Republika ng Pilipinas
KAGAWARAN NG KATARUNGAN
Department of Justice
Manila

DEPARTMENT OF JUSTICE
OFFICE OF CYBERCRIME
06 October 2020

PUBLIC ADVISORY ON PHISHING, VISHING, AND SMISHING IN RELATION TO ONLINE BANKING

This Public Advisory is issued by the Department of Justice (DOJ) – Office of Cybercrime (OOC) in light of the increasing reports from the general public involving phishing electronic mails (emails), vishing (voice/phone call), and smishing (SMS/text) in relation to online banking.

Internet usage surges as people stay at home during the quarantine. As people continue to venture into cyberspace and conduct most of their activities online, the more vulnerable they become of being a victim of cybercrimes. Based on the statistics during the community quarantine, among the most common cybercrimes reported to the specialized law enforcement authorities are phishing, vishing, and smishing.[1]

Phishing, vishing, and smishing are forms of cybercrime in which the perpetrator posing as a legitimate institution, such as a bank, online payment site, or an online commerce site, devises a message through electronic mail, phone call, or text message, respectively. The objective thereof is to lure individuals into providing sensitive data, such as personally identifiable information, banking and credit card details, and usernames and passwords.

In these forms of cybercrime, it is very often that the perpetrators convince and deceive victims that the latter's immediate action is required. The urgency usually involves a recent system upgrade or a threat of account suspension that requires the victim to click the link provided in the email in order to unlock or reactivate their accounts. Clicking the link will redirect the victim to a dummy of the legitimate company's website, where the victims are asked for their login credentials and potentially credit card information or similar data. Once such sensitive information is obtained from the victim, the perpetrator will access the victim's account to perform illegal or fraudulent transactions.

In order to prevent being victimized by phishing, vishing, or smishing, the DOJ-OOC hereby issues the following advisories:

1. **Be aware of the red flags or telltale signs of phishing, vishing, or smishing.**

[1] Discussed during the Office of Cybercrime Webinar Series Episode 1 entitled, "Cybercrime in the Time of Corona: PH Cybercrime Trends During the COVID-19 Pandemic". Recorded version thereof may be accessed via https://www.facebook.com/OfficeofCybercrimePH/videos/4030323040375924/.

a. **The email, text message or phone call, usually uses one of the following lines to trick the victims into acting on their instructions:**

   i. "We Temporarily Locked your Account in order to Protect you from Potential Fraud. If you wish to Unlock your account and start transacting again."

   ii. "Please be advised that we will deactivate the access of your account/s in *(Name of Online Banking Service)* if we don't hear any actions from you. It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account or latest transactions. You can verify your account at *(online banking website)".*

   iii. "This is to inform you that some data from your account seems inaccurate or unverified. For your protection, you have to fill out the form on the given link below and verify the necessary fields and also check your information in order to continue using our service smoothly."

   iv. "We have detected unusual activity on your *(Online Payment Service)* account and we fear possible unauthorized and limited access to your account."

   v. "You can't access your account until this process is complete. If you don't complete the verification process within 24 hours, all pending orders will be cancelled and we will lock your account permanently."

   vi. "Your account is currently being updated as we are introducing a new security system. Follow the instructions below to reactivate your account."[2]

   vii. "Your credit card is the subject of a police investigation for fraud. Please follow the instructions below."[3]

   viii. "Our records indicate that payment for your Internet account is due. We are also currently introducing a new e-payment service. Please follow the instructions below."[4]

   ix. "You are the lucky winner of our lucky draw. Please submit your credit card details so that we can verify your identity."[5]

b. **The email, text message, or phone call asks for personal information**

[2] Accessed on 25 September 2020, https://www2.aia.com.sg/common/PhishingSecurity.htm.
[3] *Ibid*
[4] *Ibid*
[5] *Ibid*

Banks, other financial institutions, and reputable online shops will never ask for personal information from their clients by email, text message, or phone call. Any request for personal information by e-mail, text message, or phone call that claims to be from a legitimate and reputable source, is most likely a scam.

REMEMBER: BANKS WILL NEVER ASK FOR YOUR OTP.

c. Badly written emails or text messages

Emails or text messages from perpetrators will usually contain grammatical and spelling errors.

d. Hidden and masked website address

The link provided in the email or text message will redirect the victim somewhere other than where it claimed to be going. Hovering the mouse pointer over the link will reveal a different website address compared to the displayed website address:

The perpetrators also use website addresses that resemble the legitimate website but are slightly altered by adding, omitting, or transposing letters. For example, the website address of the Office of Cybercrime (cybercrime.doj.gov.ph), if written by a perpetrator, could appear instead as:

cbercrime.doj.gov.ph
cybercrime-office.doj.gov.ph
cybercrime.net

e. Email comes from an unknown or slightly different email than usual

The official emails of reputable companies usually follow this format: xxxxx@(companywebsite). For example, the company website is cybercrime.com, official email normally appears in this format: xxxxx@cybercrime.com. If the email comes from xxxxx@cyber-crime.net, it is most like a phishing email.

2. Ignore any suspicious emails, text messages, or calls

If you receive suspicious emails, text messages, or calls, immediately mark the emails as “spam” and block the number that sent the message or made the call. Moreover, avoid opening or clicking any links, and downloading any attachments from suspicious and unverified senders. It is also advisable to contact your bank immediately and check the authenticity of the email, message, or call.

3. **Download and use only the official apps of your banks**

   Download only the official apps of the banks thru their official website, Google Play, or Apple App Store. Do not download and use apps from unknown and unverified sources.

4. **Use multi-factor authentication for your accounts**

   Some online accounts offer extra security by requiring two (2) or more credentials to log in to your account. This is called multi-factor authentication. The additional credentials you need to log in to your account fall into two categories:

   a. Something you have — like a passcode or one-time password (OTP) you get via text message, email, or an authentication app.

   b. Something you are — like a scan of your fingerprint, your retina, or your face.

   Multi-factor authentication makes it harder for scammers to log in to your accounts even if they do get your username and password.[6]

5. **Never share your OTP to anyone**

   Banks, financial institution, and their agents, will never ask for your OTP. If you receive an email, text message, or call asking for your OTP, immediately mark the emails as "spam" and block the number that sent the message or made the call.

6. **Avoid divulging sensitive and personal information**

   Avoid divulging personal information to anyone you don't know thru emails, text messages, or calls. Do not even share sensitive information, such as a password and log in credentials, to someone you know.

7. **Avoid online transactions while inside internet cafes or by using shared computers**

   Avoid doing online banking, online payment, and other online transactions while inside internet cafes or by using shared computers. As much as possible, online transactions should be done using your own computer or electronic gadgets that is connected to the internet using your own mobile data or WiFi. Do not undertake online financial transactions if you are connected to a public WiFi.

   However, if this cannot be avoided, make sure to properly log-out from the site after your online transaction, and clear both the browser history and browser cache of the browser you used.

[6] Accessed on 25 September 2020, https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

8. **Install security software on your computer**

   Install security software on your computer such as firewalls and anti-virus, and set the software to update automatically. These software updates usually include patches to reported security threats.

9. **Always update your mobile phone apps**

   Set your mobile banking, online payment, and online store apps to update automatically in order to be protected from security threats. These software updates usually include patches to the app's reported vulnerabilities.

10. **Check the website address**

    Make it a habit to scrutinize and validate the website address before entering any login credentials and personal information. Moreover, make it a habit to enter the full website address into your browser address bar instead of clicking the embedded links in the emails you received. Only enter your login credentials and personal information on a secure website.

    Below is a directory of banks as compiled by the Bangko Sentral ng Pilipinas as of 25 September 2020:[7]

BANK NAME	OFFICIAL WEBSITE	ONLINE BANKING WEBSITE
Al-Amanah Islamic Investment Bank of the Philippines	**https://www.amanahbank.gov.ph/**	
AllBank (A Thrift Bank), Inc.	**https://www.allbank.ph/**	
Asia United Bank Corporation	**https://www.aub.com.ph/**	**https://ebanking.asiaunited.com.ph/eBanking/**
Australia and New Zealand Banking Group Limited	***https://www.anz.com.au/personal/**	
Bangko Mabuhay (A Rural Bank), Inc.	**https://bangkomabuhay.com.ph/**	
Bangkok Bank Public Co. Ltd.	**https://www.bangkokbank.com/en**	**https://ibanking.bangkokbank.com/SignOn.aspx**
Bank of America, N.A.	**https://www.bankofamerica.com/**	
Bank of China Limited-Manila Branch	**https://www.bankofchina.com.ph/en/**	
Bank of Commerce	**https://www.bankcom.com.ph/**	**https://bankcomonline.com.ph/bankcompersonal/login**
Bank of Makati (A Savings Bank), Inc.	**https://www.bankofmakati.com.ph/**	
Bank of the Philippine Islands	**https://www.bpi.com.ph/**	**https://online.bpi.com.ph/portalserver/onlinebanking/sign-in**
BDO Private Bank, Inc.	**https://www.bdo.com.ph/personal**	**https://online.bdo.com.ph/**
BDO Unibank, Inc.	**https://www.bdo.com.ph/**	**https://online.bdo.com.ph/**

[7] Accessed on 25 September 2020, http://www.bsp.gov.ph/banking/directory.asp?BankName=&InstitutionTypeID=&submit=Find.

BPI Direct BanKO, Inc., A Savings Bank	**https://www.bpi.com.ph**	
BPI Family Savings Bank, Inc.	**https://www.bpi.com.ph**	
Card Bank, Inc. (A Microfinance - Oriented Rural Bank)	**https://cardbankph.com/**	
Cathay United Bank Co., LTD. - Manila Branch	**https://www.cathaybk.com.tw/**	
Cebuan Lhuillier Rural Bank Inc.	**https://www.cebuanalhuillier.com/cebuana-lhuilier-bank/**	
China Bank Savings, Inc.	**https://www.chinabank.ph/personal.aspx**	
China Banking Corporation	***https://www.chinabank.ph/personal.aspx**	**https://www.chinabank.ph/LoginPersonal.html**
CIMB Bank Philippines Inc.	**https://www.cimbbank.com.ph/en/home.html**	
Citibank, N.A.	**https://www.citibank.com.ph/portal/citiph_home.htm**	**https://www.citibank.com.ph/PHGCB/JSO/signon/DisplayUsernameSignon.do**
City Savings Bank, Inc.	**https://www.citysavings.com.ph/**	
Citystate Savings Bank, Inc.	**http://www.citystatesavings.com/**	**https://www.bancnetonline.com/BancnetWeb/login.do**
CTBC Bank (Philippines) Corporation	**https://www.ctbcbank.com.ph/**	
Deutsche Bank AG	***https://www.db.com/company/index.htm**	
Development Bank of the Philippines	***https://www.dbp.ph/**	**https://www.bancnetonline.com/BancnetWeb/login.do**
East West Banking Corporation	**https://www.eastwestbanker.com/**	**https://personal.eastwestbanker.com/**
Enterprise Bank, Inc. (A Thrift Bank)	**https://www.enterprisebank.ph/**	
Equicom Savings Bank, Inc.	**https://www.equicomsavings.com/**	**https://webbanking.equicomsavings.com/**
First Consolidated Bank, Inc. (A Private Development Bank)	**http://www.fcb.com.ph/**	
HSBC Savings Bank (Phils), Inc.	**https://www.hsbc.com.ph/**	
Industrial and Commercial Bank of China Limited - Manila Branch	**http://www.icbcmanila.com.cn/**	
Industrial Bank of Korea Manila Branch	**https://global.ibk.co.kr/en/**	
ING Bank N.V.	***https://www.ing.com.ph/home**	
JP Morgan Chase Bank, N.A.	**https://www.chase.com/**	**https://secure05c.chase.com/web/auth/dashboard**
KEB Hana Bank - Manila Branch	***https://www.kebhana.com/easyone_index_en.html**	
Land Bank of the Philippines	**https://www.landbank.com/**	**https://www.lbpiaccess.com/**
Malayan Bank Savings and Mortgage Bank, Inc.	***https://www.malayanbank.com/**	

Maybank Philippines, Incorporated	***https://www.maybank2u.com.my/**	**https://www.maybank2u.com.my/home/m2u/common/login.do**
Metropolitan Bank and Trust Company	**https://metrobank.com.ph/home**	**https://onlinebanking.metrobank.com.ph/signin**
Mizuho Bank, Ltd. – Manila Branch	**https://www.mizuho-fg.co.jp/index.html**	
MUFG Bank, Ltd.	**https://www.mufg.jp/english/**	
Philippine Bank of Communications	**https://www.pbcom.com.ph/**	**https://mypbcom.com.ph/**
Philippine Business Bank, Inc., A Savings Bank	**https://www.pbb.com.ph/**	
Philippine National Bank	**https://www.pnb.com.ph/**	**https://portal.pnb.com.ph/mib/login.do?app=PN**
PNB Savings Bank	**https://www.pnb.com.ph/**	**https://portal.pnb.com.ph/mib/login.do?app=PN**
Philippine Savings Bank	**https://www.psbank.com.ph/**	**https://www.psbankonline.com.ph/RemoteBankingFE/RBFELogIn.jsp**
Philippine Trust Company	**https://www.philtrustbank.com/**	
Philippine Veterans Bank	**https://www.veteransbank.com.ph/**	
Planbank "Rural Bank of Canlubang Planters, Inc."	**https://www.planbank.org/**	
Producers Savings Bank Corporation	**https://www.producersbank.com.ph**	
Queen City Development Bank, Inc. or Queenbank, A Thrift Bank	**http://www.queenbank.com.ph/**	
Rizal Commercial Banking Corporation (RCBC)	**https://www.rcbc.com**	**https://www.rcbconlinebanking.com/web/lg/Login/Index**
Rizal Microbank, Inc. - A Thrift Bank of RCBC	**https://www.rcbc.com/**	**https://www.rcbconlinebanking.com/web/lg/Login/Index**
Robinsons Bank Corporation	**https://www.robinsonsbank.com.ph/**	**https://personalonlinebanking.robinsonsbank.com.ph/**
Security Bank Corporation	**https://www.securitybank.com.ph/**	**https://www.securitybank.com/online-banking/**
Shinshan Bank – Manila Branch	**https://www.shinshan.com/en/index.jsp**	
Standard Chartered Bank	***https://www.sc.com/ph/**	**https://s2b.standardchartered.com/unifiedlogin/login/index.html?source=classic**
Sterling Bank of Asia, Inc. (A Savings Bank)	**https://www.sterlingbankasia.com/**	**https://www.sterlingbankasia.com/ebanking/online-banking**
Sumitomo Mitsui Banking Corporation-Manila Branch	**https://www.smbc.co.jp/global/**	
The Hongkong & Shanghai Banking Corporation (HSBC)	**https://www.hsbc.com.ph/**	**https://www.security.online-banking.hsbc.com.ph/gsa?idv_cmd=idv.SaaSSecurityCommand**
UCPB Savings Bank	**https://www.ucpb.com/**	
Union Bank of the Philippines	**https://www.unionbankph.com/**	**https://www.unionbankph.com/unionbankonline**
United Coconut Planters Bank	**https://www.ucpb.com/**	**https://www.ucpb.com/bankonline/**
United Overseas Bank Limited, Manila Branch	**https://www.uobgroup.com/uobgroup/index.page**	

Wealth Development Bank Corporation	**https://wealthbank.com.ph/**	**https://www.bancnetonline.com/BancnetWeb/login.do**

11. Report Phishing/Vishing/Smishing immediately

If you are a victim of a phishing, vishing, or smishing scheme, contact your financial institution immediately to prevent further damage on your account. You are likewise encouraged to report and file a complaint with the appropriate law enforcement authority for the necessary conduct of investigation.

Victims may report incidents to the following law enforcement agencies:

PHILIPPINE NATIONAL POLICE – ANTI-CYBERCRIME GROUP	Email Address:	acg@pnp.gov.ph
	Mobile No.:	(+63) 998-598-8116
	Telephone Nos.:	(+632) 8414-1560
	Website:	https://acg.pnp.gov.ph/main/
	E-Complaint:	https://acg.pnp.gov.ph/eComplaint/
	Facebook:	https://www.facebook.com/anticybercrimegroup
NATIONAL BUREAU OF INVESTIGATION – CYBERCRIME DIVISION	Email Address:	ccd@nbi.gov.ph
	Telephone No.:	(+632) 8523-8231 to 38 local 3455
	Website:	https://www.nbi.gov.ph

For your guidance and information.

ATTY. CHARITO A. ZAMORA
Officer-in-Charge
DOJ Office of Cybercrime