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:
12 August 2016

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 1208-68-2016

1. References:

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

2. As per above references, forwarded is the Cybersecurity Bulletin Number **066** with topic regarding **Cybersecurity Concerns and Smartphones.**

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 (INF) PA Chief, CMB, OG6, PA	6630
RreleaseR'S NAME AND TITLE	
COL VENER ODILON D MARIANO GSC (SC) PA AC OF S FOR C4S, G6, PA	

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

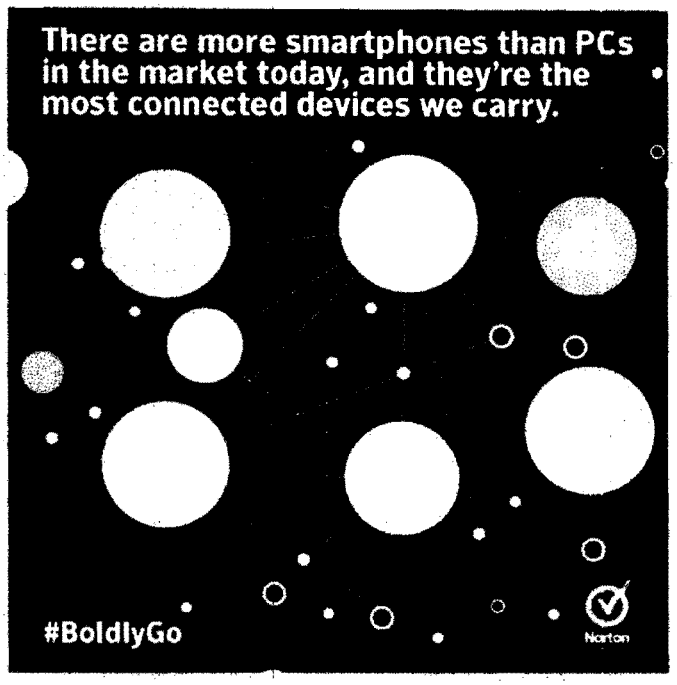
6/CMB

05 August 2016

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #66

Cybersecurity Concerns and Smartphones



More people own smartphones than PCs in today's market, and that makes the mobile platform desirable to cybercriminals. Learn how to secure your personal data. We've reached the point to where there are more smartphones than PCs in the market today. Many people use their smartphones as they would a PC. We keep tabs on our email, bank accounts, online shopping, social media accounts and more. The more tasks we do on our phones means that more personal data is being stored on them. They are the most connected devices we carry, and they're extremely vulnerable to many different kinds of attacks.

Types of Mobile Attacks

There are a multitude of ways that malware can sneak onto your phone. The first line of defense in protecting your data on your phone is being educated about these types of attacks.

Mobile malware is the most common of attack methods and is usually served up via a fake app. Malware app can do damage to your phone and data in many ways. Mobile malware can install spyware, steal or delete data, hijack your text messages and other apps, and can even lock your phone and hold it for ransom.

Phishing scams are abundant on the Internet landscape, and they don't need apps or system vulnerabilities to be delivered to you. Phishing scams are most commonly delivered via email or text messages. The main intent of phishing scams is to try to get you to divulge your personal information. Be aware of suspicious emails from banking and financial institutions that have a call to action such as clicking on a link to enter in your account credentials. In addition to trying to get you to give away your personal information, there will be attempts to get you to download mobile malware. Always be cautious about clicking on links from unknown senders or suspicious looking messages from familiar institutions that don't look quite right. Examine the sender's email address- that can sometimes be a dead giveaway. Phishers like to try to spoof recognizable companies email addresses.

Another way cybercriminals can sneak malware onto your phone is via outdated software that may have security vulnerabilities. Always be sure to update any applications and mobile operating systems as soon as there is an update available, so these security holes are patched quickly.

Despite the prevalence of mobile threats, there are ample ways to protect your mobile devices.

Basic Smartphone Security Tips

- Use a password on your phone to prevent unauthorized access. Additionally, make sure your device auto-locks when not in use.
- Turn off Wi-Fi, Bluetooth and NFC when not in use. These platforms are essentially open connections to your phone; so if you don't need to use them, turn them off.
- Turn off auto-connect to Wi-Fi networks. There are a lot of unsecured Wi-Fi networks out there, and your phone can automatically connect to them, even if you are

just passing by one. Unsecured Wi-Fi networks are another link to accessing your phone; so only connect to trusted networks.

- Only download apps from trusted sources such as the Google Play store.
- Check app permissions individually to be aware of what data apps are accessing on your phone.
- Don't click on links that are from unknown senders in SMS messages or emails. They could be a part of a phishing scam.
- Do regular software updates on all apps and your phone's OS. This patches possible security vulnerabilities that can give malware access to your phone.
- Log out of any website that you conduct financial transactions on, from buying products on Amazon to checking your bank account balance.
- Do regular backups of your phone. This will prove helpful in the event that your device gets lost or stolen.
- If your device happens to get lost or stolen, make sure you have software that allows you to remotely lock, and if necessary, wipe the data from your phone.
- Install mobile security software on your phone as an extra layer of security.

Everything is Connected

Classic science fiction novels or TV shows envisioned a future where everything in our lives would be connected and automated; from the homes we live in, to the vehicles that we drive, and even our medical data and physical activity. Well, it seems that future has finally arrived (minus the flying cars, sadly). We're starting to hear more and more about the connected future, an "Internet of Things" (IoT) where our smartphones and tablets are joined online by even more devices: cameras, thermostats, TVs, microwaves and fridges, keyless entry systems, even baby monitors. It sounds great, but every one of those Internet-connected devices is another security concern, especially since most of them connect to your smartphone.

There are reported high-profile hacks of baby monitors, security cameras and even home routers by cybercriminals. Meanwhile, security researchers dug around in the software of other devices and found ways to attack smart televisions, cars and – most horrifying of all – medical equipment. That doesn't mean criminals are actively doing so just yet, and the potential financial gain from hacking certain devices is debatable, but the rapid adoption of connected devices means a growing number of relatively untested targets.

In the future, manufacturers must thoroughly invest in and prioritize proper robust security features, especially with the amount of data these devices collect and store on users. They are improving in this regard, but right now the responsibility lies largely on you, the user, to adopt best practices and take the necessary precautions as outlined above.

And of course you can add an extra layer of protection by downloading and installing Security apps from trusted sources.

Reference:

This was cross posted from:
https://community.norton.com/blogs/norton-protection-blog/cyber-security-concerns-and-smartphones

DO YOU WANT TO KNOW MORE? TALK TO US.

POCs:

a. LTC JOEY T FONTIVEROS (INF) 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.

b. Sgt Mark Dave M Tacadena (SC) PA – Branch NCO, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0998-5342877. Email: tacadenamdm@army.mil.ph