CYBER SECURITY newsletter

SECURING YOUR MOBILE DEVICES

Problem

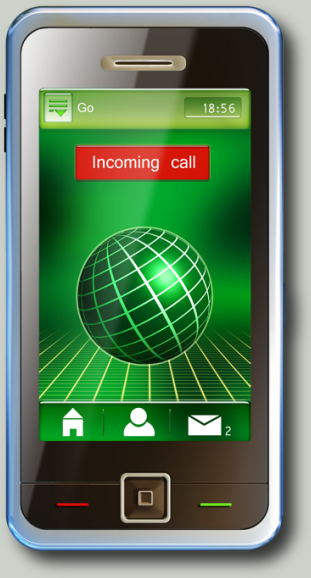
Mobile devices such as smartphones have become one of the primary ways people communicate and interact with the Internet. You can instantly talk to or message anyone else around the world. In addition, you can now carry the power of a computer in your pocket. However, with all these new capabilities come risks. In this newsletter we explain these dangers and the steps you can take to use your mobile devices securely.

Solutions

1. Passcodes. One of the greatest features about mobile devices is just how portable they are, you can take them wherever you go. However, this also makes them very simple to lose. Once lost, anyone can recover all your private information from these devices, including your emails, SMS messages, contact lists, and even your movies and photos. To protect yourself, be sure you lock your devices with a hard to guess password or passcode. This way, if you do lose your phone your information is still protected.

2. SMS Phishing. SMS allows you to quickly send and receive short text messages from anyone around the world. However, SMS messages are quickly becoming a common method for cyber criminals to attack or fool people. Just like traditional email, cyber criminals send SMS messages pretending to be a person or an organization you trust, such as your bank. They then exploit this trust to get what they want. These attacks are often called phishing attacks. While first used in email, cyber criminals are now launching phishing attacks over SMS.

One example is an SMS message telling you that you need to update your banking information and ask you to call a phone number. When you call the number, you think you are talking to your bank but you are really giving your information to cyber criminals. Another example is messages stating you won the lottery and they need your personal information to give you the money. These messages are lies designed to trick you into giving your information. Just as with email, do not trust any message that asks you for your personal information.



Using Mobile Devices Securely

Mobile devices such as your smartphone have become one of the most powerful means of communicating, in many ways replacing computers. As such, follow these steps to protect yourself.

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

Disposing Your Devices

Technology is advancing at an amazing pace. It seems like new mobile devices with must have features are coming out every month. As a result, many people replace their smartphones or tablets almost every year. However, what happens to your old device when you dispose of it? More importantly, what happens to all of your private information? After using your devices every day for so long, it has accumulated an amazing amount of very private data. Before you dispose of any mobile device, ensure that you wipe all information from it. If your mobile device does not have a wiping feature, below are two possible ways to wipe your data.

- *Delete all data (such as photos, contact information, phone call records, or SMS messages). Then overwrite this information with very large files (such as movies). Then delete the large files you just installed. This process will ensure your information is securely destroyed.*
- *Another option is to encrypt all information on the device, enable a passcode, and then turn the device off. As long as you do not share your password with anyone and your data remains encrypted, your information should be safe.*

3. Updating: Cyber criminals are constantly searching for and finding new vulnerabilities in mobile devices. This is a growing problem, especially due to the complexity and power of smartphones and tablets. Just like your computer, one of the most important steps to securing your devices is ensuring that they are always running the latest operating system. In addition, ensure that any applications you have installed are current. Be sure to update your devices at least once a week.

4. Applications: One of the most powerful advances in smartphone and tablet technology is applications. These are small programs you can download and install on your devices, adding a great deal of power and new functionality. However to protect yourself, just as with a computer, you must be sure you install, configure, and use your applications securely.

First, only install applications you absolutely need. The more applications you install, the more likely one of them is vulnerable, exposing you and your information to danger.

Second, only install well-known applications from trusted sources. New or unknown applications may be developed by cyber criminals with the intent to infect your computer. In addition, never download applications from new websites you have never heard of.

Third, never install applications advertised by SMS messages. These are usually nothing more than attempts by cyber criminals to fool you into installing their malicious applications.

Finally, once you install applications on your smart phone be sure they are configured securely. A key step is to ensure the default setting of all of your applications denies access to the Internet and your personal data. Once this is the default behavior, you can then grant access on a case-by-case basis only when specific applications need it.

5. Bluetooth: Bluetooth allows your mobile devices to wirelessly communicate with other devices, such as your headphones or with your computer. However, you must be careful how you setup Bluetooth. Be sure to enable Bluetooth only when you need it. In addition, make sure your devices are configured to not be discoverable. These steps ensure that malicious users cannot remotely connect using Bluetooth and then either steal your information or infect you. This is especially important when you are traveling in public places, such as airports, hotels, or restaurants.