MESSAGE FORM

(INSTRUCTION: FILL-UP BOXES INSIDE DOUBLE LINES ONLY)

FOR COMCEN/SIG USE

PRECEDENCE ACTION/PRECEDENCE INFO
"PRIORITY"

FM: CG, PA

TO: All Unit Commanders
Attn: G6/Signal Officer/IS Officer

INTERNAL: All G-Staff, Personal, Special & Tech Staff, C, AOC/SAGS/XA

INFO: CSAFP
Attn: J6

GROUP:
22 December 2016

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 2212-82-2016

1. References:

   a. Command Guidance, and;
   b. VAPT and PANET Monitoring Result.

2. As per above references, forwarded is the Cybersecurity Bulletin Number **077** with topic regarding **Four Mobile Threats that May Surprise You**.

3. ITR, all concerned G6/Signal Officers/Information System Officer/NCOs are reminded to include this information as part of TI & E on all of its subordinate units as part of enhancing the Cybersecurity Awareness of the Philippine Army.

4. For information and widest dissemination.

DRAFTER'S NAME AND TITLE	**PHONE NR:**
LTC JOEY T FONTIVEROS (SC) PA Chief, CMB, OG6, PA	6630
RELEASER'S NAME AND TITLE	
COL VENER ODILON D MARIANO GSC (SC) PA AC of S for C4S, G6, PA	

Army Vision: By 2028, a world-class Army that is a source of national pride.

HEADQUARTERS
PHILIPPINE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR
COMMAND, CONTROL, COMMUNICATION, AND CYBER SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

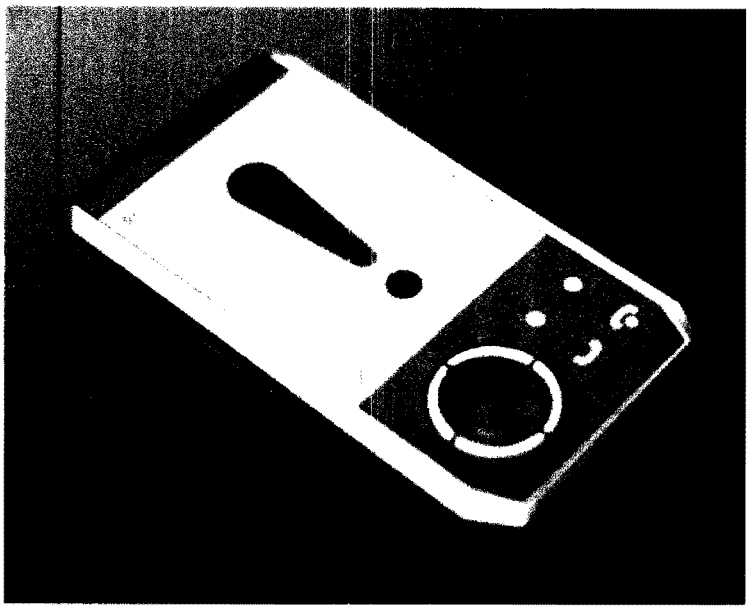
6/CMB

22 December 2016

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #77

Four Mobile Threats that May Surprise You



Viruses and malware are targeting mobile devices more than ever today. Viruses, malware, phishing — by now, these are familiar terms. Many of us think of these and other cyber threats as risks only to desktop and laptop computers, but they are increasingly targeting mobile devices. With more personnel relying on these devices and storing sensitive information on them, a cyber-attack can have serious consequences.

A key reason mobile devices are vulnerable is that many users are unaware of the potential hazards. In fact, only 46 percent of the small- and medium-business owners recently surveyed by Symantec believe smartphone and tablet use in their company poses a security risk. Among the smallest businesses, only 29 percent do.

Learning about the potential dangers is the first step to combatting them. Here are four mobile threats that you should be aware of:

Malicious Apps

Mobile apps infected with malware often resemble legitimate apps such as games, instant messaging and even antivirus software. Once installed on a device, they can reconfigure settings, install mobile ransomware, send emails to your contacts or cause damage in other ways. Malicious apps are generally found in third-party app stores — stores outside of official app marketplaces such as Google Play or the Apple App Store.

Mobile Greyware

Less destructive than mobile malware, but far more common, mobile greyware refers to apps that do not contain recognizable malware but can still be harmful or annoying. These apps might track users' locations, monitor web browsing habits or raise mobile bills by accessing the Internet without users' knowledge. A common type of greyware called mobile adware, or "madware," includes apps that display ads in a phone's notification bar, replaces the dial tone with voice ads or, worse, expose private data, such as phone numbers or user account information. As many as 55 percent of Android apps contain madware or other greyware, research from Norton has found.

Smishing

Many of us have learned to spot phishing emails — attempts to elicit financial or other private information through messages purporting to be from legitimate companies. As a result, some fraudsters have turned to SMS phishing, or "smishing," to target people through text messages. The practice also appeals to fraudsters because it enables geographic targeting - for example, they might pose as a local bank or credit union and send messages to nearby mobile phone users. Smishing poses risks to companies because it can also trick users into downloading infected files, potentially exposing sensitive data.

Fake Networks

Just as it's a bad idea to hop on an open Wi-Fi network with your laptop, it's equally risky to do so using a smartphone or tablet. Hackers can exploit these networks to intercept email messages, passwords, login credentials to unsecured sites or other information. Some can even set up fake hotspots to read the wireless traffic flowing over them. These networks often have generic names such as "airport" or "free Wi-Fi."

How can we be protected?

Encourage personnel to use best practices, such as downloading apps from official app stores and researching them beforehand. Even then, it's wise to research apps and read reviews beforehand — fake security apps have found their way into official app stores, and nearly one-quarter of apps in the Google Play store contain mobile adware. Instruct personnel to never give out confidential information over email or text message. If they receive a message purporting to be from a bank or another institution, they should contact the business to verify the message's authenticity.

Read the weekly publication of cyber bulletins to equip you with the protection of knowing and be educated about different cyber threats. Also, consider developing a mobile device-use policy for your unit, if you don't have one already. A good policy should provide guidelines for downloading apps, connecting to unit's resources remotely, setting passwords and other aspects of mobile security. Explore security products that include protection for mobile devices, such as Norton Small Business or Norton Mobile Security, which support app scanning to identify apps that include malware and greyware, and blocking for fraudulent websites. These products can help your team work productively while helping to minimize risk.

Reference:

This was cross posted from:
https://community.norton.com/en/blogs/norton-protection-blog/four-mobile-threats-may-surprise-you

DO YOU WANT TO KNOW MORE? TALK TO US.

POC: LTC JOEY T FONTIVEROS (SC) PA – Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-6281057. Email: fontiverosjt@army.mil.ph.