UNIVERSITY OF THE PHILIPPINES

OFFICE OF THE VICE PRESIDENT FOR DEVELOPMENT

upitdc
UP Information Technology Development Center

REMINDER on Recognizing Phishing Emails
January 27, 2025

Dear UP User,

Please be reminded of fraudulent phishing emails that may be culprits masquerading as officials in our organization, asking for donations or personal/sensitive information.

Below are some pointers on how to recognize and identify potential phishing emails and scams:

1. **Phishing emails may use a generic greeting/salutation.** They might state "Dear Customer" or "Dear Valued Member," or some other unfamiliar salutation.

2. **Phishing emails may contain suspicious attachments**. They might have files that have unfamiliar names or extensions, such as .ZIP, .RAR, .SCR, TAR.GZ, etc. These types of files are commonly associated with harmful software such as malware. **DO NOT** click or open these files/attachments.

3. **Phishing emails may ask for your personal or sensitive information.** They may request you to send information such as full names, contact numbers, addresses, financial information, etc. **DO NOT** provide your information to suspicious emails or messages.

4. **Phishing emails may ask for donations or financial assistance.** Culprits may **pretend** to be **important people in your organization** (e.g. **officials** or **upper management**), or family members, and ask for any form of financial or monetary support (donations, solicitations, etc.). **DO NOT** send money to suspicious senders; always verify first with other people and sources.

5. **Phishing emails may have links and email addresses that are fake**. Culprits may try to trick recipients by including names of legitimate organizations/companies and websites or links. However, these fake links may direct you to harmful or malicious websites or allow the culprit to access your information. If you receive a suspicious email that might be a scam, **DO NOT** click on any of the links.

6. **Phishing emails may have alarming or "urgent" titles/subject names.** They may state words like "urgent," "account at risk," "immediate attention," etc. The culprit's goal is to make the reader panic and react to the fraudulent alarming message. Make sure to double check if you receive such emails.

7. **Phishing emails may say that you received rewards or won a contest.** They may tell you that you won a contest or prize, and you have to click a link or log in somewhere to claim your rewards. However, the culprit's goal is to make you enter your account information or give your personal/sensitive information. **DO NOT** click or log in to links sent by suspicious messages, especially if you did not join any kind of contest at all.

8. **Phishing emails may have obvious grammar and spelling errors.** If it is in English, it may have numerous obvious mistakes in grammar and spelling as it may have been hastily written and released by the culprit.

You may report suspicious emails and senders to the UP System ICT Support at https://ictsupport.up.edu.ph/

For your information and guidance.