COMPUTER SECURITY BULLETIN

Risk/Impact Rating: SERIOUS

< Phishing Attempt Threat Advisory >

CSB17-008

Description:

Phishing email messages, websites and phone calls are designed to steal money.

Cybercriminals use social engineering to convince you to install malicious software or hand over your personal information under false pretenses. They might email you, call you on the phone, or convince you to download something off of a website.

Phishing scam:

- Wrong spelling and bad grammar;
- Suspicious links in email;
- Threats; and
- Spoofing popular websites, companies, or government agencies.

Last February 17, 2017 CPSM received a Private Message from Mr. Dolojan inquiring if an e-mail he received was actually come from the said Office. But when he forwarded a copy of the said e-mail, the IT Officer concluded that it might be a form of phishing.

The recipient was advised to click the link to view the document to fill the 2017 support form and give suggestion on the issues as per sender that was stated in the document. There was also a time frame for the recipient to send back the file. The IT Officer noticed also the address “formerly PMO”, which the IT Officer told the recipient that

they don’t use that kind of address. Also, the IT Officer told the recipient that the Office don’t have any survey asking for compliance.

When the IT officer clicked on the link, the login option appeared and need to insert email address and password to view the document.

Recommendations:

- Delete emails of unknown sender;
- Back up your files to an external drive;
- Verify any emails sent;
- Do not visit illegal websites;
- Avoid filling out forms in emails; and
- Never click any links from unknown e-mail.

References:

https://tiptopsecurity.com/the-truth-about-clicking-links-in-email-and-what-to-do-instead/

https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

http://searchsecurity.techtarget.com/definition/phishing

http://www.actionfraud.police.uk/fraud-az-phishing

https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx

http://www.dslreports.com/faq/11081

For inquiries, please contact WSCSD thru:

a. Telephone number: (02)723-0401 local 4225
b. E-mail address: wscsditms@pnp.gov.ph
c. Chat service: www.itms.pnp.gov.ph

*For dissemination to All PNP Personnel