Information Security Updates

Mobile Security – Best Practices for General User

According to research figures from Business Intelligence[1], the number of smartphones sold worldwide has already surpassed the number of personal computers. Two to three years from now, tablet sales are also expected to exceed personal computer sales. In less than twenty years, we have evolved from using traditional, personal computers as productivity tools to a new mobility era in which people are using mobile devices extensively for both work life and personal life.

It is foreseeable that more information such as people's contact lists, personal information, files, photos, videos, and even passwords, will be stored in mobile devices. Not only are mobile devices small, and easily transportable, but they also have high reselling values, making them the cause behind petty crimes, malicious attacks and organized syndicates.

There are a vast number of malicious and risky mobile apps targeting different platforms. However, due to Android's popularity and dominance, there are more mobile apps developed for Android compared to other mobile OS. Since the discovery of the first Android Trojan in 2010, TrendsLabs estimates in just 3 years, there are already over 1.4 million malicious and high-risk mobile apps on Android platform6.

If malicious apps, malware and insecure wireless connections infiltrate mobile devices, an attacker may be able to monitor and read messages, send out predefined messages, steal data, access and view contact lists and track locations. Some are even able to register victims for overpriced services.

In lieu of the aforementioned mobile device security threats, it is highly advised to follow certain practices like: locking a mobile device with a secure password, backing up the mobile device data, using Wi-Fi Protected Access encryption and others (refer to the below table).

I Lock device with PIN or password	VII. Keep software updated
II. Install trustworthy mobile apps	VIII. Install security software
III. Minimize installation of unnecessary mobile apps	IX. Do not follow links sent in suspicious emails or text messages
IV. Beware of wireless connections	X. Backup mobile device data
V. Physically protect devices	XI. Be cautious about privacy services
VI. Do not jailbreak or root mobiles devices	

Solutions to Security Problems in Depth

Physical Loss and Theft

Some thieves are only interested in the mobile device hardware to resell for monetary gain. Others however, try to break into the mobile device to look for valuable information such as contact information, personal information, photos and videos, which can be leveraged for other malicious criminal activities.

Physically Protect Devices
Maintain physical control to safeguard mobile devices. Do not leave the devices unattended. Keep the devices secured in bags. Users are also encouraged to activate the remote disable feature in their phones, which can completely wipe out the device's content remotely, lock the mobile and see its last active location. An example of this feature is the "Find my iPhone" default for Apple phones.

Lock Device with PIN, Password or Finger Print
If the mobile device is lost or stolen and the device is not locked, not only the information in the mobile device will be exposed, but the device can also be used to conduct online transactions, download apps and perform other actions on behalf of the victim. Some mobile devices also use the PIN or password to generate a unique key to encrypt stored data. This will add an additional layer of protection by increasing the difficulty of retrieving data from the stolen mobile device.

FACTS

The average person checks their phone up to 110 times a day by pressing the home button or unlocking the mobile device to activate the screen[13]. Some people will therefore ignore security to facilitate the use of the mobile device.

In Hong Kong, the Police handle an average of 5,000 reported stolen mobile phones every year and the number was gradually rising.[7]

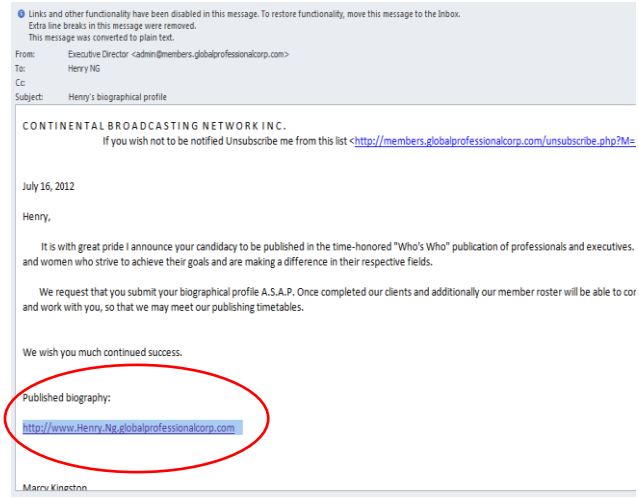
Backup Mobile Device Data
If a mobile device is broken, lost or stolen, data can be restored if the user previously backed up the mobile device by synchronizing it to a computer or cloud.

Keep in mind that if the mobile device contains data such as calendars, work files, photos, passwords and contact lists, and the user synchronizes the device with his or her home computer, this information can be compromised once the computer has been hacked or stolen.

Social Engineering Attacks

Social engineering is a technique used to trick innocent users to disclose information without the need to use any technical means to break into a mobile device. The most common social engineering attack is phishing. It is the use of email or instant messaging to acquire a victim's personal information. Below is an example of a real phishing message from the Who's Who scam[12]. The e-mail is crafted in a way that the victim is deceived into believing it is legitimate. If a user clicks on the embedded link, the user will be redirected to a web page requesting to submit personal information.

Do not follow links sent in suspicious email or text messages


Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox.
Extra line breaks in this message were removed.
This message was converted to plain text.

From: Executive Director <admin@members.globalprofessionalcorp.com>
To: Henry NG
Cc:
Subject: Henry's biographical profile

CONTINENTAL BROADCASTING NETWORK INC.
If you wish not to be notified Unsubscribe me from this list <http://members.globalprofessionalcorp.com/unsubscribe.php?M=

July 16, 2012

Henry,

It is with great pride I announce your candidacy to be published in the time-honored "Who's Who" publication of professionals and executives. and women who strive to achieve their goals and are making a difference in their respective fields.

We request that you submit your biographical profile A.S.A.P. Once completed our clients and additionally our member roster will be able to cor and work with you, so that we may meet our publishing timetables.

We wish you much continued success.

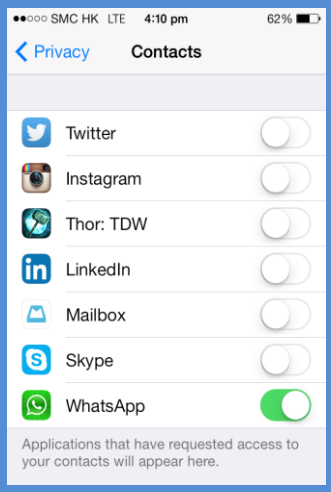
Published biography:

http://www.Henry.Ng.globalprofessionalcorp.com

Marcy Kingston

Unnecessary Access to Personal Information

In the diagram below, there is a downloaded game called "Thor: TDW". Thor wants to access contact information. Why would a game wants to access your contact information? For advertisement purposes? For cross selling purposes? Or for other malicious reasons? One should think hard before allowing a mobile app such as the "Thor: TDW" game retrieve all your contact information.



Malware

Malware is a computer contaminant that can gain access to private information on mobile phones or computer systems. Malware can sometimes appear to be legitimate software. Note that defective software is not malware, as it is not meant for harm or fraud. For an example of these disrupting programs, refer to the case studies at the bottom.

Install Security Software
To protect from malware, it is recommended that software like anti-virus or firewalls be implemented. Particularly on the Android platform, users should consider installing security software to booster the security protection. Some software can even protect from call blocking, SMS filtering, anti-data theft and viruses.

Insecure Wi-Fi

Very often, users will connect to wireless access points that pretend to be legitimate but are actually not secure. Some access points use weak encryption (e.g. WEP) and some do not even provide encryption capabilities. This means that all communications between the mobile devices and the Internet, through such access points, can be eavesdropped.

Beware of Wireless Connections – Choose Wisely.
When choosing a wireless access, users should opt for wireless connections which are from reputable sources and support Wi-Fi Protected Access 2 (WPA2) encryption.

Rogue Wi-Fi
There are malicious attackers setting up a rogue access point using a recognizable Service set identification (SSID) name pretending to be a lawful wireless access point in order to lure a victim to connect to it. Once a victim connects to a rouge access point, all the communications between the victim's mobile device and the external world can be eavesdropped by the malicious attacker.

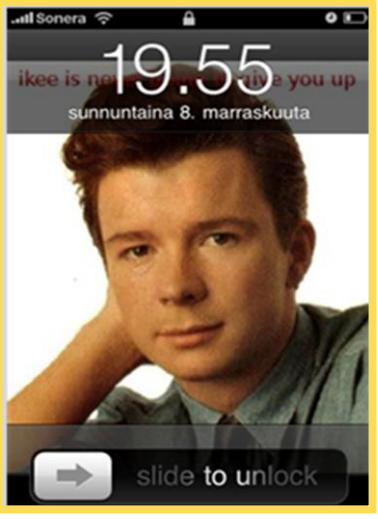
Wi-Fi Services from Hong Kong Government
In Hong Kong, the Government provides free Wi-Fi services at designated Government premises. Users can connect to two types of wireless SSIDs – *freegovwifi* which does not support encryption and *freegovwifi-e* which supports encryption. *Freegovwifi-e* should be used for wireless connection.

Pjapps malware

Targeting Android platform, Pjapps is designed to steal information, send and monitor incoming SMS messages, read and write on a user's browsing history and install software packages on open network sockets to launch attacks on web sites.

Ikee malware

Ikee could be spread over the air targeting jail-broken iOS mobile devices and SSH application installed with default password set. Ikee would change the background wallpaper of the infected iPhone to a picture of the 80's pop singer Rick Astley. Once a device was infected, the screen would lock and display a text message saying "Your iPhone's been hacked because it's really insecure! Please visit doiop.com/iHacked and secure your iPhone right now!" The victim would have to pay a ransom fee to the attacker's PayPal account in order to unlock the mobile device.



Careful on third-party app stores

Apart from "premium service abuser" malicious mobile apps, some other malicious mobile apps are posted on the app stores pretending to be from legitimate companies tricking users to download and install. There are also malicious mobile apps which are reverse engineered from the legitimate source but embedded with malicious codes and re-posted to third-party app stores tricking users to download and install.

Minimize installation of unnecessary mobile apps

According to the Google's Our Mobile Planet data, average global smartphone users downloaded 26 apps on their smartphone devices. In countries like South Korea, the number can shoot up to over 40[5]. Most of these downloaded apps go unused and are just left installed in the mobile device.

Depending on the sophistication of the mobile app developers, some mobile apps may not be well written; resulting in security vulnerabilities on the mobile devices. Users can reduce such risk by limiting the installation of unnecessary mobile apps.

Exploitation of Mobile Apps

According to TrendsLabs, out of the 1.4 million high-risk or malicious mobile apps in the Android market, 53% of these are classified as premium service abusers. Premium service abuser mobile apps are capable of accessing the SD card data of the mobile device, monitoring and reading messages, sending out predefined messages, accessing and viewing contact list and tracking locations. Some are even able to register victims to overpriced services while adware aggressively pushes ads and can even collect personal information without the victim's consent[7].

Install Trustworthy Apps
Since some apps may have hidden behaviors that can steal private data, modify user settings and initiate unauthorized messages and transactions:

- Users should only download mobile apps from legitimate app stores.
- Users should not jailbreak or root their mobile devices in order to download and install mobile apps from third party app stores.
- Users should consider to download those mobile apps with good ratings and reviews.
- Users can install security software which can detect and alert users of mobile apps containing malware and of high risk nature.
- Users should minimize the installation of unnecessary mobile apps.

Keep Software Updated
Application and software updates may include fixes to software bugs and security vulnerabilities.

Security Update of Software
For instance, Apple released an update for its iOS 6 and iOS7 operating systems to provide a fix for the SSL connection verification issue[11]. Without installing the update, iPhone and iPad devices are vulnerable to man-in-the-middle attacks, which mean attackers can spy on user connections to websites over untrusted Wi-Fi network that are supposed to be using encrypted communications.

Privacy and Caution

Some apps ask for permission to access contact information and/or location services within the mobile device. Once permission is granted, the mobile app can read all contact information and track the physical location of the mobile device.

Some mobile apps such as Google Map have legitimate reason to use a mobile device's location tracking to facilitate its service. However, other mobile apps may track the user's whereabouts for advertisement pushing and user behaviour analysis. Some apps may even collect location services data surreptitiously without user knowledge, and thus compromise the privacy of the owner of the mobile device.

References

1."Cell Carriers Launch Anti-theft Effort." IT News. 10 Apr. 2010. Web. June 2014.
2. Cocotas, Alex. "The Future of Mobile." Business Insider. 22 Mar. 2012. Web. May 2014.
3."First Case of Android Trojan Spreading via Mobile Botnets Discovered | ZDNet." ZDNet. 05 Sept. 2013. Web. June 2014.
4. "Gartner Says Worldwide Traditional PC, Tablet, Ultramobile and Mobile Phone Shipments On Pace to Grow 7.6 Percent in 2014." Newsroom. Gartner, 7 Jan. 2014. Web. May 2014.
5. H., Michael. "The Average Global Smartphone User Has Downloaded 26 Apps." Phone Arena. 06 Sept. 2013. Web. June 2014.
6. Incorporated, Trend Micro. "Cashing in on Digital Information." TrendLabs 2013 Annual Security Roundup: Cashing in on Digital Information (2013). Trend Micro. Web. May 2014.
7. Incorporated, Trend Micro. "The Invisible Web Unmasked." TrendLabs 3Q 2013 Security Roundup. Global Technical Support & R&D Center of TREND MICRO, 2013. Web. June 2014.
8. "Over the past Three Years Handset Lost Upward Trend." Hong Kong News. 06 June 2012. Web. June 2014.
9. Pidathala, Vinay, and Jinjian Zhai. "MisoSMS: New Android Malware Disguises Itself as a Settings App, Steals SMS Messages." FireEye Blog. 16 Dec. 2013. Web. 11 June 2014.
10. "Virus and Malicious Code." InfoSec. The Government of the Hong Kong Special Administrative Region, June 2014. Web. June 2014.
11. "Vulnerability Summary for CVE-2014-1266." National Cyber Awareness System. DHS National Cyber Security Divison2, 22 Feb. 2014. Web. May 2014.
12."Who's Who Scam." Wikipedia. Wikimedia Foundation, 06 June 2014. Web. June 2014.
13. Woollaston, Victoria. "How Often Do You Check Your Phone? The Average Person Does It 110 times a DAY (and up to Every 6 Seconds in the Evening)." Mail Online. Associated Newspapers, 08 Oct. 2013. Web. June 2014.