier for them to talk to you. In addition, ensure—to the extent that you can—all online activity takes place in central areas of the home and create time boundaries for usage. By having home computers in a central location, kids are far less likely to engage in dangerous behavior. Also, consider a central charging station for mobile devices, with the rule all mobile devices go there before kids go to bed at night.

Safety with Others: When children are away from home, they are at risk even more. Help them understand that your cyber rules apply wherever they are and communicate your restrictions to whomever you trust with their care. If they have mobile devices, check usage patterns (time and bandwidth) to see if there are signs of them taking advantage of the inherently fewer restrictions there are when away from home. You won't be able to stop all of the infractions, but your caring words will come to mind whenever their mobile devices are about to wander.

Safety in Numbers: You are not alone in this cyber watch. You should engage other parents, guardians, siblings, teachers and friends to help keep an eye out for potentially harmful behavior. Try to have your community keep up with the kids and encourage them to have positive interactions with them when they see kids starting down a dangerous path.

Finally, when kids make mistakes, treat each one as an experience to learn from instead of engaging in an immediate disciplinary action. Explain “why” each time and remind them that you are only trying to protect them from the dangers they cannot yet see. Let them know they can come to you if and when they experience anything uncomfortable in an online interaction, perhaps even have them take a screenshot to share with you. Make sure they also feel comfortable approaching you when they realize they have done something inappropriate. Keeping real-world communication open and active is the best way to help kids stay safe in today’s digital world.