- Data privacy / Computer crimes

PROTECT YOUR PERSONAL INFO

As we celebrate the Chinese New Year, the festive atmosphere should not be a reason for you to let your guard down against fraudsters and their deceitful activities.

Fraud comes in various forms. Shockingly, fraudsters are becoming more and more sophisticated in tricking bank clients into revealing their personal information and account details.

One of the methods these fraudsters have been using is called phishing. Phishing is the criminal intent to obtain a person's sensitive bank information to steal their money. It usually involves sending an email or text message that appears legitimate but will contain links to a fake website requesting sensitive information like username, password, account details, mobile number, and one-time passwords. Once these details are stolen, the fraudster now has access to your account and is free to do money transfers to his/her account.

Here are tips to outwit these fraudsters:

01 Never give out confidential information, such as internet banking username, password, or one-time passwords (OTP). Banks never ask for these.

02 Do not change passwords through an email request sent by suspicious senders. The change of internet banking passwords should be done only after customers have successfully logged on to their secure online banking site.

03 Do not click on website links included in suspicious emails. They may redirect you to a different site that looks like the official bank website. Tip: Check if the website address begins with "https," which means that information provided will be encrypted.

04 In relation, never click on any link provided by emails to change bank account details.

05 If you suspect that an email is attempting to phish your information, please report it immediately by forwarding the email to ReportPhish@bdo.com.ph.

06 If you think that you may have responded to a suspicious email, change your account's password by logging on to BDO Personal Online Banking at www.bdo.com.ph as soon as possible. Likewise, do not hesitate to call your branch and inform them of this incident.

How Juan dela Cruz is phished

1. Fraudsters **send out click-bait emails** mimicking a bank's official look to Juan dela Cruz.

2. Juan receives and opens his email which includes a call to action. He responds by **clicking on the included link**.

3. The link takes him to a fake but legitimate-looking website. Here, Juan is asked to **provide his personal information** like username, password, and mobile number.

4. Fraudsters gather Juan's personal information and use it to access and **steal money from his bank account**.

BDO