PENTAGON FORCE PROTECTION AGENCY

THREAT INTELLIGENCE CENTER

9000 Defense Pentagon
Washington, D.C. 20301
703-693-5000

Protect Yourself: Mobile Phone / Wi-Fi Security

iPhones / Smartphones and Identity Theft

Here are a few precautions you can take to help proactively protect your identity, in the event that your smartphone is somehow lost or stolen:

1. **Use a Strong Password:** Securing your smartphone with a password is probably the simplest precaution you can take. Of course, setting up a password on your phone will by no means protect it completely. You may also be able to set up your smartphone so that it will automatically erase all of your data after a certain number of failed password entry attempts. (Of course, if you decide to do this, you should make sure you have your data backed up somewhere else, like on your home computer.)

a. A four-digit password is better than nothing. But on Android phones and iPhones earlier than iPhone 5, a thief using the right software can crack such a code in 20 minutes, according to Charlie Miller, security engineer for Twitter and author of books on hacking and mobile security. A longer code that includes letters and symbols is far stronger.

2. **Treat your Phone like a Computer:** Always remember that your smartphone is essentially a mini computer. The security precautions you take with your smartphone should mirror the precautions you take with your personal computer. When reading emails on your phone, be careful about opening anything suspicious in order to avoid phishing attacks.

3. **Install Apps Cautiously**: One popular survey suggested that 1.6 million users had been fooled into installing what seemed to be a well-known brand-name app but was actually a malicious imposter.

a. iPhone users have one source for apps, iTunes. If you use an Android-based phone, you can get apps from numerous sources. Stick with the two most reputable, Google Play and Amazon's Appstore. You should be very wary of apps that you can download onto your iPhone for free; some criminals are able to tamper with popular apps and infect them with viruses or malware.

b. If you're an Android user, you can minimize exposing your privacy by refusing to install an app if it asks to use phone features you don't want it to use. A flashlight app, for example, shouldn't ask to access your location, like the Brightest Flashlight Free app did.

c. Install a "phone finder" app. These apps are designed to help you find your phone if it becomes lost or stolen.

4. **Be Alert to Unsecure Wi-Fi:** Be extremely cautious if you decide to use your smartphone for online banking or just accessing your bank account. Making online transactions on a public, unsecure Wi-Fi network could seriously compromise your account's security.

a. Before using any app to do business at a hot spot, check its privacy policy to see whether it secures wireless transmission of such data. Otherwise, you may disclose an account number or password to a nearby criminal.

5. **Don't Acknowledge Text Spam**: The Federal Trade Commission recently charged 29 scammers with collectively sending more than 180 million texts containing links to websites enticing users to enter personal information.

a. Links in text spam can lead to websites that download malicious software or to fake websites. The safest practice is to not click on unfamiliar links within a text. You can also go to your wireless carrier's website and ask to have texts sent over the Internet blocked. Or install an app that can block them.

6. **Turn OFF Location Tracking**: Disable it except when you need it, such as for driving directions or finding a nearby store. Most mobile phone's operating systems lets you selectively turn it off for individual apps, use that feature for greater control.

Wi-Fi Security and Your Smartphone

1. More than 20 percent of smartphone owners used their phones to make a financial transaction over a Wi-Fi connection other than the one in their home or office, according to the newest State of the Net survey.

2. How can you protect yourself from having your transactions intercepted?

a. If the transaction is being done from a website, make sure the URL starts with [https://] (no brackets), which signals a more-secure page.

b. Turn off Wi-Fi and switch your phone to 3G/4G mode (which is less risky) before you send or receive sensitive data.

c. There is the ability to purchase a Virtual Private Network (VPN), which encrypts data before sending it.

Dangers Using Public WiFi Networks

The following list contains some additional ways in which you may be in danger when using a public WiFi network:

a. Some web-based email providers (such as Yahoo) do not use HTTPS/SSL encryption for email access by default, which means that eavesdroppers can capture your login details

and view your email messages.

b. Instant messaging and FTP file transfers are vulnerable to WiFi hackers. These services transfer their data in easy to read text, including the login credentials. These login credentials and messages may be vulnerable to hackers when accessed via email software, such as Microsoft Outlook, over an unsecured network.

c. Hackers can also connect to your laptop or other WiFi device. If you use Windows XP, for instance, you are vulnerable if you have configured your system to share any folders. These folders are also shared on public networks, so other hotspot users can access them if they aren't password-protected.

d. You may also be vulnerable to man-in-the-middle attacks, where a hacker deliberately mimics a legitimate connection to intercept information from your computer. The hacker can then use that connection to snoop around your computer and pull out not just data perhaps also your user ID and password to gain access to web sites you visit.

How You Can Protect Your Data

Below are some steps you can take to help you protect your data when you use WiFi networks:

a. As a rule, you should only connect only to WiFi networks that you absolutely trust. Make sure that your communication is secure, and disconnect the WiFi network when you stop using it.

b. Turn off shared folders. In some circumstances, hackers can actually reach into your PC and access information in shared folders.

c. Run a comprehensive security suite and keep it up to date to prevent spyware and viruses.

d. Beware of the information you share in public locations. Even seemingly innocuous logins to web-mail accounts could give hackers access to your more important data, since most of us use similar passwords for almost all online activities.

e. Be sure that your home WiFi network uses encryption, specifically WPA encryption, as opposed to WEP encryption. WEP and WPA are types of security that are used to protect home wireless networks. WEP was intended to provide confidentiality comparable to that of a traditional wired network. However, several serious weaknesses in the protocol have been identified so that today it is more secure to use WPA. You should be using WiFi Protected Access, Version 2 (WPA2).

f. However, the best way to protect your sensitive information is to use a Virtual Private Network, or VPN, which encrypts the data moving to and from your laptop. The encryption protects all your Internet communication from being intercepted by others in

WiFi hotspots.

Register Your Home and Cellular Telephones with the National Do Not Call Registry

https://www.donotcall.gov - The National Do Not Call Registry gives you a choice about whether to receive telemarketing calls at home. Most telemarketers should not call your number once it has been on the registry for 31 days.