IT Defender

From the OIM Information Security Program

February 2012

Issue 7

Inside this issue:

Report an Incident

If you suspect lost, misplaced or stolen equipment or a breach of Personally Identifiable Information (PII), notify your equipment manager **AND** contact the FDA IT Security Operations Center (SOC) at:

- **Email:** [redacted]
- **Toll Free Number:** [redacted]

Are you trading security for convenience?

Think your iPhone or Droid is secure? You're not alone. The majority of mobile device users feel that way… the truth is, these devices are not as secure as you might think. And we're not talking about people wanting to highjack your Angry Birds apps to erase your high scores either.

"Smartphones today handle a great quantity of private and sensitive data, in a highly portable, network-connected mobile computer. The data stored and transmitted can include security credentials, personal financial information, private communications, sensitive company data and more.

The appWatchdog tests focus on what is stored on the device. Smartphone apps handle usernames, passwords and private app data, all of which should be stored securely or not at all. In the event of a lost device or malware infection, data stored insecurely can be compromised."
– *Source: www.viaforensics.com "Mobile App Security Study"*

Perhaps the hottest topic with regard to mobile app security is banking. In fact, according to Juniper Research, over 200 million people took advantage of mobile banking in 2010, and they say that number will double by 2013. It's quick, easy and readily available from our back

Are you trading security for convenience? continued...

pockets on a moments notice. The price for our convenience is increased vulnerability, and with users storing much of their personal information on these devices, it should at the very least prompt everyone to take additional steps to protect their interests when it comes to mobile devices.

A Wall Street Journal article talks about how Citibank disclosed a major flaw in their iPhone app back in 2010. Citibank said its “iPhone app accidentally saved information—including account numbers, bill payments and security access codes—in a hidden file on users’ iPhones. The information may also have been saved to a user’s computer if it had been synched with an iPhone.” This means if you knew where to look, you could access information about someone’s bank account… scary right? Citibank has since corrected the issue with its app, and according to an article from Technology Review, it’s not an Apple-only problem and not an isolated incident.

There are security issues when it comes to iPhone apps, specifically because apps all have access to the data of other apps. Occasionally the user has to give an app permission to do certain things, but this is usually very limited. Apple is supposed to screen all the apps that go into the App Store to prevent shady apps from getting on your phone and stealing your data, but the key phrase in that sentence is “supposed to”. The bottom line is you don’t want to put the security of your personal information in the hands of a third party even if it’s Apple.

Apps on the Google operating system don’t automatically get to access each other’s information, and they are required to ask permission from the user before they access the Internet, write to the phone’s SIM card, or access GPS data. But just because an app asks you for permission, it doesn’t mean it has to tell you why it’s asking permission.

“On May 19 remind me it’s dad’s birthday”
Here’s your reminder for May 19, 2012 at 9 am:
19 Saturday May 2012
Dad’s birthday
Cancel
Confirm
Crop Photo

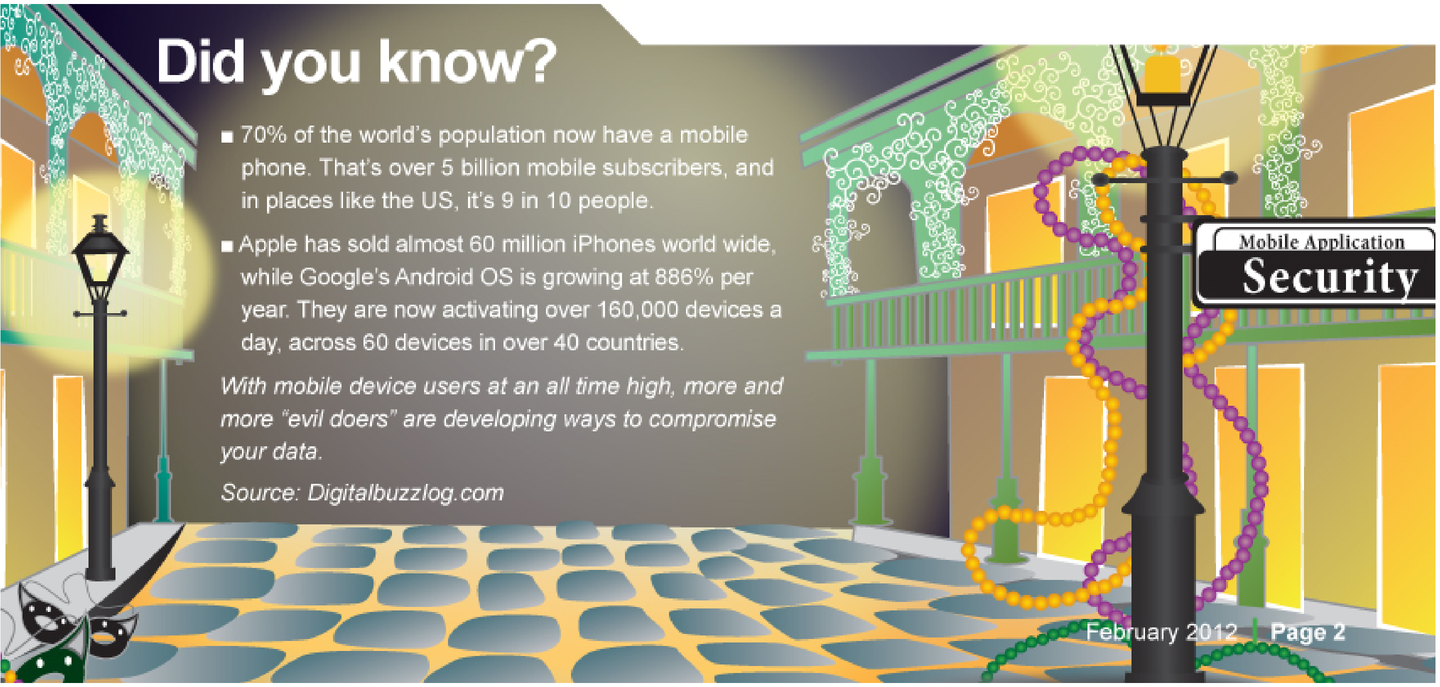
PHOTO/APPLE

How to Protect Yourself

So what can you do? Well, according to www.cio.com there are several practices you can enlist to help protect yourself.

Below we’ve listed their top five ways to protect your mobile device.

1) Don’t jailbreak your iPhone. Apple’s tight control over the iPhone and the apps on its store is a strength of the platform. However, owning a device that someone else has so much control over annoys some users who then “jailbreak” their iPhones. Be warned. Jail breaking, using a software download that changes and opens the operating system, leaves your phone vulnerable to numerous hacks that would otherwise be repelled by the locked phone.



Did you know?

- 70% of the world’s population now have a mobile phone. That’s over 5 billion mobile subscribers, and in places like the US, it’s 9 in 10 people.
- Apple has sold almost 60 million iPhones world wide, while Google’s Android OS is growing at 886% per year. They are now activating over 160,000 devices a day, across 60 devices in over 40 countries.

With mobile device users at an all time high, more and more “evil doers” are developing ways to compromise your data.

Source: Digitalbuzzlog.com

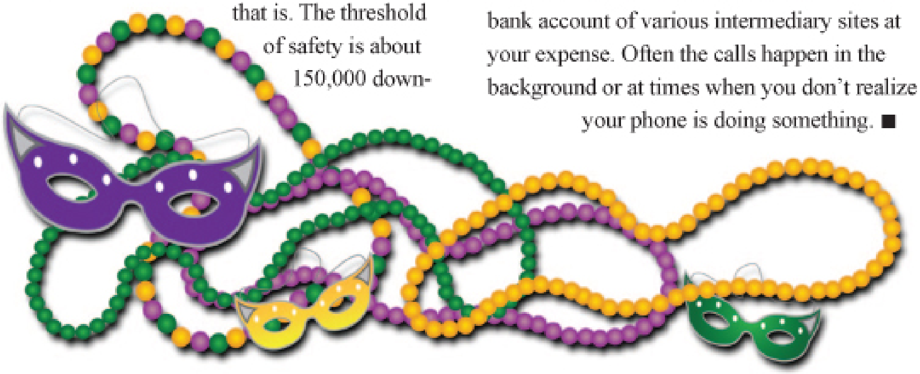
Are you trading security for convenience? continued...

2) Bank with authorized apps only. Online banking and bill pay is a great convenience, and being able to do it with a mobile device could be even more convenient. But if you opt to do so, only use apps supplied by your bank. Otherwise you could go to the ATM and find that you've got zero money in your account.

3) Only download popular apps. I know this sounds pretty stodgy. But there's a reason for it. Apps that have been downloaded a lot aren't likely to be poisoned. For that matter, they're likely to be worth downloading -- if you believe in the wisdom of crowds, that is. The threshold of safety is about 150,000 downloads. Apps on iTunes have been vetted by Apple, but even those folks can miss a threat, so it's good advice for users of any platform. And of course, read the comments about the app itself.

4) Download from reputable publishers. If you're uncertain about an app, do a quick search under the publisher's name. If you find a number of apps with good reviews and lots of downloads, chances are you're dealing with an OK outfit.

5) Keep an eye on your wireless bill. Some rogue apps do things like make expense calls to foreign numbers to fatten the bank account of various intermediary sites at your expense. Often the calls happen in the background or at times when you don't realize your phone is doing something. ■



Did you know?

- In 2011 there was a 200% increase in mobile malware!

  Source: Michael Davis -Information Week

- 75% of those surveyed in the US have never installed data protection applications or security software of any kind on their smartphones.

- 70% of smartphone owners say they feel their device is safe from hackers, malware and other types of cybercrime.

  Source: National Cyber Security Alliance (NCSA) and McAfee

Modern Malware

One of the most common misconceptions about malware is that something must be downloaded in order to infect the user's computer. People often think, "I don't download music or movies. I don't click on any links I don't recognize. I must be totally safe." Sadly, this is no longer true in today's world.

For example, one form of malware known as "Drive-by installation" can infect a computer without any further action required than simply visiting a website. The website themselves may seem completely innocuous. In the past, hackers have compromised everything from relatively obscure blogs to major news websites. Once these sites have been loaded with malware, any user who visits the site can become infected. This is one reason the FDA is so vigilant in regards to "blocking" websites on our network. Once a site is known to have been compromised, all traffic to it from the FDA network is blocked, thus eliminating that particular threat.

X

WARNING

YOUR COMPUTER IS INFECTED

Please click here to update your anti-virus with the necessary patch.

Another threat people are often unaware of is "Ransomware". A typical ransomware will infect a user's computer, often via a drive by installation, and cause a pop up to appear stating something to the effect of, "Your computer is infected!" or "Illegal material has been discovered on your computer!" These pop ups, while irritating, are essentially harmless unless the user clicks them. Once clicked, they will download a nasty virus and then inform the user that the only way to rid one's self of the malware is to either A: purchase whatever "Anti-Virus" product they have made up or B: simply wire money to the hackers. Ransomware is a crude method, but highly effective.

In summation, the threats to today's web surfer are vast and varied. Assistance from individual users is not only appreciated, but necessary. If you notice any strange behavior with your FDA computer, please do not hesitate to notify the appropriate personnel. While it is highly unlikely we will ever be able to completely nullify all threats to the FDA network, early detection can be invaluable in reducing threats of all kinds. ■

CAPTCHAs: What Are They?

A CAPTCHA is a program that can generate and grade tests that humans can pass but current computer programs cannot.

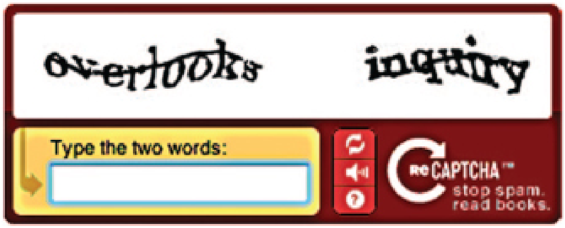
The term CAPTCHA (Completely Automated Public Turing Test To Tell Computers and Humans Apart) was coined in 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University. At the time, they developed the first CAPTCHA to be used by Yahoo.

Source: Carnegie Mellon University

Why Are They Used?

Requiring the use of CAPTCHAs makes it much more difficult for an automated computer process to perform certain actions large scale. For example:

- **Preventing Comment Spam in Blogs.** Most bloggers are familiar with programs that submit bogus comments, usually for the purpose of raising search engine ranks of some website (e.g., "buy penny stocks here"). This is called comment spam. By using a CAPTCHA, only humans can enter comments on a blog. There is no need to make users sign up before they enter a comment and no legitimate comments are ever lost!



- **Protecting Website Registration.** Several companies (Yahoo!, Microsoft, etc.) offer free email services. Up until a few years ago, most of these services suffered from a specific type of attack: "bots" that would sign up for thousands of email accounts every minute. The solution to this problem was to use CAPTCHAs to ensure that only humans obtain free accounts. In general, free services should be protected with a CAPTCHA in order to prevent abuse by automated programs.

- **Online Polls.** In November 1999, *http://www.slashdot.org* released an online poll asking which was the best graduate school in computer science (a dangerous question to ask over the web!). As is the case with most online polls, IP addresses of voters were recorded in order to prevent single users from voting more than once. However, students at Carnegie Mellon found a way to stuff the ballots using programs that voted for CMU thousands of times. CMU's score started growing rapidly. The next day, students at MIT wrote their own program and the poll became a contest between voting "bots." MIT finished with 21,156 votes, Carnegie Mellon with 21,032 and every other school with less than 1,000. Can the result of any online poll be trusted? Not unless the poll ensures that only humans can vote.

A bot (short for "robot") is a program that operates as an agent for a user or another program or simulates a human activity. (Definition by Search Security Tech Target)

- **Preventing Dictionary Attacks.** CAPTCHAs can also be used to prevent dictionary attacks in password systems. The idea is simple: prevent a computer from being able to iterate through the entire space of passwords by requiring it to solve a CAPTCHA after a certain number of unsuccessful logins.

- **Search Engine Bots.** It is sometimes desirable to keep web pages unindexed to prevent others from finding them easily. There is an html tag to prevent search engine bots from reading web pages. The tag, however, doesn't guarantee that bots won't read a web page; it only serves to say "no bots, please." Search engine bots, since they usually belong to large companies, respect web pages that don't want to allow them in. However, in order to truly guarantee that bots won't enter a website, CAPTCHAs are needed.

- **Worms and Spam.** CAPTCHAs also offer a plausible solution against email worms and spam: "I will only accept an email if I know there is a human behind the other computer." A few companies are already marketing this idea.

Source: Carnegie Mellon University ■

What is the Turing Test?

Alan Turing, an English mathematician, logician, cryptanalyst, and computer scientist addressed the problem of artificial intelligence, and proposed an experiment which became known as the Turing test, an attempt to define a standard for a machine to be called "intelligent". The idea was that a computer could be said to "think" if a human interrogator could not tell it apart, through conversation, from a human being.

A reversed form of the Turing test is widely used on the Internet; the CAPTCHA test is intended to determine whether the user is a human or a computer.

Source: Wikipedia

If you have any questions, comments or suggestions on topics to include in future newsletters, please contact...

ITSecurityAwareness@fda.hhs.gov