



FRAUD & SCAM PREVENTION



Financial Fraud Investment Scam

FRAUD

A wrongful or criminal act, resulting to a victim's financial loss

SCAMS

A dishonest, illegal scheme for making money, one that involves swindling or tricking victims



Common Types of **FRAUD**

**Card replacement
Card cloning**



**ATM Skimming
ATM Jackpotting**



Unauthorized financial transactions made on a victim's account



ATM Skimming, Jackpotting



Illegal installation of malicious hardware (e.g. camera, scanning device) and/or software in ATMs or POS devices



Scanning device copies card information to create counterfeit or clone cards



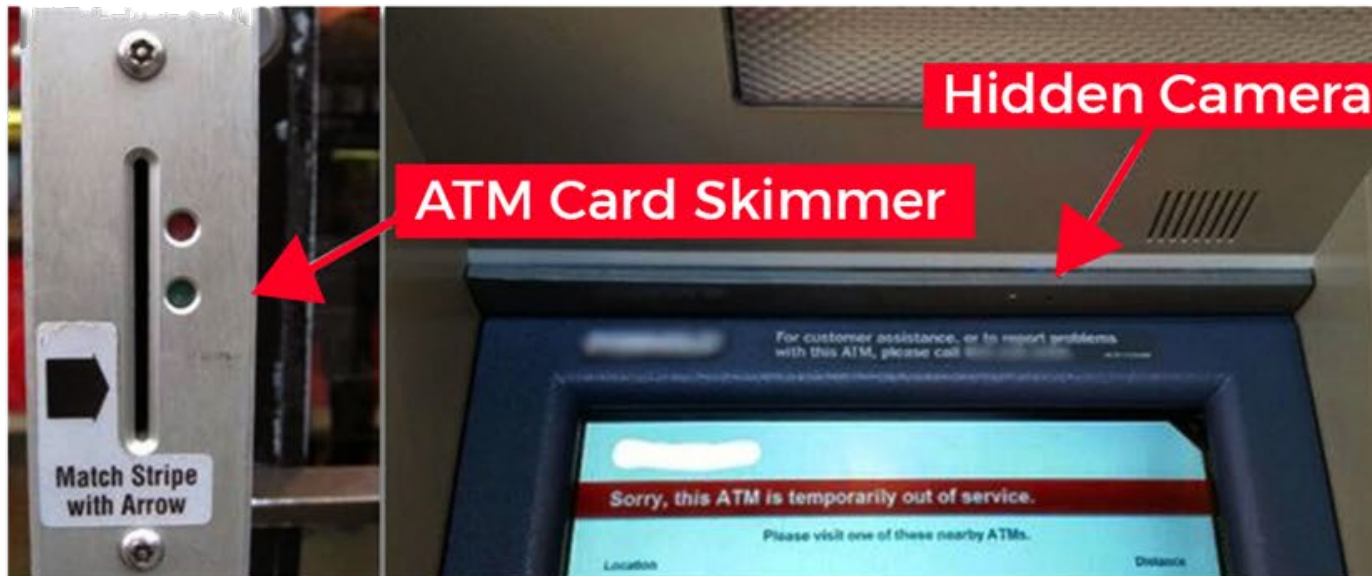
Camera captures PIN information, allowing access to accounts



Jackpotting software gives hackers control over ATM functions



ATM Skimming Devices



ATM Skimming Devices



Protect Yourself from Skimming

- ✓ Make sure that your ATM card, debit card and/or credit card is equipped with an EMV chip.
- ✓ Observe and remember the standard appearance of ATM machines and POS devices.
- ✓ If an ATM does not have a keypad shield, cover the keypad while entering your PIN.
- ✓ Withdraw only in trusted, well-lighted ATM locations. If uncomfortable, postpone your transaction or find a more secure location.
- ✓ If transacting with merchant using a POS device, keep an eye on your card and the cashier.
- ✓ Regularly check your account balance and/or billing statements. Report unauthorized or suspicious transactions to your bank or credit card issuer immediately.



Identity Theft

Root cause of fraudulent financial transactions

THEFT



FRAUD

of victim's personal
and account
information

committed using
stolen information
to access victim's
account

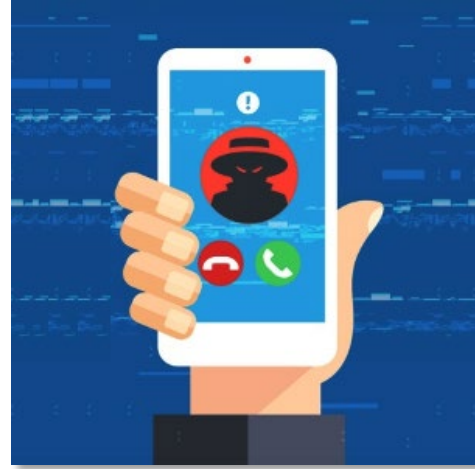
**Keep account info confidential.
Protect your personal data.**



Common Modes of Identity Theft



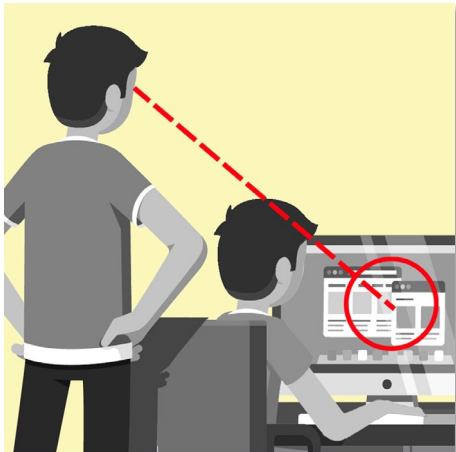
Phishing



Vishing



SMiShing



Shoulder Surfing



Dumpster Diving



Spoofing

Have you seen a phishing email?

From: xyzbank@yahoo.com → **suspicious looking email address**

Dear Internet Banking Customer, → **generic greeting**

**misspellings and
sometimes bad
grammar**

We have detected an unauthorized transaction from your **internit** banking account. In order to ensure that your account is safe and secure please click [here](#) an update your account immediately.

→ **link to spoofed website**

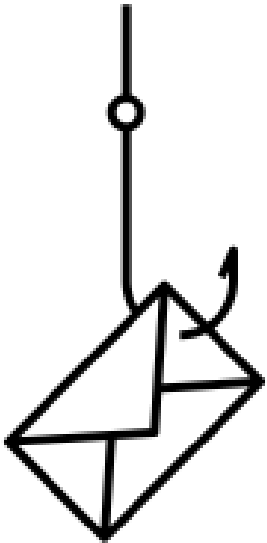
→ **sense of urgency**

We hope to serve you better.

Regards, → **no contact information**
XYZ Bank Internet Banking Help Desk



How about this email?



File Me
Ignore X
Junk - Dele
Delete
A Ap
Yo
e pdf Billing_ 161 KB
Dear Valued
Recently, the
This is detail
- Location: 3
- IP Address:
- Time: Thurs
- Browser : U
- Platform : V

Apple <olfulss@xoyceoza.dfrj>
Your account has been locked [Document ID : 2Q0102C8]

Billing_Agreement_11102017.pdf
161 KB

Attachment that contains malware

Dear Valued Client,

Generic greeting

Recently, there's been activity in your account that seems unusual compared to your normal account activites.

Deactivation scare to prompt you to act quickly

This is detail your activity:

- Location: 36 Paraduta Street, Carabobo, Spain
- IP Address: 74.77.65.54(74.77.65.54.net-uno.net)
- Time: Thursday, 12 October 2019, 02:37:05 AM
- Browser : UCWEB/2.0 (Linux; U; Opera Mini/7.1.32052/30.3697; en-US; Micromax Q334 Build/LMY471)
- Platform : Windows NT 6.1

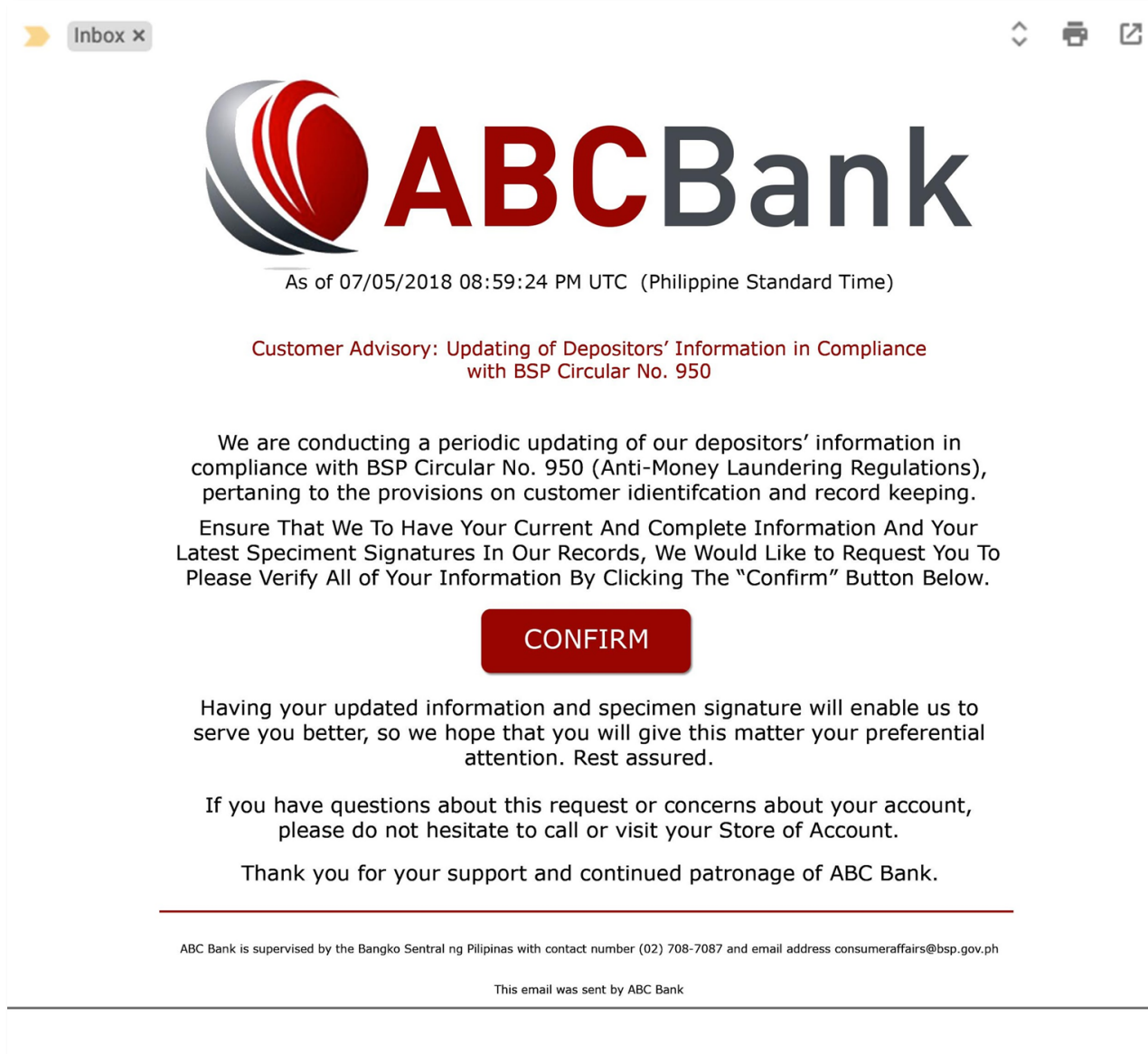
* YOUR ACCOUNT HAS BEEN DISABLE TEMPORARY

To view the details of your case please download & read (Billing_Agreement_11102017.pdf) in attachment.

If you do not

attachment.

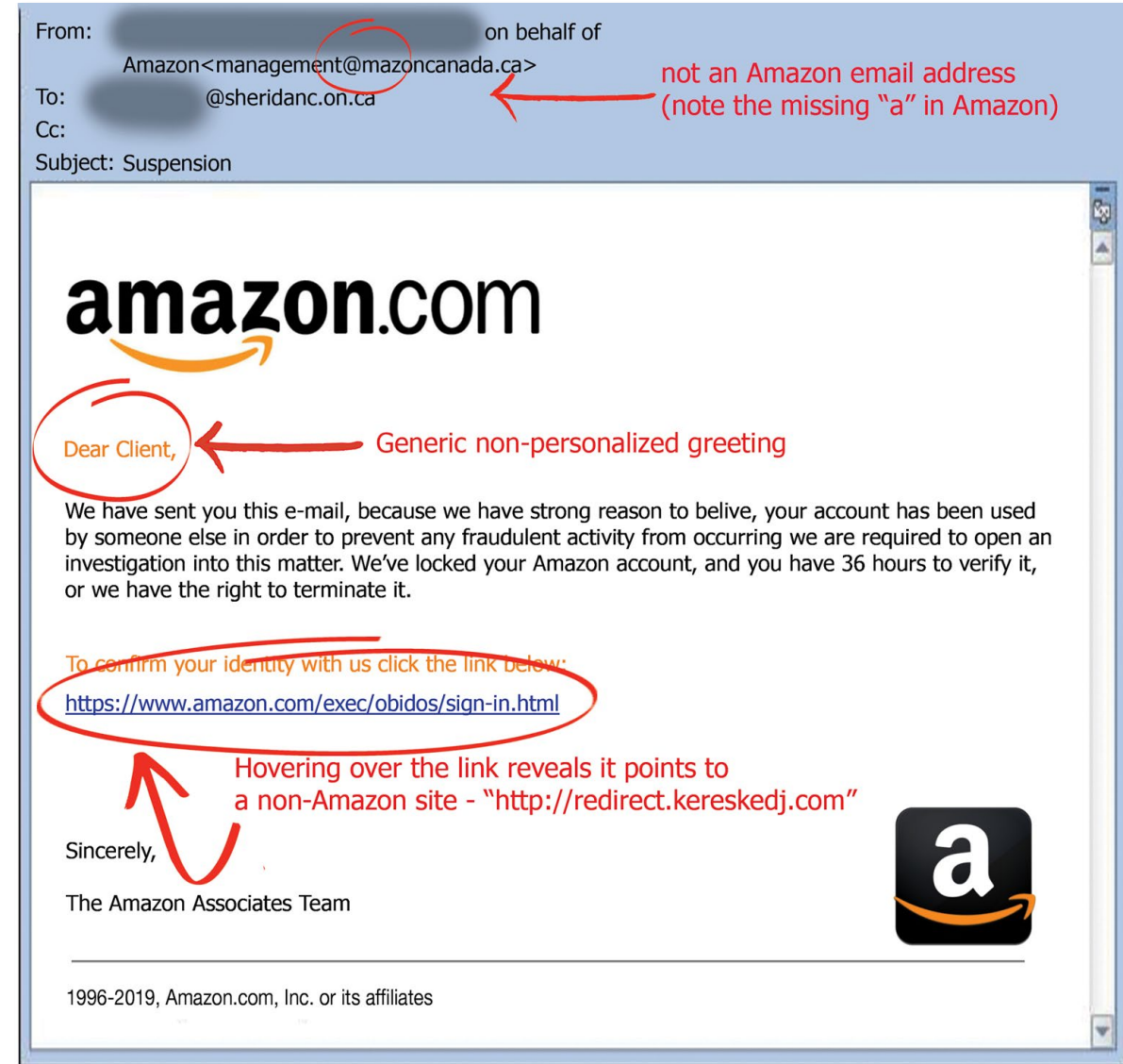
Chatbox Activity: Is this a phishing email?



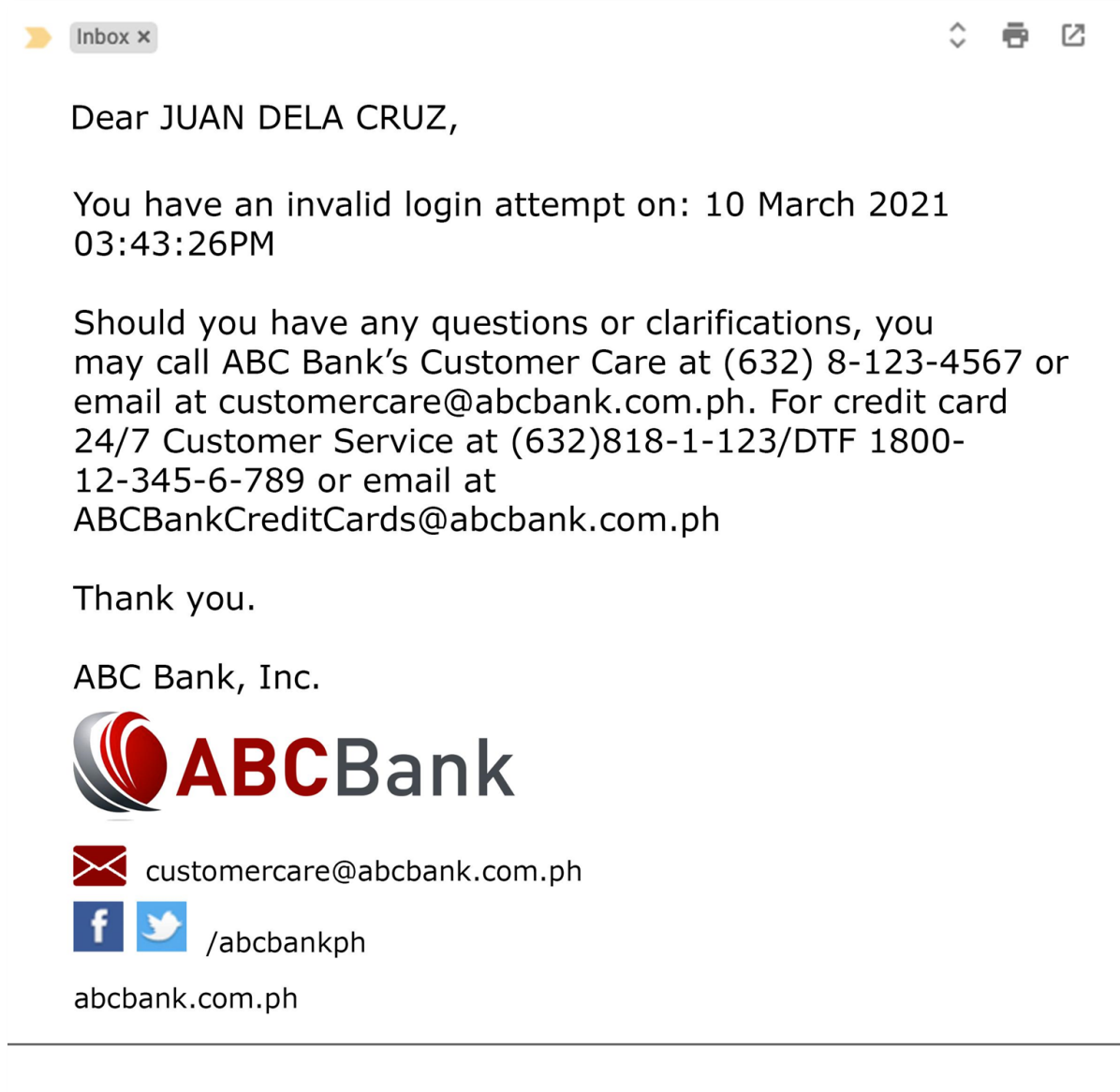
- a. Yes
- b. No
- c. I don't know

**Please type your
answer in the chatbox**

Sample phishing email



Chatbox Activity: Is this a phishing email?



a. Yes

b. No

c. I don't know

**Please type your
answer in the chatbox**

Sub-categories of phishing



Pharming – manipulation of Domain Name Server (DNS)



Spear phishing – highly targeted attacks



SMiShing – uses SMS on mobile phones



Vishing – leverages Internet Protocol (IP) based voice calling



Vishing



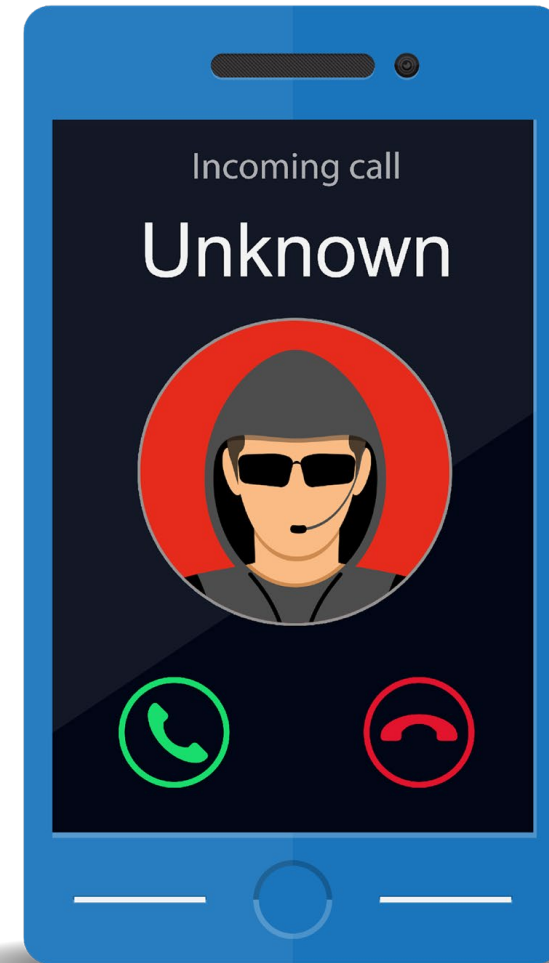
Caller claims to represent a financial institution



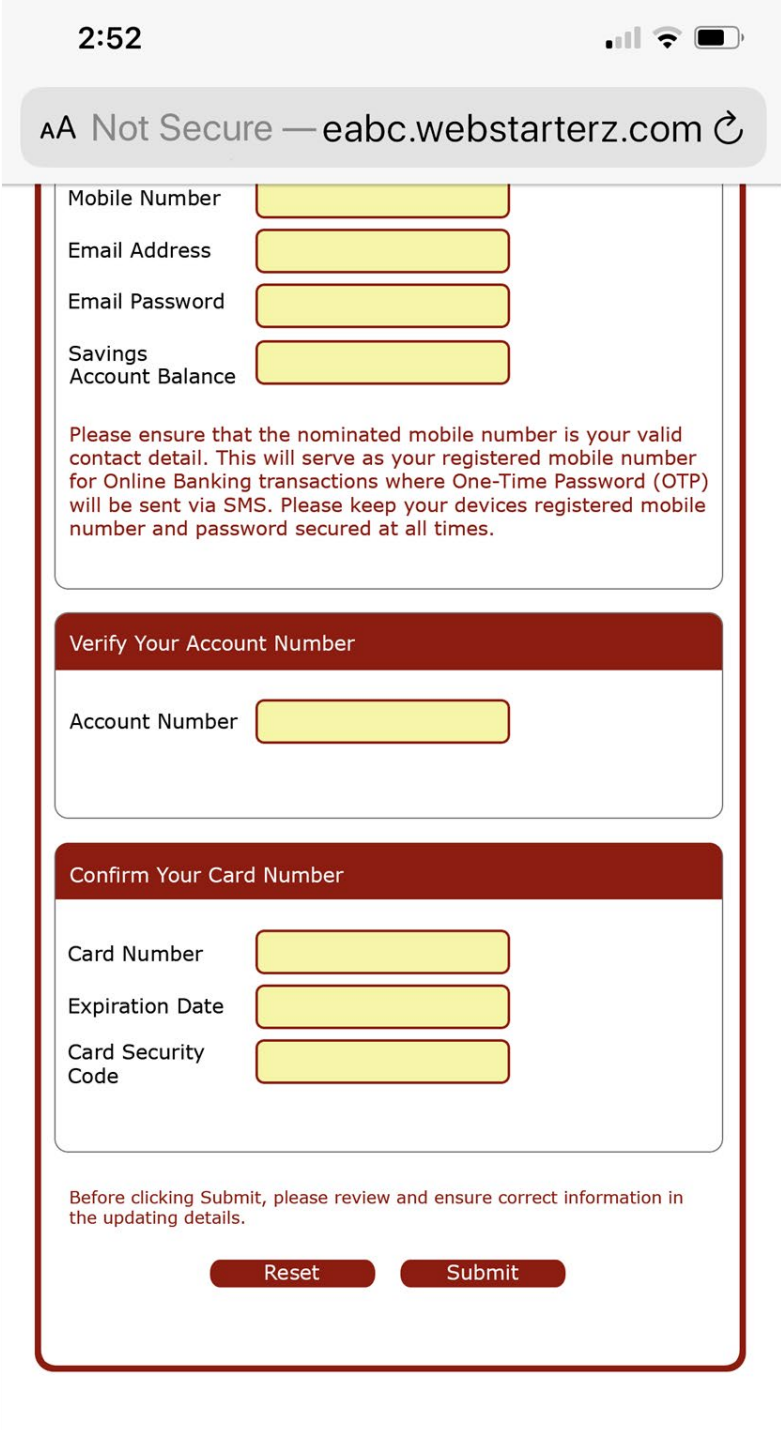
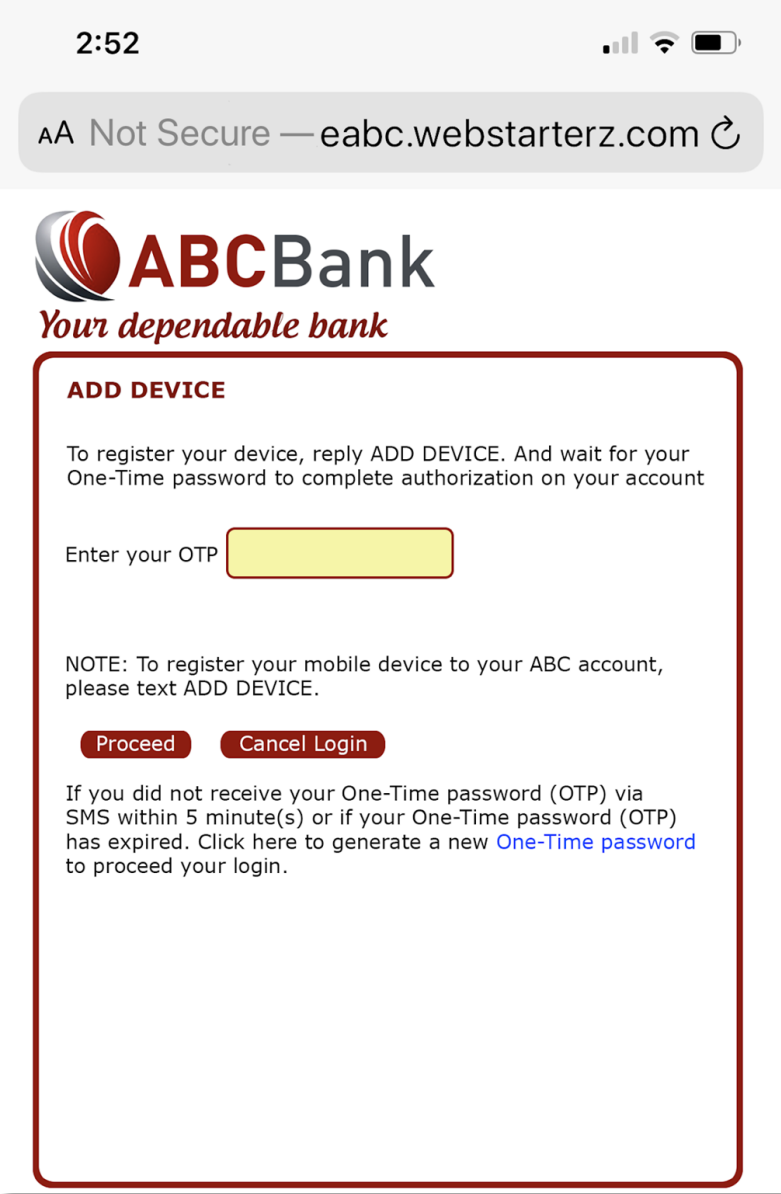
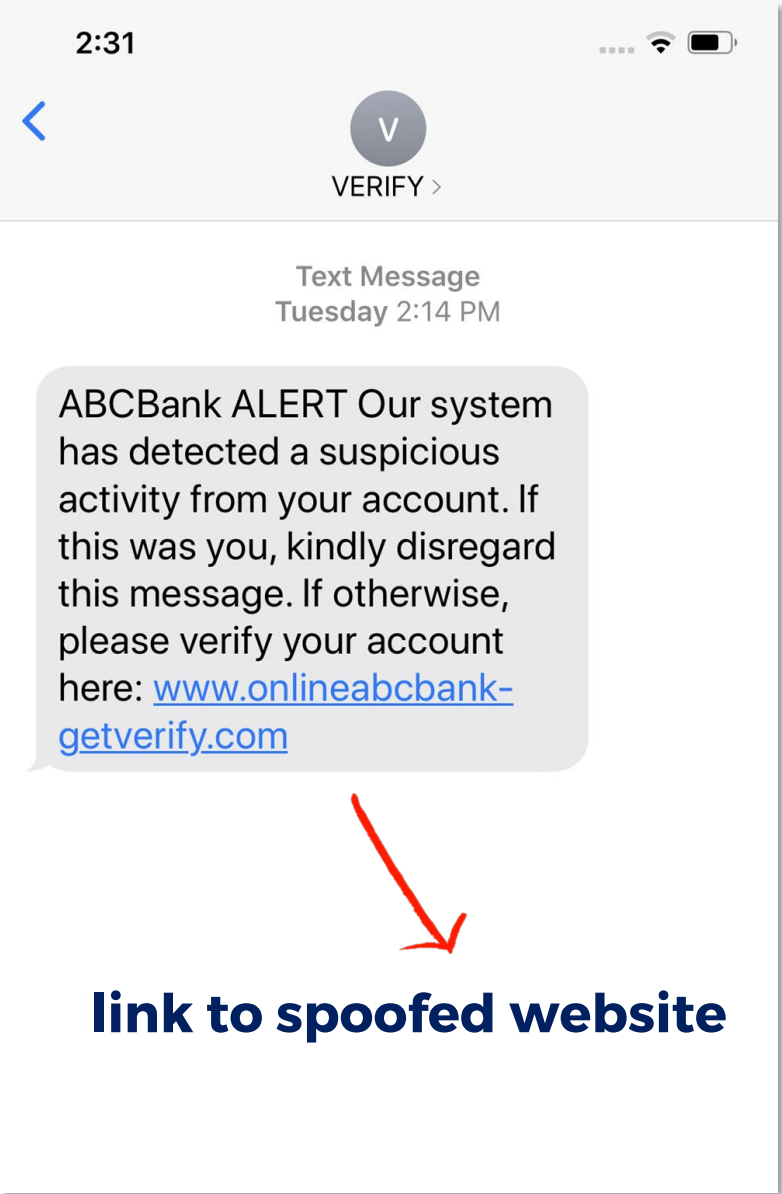
Caller creates a sense of urgency



Caller asks for personal information



Sample of SMiShing



Chatbox Activity: Is this SMiShing?

Text Message
Today 9:38 AM

someone who came in contact with you tested positive or has shown symptoms for COVID-19 & recommends you self-isolate/get tested. More at COVID-19anon.com/alert

- a. Yes
- b. No
- c. I don't know

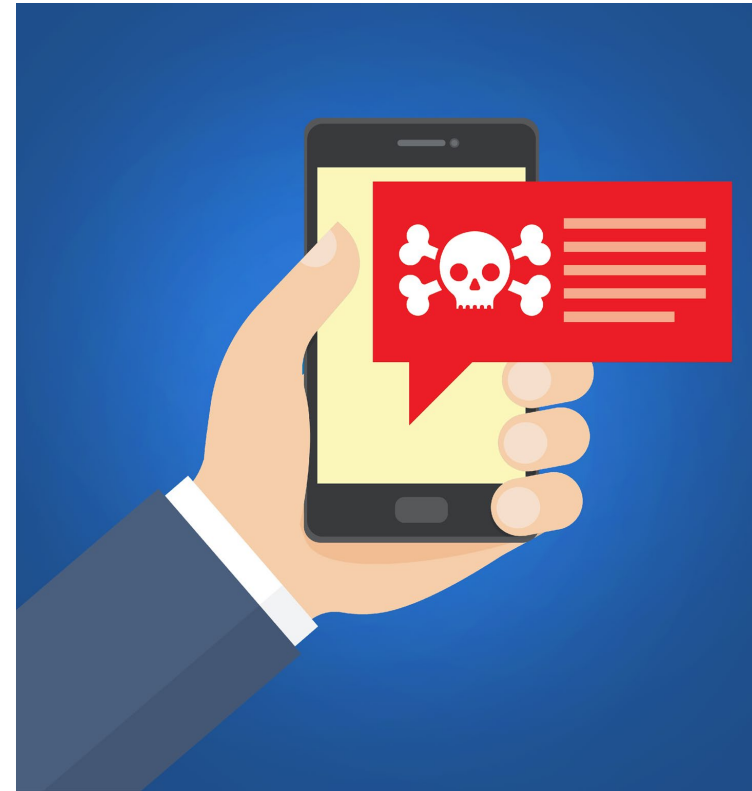
Please type your answer in the chatbox



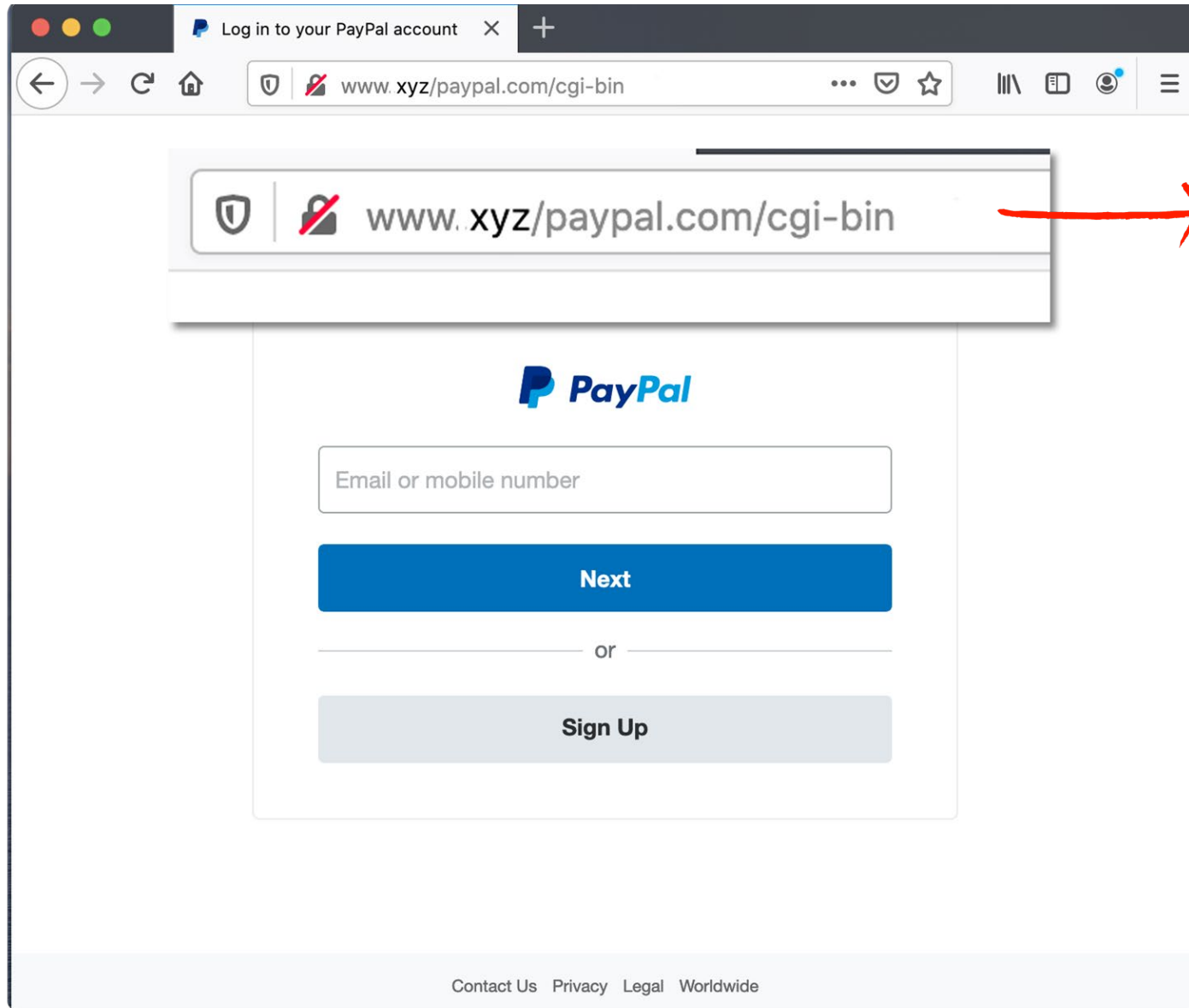
Sample of SMiShing

Text Message
Today 9:38 AM

someone who came in contact with you tested positive or has shown symptoms for COVID-19 & recommends you self-isolate/get tested. More at COVID-19anon.com/alert



Have you seen a spoofed website?



The correct PayPal url or website address is: <https://www.paypal.com>

SPOOFED



How to check if a website is fake?

The image shows a web browser window displaying a login page that mimics PayPal. The address bar shows the URL `www.xyz/paypal.com/cgi-bin`. The page features the PayPal logo, a text input field for "Email or mobile number", and two buttons: a blue "Next" button and a grey "Sign Up" button. Red arrows point from the text "NOT PayPal" to the "Next" button and from "NOT Encrypted!" to the "Sign Up" button.

Overlaid on the right is the "Page Info" window for the URL `http://xyz.paypal.com/cig-bin`. The "Security" tab is active, showing several red warning icons. The "Website Identity" section indicates the website is `www.xyzpaypal.com/cgi-bin` and that the owner has not supplied ownership information. The "Privacy & History" section shows that cookies are used and no passwords are saved. The "Technical Details" section, which is circled in red, displays a red warning icon and states: "Connection Not Encrypted. The website `www.bsp.gov.ph` does not support encryption for the page you are viewing. Information sent over the Internet without encryption can be seen by other people while it is in transit."

At the bottom of the browser window, there are links for "Contact Us", "Privacy", "Legal", and "Worldwide".

Protect yourself from phishing and spoofing!

Be wary of emails, calls, or text messages that...



Ask for your personal information



Have a generic greeting, misspelling or bad grammar



Are unexpected or not typically received



Link you to another website



Does not give you full contact details of the sender



Chatbox Activity: What will you do if you received this email?

XYZ Bank

As of 07/05/2020 08:59:24 PM UTC (Philippine Standard Time)

Customer Advisory: Updating of Depositors' Information in Compliance with BSP Circular No. 950

We are conducting a periodic updating of our depositors' information in compliance with BSP Circular No. 950 (Anti-Money Laundering Regulations), pertaining to the provisions on customer identification and record keeping.

Ensure That We To Have Your Current And Complete Information And Your Latest Specimen Signatures In Our Records, We Would Like to Request You To Please Verify All of Your Information By Clicking The "Confirm" Button Below.

VERIFY

Having your updated information and specimen signature will enable us to serve you better, so we hope that you will give this matter your preferential attention. Rest assured.

If you have questions about this request or concerns about your account, please do not hesitate to call or visit your Store of Account.

Thank you for your support and continued patronage of XYZ Bank.

XYZ Bank is supervised by the Bangko Sentral ng Pilipinas with contact number (02) 708-7087 and email address consumeraffairs@bsp.gov.ph

This email was sent by XYZ Bank

a. Click the link to verify my account

b. Verify with my bank by calling its hotline directly

Please type your answer in the chatbox








When you encounter phishing or spoofing...

- Verify with your bank by calling its hotline directly.
- Report the phishing and spoofing attempts to your bank immediately!



Safeguard your gadgets

-  Update security and anti-virus features. Upgrade operating systems and apps.
-  Download only the legitimate banking apps and online shopping apps.
-  Do not download and install suspicious software, files and email attachments.
-  Do not use jailbroken or rooted mobile phones or gadgets.
-  Do not let other people use your gadgets.



Secure your connectivity

- 🔒 Avoid using public computers and free WiFi connections.
- 🔒 Set your WiFi router to the highest security settings.
- 🔒 Enable router firewall and encryption.
- 🔒 Reduce your WiFi signal range.









Secure your online activity

- 🔒 Type the address or url directly on the address bar.
- 🔒 Make sure the website is secure and legitimate (“https”).
- 🔒 Clear your browsing history or cache regularly.
- 🔒 Disable plug-ins, and the “Save passwords” feature.
- 🔒 Always log-out from websites and apps after every use.



Protect your online transactions

-  Transact only with legitimate and trustworthy online vendors.
-  Activate a 2-step verification process or multi-factor authentication.
-  Keep transaction records and regularly review your transaction history.
-  Enable text or email alerts for any activity on your accounts.
-  Report suspicious account activity to your bank immediately.
-  Do not share account and personal information (e.g., account number, card number, full name, passwords, PIN, CVV) with anyone.



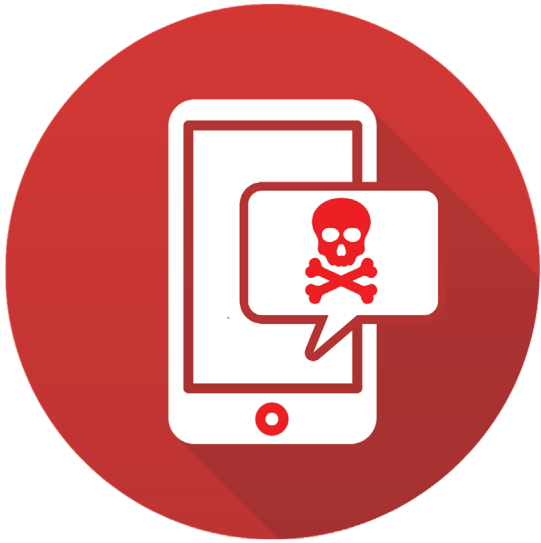
Chatbox Activity

The best way to create a strong password is to use:

- a. Your initials, or birthday, or your mother's maiden name
- b. PassWord12345
- c. Capital and small letters, with numerals and symbols, in a combination that only you can remember
- d. Same passwords for all accounts, including email and social media
- e. A list of passwords written on a piece of paper



Common Types of SCAMS



**Text
Scams**



**Unexpected
Money Scam**



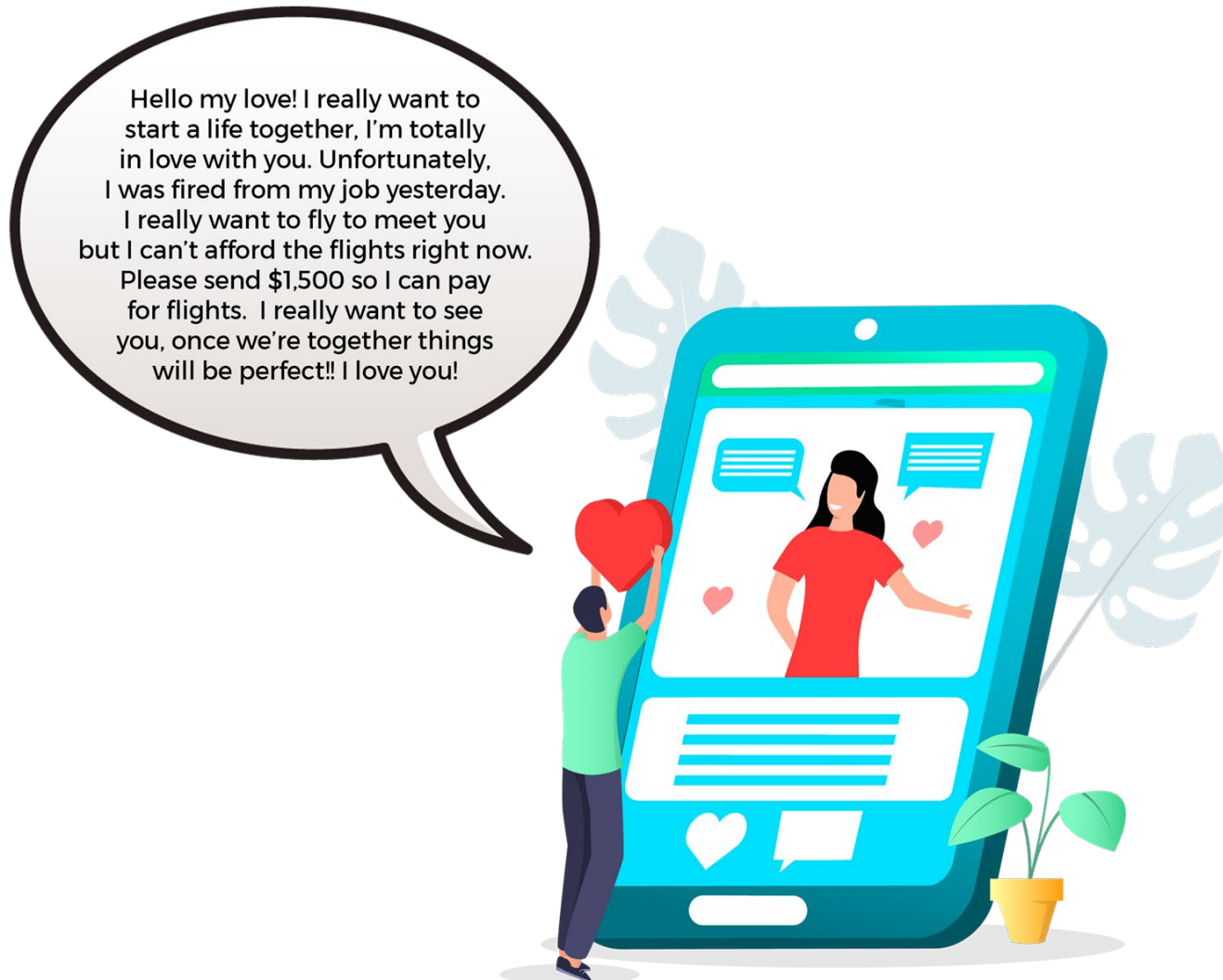
**Romance
Scam**



**Threat,
Extortion
Scam**



Chatbox Activity: Is this a scam?



- a. Yes**
- b. No**
- c. I don't know**

**Please type your
answer in the
chatbox**



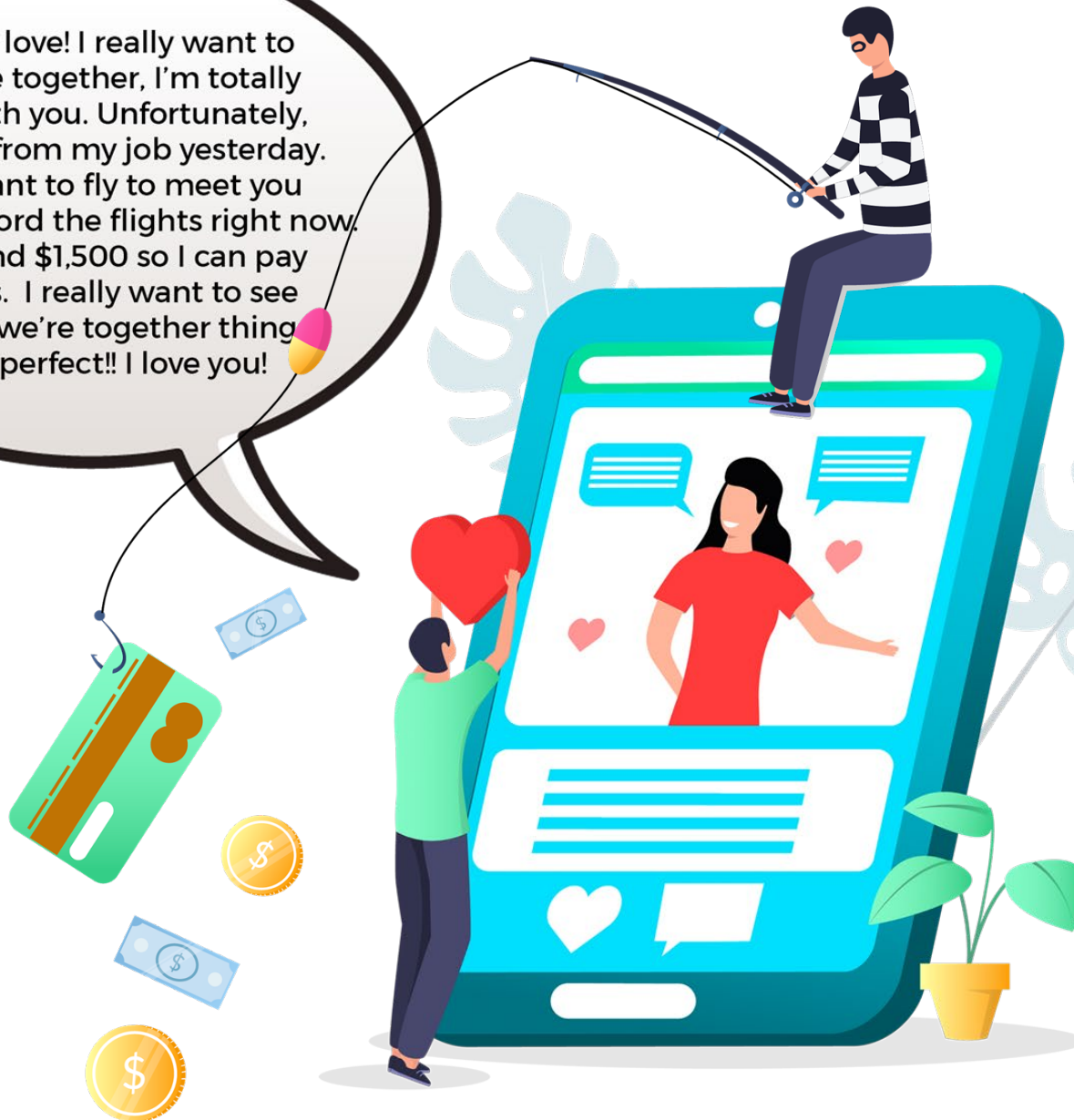
Chatbox Activity: Is this a scam?

Hello my love! I really want to start a life together, I'm totally in love with you. Unfortunately, I was fired from my job yesterday. I really want to fly to meet you but I can't afford the flights right now. Please send \$1,500 so I can pay for flights. I really want to see you, once we're together thing will be perfect!! I love you!

Answer:

YES

A Romance Scam



Common Types of SCAMS



**Donation,
Charity Scam**



**Travel
Troubles Scam**



**Job Offer
Scam**



**Unexpected
Prize Scam**



SCAMS During This Pandemic



**Money Mules
Scam**



**Sim Swap
Scam**



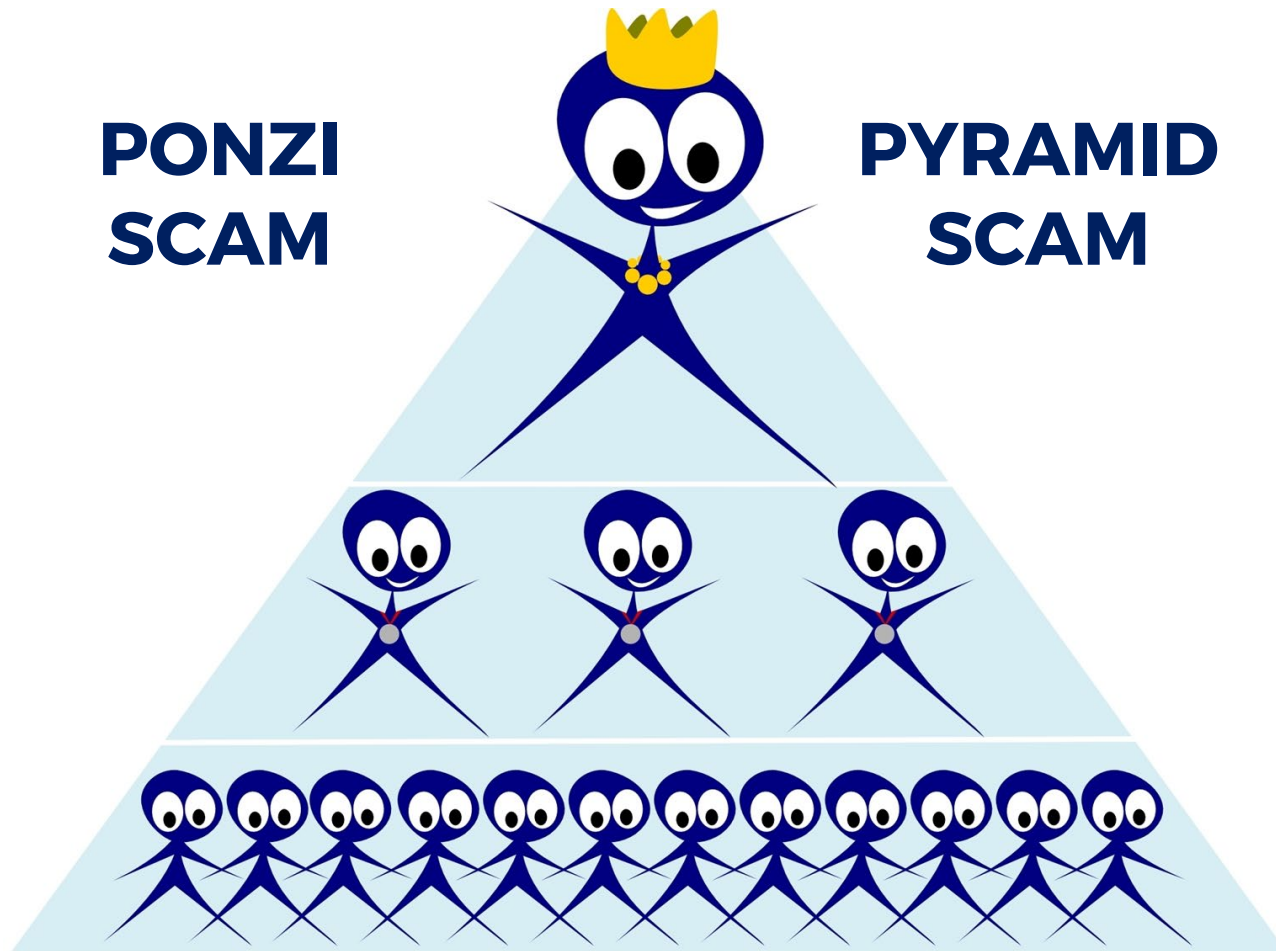
**Bogus Online
Seller/Agent**



**Advance
Fee**



Investment Scams

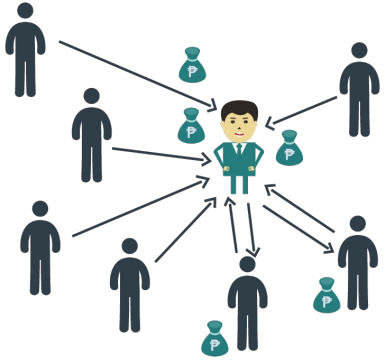


No legitimate businesses or investments



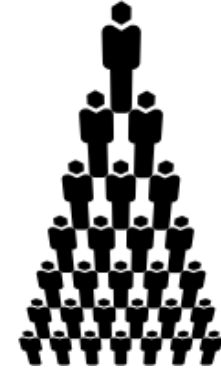
Main source of funds are money from new recruits or investors





Ponzi

Pyramid



Focus on cash investment and recruitment



Focus on products and recruitment



Promises high interest/return on investment within a short time period



Products have little or no real value



Earns from cash investment paid by new recruits



Members are compensated based on new recruits and downlines



Chatbox Activity

Is multi-level marketing a pyramid scam?

- a. Yes
- b. No
- c. It depends on certain factors
- d. I don't know



Multi Level Marketing

DSAP 8-Point Test

1. Is there a **product**?
2. Are **commissions paid on sale** of products and not on registration/entry fees?
3. Is the **intent to sell** a product not a position?
4. Is there **no direct correlation** between the number of **recruits and compensation**?
5. If recruitment were to be stopped today, will the participants **still make money**?
6. Is there a reasonable **product return policy**?
7. Do products have **fair market value**?
8. Is there a compelling **reason to buy**?

CAUTION

If the answer to any of the questions is **NO**, it might be a SCAM!

Protect yourself from investment scams!



Do not believe offers that are too good to be true (e.g., double your money, no risk, returns guaranteed).



Check if company is licensed by the Securities and Exchange Commission (SEC). Report suspicious companies to SEC.



Verify if investment product being sold is also licensed by SEC (secondary license). Report suspicious investment products and activities to SEC.



Always remember...



Protect your personal and account information.

Report suspicious account transactions to your Financial Institution immediately.

Offers that are too good to be true, are usually not true.

Report suspicious investment schemes to SEC and/or NBI.

