News You Can Use

Issue 1
Nov. 2015

A periodic update from
President Greg R. Weisenstein

Smartphone Security Tips

Smartphone use is increasing exponentially – by 2017, 65 percent of all Americans will own a smartphone. But many are unaware of the cyber security risks in using a smartphone.

Frank J. Piscitello Jr., WCU's information security officer, suggests these ways to stay safe on your smartphone:

Regularly Update Your Device

Mobile malware increased 75 percent in 2014 from 2013, and further increases in malware are expected in 2015, particularly in mobile ransomware. Updated operating systems and security software are critical in protecting against emerging threats.

Enable Encryption

Enabling encryption on your smartphone is one of the best ways to safeguard information stored on the device, thwarting unauthorized access.

Use a Passcode

In case your phone ever falls into the wrong hands, don't make it easy for someone to access your important information. Enable strong password protection on your device and include a timeout requiring authentication after a period of inactivity. Secure the smartphone with a unique password - not the default one it came with. Do not share your password with others.

Do Not Automatically Use Public Wi-Fi

Do not log into accounts and do not conduct any sensitive transactions, such as shopping or banking, while using public Wi-Fi. Disable the "automatically connect to Wi-Fi" setting on your device.

Install Applications from Trusted Sources

It's been estimated that more than 75 percent of mobile applications will fail basic security tests this year. When downloading apps, be proactive and make sure that you read the privacy statement, review permissions, check the app reviews and look online to see if any security company has identified the app as malicious.

Install a Phone Locator/Remote Erase App

Misplacing your device doesn't have to be a catastrophe if it has a locater app. Many such apps allow you to log on to another computer and see exactly where the device is. Remote erase apps allow you to remotely wipe data from your device, helping minimize unauthorized access to your information in the event you cannot locate the device.

Disable Unwanted Services When Not in Use

Bluetooth and Near Field Capabilities (NFC) can provide an easy way for a nearby unauthorized user to gain access to your data. Turn these features off when they are not required.

Carefully Dispose of Mobile Devices

When you upgrade to a new device, make sure you wipe the information from your old smartphone before you sell or donate it. For information on how to do this, check the website of your mobile provider or the manufacturer.