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 : **Cyber Security Advisory: "Hi Mum" Scam**

DATE : September 16, 2022

---

1. Reference: Article from ABC News Australia with the headline "John and Patricia thought they were helping their daughter in a crisis. They were actually being scammed".

2. The aforementioned phrase pertains to the developing "hi mum" scam, a type of scam/fraud that impersonates a family member or friend asking for personal or financial information, which leads to a request for money for an urgent situation.

3. By leveraging personal information available online, criminals have become professionals at scams and fraud. This information is frequently used to impersonate close relatives and friends to advance hoax.

4. If you have received an unwanted phone call or text message from someone pretending to be a family member or close friend, you are already a victim of fraud. Other techniques used by fraudsters in phony emergency schemes include:

   a. Typically depicts as an authoritative figure, which makes them sound more credible;

   b. Imposes an urgent situation in which you are the only person who can help; and

   c. Insists on secrecy to prevent the victim from telling other family members about the scam and exposing it.

5. In this regard, this Service recommends the following practices to help avoid being a victim of online scams/frauds:

   a. Do not post personal or financial information online;
   b. Be wary of unsolicited communications requesting information;
   c. Take advantage of default anti-phishing capabilities on mobile devices;
   d. Implement multi-factor authentication (MFA); and
   e. Protect your privacy settings.

6. Further, the following procedures should be taken if a scam or fraud is suspected:

a. Always confirm unexpected or urgent calls or messages with other family members or close acquaintances;

b. Be wary with online money transfers;

c. If confirmed to be a scam or fraud, block the number immediately; and

d. Report the incident to the National Computer Emergency Response Team (NCERT-PH), the National Bureau of Investigation, or the Philippine National Police, Anti-Cyber Crime Group (PNP-ACG).

7. In relation to the foregoing, this Service recommends the uploading of the attached info-graphic material on your respective websites and social media platforms to promote information security awareness to PNP personnel and to the community.

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

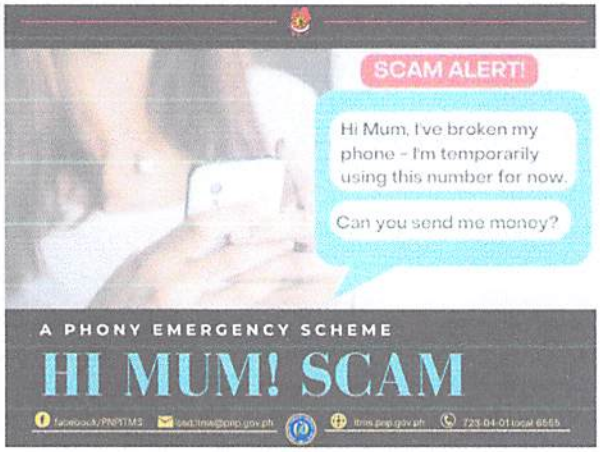
9. For widest dissemination.

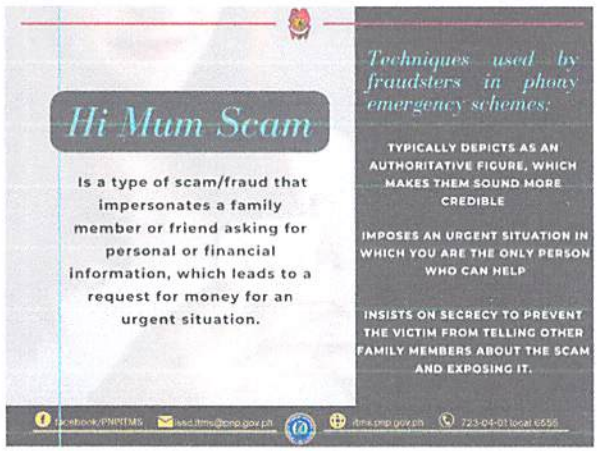
HARRIS R FAMA
Police Brigadier General

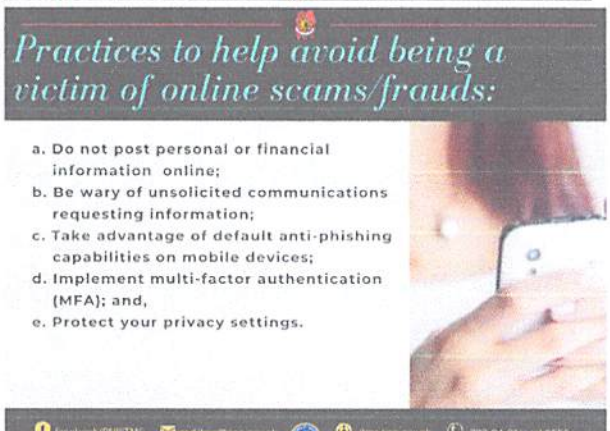
Distribution:
IG, IAS
Cmdr, APCs
D-Staff
P-Staff
D, NSUs
RD, PROs

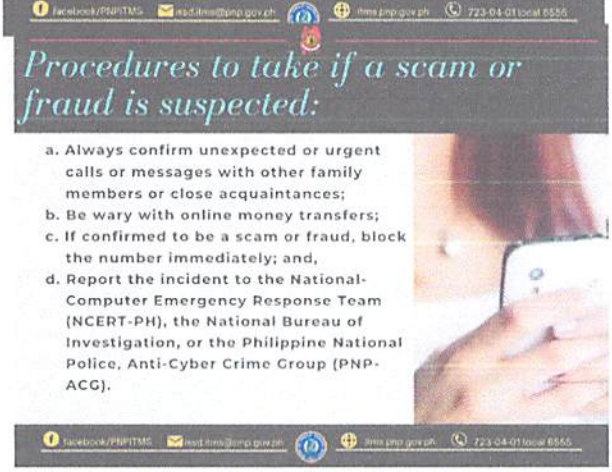
Copy Furnished:
Command Group
SPA to the SILG

Hi Mum Scam


SCAM ALERT!
Hi Mum, I've broken my phone - I'm temporarily using this number for now.
Can you send me money?
A PHONY EMERGENCY SCHEME
HI MUM! SCAM


Hi Mum Scam
Is a type of scam/fraud that impersonates a family member or friend asking for personal or financial information, which leads to a request for money for an urgent situation.
Techniques used by fraudsters in phony emergency schemes:
TYPICALLY DEPICTS AS AN AUTHORITATIVE FIGURE, WHICH MAKES THEM SOUND MORE CREDIBLE
IMPOSES AN URGENT SITUATION IN WHICH YOU ARE THE ONLY PERSON WHO CAN HELP
INSISTS ON SECRECY TO PREVENT THE VICTIM FROM TELLING OTHER FAMILY MEMBERS ABOUT THE SCAM AND EXPOSING IT.


Practices to help avoid being a victim of online scams/frauds:
a. Do not post personal or financial information online;
b. Be wary of unsolicited communications requesting information;
c. Take advantage of default anti-phishing capabilities on mobile devices;
d. Implement multi-factor authentication (MFA); and,
e. Protect your privacy settings.


Procedures to take if a scam or fraud is suspected:
a. Always confirm unexpected or urgent calls or messages with other family members or close acquaintances;
b. Be wary with online money transfers;
c. If confirmed to be a scam or fraud, block the number immediately; and,
d. Report the incident to the National-Computer Emergency Response Team (NCERT-PH), the National Bureau of Investigation, or the Philippine National Police, Anti-Cyber Crime Group (PNP-ACG).