BANGKO SENTRAL NG PILIPINAS

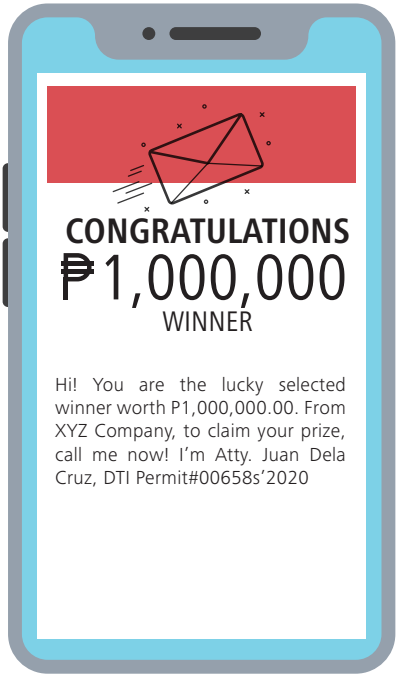
HOW MUCH DO YOU KNOW ABOUT FRAUD AND SCAMS

Note:

- This quiz is for educational purposes only. Companies and individuals named in the quiz are all fictitious. Any similarity of names with an actual person or company is purely coincidental.
- Put a checkmark (✓) in the box corresponding to the correct answer.

Question #1

Is this a scam?



☐ Scam

☐ Not a scam

Answer:

Scam. Text scams come in many forms. Common ones include winning a raffle you did not join and asking you to pay shipping fee to receive the prize. Remember to always be cautious when dealing with unexpected text messages from strangers or random people.

Question #2

Which of the following should never be disclosed to anyone?

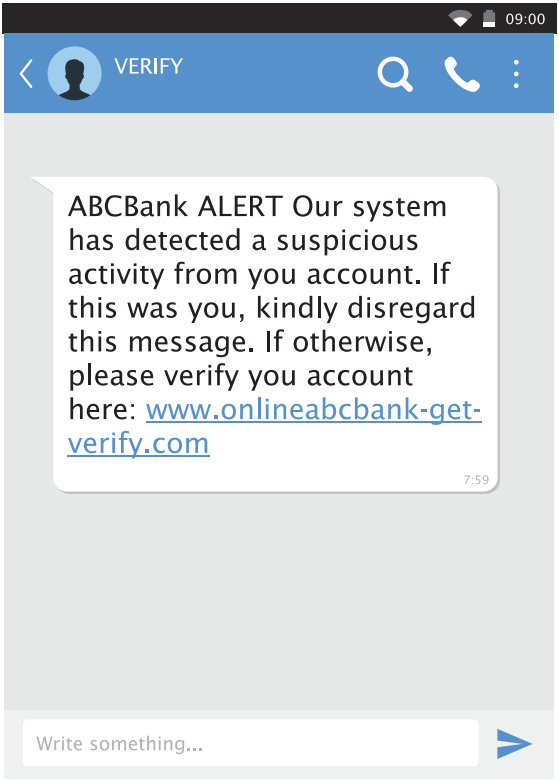
- ☐ Your ATM card's Personal Identification Number (PIN)
- ☐ Your One-Time Password (OTP) sent to your mobile number
- ☐ Your credit card's Card Verification Value (CVV)
- ☐ All of the above

Answer:

All of the above. Your credit card number, CVV, OTP, PIN, ID number and other personal and sensitive information should never be disclosed to anyone.

Question #3

Is this a scam?



☐ Scam

☐ Not a scam

Answer:

Scam. Fraudsters use SMS on mobile phones to get your personal details. The link may lead you to a fake website. Make sure all account transactions are done in the actual website or mobile app of your Financial Service Provider.

Question #4

Is this a scam?

☐ Scam

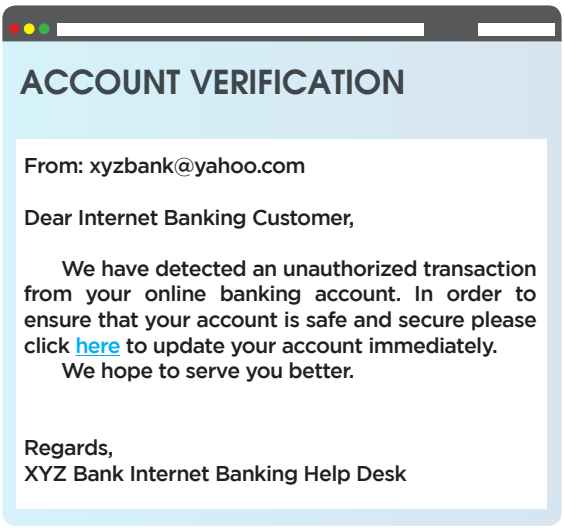
☐ Not a scam

Answer:

Scam. You are contacted unexpectedly with an investment offer and claims that the investment opportunity will guarantee you a high return. You are also pressured into signing up immediately. Remember to always be wary of high-pressure offers that are too good to be true.

Question #5

What will you do if you receive this email?



ACCOUNT VERIFICATION

From: xyzbank@yahoo.com

Dear Internet Banking Customer,

We have detected an unauthorized transaction from your online banking account. In order to ensure that your account is safe and secure please click here to update your account immediately.
We hope to serve you better.

Regards,
XYZ Bank Internet Banking Help Desk

☐ Click the link to verify my account

☐ Verify with my bank by calling its hotline directly

Answer:

Verify with my bank by directly calling its hotline. Phishing scams usually involve a suspicious looking email, a generic greeting, misspellings and bad grammar, a link to a fake website, and a signature that does not include any contact information. If you receive phishing and spoofing attempts, immediately report it to your bank.

Question #6

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

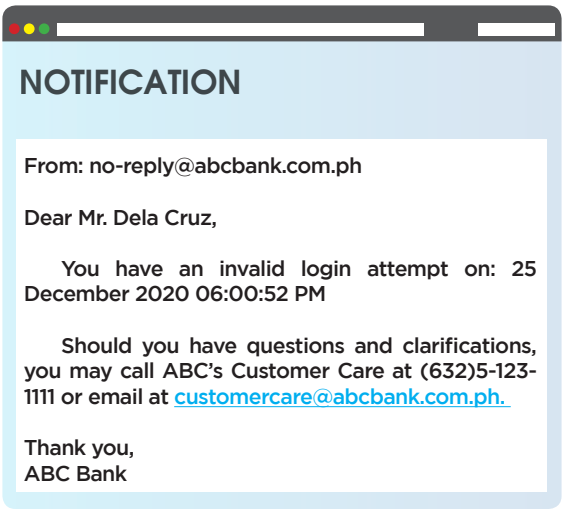
- ☐ Your initials, or birthday, or your mother's maiden name
- ☐ PassWord12345
- ☐ Capital and small letters, with numbers and symbols, in a combination that only you can remember
- ☐ Same password for all accounts, including email and social media
- ☐ A list of passwords written on a piece of paper

Answer:

Capital and small letters, with numerals and symbols, in a combination that only you can remember. Using passwords that contain words in the dictionary or contain your personal details like birthday and initials are easy to guess for hackers. Having different passwords across different online accounts and not writing it down in a piece of paper, and using mnemonics to create and remember your passwords can provide additional security.

Question #7

Is this a scam?



NOTIFICATION

From: no-reply@abcbank.com.ph

Dear Mr. Dela Cruz,

You have an invalid login attempt on: 25 December 2020 06:00:52 PM

Should you have questions and clarifications, you may call ABC's Customer Care at (632)5-123-1111 or email at customercare@abcbank.com.ph.

Thank you,
ABC Bank

☐ Scam

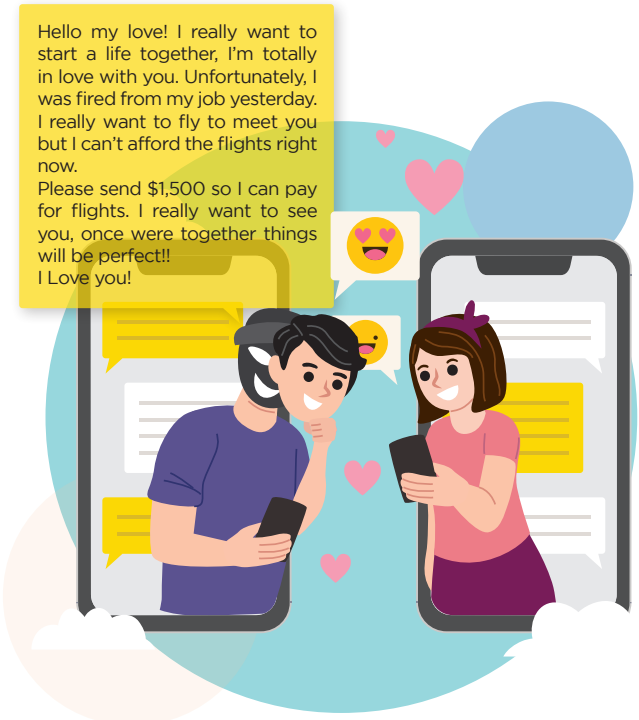
☐ Not a scam

Answer:

Not a scam. ABC Bank is informing its client about an invalid login attempt that is detected from its systems. If this happens to you, and you did not log in at the date and time stated in the email/text, contact your bank immediately.

Question #8

Is this a scam?



☐ Scam

☐ Not a scam

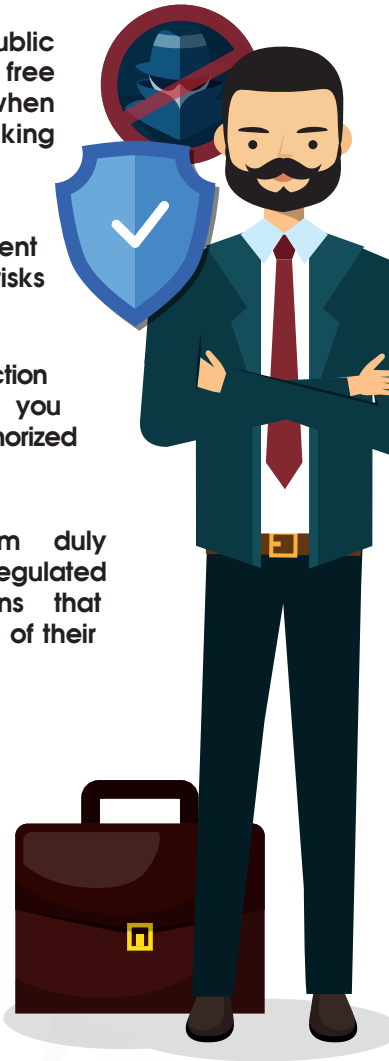
Answer:

Scam. Scammers target victims by creating fake profiles on social media or legitimate dating websites. Scammers will then express strong emotions and gain trust of victims then ask for money, financial and personal details for a variety of reasons (e.g., loss of job, involvement in accident, or serious illness).

Question #9

Which statement is NOT correct?

- ☐ Avoid using public computers and free WIFI connections when making online banking transactions
- ☐ Legitimate investment products have no risks
- ☐ You have no protection or recourse when you transact with unauthorized online lenders
- ☐ Borrow only from duly registered and regulated financial institutions that protect the welfare of their clients



Answer:

Always remember that all investments (i.e., business, financial and non-financial assets) are subject to the risk-return trade-off: The higher the expected return, the higher the potential risk. There is no such thing as risk-free investments.

Question #10

How can you protect yourself from identity theft?

- ☐ Activate a 2-step verification process or multi-factor authentication
- ☐ Shred personal documents and bank statements before putting them in the trash bin
- ☐ Visit your bank to update your contact information
- ☐ All of the above

Answer:

All of the above. Activate a multi-factor authentication such as One-time Password (OTP), security questions, biometrics, email and text alerts to get notified every time there is a transaction involving your accounts and cards. Safeguard your ID/ATM/Debit/Credit cards, bank statements and billing statements. Immediately report incidences of skimming, cloning, phishing, vishing, and spoofing to your bank or financial institution.

Question #11

How to check if a website is legitimate?

- ☐ Look for the contact information and try them out
- ☐ Check if the web address starts with https:// and the closed padlock icon should be visible
- ☐ Be familiar with addresses and domain names of legitimate websites and type them directly on the address bar
- ☐ Watch out for poor grammar and spelling
- ☐ All of the above

Answer:

All of the above. Always check the address bar and domain name of the website. Watch out for poor grammar and spelling. Try the contact information and do your research before using the website.

Question #12

If there is only a small amount of money involved, it is probably not a scam.

☐ True

☐ False

Answer:

False. Regardless of the amount of money involved, you should always be alert and think critically before giving money. Be aware of the warning signs of scams.

Congratulations!

You have finished the FRAUD and SCAM Quiz. Remember that scammers are getting smarter so always be on guard!

For more information on the common types of frauds and scams, check out our brochure, ***"Protect Yourself from Fraud and Scam".***

BANGKO SENTRAL NG PILIPINAS

A. Mabini Street, Malate, Manila 1004

Consumer Protection and Market Conduct Office
Strategic Communication and Advocacy
Email: consumeraffairs@bsp.gov.ph
Direct Line: (02) 5306-2584 | (02) 8708-7087
Trunkline: (02) 8708-7701 loc. 2584
Facsimile: (02) 8708-7088

BSP Online Buddy (BOB) Chatbot

Webchat
https://www.bsp.gov.ph

Facebook Messenger
@BangkoSentralngPilipinas

SMS
21582277
(for Globe subscribers only.