The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Using your smartphone securely
- Smartphone security references

Your smartphone has tremendous capabilities, but with those capabilities come risks. In this month's issue we explain what those risks are and how to use your smartphone securely.

Using Your Smartphone Securely

GUEST EDITOR

The OUCH! team would like to welcome and thank Mr. Joshua Wright as our guest editor. Mr. Wright is a senior security analyst with InGuardians, Inc, a SANS senior instructor, and the lead author of SANS' wireless security course SEC617. You can follow Mr. Wright on Twitter at @joswr1ght or on his website at http://www.willhackforsushi.com.

THE PROBLEM

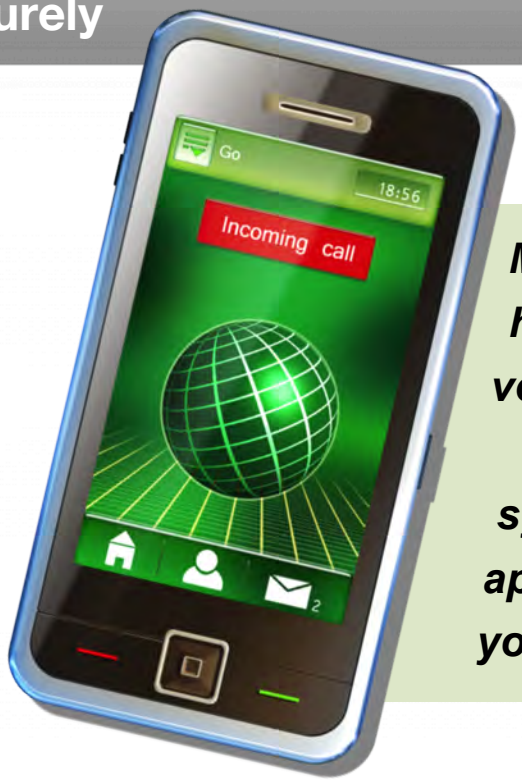
They are everywhere – iPhones, Androids, and Blackberrys. Whether you call them smartphones, handhelds, feature phones, or pocket PCs, they are cellular telephones with integrated computers. They differ from traditional cell phones in that they are also microcomputers, and like other computers, they have an elaborate operating system, can run a variety of software applications, and provide access to the web. They can send and receive e-mail (not just text messages), have embedded memory, and include a fully functional keyboard. Most newer smartphones provide one or more types of wireless network connectivity, be it 3G, 4G, Wi-Fi, and/or Bluetooth.

It is no surprise that an Internet-enabled computer you can hold in your hand that costs less than $300 is an extremely popular device. New models appear at a dizzying pace, leapfrogging each other with new features and all promising to give you the fastest, most advanced, most versatile capabilities and the greatest ease of use. The combination of popularity, enticingly low prices, rapid turnover, and new features can lead users to overlook the security fundamentals that apply to all networked computers regardless of their size.

Unfortunately, today's smartphone users are in a situation strikingly similar to that faced by computer users fifteen years ago. Security resources for smartphones are very limited and not fully developed. As a result, most smartphones lack the level of security you find on your desktop or notebook computer. Meanwhile, the complexity of smartphones continues to grow along with the number and types of network-borne threats. This makes smartphones both an easy target for bad guys and malware and a more inviting one than well-protected desktop and notebook systems.

© The SANS Institute 2011

Using Your Smartphone Securely



USING YOUR SMARTPHONE SECURELY

The most important thing you can do to protect your smartphone is to understand how to use it safely. We've put together a list of the top 10 most effective steps you can take to protect your smartphone. These apply regardless of the model of smartphone you have or the operating system it uses.

Make sure you have the latest versions of both the operating system and any apps installed on your smartphone.

1. Passwords

One of the greatest features of smartphones is how mobile they are. Unfortunately, this also makes them easy to lose. If you lose an unprotected smartphone, anyone who finds it can access your personal information, as well as information about others, and place calls at your expense until you report the loss to your carrier. Use a strong PIN, password, or passphrase to protect the contents of your handheld. If your smartphone supports data encryption, we recommend that you use it.

2. E-mail and Web

Most smartphones support e-mail and web browsing. These services entail the same threats on a smartphone as they do on any computer, including phishing attacks, malicious websites, infected attachments, and scams. If you receive an e-mail that sounds too good to be true or looks suspicious, do not respond to it or click on any embedded links it contains. Limit your browsing to well-known and trusted websites. Use SSL encryption (https://) for browsing and webmail whenever possible.

3. Wireless Networks

Your smartphone may connect automatically to wireless networks without your knowing it. Common sense says that if you are connected to a public Wi-Fi hotspot, it's probably being used by other people too, and someone could eavesdrop on your connection. Keep optional network connections (e.g., Wi-Fi and Bluetooth) turned off except when you are using them.

4. Applications

Install only the applications you need. The more applications you install, the more potential vulnerabilities you add to your smartphone. Download applications from trustworthy sources only. Attackers can create malicious applications that appear legitimate but are designed to infect your smartphone. Do not be in a hurry to install a brand new application; wait a while until it has established a good reputation.

© The SANS Institute 2011

Using Your Smartphone Securely

5. Updating

Be sure to keep both your smartphone operating system and your applications up to date. Doing so will help protect your smartphone against known threats for which there are countermeasures.

6. Documentation

Read the documentation and terms of service for each software application before you install it. They often require you to grant permission to the vendor to collect, use, and sell personal information about you, your use of the device, and your geographic location.

7. Lost Smartphone

Attach an ID label to the back of your handheld with your name, e-mail address, and an alternate phone number where you can be reached. This increases the chances of your smartphone being returned to you if you misplace it, for example, while you are going through airport security. Many smartphones support a locater service that queries the GPS on your handheld and pinpoints its geographic location. Be sure to back up your smartphone; in a worst case scenario, you can restore its contents.

8. Wiping

Remote wiping allows you to erase everything on your lost or misplaced handheld to prevent your personal information from falling into the hands of a bad guy. But be aware that your handheld will not receive the wipe command unless it is connected to the network.

9. Disposal

Be sure to erase all personal information securely from your smartphone before you dispose of it.

10. On the Job

Before using your personal smartphone to access your company's e-mail or other work-related online services, be certain that this is permitted by your employer's policies and any regulatory guidelines applicable to your industry.

ADDITIONAL SMARTPHONE SECURITY REFERENCES

NIST SP800-124 – http://preview.tinyurl.com/4urvel9
Smartphone Security – http://preview.tinyurl.com/4qu3rjj
Android – http://preview.tinyurl.com/m4xv3f
Blackberry – http://preview.tinyurl.com/48cg8pv
iPhone – http://preview.tinyurl.com/6q323p

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org.

OUCH! is published by the SANS Securing The Human program and is distributed under the Creative Commons BY-NC-ND 3.0 license. Permission is granted to distribute this newsletter as long as you reference the source, the distribution is not modified and it is not used for commercial purposes. For translating or more information, please contact ouch@securingthehuman.org.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy