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 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 the dangers and the steps you can take to use your mobile devices securely.

Solutions

1. Passcodes

One of the greatest mobile device features is 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, 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 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. 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 to update your banking information and asking you to call a phone number. When you call the number, you believe you are speaking with your bank but you are providing your information to cyber criminals. Another example is messages stating you won the lottery and they need your personal information to release the money. These messages are lies designed to trick you into providing your information. 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 and tablet, have become one of the most powerful means of communicating -- in many ways replacing computers. As such, follow these steps to protect yourself.

Idaho State UNIVERSITY

This newsletter is published by Idaho State University, for more information please contact us at:

help@isu.edu

Disposing Your Devices

Technology is advancing at an amazing pace. 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. 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 uploaded. This process will ensure your information is securely destroyed.*
- *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 they are always running the latest operating system. In addition, ensure any apps you have installed are current. Be sure to update your devices at least once a month.

4. Mobile Apps

One of the most powerful advances in smartphone and tablet technology is apps. 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 apps securely.

First, only install apps you absolutely need. The more apps you install, the more vulnerable you are, exposing you and your information to danger.

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

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

Finally, once you install an app, be sure it is configured securely. A key step is to ensure the default setting of all of your apps 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 apps need it. For example, many apps will request access to your location. Only authorize this if you need the functionality.

5. Bluetooth

Bluetooth allows your mobile devices to wirelessly communicate with other devices, such as your headphones or your computer. You must be careful how you setup Bluetooth. Be sure to turn on Bluetooth only when you need it. In addition, make sure your devices are configured to not be discoverable. These steps ensure 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.