UNIVERSITY OF THE PHILIPPINES
OFFICE OF THE VICE PRESIDENT FOR DEVELOPMENT

upitdc
UP Information Technology Development Center

REMINDER on Online Security
March 08, 2022

To All UP Users:

Please be wary of phishing websites, emails, social media posts, and other online avenues masquerading as being associated with the University.

Possible methods of attack that may be initiated against online users are the following:

- **Phishing** is a cyber attack that obtains an individual's sensitive data with the culprit posing as a legitimate and trustworthy institution or entity in an electronic communication. This is usually done through unsolicited email and messages on Facebook (especially fake accounts), and other social media.
- **Whaling** is similar to phishing, but the culprit poses as an influential member or senior management in an organization in an attempt to use their authority, to lure other important members of that organization into providing sensitive personal information or company data. Culprits also usually do this through unsolicited email, and messages through Facebook and other social media.
- **Vishing** is also similar to phishing but is done through voice technology.
- **Smishing** is a phishing attack through SMS or text messages.
- **Spear Phishing** is a cyber attack personalized to target a specific individual, with the culprit masquerading as someone the victim is familiar with, such as a friend or a family member. This is also done by sending unsolicited emails and messages through email and social media, like phishing.
- **Man in the Middle** is a form of attack where the culprit acts as a relay or proxy in a communication between parties. The culprit can eavesdrop, impersonate one of the involved parties, or alter the communication, all while everything still seems normal to the users.
- **Man in the Browser** is a similar approach to Man in the Middle, but instead there is a Trojan Horse (a type of malware) that manipulates web pages while still appearing as normal, thus possibly gaining access to the users' transactions in said web page.

Be reminded that the University will never ask for your username, password, or any other access credentials.

You are advised to visit https://haveibeenpwned.com and check if any of your email accounts have been compromised. If any of your email accounts have been affected, we strongly advise that you IMMEDIATELY change your passwords for the affected accounts, as well as passwords for all other online services that are connected to it (social media, etc.). We also highly encourage that you enable Multi-Factor Authentication for all your email accounts.

We strongly encourage you to be extra vigilant when accessing websites or corresponding through email, social media, and other online platforms. If you encounter suspicious websites, emails, and posts on social media sites, please immediately inform our Helpdesk at helpdesk@up.edu.ph

For your guidance and information.

Please be safe always.

Information Technology Development Center (ITDC)
Office of the Vice President for Development (OVPD)

2/F Vidal A. Tan Hall, Quirino Ave. cor. Velasquez St.
University of the Philippines, Diliman,
Quezon City

Tel: +(63) 02 436 2217, +(63) 02 920 2080
Telefax: +(63) 02 920 2036
Website: itdc.up.edu.ph