BCSI Investigations

THE INVESTIGATOR

March 2014

Volume No. 6

Issue No. 1

SMARTPHONES.....NOT ALWAYS THAT SMART!

Your smartphone contains access to your private information as well as e-mails, text messages, pictures, and much more. Therefore, the damage that can be done if you lose your phone is substantial.

You can prevent serious damage with these simple steps:

1. Always secure your smartphone with a password
A strong password is a must and encryption is highly recommended.

2. Ensure that your smartphone locks automatically
If you set up a password-protection on your phone but then leave it unlocked on your desk for 15 minutes you are still at risk. Most smartphones allow you to set them up to automatically lock themselves after a period of inactivity. Make sure you choose the shortest time you are comfortable with. Two to five minutes is better than ten to thirty, even if it does feel slightly inconvenient.

Each operating system has their own procedure; Android, Blackberry, iOS, and Windows Phone 7 all use different protocols; consult your on-line support to obtain the appropriate procedure.

This is your first line of defense. Your second line of defense is a "remote wipe". This "remote wipe" ensures that you can remotely clear all of your data including e-mails, contacts, text messages, and documents off of the device.

Android, Blackberry, iOS, and Windows Phone 7 all operate under different operating systems and must be dealt with accordingly.

3. Install security software
Your smartphone is a computerized device and shall be protected accordingly. Look for an app like Sophos Mobile Security that includes malware protection, remote data wipe, and privacy review of apps. This security software is perfect for Android operating systems.

An automatic security advisor sends you alerts about potential risks when you change a device setting. If you are in charge of securing your organization's phones and tablets, then choose a mobile device management solution like Sophos Mobile Control.

4. Only download from approved sources
The Google Play Store and Apple's App Store both take security seriously and they are careful when releasing apps.

5. Check your permissions
Many apps require more than the basic default permissions. For instance you can reasonably expect an SMS app to send and receive text messages just as a mapping app will request a GPS location. Meanwhile an app like a calculator or alarm clock that needs a network connection must be treated with extreme caution.

6. Don't miss operating system updates
It is very important that you update your operating system (OS) on a regular basis. You may want to be advised of updates rather than having them automatically installed, as early adopters sometimes experience teething problems. Meanwhile if you are the forgetful type you may prefer the automatic update.

7. Be cautious of links you receive via e-mail and text
Now that you can pick up e-mails on your phone, exercise caution when clicking on any link. Phishing scams can also entice you to click on dodgy links asking for personal information. Even simply responding to unknown text messages or e-mails can raise the criminal's interest in you, leading to more pressure for a response.

8. Encrypt your smartphone
Even when you secure your smartphone with a password, a criminal could still plug the device in to a computer and gain access to all of your personal information. Using encryption on your smartphone can help you prevent such data theft.

9. Turn-off automatic Wi-Fi connections
One of the great things about modern mobile phones is their ability to connect to the internet in various ways. Meanwhile continuously probing for wireless networks gives away information about your identity and location. Blindly connecting to un-encrypted wireless access points can let your phone leak all sorts of useful information to criminals to intercept and act upon.

Therefore, change the settings on your phone so it forgets the networks you no longer use, to minimize the amount of data leakage. You can configure your phone to automatically turn on/off wireless networks in certain places using a location aware smartphone app.

10. Turn off Bluetooth and NFC when not in use
Bluetooth and NFC (near field communication) are great in terms of connectivity, allowing you to use accessories such as wireless keyboards and headsets or make payments with a wave from your smartphone. But it does open the door for the criminals to gain access to your device and data. We should either switch these features off or put your device in "not discoverable" mode whenever possible. You also need to be careful when pairing devices and remember to never accept requests from unknown devices.

It is clear that your phone can give criminals the key to your private information and cause serious damage to your identity. An integrated comprehensive approach will ensure that you are protected from external privacy breaches.

NEWS FLASH

On-line crime on the rise
On-line crime rates are rising and a study conducted by Ponemom of 234 companies from around the world shows $11.56 million is the actual cost (a 26% increase) based on 2013 figures. Cyber-attacks refer to criminal activity conducted on the internet which includes theft of intellectual property, confiscating on-line bank accounts, creating and distributing viruses on other computers, posting confidential information on the internet, and more.

New website
Our new website will be launched by April 1, 2014. We will send you an e-mail once our new and exciting website has been launched.

Due diligence and on-line identity protection
Our new due diligence program protects you from doing business with fraudulent individuals or shady characters that you meet on-line. We have several levels of protection from individual to family as well as our small business and corporate program.

BCS Investigations
104-2420 Marine Drive, West Vancouver, BC V7V 1L1

info@picanada.ca
www.picanada.ca