GENERAL HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES
OFFICE OF THE DEPUTY CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, J6
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: 2016–12

Phishing and Spear Phishing

The Threat

Phishing is a high-tech scam that uses e-mail to deceive you into disclosing personal information. It puts your personal information and your organization's information at risk. **Spear phishing** is a type of targeted phishing that appears to be directed towards a specific individual or group of individuals.

Indicators

The following are suspicious indicators related to phishing and spear phishing:

- Uses e-mail
- May include bad grammar, misspellings, and/or generic greetings
- May include maliciously-crafted attachments with varying file extension or links to a malicious website
- May appear to be from a position of authority or legitimate company:
  - Your employer
  - Bank or credit card company
  - Online payment provider
  - Government organization
- Asks you to update or validate information or click on a link
- Threatens dire consequence or promises reward
- Appears to direct you to a web site that looks real

Spear phishing specifically:

- Has a high level of targeting sophistication and appears to come from an associate, client, or acquaintance
- May be contextually relevant to your job
- May appear to originate from someone in your email address book
- May contain graphics that make the email look legitimate

Effects include, but are not limited to:

- Deceiving you into disclosing information
- Allowing adversary to gain access to your and/or your organization's information

Countermeasures

The following countermeasures can be taken to guard against phishing and spear phishing:

- Watch out for phishing and spear phishing
- Delete suspicious e-mails
- Contact your system security point of contact with any questions
- Report any potential incidents
- Look for digital signatures
- Configure Intrusion Detection Systems (IDS) to block malicious domains / IP addresses
- Ensure anti-virus software and definitions are up to date

Do not:

- Open suspicious e-mails
- Click on suspicious links or attachments in e-mails
- Call telephone numbers provided in suspicious e-mails
- Disclose any information

In case of any cyber-related incidents, report immediately to the AFP Computer Security Incidents Response Team (AFPCSIRT), Cyberspace Security Group, CEISSAFP, at AFPTSN 911-6001 local 5873.

Reference:

This was cross posted from:
https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/

http://www.trendmicro.com.ph/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

as referenced by CMB, G6, PA Cyber Security Bulletin #61 with minor additions/modifications.