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:
05 October 2015

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 0510-18-2015

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 028 with topic regarding **"YOUR ACCOUNT WILL BE CLOSED IN 24 HOURS!"**

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	

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

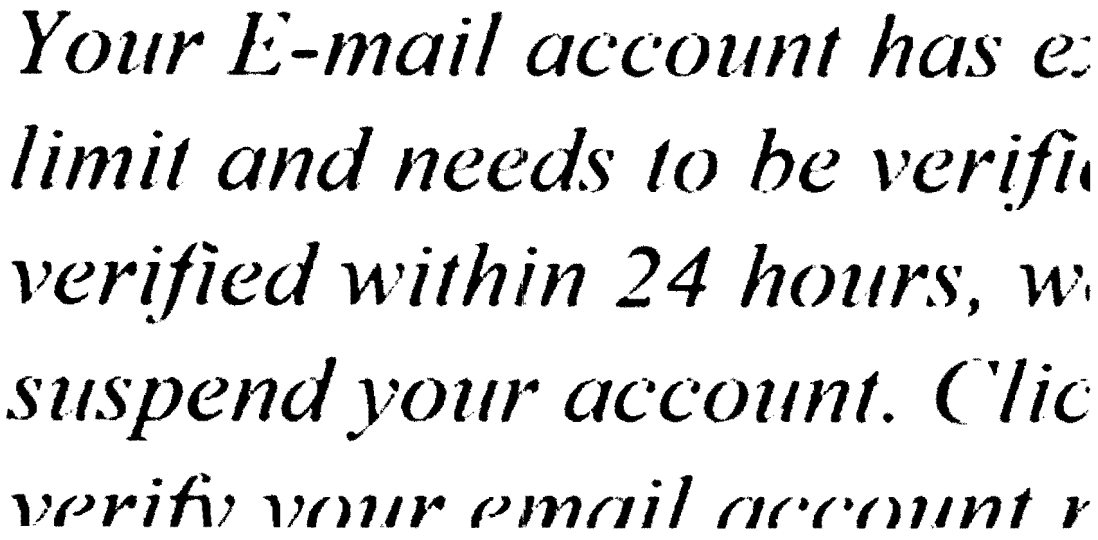
6/CMB

05 October 2015

CYBER SECURITY BULLETIN

Cyber Security Bulletin: #028

"YOUR ACCOUNT WILL BE CLOSED IN 24 HOURS!"



"Your E-mail account has exceeded its limit and needs to be verified, if not verified within 24 hours, we shall suspend your account. Click Here to verify your email account now." And when you try to resolve it, it doesn't even work. You just end up on the login page! This message is not about a problem with the mail system, it's a very typical phishing mail.

How to spot a phishing attempt?

- It arrives as a mail message. Mail can be sent by anyone and it is trivial to spoof the sender's address so that it seems to come from your mail operator or some other company you trust.
- People think less when they are afraid so it tries to create a sense of danger. Something bad will happen unless you react. The closure of your account is a very common threat when phishing for e-mail accounts.

- People think less when in a hurry so it tries to create a sense of urgency. You need to act right now. This lowers the risk that the victim checks out the facts first. The 24h deadline is a typical trick to achieve this.
- It links to a web page that looks like an official page of, for example,your mail operator. But it is actually controlled by the attacker, who also receives any information you enter. You are hacked if you enter your mail user name and password, or other valuable information.

What should I do to avoid being phished?

- First of all, do not click links in mails! This is not just about phishing, many get malware too by clicking links. But there are also legitimate links that friends send to you. So you should always think about who the sender is (remember, the apparent sender can be spoofed), in what style and language the message is written, what the claimed content of the link is and how does all this fit together? To summarize, do I expect this kind of message from this person (or company) at this time? This way you should be able to spot the legit links.
- If in doubt, check what address the link is taking you to **before you click**. Note that the text forming the visible part of the link may look like a web URL but still be linked to a totally different address. Examine the address that the mail client or browser shows you. Make sure that the address match the company or site that the link is claimed to point to. For example: The login to Gmail should start with **"https://accounts.google.com/"** but a phishing site targeting Gmail may use an address like **"http://accounts.google.com.etw368hj.nu/". The latter does NOT belong to Gmail.**
- Get familiar with the login URLs of your favorite services BEFORE you run into a phishing mail. Then it is a lot easier to spot the spoof. The address may look long and nerdy, but you only need to mind the part after the **double-slash "//"** but before the **first single slash**. That part identifies the server that you will access. (Your browser may show the address without the initial **"http://"**, in that case just examine the part before the first slash.)
- Get familiar with the concept of secured web pages and how to recognize them. Login pages of important services are typically protected this way. Their addresses start with **"https://"** instead of **"http://"** and your browser shows a lock or similar symbol next to the address field. You can examine the certificate of the server you are connected to by clicking the lock, and this is reasonable hard proof about who's running the service. Needless to say, the phishing sites can't duplicate these cryptographic certificates.

- If you suspect that there really may be a problem with your mail account, then log in with the link that you normally use to access the account. Do not use a link in a mail message. Look for info banners and pop-up messages shown in the browser after you have logged in. These messages are a lot more reliable and can generally be trusted. Mail operators are well aware of the phishing threat. If you get a mail claiming that there's a problem, then you can be pretty sure that it isn't true. The mail operators do not communicate in that way.
- If you still fall for the scam, attempt to change your password right away. This is also a good time to think about if you have used the same password on other services. Say that **john.doe@gmail.com** is using the same password as **john.doe@hotmail.com**. If one get hacked, then the hacker just need to try some of the common mail services to get access to more accounts. This would be a good time to brush up your password practices.

Reference:

http://safeandsavvy.fsecure.com/2013/02/27/your-account-will-be-closed-in-24h/