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| Quishing**

DATE : August 10, 2022

---

1. Reference: Public Service Announcement from Federal Bureau of Investigation (FBI) with subject "Cybercriminals Tampering with QR Codes to Steal Victim Funds".

2. The above reference pertains to a FBI alert to raise awareness of malicious Quick Response (QR) codes. Cybercriminals manipulate QR codes to drive victims to malicious websites that steal login and financial information.

3. A QR code is a square barcode that can be scanned and read by a smartphone camera to enable quick access to a website, trigger the download of an application, and direct payment to an intended recipient. During the COVID-19 pandemic, it is also properly employed to give convenient contactless access. However, cybercriminals are using this technology by sending QR code scans to rogue websites in order to steal personal information and sensitive data, inserting malware in order to get access to the victim's device, and routing cash for Cyber criminal use.

4. Quishing scams first need the QR code itself to be delivered to the victims (usually via email). The victim then uses their camera to scan the QR code, which opens their browser to a phishing website where sensitive data and personal information can be collected.

5. The following are some suggestions for avoiding the Quishing attack:

   a. Check the URL associated with the QR Code to see if it is the desired site and appears real. A malicious domain name may be identical to the desired URL yet contain errors or misspellings;
   b. Use caution when inputting login, personal, or financial information from a website accessed using a QR code;
   c. When scanning a physical QR code, be sure it hasn't been tampered with, for as by placing a sticker on top of the original code;
   d. Use QR codes to verify all online bank payments; and

e. Avoid making payments through a website accessed via a QR code. Instead, manually enter a known and trusted website URL to complete the payment.

7. In relation to the foregoing, this Service recommends the uploading of the attached info-graphic material on the 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 and 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 RFAMA
Police Brigadier General

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

Copy Furnished:
Command Group
SPA to the SILG

Quishing Attacks