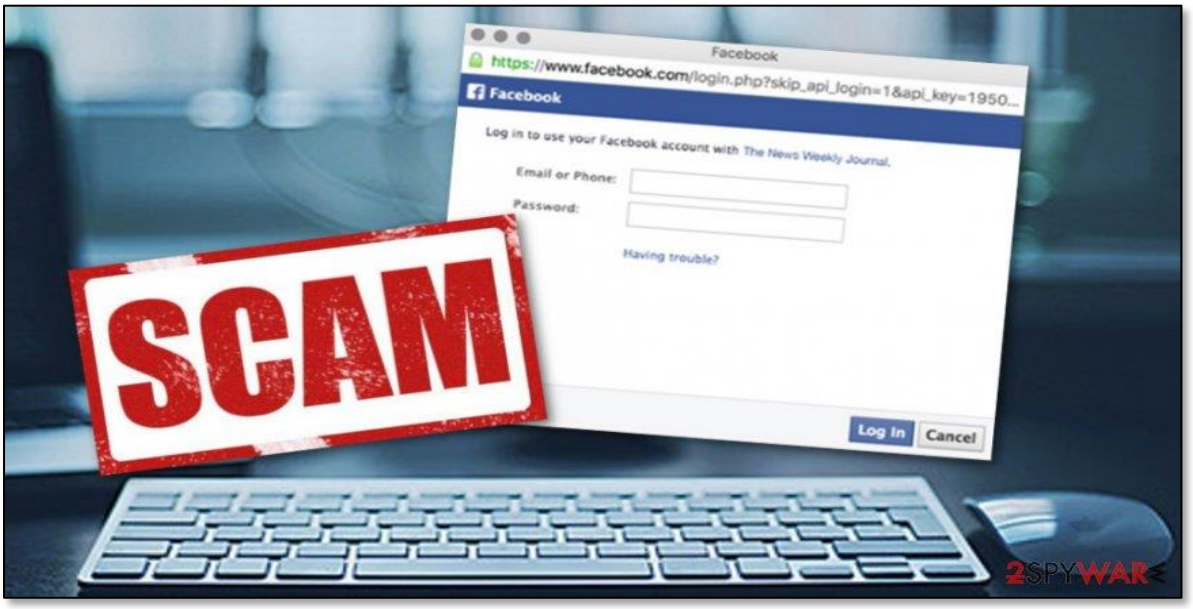
H E A D Q U A R T E R S
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-05

SNEAKY PHISHING ATTACK TRIES TO STEAL YOUR FACEBOOK PASSWORD



1. Background:

A sneaky phishing campaign aims to steal passwords from Facebook users – including administrators of company Facebook Pages.

The attack begins with a phishing email claiming to be from 'The Facebook Team', which warns that the user's account "might be disabled and [the] page might be removed" due to repeatedly posting content that has been reported as infringing the rights of another user. The victim would be invited to appeal the report by clicking on a link that the security researchers said redirects to a Facebook post – and within this post there is another link that directs the user to a separate website in order to make the "appeal".

As part of the fake appeals process, the user is asked to provide sensitive information, including the user's name and email address. Before submitting the form, the user is also asked to enter his/her Facebook password.

All this information is sent to the attacker, who can use it to log in to the victim's Facebook page, collect information from his/her account and potentially lock him/her out of it. If the victim reuses his/her Facebook email address and password for other websites and applications, the attacker can access those too.

2. Reasons for the Success of this Particular Attack

One of the reasons phishing attacks like this are successful is because they create a sense of urgency. What made this particular phishing campaign interesting to the security researchers was that it connects to a post on Facebook and that there

is a link to a credential-phishing site within the post, disguised as a form to request for an appeal.

However, while the phishing email and phishing domain might have looked legitimate at first glance, there were clues that would have suggested that something might be off. For example, while the email contained Facebook branding and claimed to be from Facebook itself, the sender email address was not related to Facebook at all. In addition to this, attempting to reply to the sender email directs messages to an unrelated Gmail address.

The language of the email is designed to create fear in the victim, scaring them into losing his/her account. It is unlikely that an actual online service will send an email like this, but if you receive a message and do get worried, DO NOT CLICK the link in the email. Instead, log in to the website directly. If something is wrong with your account, you will be able to find out there – without handing your password to cyber criminals.

3. Recommendations

Facebook's Help Centre says users who think that their account had been phished should report it, change their password, and – in the security settings – log out of any devices that they do not recognize.

It is also recommended that users turn on the multi-factor authentication (MFA) to increase account security against unauthorized logins. MFA is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack. Examples of Multi-Factor Authentication include using a combination of these elements to authenticate:

a. Knowledge
   - Answers to personal security questions
   - Password

b. One-Time Passwords (OTPs)
   - OTPs generated by smartphone apps
   - OTPs sent via text or email

c. Possession
   - Access badges, USB devices, Smart Cards or fobs or security keys
   - Software tokens and certificates

d. Inherence
   - Fingerprints, facial recognition, voice, retina or iris scanning or other Biometrics
   - Behavioral analysis

4. Dissemination

The information provided is intended to increase the security awareness of AFP personnel and to help them behave more securely within their work environment. The increased awareness is intended to help improve the organization's overall cybersecurity posture. All units and offices are given permission and are encouraged to redistribute this bulletin that will benefit the AFP organization as a whole for educational, and non-commercial purposes.

References:

- *https://www.zdnet.com/article/this-sneaky-phishing-attack-tries-to-steal-your-facebook-password*
- *https://www.onelogin.com/learn/what-is-mfa*