UNIVERSITY OF THE PHILIPPINES

OFFICE OF THE VICE PRESIDENT FOR DEVELOPMENT

upitdc
UP Information Technology Development Center

**SECURITY REMINDER: Phishing Attacks Asking for Access Credentials**
*Sept. 18, 2023*

To All UP Users:

Please be wary of phishing attempts through emails, SMS, social media and online platforms, or phone calls that are asking for your phone number, email, or any other personal information.

DO NOT provide any information, and DO NOT reply to these phishing emails/messages. Likewise, DO NOT click any files and links, if there are any. Please DELETE and ignore these emails or messages IMMEDIATELY.

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

- **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 colleague, friend, or a family member. Culprits also attempt this by sending unsolicited messages through email, social media, and other online platforms.

- **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 social media and other online platforms.

- **Smishing** is a phishing attack through SMS or text messages. Culprits using this method might ask you to reply to their text with your personal information, or to click a link that they sent. Culprits might also send fake One-Time-PINs (OTPs) via text messages using a normal or unlisted phone number.

- **Vishing** is a phishing attack that is done through a phone call. When the culprits call their victims, they might have a pre-recorded audio or a script to deliver their message.

Please be reminded that the University will never ask for your password or any other access credentials. We strongly encourage you to be extra vigilant when accessing websites or corresponding through SMS, email, social media, messaging services, and other online platforms.

If you encounter suspicious websites, emails, messages, and posts on social media sites, please immediately inform us at the UP System ICT Support at https://ictsupport.up.edu.ph/.

For your guidance and information.