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:
11 December 2015

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 1412-28-2015

1. References:

   a. Command Guidance
   b. Cybersecurity Awareness
   c. VAPT and PANET Monitoring Result

2. As per above references, forwarded is the Cyber Security Bulletin number 037 with topic regarding **10 Steps to Defeat Hacking Attacks (And what to do after you've heen hacked).**

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 Cyber Security Awareness of the Philippine Army.

4. For information and widest dissemination.

DRAFTER'S NAME AND TITLE	**PHONE NR:**
MAJ JOEY T FONTIVEROS (INF) PA Chief, CMB, OG6, PA	6630
RELEASER'S NAME AND TITLE	
COL VENER ODILON D MARIANO GSC (SC)PA AC OF S FOR CEIS, G6, PA	

Army Core Purpose: Serving the people. Securing the land.

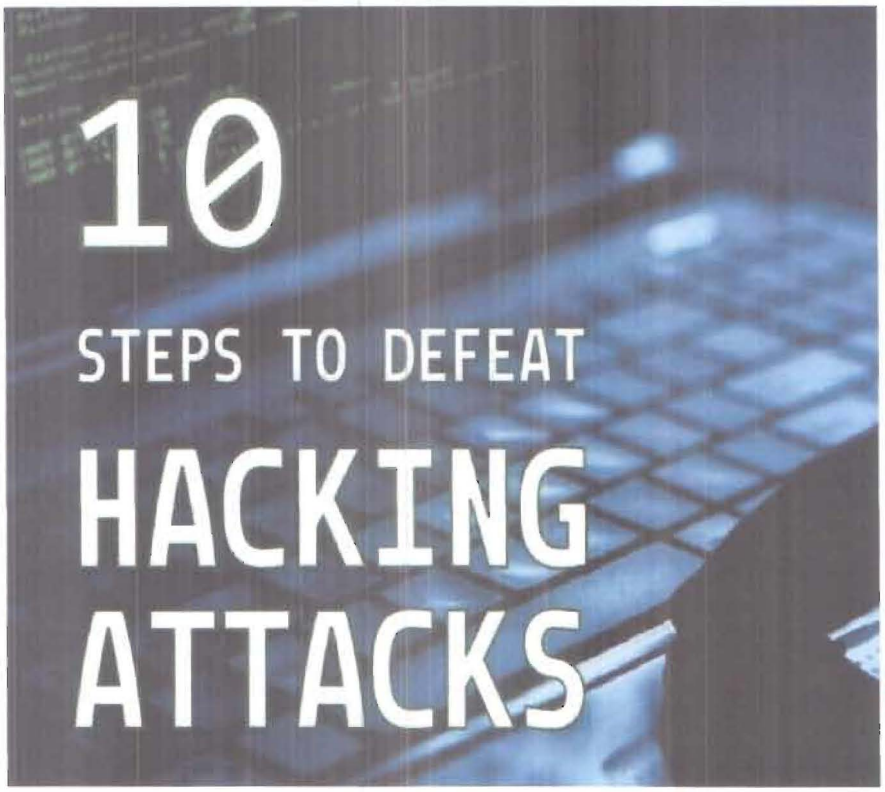
HEADQUARTERS
PHILIPPINE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB 10 December 2015

CYBER SECURITY BULLETIN

Cyber Security Bulletin: #37

10 Steps to Defeat Hacking Attacks (And what to do after you've been hacked)



This article discusses the first steps that you need to take to defeat hacking attacks – and after you've been hacked. These days, getting phished, hacked or becoming a victim of some malware attack isn't uncommon. The data breaches are on the rise and each day numerous types of malware are being discovered in the wild.

If you've realized that you've been hacked or you're vulnerable to hacking attacks- what is the next step? What to do after you've been hacked? How to defeat hacking attacks?

HERE ARE SOME SIMPLE STEPS:

1. CALM DOWN. IT HAPPENS. BUT IT'S TIME TO ACT

If you've found that you are a victim of some data breach, most of the time it's not even a threat. However, you need to ask yourself some questions. You need to introspect and revisit the security measures you are taking to secure your online life.

2. NOW, RESET ALL YOUR PASSWORDS AND DEFEAT HACKING ATTACKS

The first and foremost step after you've been hacked it to **reset all your passwords**. Use new and strong passwords that are a combination of uppercase and lowercase letters, digits and symbols.

Also, avoid reusing a password as it's something that we do unconsciously. Another thing that you must keep in mind while creating strong passwords, don't ever create a password that have your personal information.

3. CHECK YOUR ACCOUNT STATEMENTS AND MAKE CHANGES

Thoroughly review financial account statements related to the affected accounts for some unusual activity. Look for new payment methods, new accounts linked, or new shipping addresses. Hackers are targeting your online accounts with one obvious reason - related to money.

You need to check your credit card reports for suspicious activities and of you find anything fishy, cancel that card and book a new one.

4. CONNECTED ACCOUNTS TOO CAN DO THE DAMAGE

Very often, one online account is linked to other accounts. The compromised email account could be the one you used to verify some other email account. Same applies to your online banking and e-commerce accounts. So, it's a safe practice to perform a security checked for all accounts and update the passwords.

5. DE-AUTHORIZE ALL CONNECTED APPS

All the apps you're using on your phone are connected to some email account or your Facebook account. So, it would be an obvious decision to de-authorize all these apps. This could be a pain to re-authorize all the apps, but it's the right to do.

6. USE TWO-FACTOR AUTHENTICATION TO DEFEAT HACKING ATTACKS

While setting up the new accounts, enable the option of two-factor authentication. This method adds an extra layer of security to your accounts. Don't skip it, it makes your account 4-5 times more secure.

7. RECOVER YOUR ACCOUNTS

All the major services like Facebook, Microsoft, Twitter, Google, Yahoo and Apple provide a detailed guide to get back your account after you lose its control. Just search for account recovery for your service and follow the steps.

8. UPDATE YOUR PC AND PHONE

There is a very high percentage of hackers target using the vulnerabilities in your PC and phone operating systems. If you are running older versions, there is a possibility that your device isn't getting regular security updates.

Go to system settings and find the update system to perform the update. Make this a regular habit to protect yourself.

9. SCAN YOUR DEVICES FOR MALWARE

Using a worthy anti-malware tool is another important step. Download some good antivirus product and don't hesitate to pay for it. If you choose to go for free products, you can check out this top free antivirus list.

Don't forget to update your product no matter how solid your antivirus product is, it's useless if its virus database definitions are outdated.

10. TELL YOUR FRIENDS AND FAMILY. SPREAD AWARENESS TO DEFEAT HACKING ATTACKS

After fixing all the loopholes, it's time to go to your friends and family members. Tell them about the basic steps to keep themselves secure and tell them where they are lacking.

Educate people to defeat hacking attacks. If this happened to you, it could happen to anybody.

Army Core Purpose: Serving the people. Securing the land.

Reference:

http://fossbytes.com/10-steps-to-avoid-hacking-attacks/