Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
INFORMATION TECHNOLOGY MANAGEMENT SERVICE
Camp BGen Rafael T Crame, Quezon City

MEMORANDUM

FOR : See Distribution

FROM : D, ITMS

SUBJECT : **Cybersecurity Advisory | Smishing/SMS Scams**

DATE : November 29, 2021

---

1. References:
   a. https://newsinfo.inquirer.net/1519138/telcos-summoned-asked-to-do-more-vs-text-scams;

   b. https://mb.com.ph/2021/11/20/contact-tracing-apps-are-not-leaking-your-information; and

   c. Approved ITMS SOP re ITMS Computer Emergency Response Team (CERT) Guidelines and Procedures.

2. Para 1.a and 1.b pertains to the articles published by Inquirer.Net and Manila Bulletin on their respective websites regarding the rampant rise of Smishing or SMS Scams on supposed job offers. Although it has been prevalent in the country, it has been reported that these attacks are not exclusive to the Philippines as it also targets Mexico, Brazil, India, and Thailand.

3. Scammers are posing as representatives of a legitimate company or organization, asking their victims to allegedly help merchants improve their sales by making an advance purchase. They will then require their victims to register in their platform to earn commissions if they help facilitate sales promising a commission after the registration process.

4. Although it is not clear where these scammers got the phone numbers, PNP personnel must be vigilant in sharing their personal information, including their mobile numbers, to avoid getting spam messages and becoming a victim of phishing.

5. As part of the PNP's initiative in today's technology and security, PNP personnel must be aware of these types of cyber-attacks and increase their resiliency in these kinds of cyber incidents.

6. Listed hereunder are the common characteristics of Smishing or SMS Spams:

a. **Suspicious sender's address**. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters.
b. **Generic greetings and signature**. A generic greeting such as "Dear Valued Customer" or "Sir/Ma'am" and a lack of contact information in the signature block are strong indicators of a phishing email.
c. **Spoofed hyperlinks and websites**. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs .net).
d. **Spelling and layout**. Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt.

7. In this regard, this Service recommends the following tips in avoiding Smishing or SMS Scams:

a. Be suspicious of unsolicited messages asking for information;
b. Do not provide personal details or information;
c. Do not reveal personal or financial information;
d. Take advantage of default anti-phishing features in mobile phones; and
e. Enforce multi-factor authentication (MFA).

8. Further, kindly upload the attached website banner on your respective websites to raise awareness on detecting and avoiding Smishing or SMS Scams.

9. You may visit itms.pnp.gov.ph to download learning materials regarding cybersecurity under the Computer Security Tab. Should you have any inquires and concerns, you may contact ISSD at 8723-0401 local 6546 or email us at issd.itms@pnp.gov.ph.

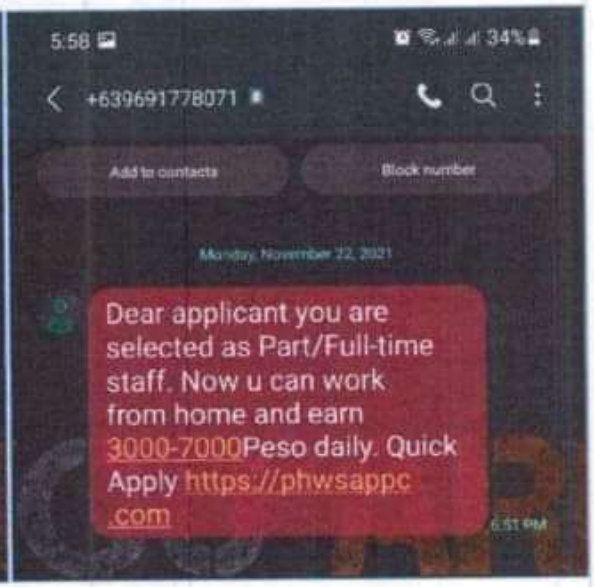
10. For widest dissemination.

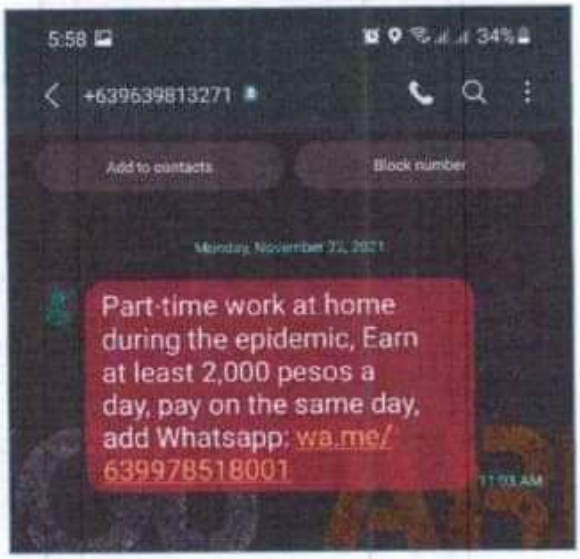
BENJAMIN H SILO JR
Police Brigadier General

Distribution:
IG, IAS
Cmdr, APCs
D-Staff
P-Staff
D, NSUs
RD, PROs

Copy Furnished:
Command Group
SPA to the SILG

Sample SMISHING/SCAM MESSAGE





SMISHING or SMS SCAMS Website Banner