MODULE 7

DIGITAL TAYO

Avoiding Scams

This module was reviewed by Get Safe Online.
To learn more about this partner, visit getsafeonline.org

Meta | Digital Tayo

Check-In

In our Zoom chat, type out your answer to the question:

What’s the most common type of scam you’ve encountered online?

House Rules

Kindly change your name to:

ORG_NAME
(e.g. AHA! BD_Juan Dela Cruz).

Always show respect. This is a safe space.

Unmute only when you are speaking.

Press Zoom's Raise Hand button if you want to speak. When called, kindly unmute yourself and answer.

Learning Objectives

Understand what scams are and the common types

Be able to identify the different types of scams

Understand the ways to avoid scams

Understand the actions steps or how to respond if you are scammed

Relevant Facebook Community Standards

- Regulated Goods
- Fraud and Deception
- Cybersecurity

To learn more about **Facebook's Community Standards**, visit:

REGULATED GOODS
facebook.com/communitystandards/regulated_goods

FRAUD AND DECEPTION
facebook.com/communitystandards/fraud_deception

CYBERSECURITY
facebook.com/communitystandards/cybersecurity

What are scams?

What are scams?

Scams are fraudulent actions that can be used to cheat someone out of money or confidential information.

Scams can happen in a variety of ways, including through online dating apps, email, social media sites, phone calls, text messages and even traditional letters or other documents.

What scams have you experienced?

Common Scams

- Romance Scams
- Lottery Scams
- Loan Scams
- Access Token Theft
- Job Scams

Learn more about how to avoid scams on Facebook, by visiting: facebook.com/help

Common Scams

- Financial scams that can include charity, lottery, employment scams, and other payment scams
- Identity or medical information theft
- Romance scams that can include catfishing and online dating scams
- Tech support scams that can include access token theft

Why do you think it’s important to learn about scams? How can it benefit you?

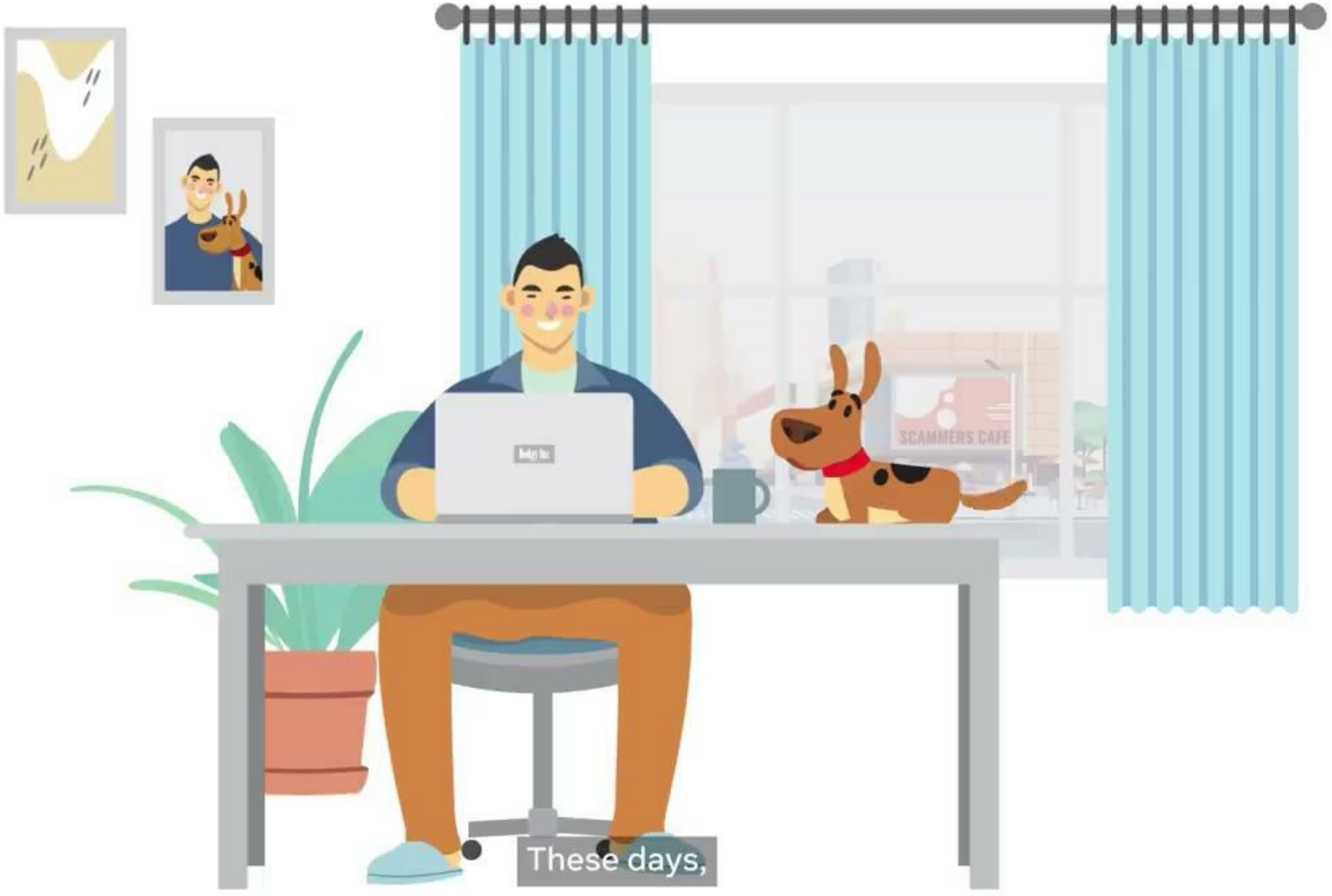
List and discuss!

Who is a target for scams?

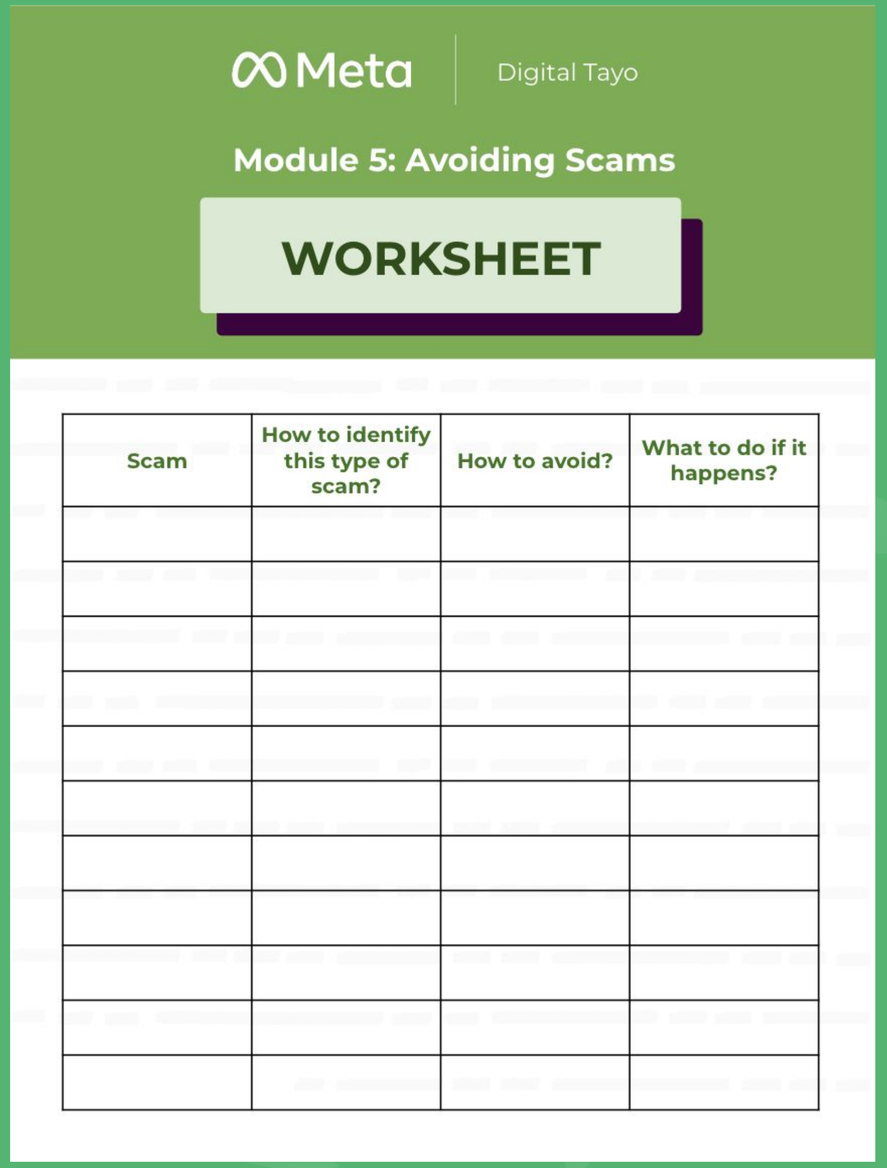
- **Anyone** can be a target.
- If you regularly click links, attachments, and images within emails from unknown sources, this can put you at risk and let scammers know that you might be more susceptible to scam messages.

Now that it is clear why this is important, we'll:

1. Learn how to identify scam and what you can do to avoid it (tips and things to remember);
2. Learn how to respond if it happens; and.
3. Test what we learned.


SCAMMERS CAFE
These days,

As we go through each type of scam, write on your worksheet what the scam is and what you can do about it (tips)!


Meta | Digital Tayo

Module 5: Avoiding Scams

WORKSHEET

Scam	How to identify this type of scam?	How to avoid?	What to do if it happens?

We'll have **tip stops** to hear from you if you have any experiences or tips to share!

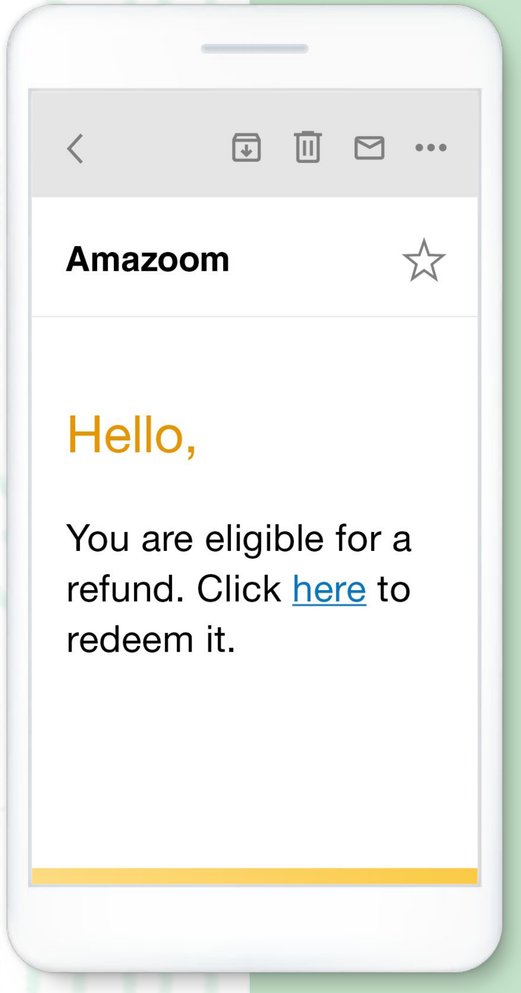
Which scams are new to you?

- Phishing
- Tech Support Scam
- Online Shopping
- Lottery Scam
- Catfishing
- Tax Scam
- Donation Scam
- Financial Scam
- Online Dating Scam

Now that it is clear why this is important, we'll:

1. **Learn how to identify scam, and what you can do to avoid it (tips and things to remember)**
2. How to respond if it happens
3. Test what we learned

Phishing



Phishing is a type of scam that tricks people into sharing their login or personal information.

- Usually via **emails**, **text** messages, phone **calls**, and **social media** posts.
- The messages or emails might look like they are from a real company that you know or trust, like a bank, online store, social networking site, parcel delivery service, or government department.

What is Phishing?

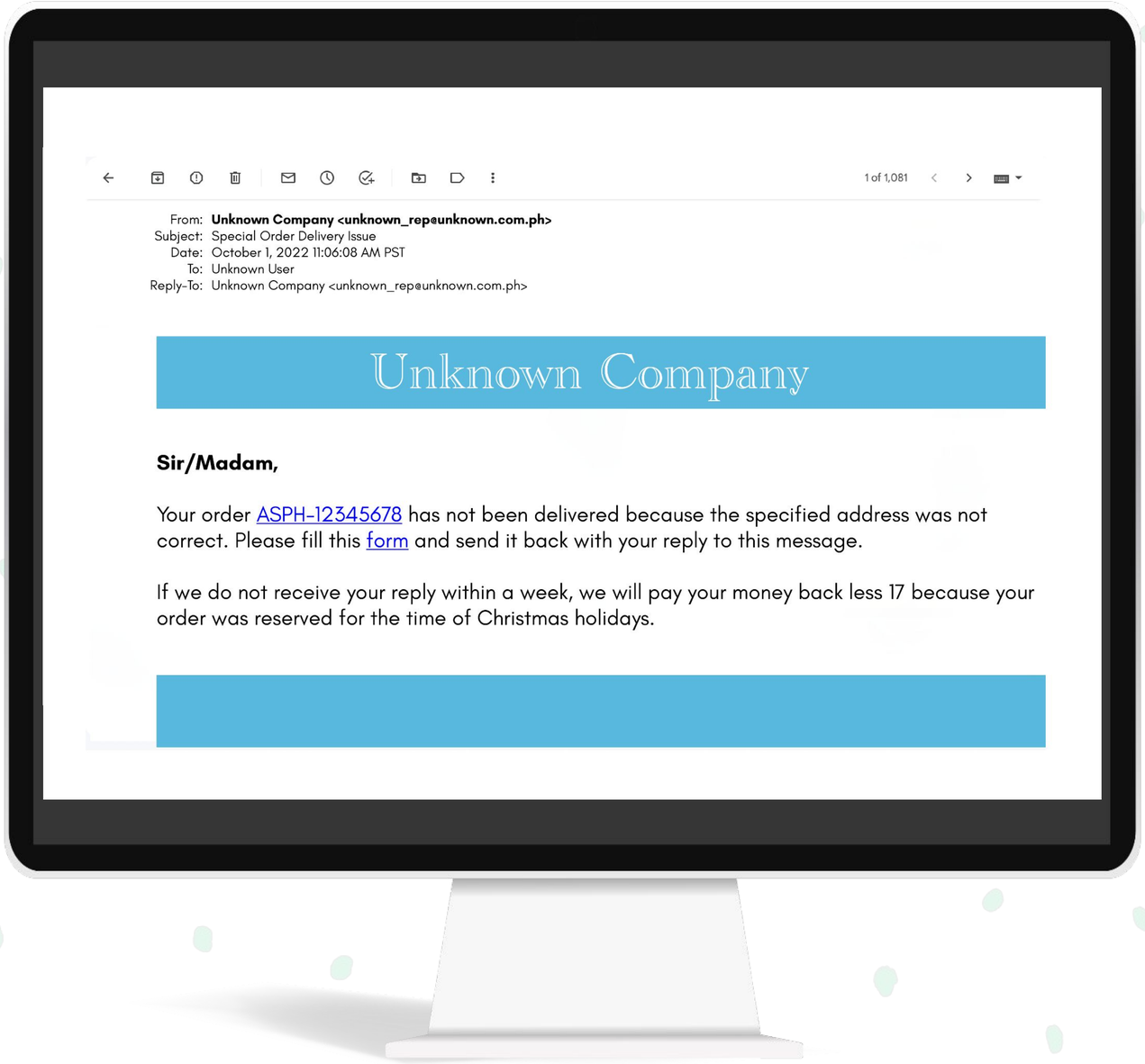
Phishing messages might use the following strategies to entice people to click on a link, open an attachment, or share login or personal information:

- Ask for confirmation of your personal information, such as bank account login details, date.
- Claim there is a problem with your account or payment information.
- Include a fake bill or invoice, or a link to make/view a payment.
- Offer a coupon for free stuff that seems too good to be true.
- Send a notice about suspicious activity or login attempts for one of your accounts.
- Tell you that you are eligible for a payment or refund.

PHISHING OR NOT PHISHING?

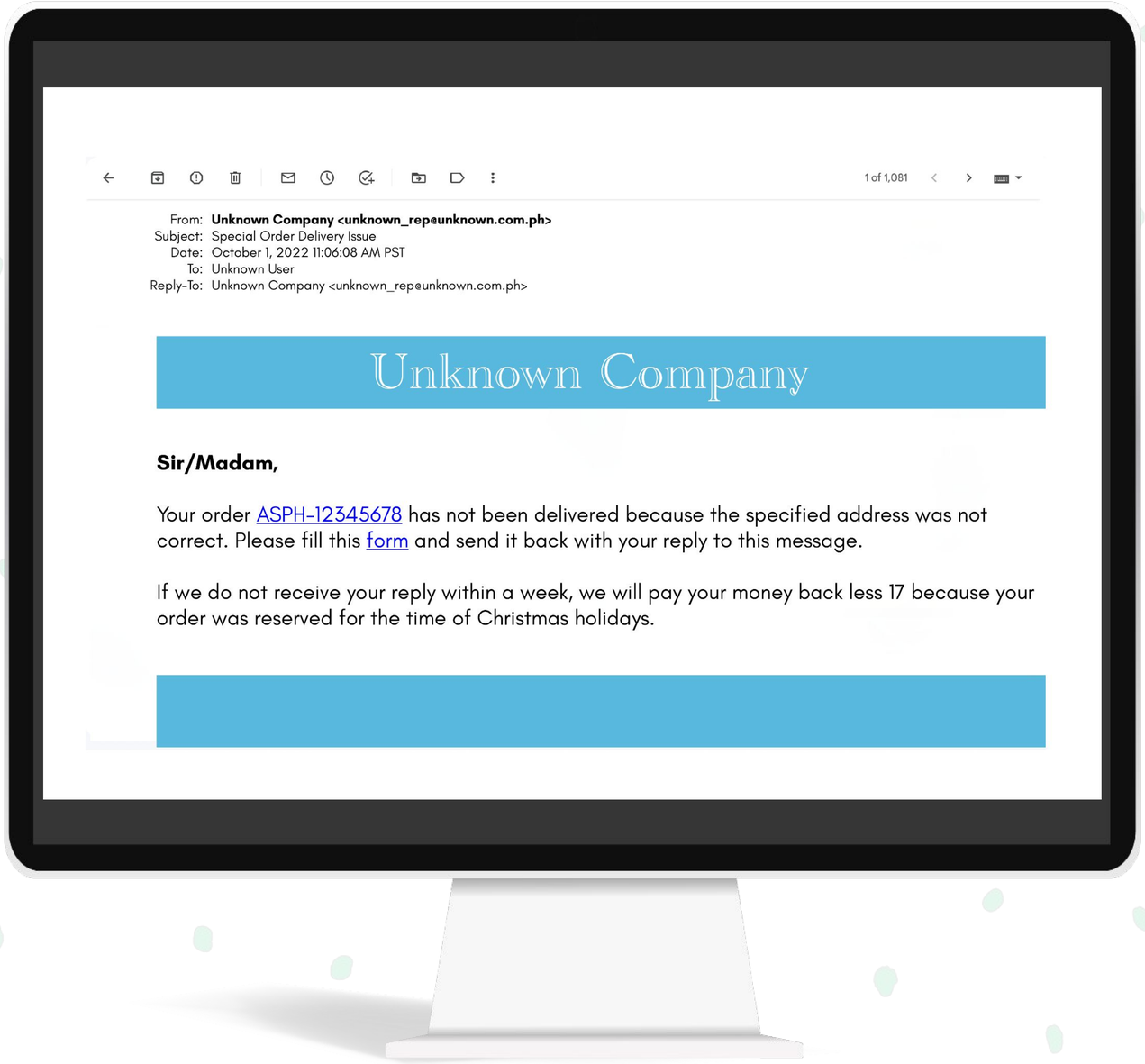
Raise your hands on Zoom!

Phish or no phish



Phish or no phish?

Legit companies **know how to spell and have correct grammar**!

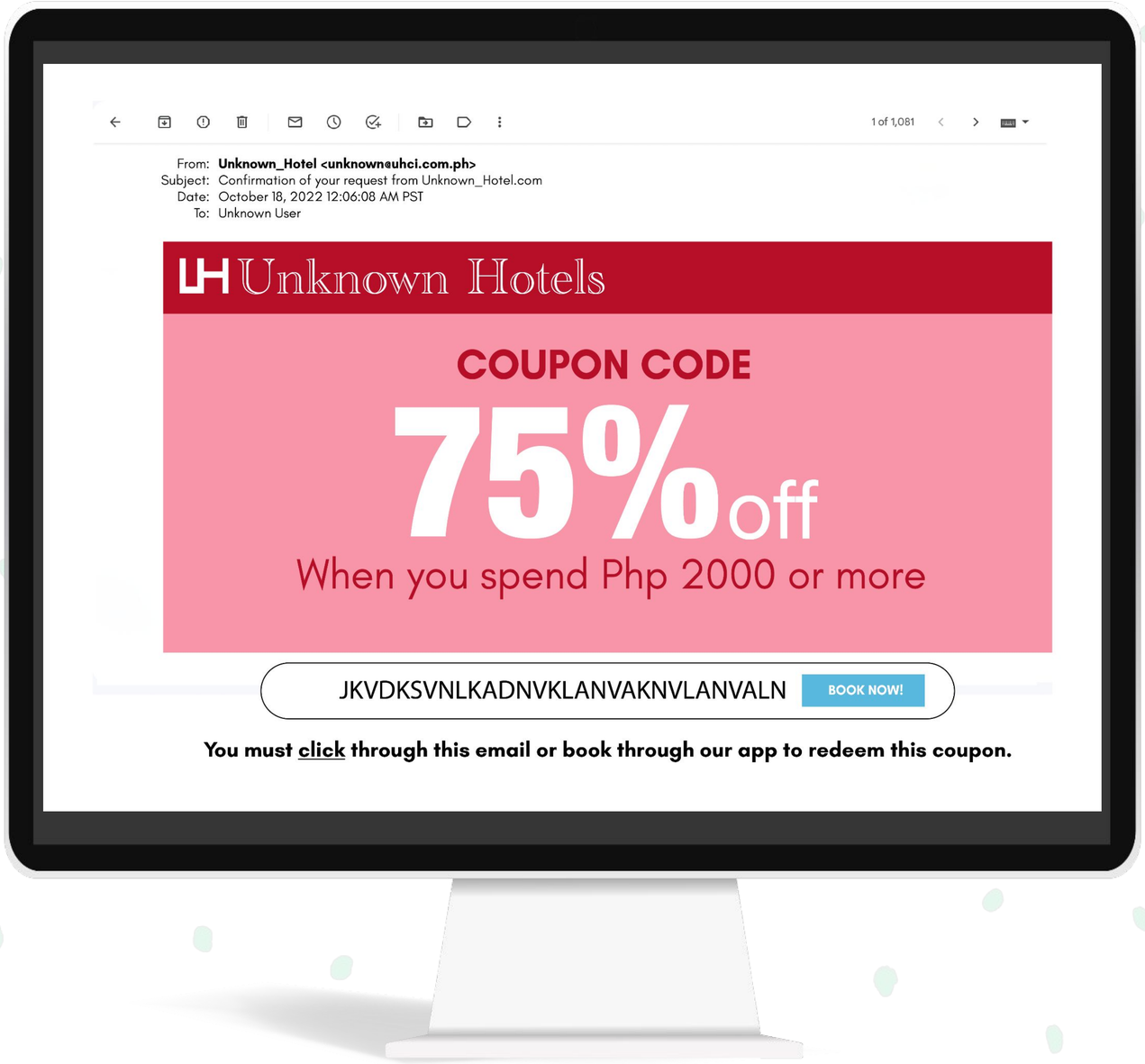


Phish or no phish?

Phish or no phish?

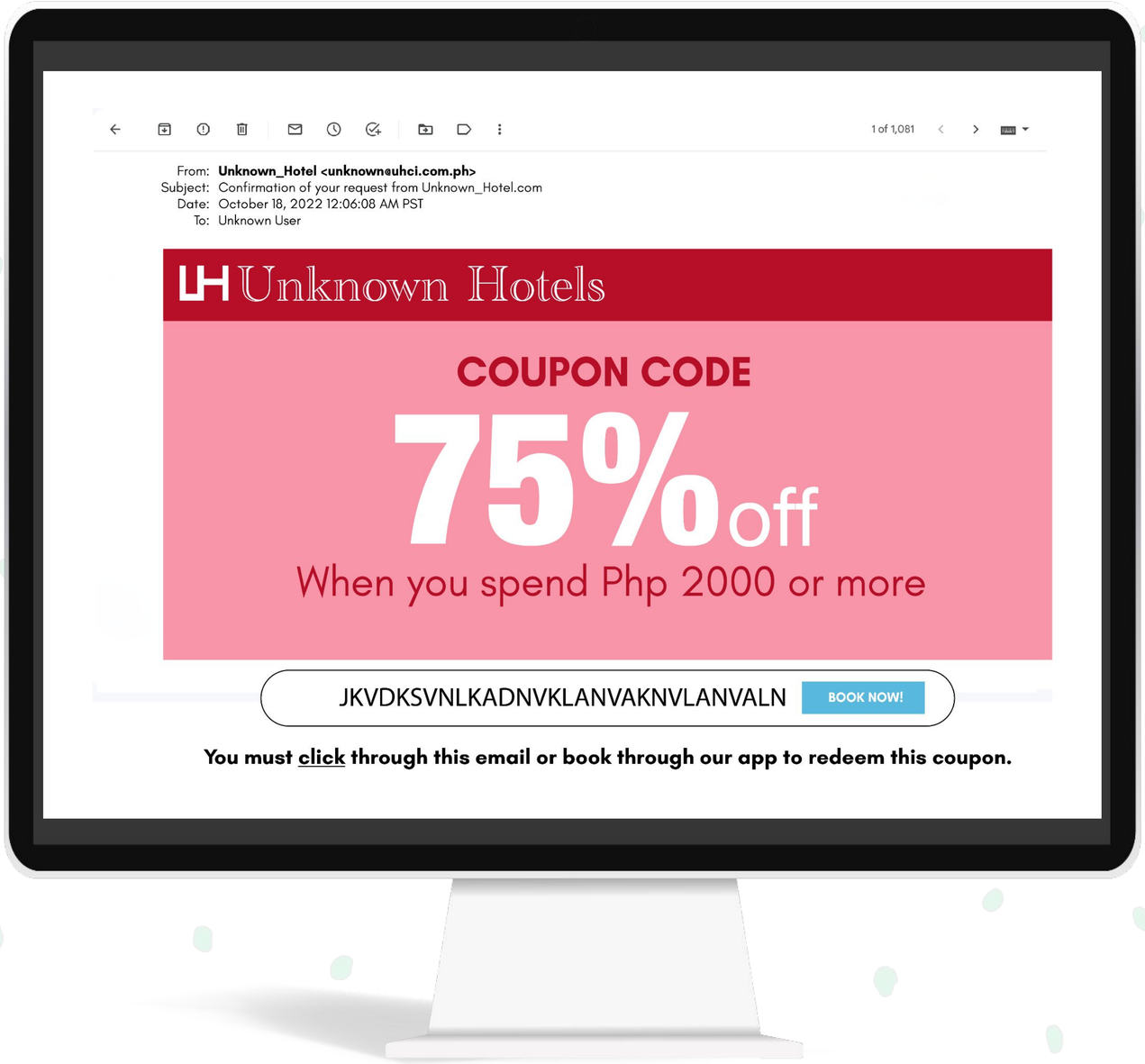
Legit companies **don't request for your sensitive information** via email

Phish or no phish?



Phish or no phish?

Legit companies
call you by your name



Remember!

Anyone asking you to pay a fee in order to apply for a job or get a resume check.

Remember!

Messages or posts with poor spelling and grammatical mistakes.

Remember!

People asking you for money
who you don’t know in person.

Remember!

People asking you to move
your conversation off Facebook to a less public
or less secure setting, such as a separate email.

Remember!

People asking you to send them money
or gift cards to receive a loan, prize, or other winnings.

Remember!

People claiming to be a friend or relative in an emergency.

Remember!

People or accounts directing you
to a separate webpage to claim a prize.

Remember!

People who misrepresent where they are located.

Catfishing

Catfishing is when a scammer creates a fake account or identity to trick people into believing they are talking to a real person.

Remember!

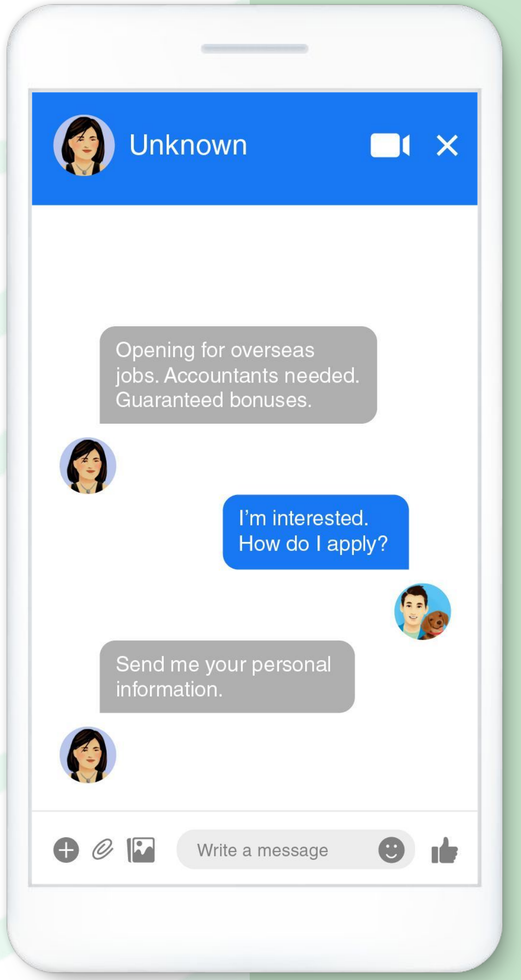
Identifiers of catfishing

- Fake profile pictures (check different social media platforms)
- Complete avoidance of video calls or real-life meetings
- Poor language skills
- Unrealistically perfect
- Have no network of friends
- Sob stories and requests for money

TIP STOP!

Kwento naman kayo!
Any experiences or tips?

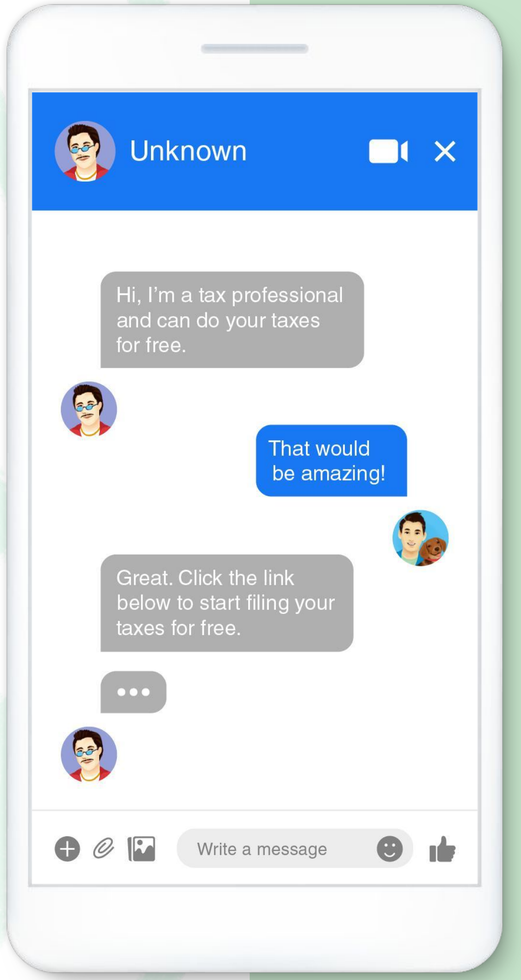
Financial Scams



REMEMBER

- These scams include tax, charity, inheritance, lottery, donation, loan, e-commerce, and other payment scams.
- Someone claiming to be from a financial institution or government organization may contact you and leave a message saying that you owe taxes or other money.
- They may say that if you don't pay the outstanding balance immediately, legal action will be taken against you.

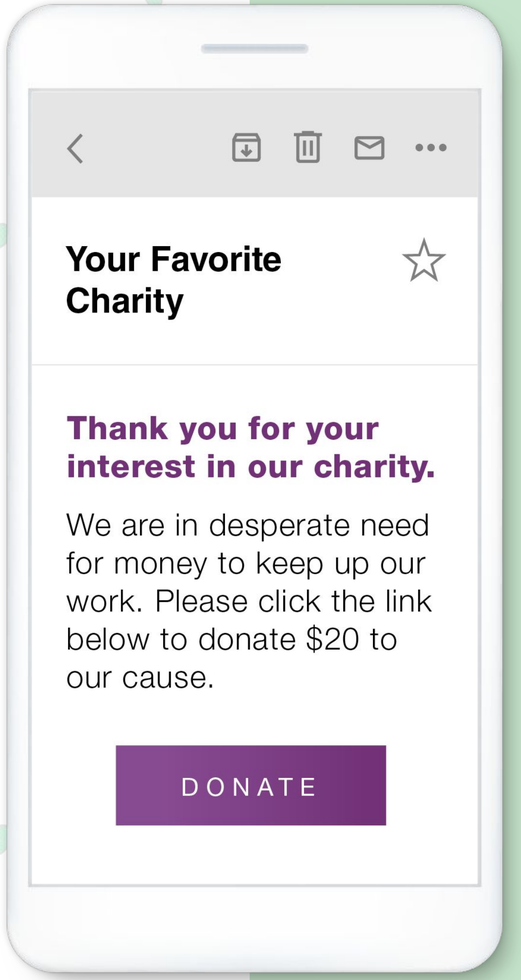
Tax Scams



REMEMBER

- Be suspicious of messages from people claiming to be tax professionals.
- Use only legitimate software or websites to file your taxes.

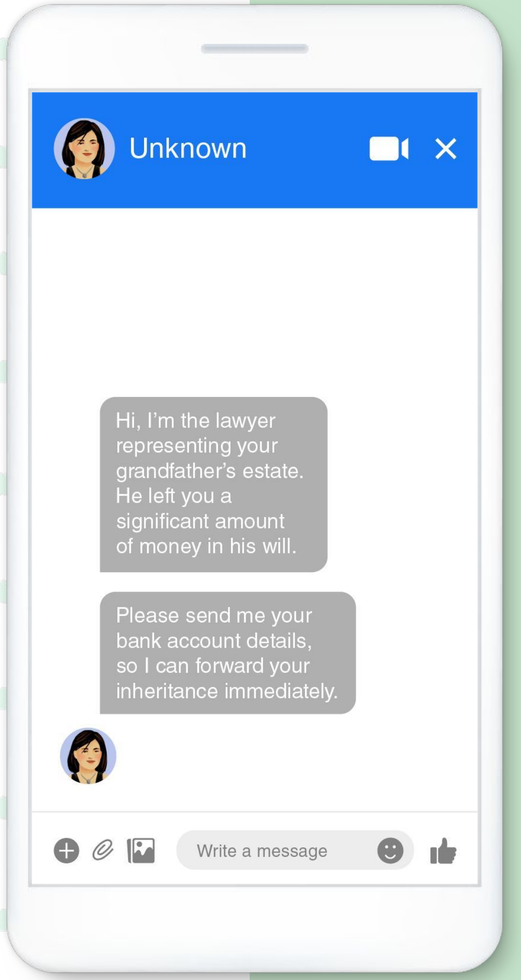
Charity Scams



REMEMBER

- Be cautious if you receive an unsolicited email, text, or DM from a charitable organization asking for online donations.
- If you are unfamiliar with a charitable organization or unsure whether it is a legitimate charity:
  - Review the charity's information at **CharityNavigator.org**, &/or
  - Make sure that you are going to the charity's official website before donating.

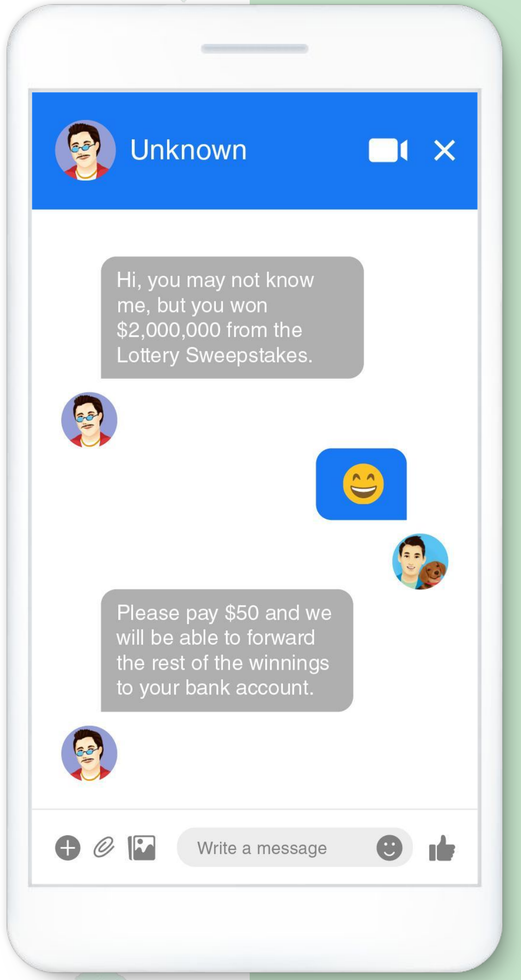
Inheritance Scams



REMEMBER

- The scammer may claim to be a lawyer, close friend, or relative pretending to represent the estate of a deceased person.
- They may say that you're entitled to the inheritance.
- The scammer may ask you to provide personal information such as your physical address or bank details.
- You may also be asked to pay an advance 'processing fee.'

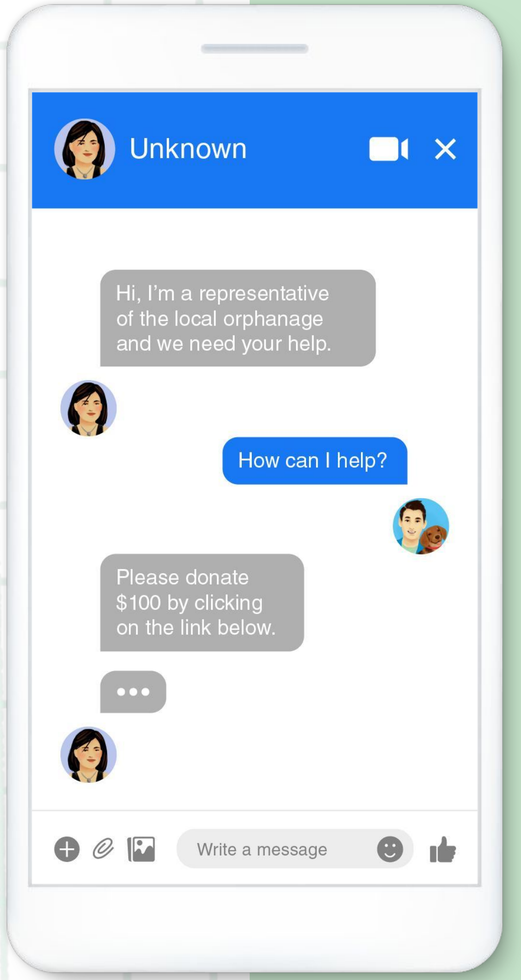
Lottery Scams



REMEMBER

- Lottery scams are often carried out from accounts impersonating someone you know or fake profiles pretending to represent an organization.
- The messages may claim that you're a winner of a lottery and that you can receive your money for a small advance fee.

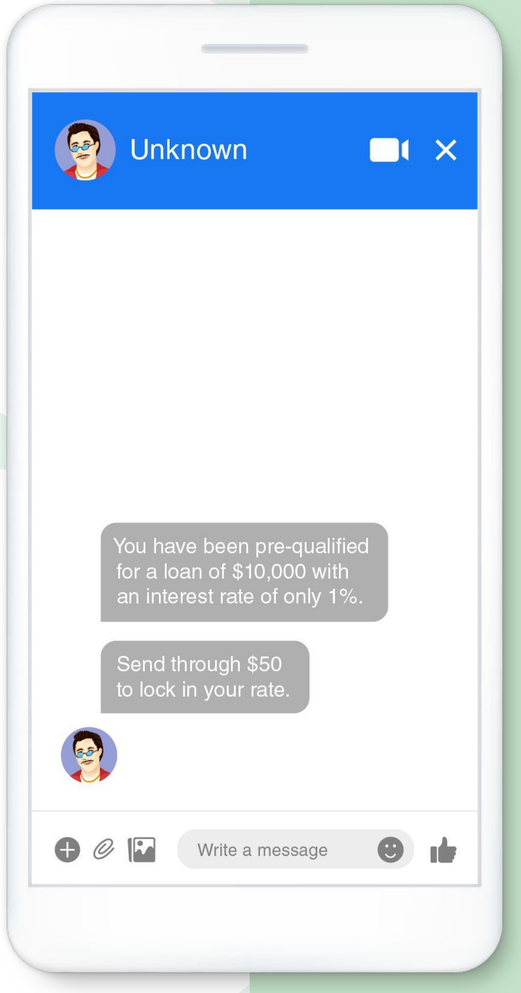
Donation Scams



REMEMBER

- These scams are done by accounts impersonating famous religious figures or accounts pretending to be representatives from various charities or orphanages.
- The scammers will ask for donations.

Loan Scams



REMEMBER

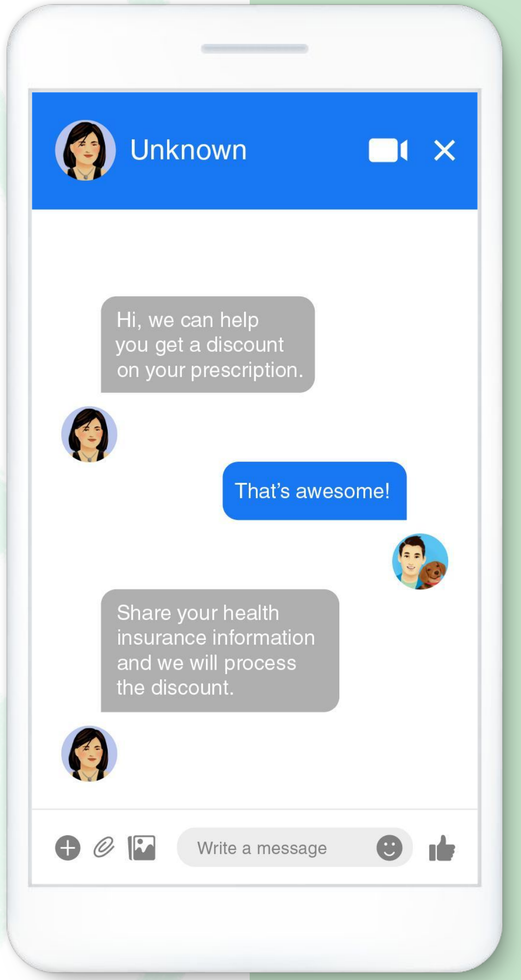
- Loan scammers send messages and leave posts and comments on Pages and in Groups offering, or claiming to know someone offering, instant loans at a low interest rate for a small advance fee.

TIP STOP!

Kwento naman kayo!
Any experiences or tips?

Medical Identity Theft

Scammers might use your stolen personal information to get prescription drugs, diagnostic tests, and even medical operations or procedures.

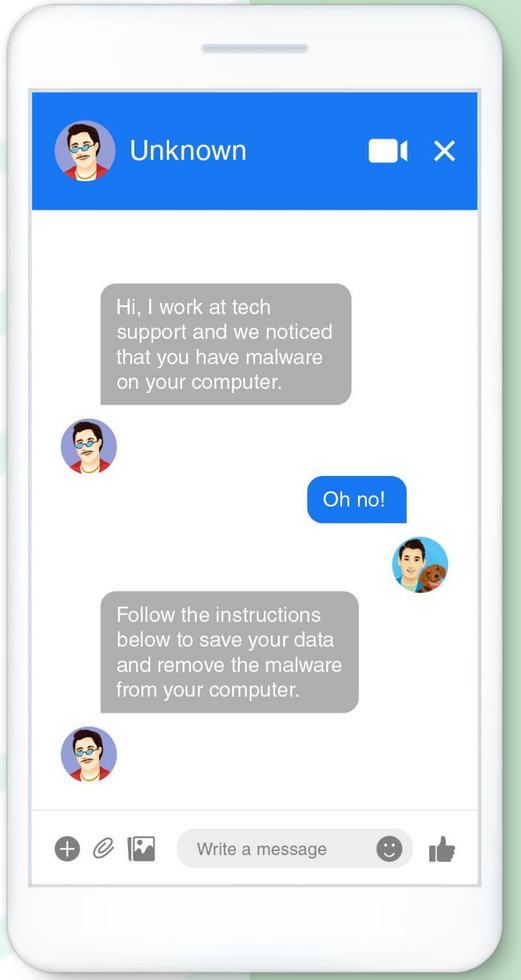


REMEMBER

To avoid medical identity theft, keep the following tips in mind:

- Be very cautious about giving out your health insurance, or other personally identifiable information to unknown companies or people.
- While medical providers may wish to take a photocopy of your insurance card, try to avoid allowing others to photocopy your insurance card or sign a blank insurance claim form.
- Always review your insurance statements/ explanations of benefits (EOBs).
- Be careful when shopping for prescription drugs or other medical supplies online. If the price seems too good to be true, it probably is.

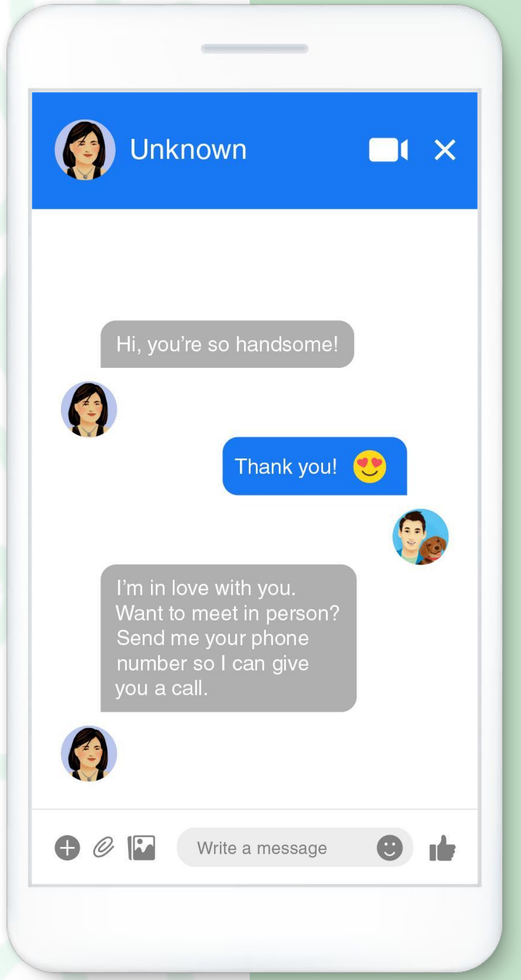
Infected Computer or Tech Support Scams



REMEMBER

- Someone claiming to be tech support for a real company may say that viruses have been detected on your computer or broadband router.
- Then they may ask you to follow instructions to save your data, or grant them remote access to your computer, which will allow them to install malicious software on your computer, access your bank or steal your personal information.
- To avoid these scams, hang up the phone or ignore the message and then reach out to the company directly through channels listed on their website.
- Do not interact with the unsolicited message.
- If you think that your computer or other device has been infected with malware, immediately run a scan, or seek professional help.

Online Dating or Romance Scams



REMEMBER

- If you choose to participate in online dating apps or websites, remember that anyone online could be saying they are someone who they are not.
- You may want to be more careful with someone you meet online if they display any of the following:
  - Their photos are stock or professional photos.
  - They make you uncomfortable by immediately professing their love using strong language.
  - They make you uncomfortable by pressuring you to leave the dating site and communicate with them through email or text messaging.

Common Warning Signs

- Wants to leave a dating app immediately and use personal email or a messaging app to chat.
- Claims to be in love very quickly to persuade you to speak with them.
- Plans to visit, but claims that something bad happened and cancels plans.
- Asks you to wire money or send gifts or gift cards.

Remember that any online love interest that asks for money is likely a scammer.

Tips for staying safe when meeting in person

- Share your location with family or friends.
- Meet and stay in public.
- Familiarize yourself with the meeting spot.
- Monitor any alcohol or substance consumption.
- Make sure your mobile phone is charged.
- Arrange your own transportation.
- Share personal information carefully.

Take your time!

- People may misrepresent themselves and their intentions in their **Facebook Dating** profile, including their gender, sexual orientation or age. This could lead to harassment or harm if you decide to meet them in person.

- Keep your communications within Facebook Dating, do your research and really get to know the other person before you meet for the first time.

Tips for staying safe when meeting in person

- Don’t share personal information like your home address. Instead, meet up in a public, well-lit area during the day.
- Create a meeting plan and share it with a trusted friend or family member.
- Tell someone about your plans.
- Consider asking someone to join you when you make the in-person exchange.
- Bring your fully charged cell phone in case you need to contact someone for help.

Fighting Fraud: Protect your device

- Install antimalware and antivirus software and run regular scans.
- Install any updates to apps, plug-ins, and software.
- Set up multi-factor or two-factor authentication for personal accounts.
- Back up important files and personal information using a secure method.

If You Feel Uncomfortable or Unsafe

- If you or someone you know is the victim of a crime or is in immediate danger, contact your local law enforcement for help.
- If you ever feel pressured or uncomfortable, you can:
  - End the date and arrange your own transportation home.
  - Block anyone who makes you feel uncomfortable.
  - Report anyone you think is suspicious.

Now that it is clear why this is important we'll:

1. Learn how to identify scam, and what you can do to avoid it (tips and things to remember)
2. **How to respond if it happens**
3. Test what we learned

What do I do?

- If you gave a scammer your login information, change your password right away.
- If you use the same password for multiple accounts or websites, change them all.
- Create new passwords that are strong and unique.
- If you paid a scammer with a credit or debit card, contact your bank or credit card company right away.

Reporting a post through feed

1. Tap ••• (iPhone) or ⋮ (Android) above the post.

2. Tap **Report**.

3. Follow the on-screen instructions.

You can learn how to report a profile on Instagram, by visiting: help.instagram.com/192435014247952

You can learn how to report a comment, by visiting: help.instagram.com/198034803689028

You can learn how to report a message, by visiting: help.instagram.com/568100683269916

Reporting someone through direct message

To restrict someone through Direct Message:

1. Tap or in the top right of their Feed.

2. Tap the chat with the person you want to report.

3. Tap the person's name at the top of your chat.

4. Tap **Report**, then follow the on-screen instructions.

You can learn how to report a profile on Instagram, by visiting: help.instagram.com/192435014247952

You can learn how to report a comment, by visiting: help.instagram.com/198034803689028

You can learn how to report a message, by visiting: help.instagram.com/568100683269916

Reporting someone through their profile

1. Tap their username from their Feed or story post, or tap Q and search their username to go to their profile.
2. Tap ••• (iPhone) or ⋮ (Android) above the post.
3. Tap **Report**.
4. Follow the on-screen instructions.

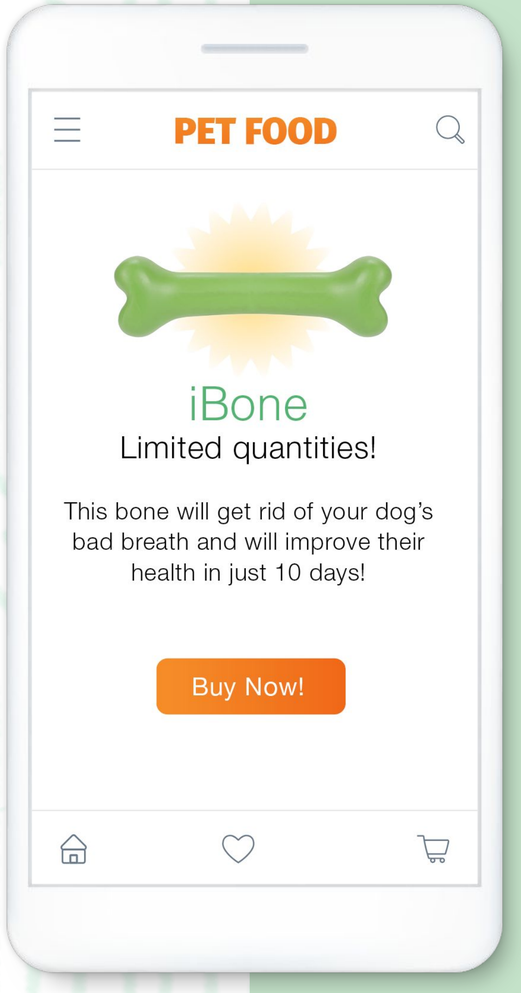
You can learn how to report a profile on Instagram, by visiting: help.instagram.com/192435014247952

You can learn how to report a comment, by visiting: help.instagram.com/198034803689028

You can learn how to report a message, by visiting: help.instagram.com/568100683269916

Shopping Safely Online

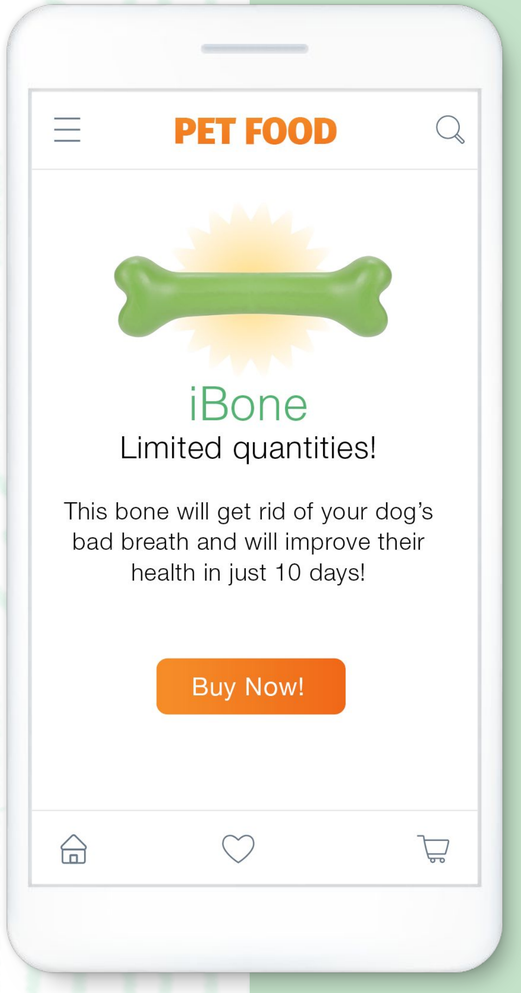
Commerce Scams



REMEMBER

- Always be cautious when using person-to-person transactions to purchase e-commerce items, especially if an item needs to be shipped.
- Be wary of gift card scams.
- Communicate on Facebook.
- Consider delivery options.
- Don't buy or sell recalled items.
- Learn which items are not allowed on Facebook.

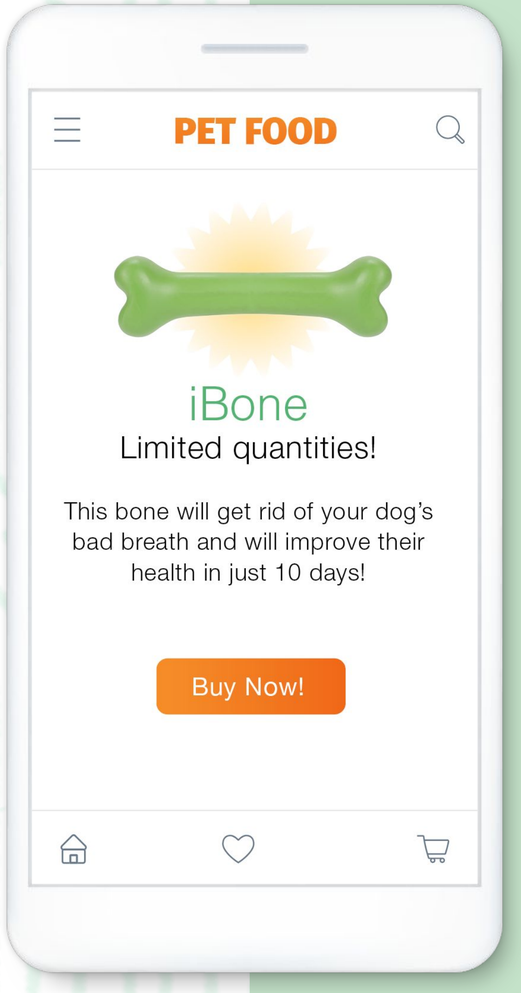
Commerce Scams



REMEMBER

- Use online payment methods.
- Verify the item.
- Be careful and alert when paying by bank transfer.
- Watch out for counterfeit items.
- Be sure to review product-specific guidelines about what is allowed on the marketplace.
- Watch out for counterfeit and recalled items and compare prices before buying an item.

Commerce Scams



REMEMBER

- Checks can be counterfeit so use online payment methods such as PayPal.
- Reach out and double check that you can actually contact them!

ONLY USE ENCRYPTED WEBSITES.

What does encryption really mean?

- When a website is encrypted, that means the data and information on the site is protected from being viewed by third parties.

- When you share and receive information from an encrypted website, that transaction is secure and only accessible by you and the site you are sharing it with.

How to Spot an Unencrypted Website

- An unencrypted website does not use a private connection.
- You can spot an unencrypted website if:
  - It uses **“http://”** instead of **“https://”** in the address bar.
  - Some internet browsers will flag it as a potentially dangerous website.

Facebook’s Commerce Policies

- Facebook’s Commerce Policies provide rules on the types of products and services that can be offered for sale on Facebook, Instagram, and WhatsApp.
- Buyers and sellers are also responsible for complying with all applicable laws and regulations.
- Failure to comply may result in a variety of consequences, including, but not limited to, removal of listings and other content, rejection of product tags, or suspension or termination of access to any or all Facebook, Instagram, or WhatsApp commerce surfaces or features.

Learn more about Facebook’s Commerce Policies, by visiting:
facebook.com/policies_center/commerce

Reporting a Shop or Product on Instagram

To report a shop:

Step 1	Step 2	Step 3
Go to the profile of the seller you want to report.	Tap ••• (iPhone) or ⋮ (Android) in the top right.	Tap Report and follow the on-screen instructions.

Learn how to report a seller or product on Instagram, by viewing: help.instagram.com/396314741132037

Learn what to do if you see an ad you don't like on Instagram, by viewing: facebook.com/help/instagram/615366948510230

Reporting a Shop or Product on Instagram

To report a product:

Step 1	Step 2	Step 3
Go to the product page of the product you want to report.	Tap ••• (iPhone) or ⋮ (Android) in the top right.	Tap Report and select a reason.

Learn how to report a seller or product on Instagram, by viewing: help.instagram.com/396314741132037

Learn what to do if you see an ad you don't like on Instagram, by viewing: facebook.com/help/instagram/615366948510230

Reporting a Shop or Product on Instagram

To report a post containing a tagged product:

Step 1	Step 2	Step 3
Go to the post with a tagged product.	Tap ••• (iPhone) or ⋮ (Android) in the top right.	Tap Report and select a reason.

Learn how to report a seller or product on Instagram, by viewing: help.instagram.com/396314741132037

Learn what to do if you see an ad you don't like on Instagram, by viewing: facebook.com/help/instagram/615366948510230

Local pickup on Facebook Marketplace

LOCAL PICKUP

Buyers can message the seller to arrange a transaction. Dropping off or picking up items helps you avoid interacting with people directly. Items purchased with local pickup aren't covered by **Purchase Protection**.

Read Facebook's tips for **buying and selling responsibly** on Marketplace and **meeting someone from Marketplace in person**.

We learned so much today!

Ready, raise your hands on Zoom
if you want to answer!

The group with the most points will win a prize!

Activity: Check for Understanding

QUESTION 1

_____ is a type of scam that tries to trick people into sharing their login or personal information.

A. SPAMMING

B. PHARMING

C. PHISHING

D. TROLLING

Activity: Check for Understanding

QUESTION 1

_____ is a type of scam that tries to trick people into sharing their login or personal information.

A. SPAMMING

B. PHARMING

C. PHISHING

D. TROLLING

Activity: Check for Understanding

QUESTION 2

_____ is when a scammer creates a fake account or identity to trick people into believing they are talking to a real person.

A. CATFISHING

B. PHARMING

C. SPAMMING

D. TROLLING

Activity: Check for Understanding

QUESTION 2

_____ is when a scammer creates a fake account or identity to trick people into believing they are talking to a real person.

A. CATFISHING

B. PHARMING

C. SPAMMING

D. TROLLING

Activity: Check for Understanding

QUESTION 3

You should always verify the authenticity of calls and emails from government services/agencies by contacting them through the official channels listed on their website.

TRUE

FALSE

Activity: Check for Understanding

QUESTION 3

You should always verify the authenticity of calls and emails from government services/agencies by contacting them through the official channels listed on their website.

TRUE

FALSE

Activity: Check for Understanding

QUESTION 4

One strategy for avoiding online scams is to share your personal information only with people or organizations that you know and trust.

TRUE

FALSE

Activity: Check for Understanding

QUESTION 4

One strategy for avoiding online scams is to share your personal information only with people or organizations that you know and trust.

TRUE

FALSE

Activity: Check for Understanding

QUESTION 1

An encrypted website means that you can trust the organization behind the website.

TRUE

FALSE

Activity: Check for Understanding

QUESTION 1

An encrypted website means that you can trust the organization behind the website.

TRUE

FALSE

Activity: Check for Understanding

QUESTION 2

What are signs of an encrypted website?

Select all that apply

A.
A padlock icon

B.
A pop-up window when you first visit the site that says “SECURE”

C.
https:// at the beginning of the URL

D.
A five-star rating on Google

Activity: Check for Understanding

QUESTION 2

What are signs of an encrypted website?

Select all that apply

A.
A padlock icon

B.
A pop-up window when you first visit the site that says “SECURE”

C.
https:// at the beginning of the URL

D.
A five-star rating on Google

Activity: Check for Understanding

QUESTION 3

Online marketplace postings are often public on the web.

TRUE

FALSE

Activity: Check for Understanding

QUESTION 3

Online marketplace postings are often public on the web.

TRUE

FALSE

Activity: Check for Understanding

QUESTION 1

Which of the following are ways to be proactive in preventing scams?

Select all that apply

A.
Installing antimalware and antivirus software on your computer

B.
Updating apps, software and operating (OS) regularly on all personal devices

C.
Using multi-factor authentication when possible

D.
Using public devices or Wi-Fi without protection

Activity: Check for Understanding

QUESTION 1

Which of the following are ways to be proactive in preventing scams?

Select all that apply

A.
Installing antimalware and antivirus software on your computer

B.
Updating apps, software and operating (OS) regularly on all personal devices

C.
Using multi-factor authentication when possible

D.
Using public devices or Wi-Fi without protection

Activity: Check for Understanding

QUESTION 2

App and software updates are not important to keep your devices secure.

TRUE

FALSE

Activity: Check for Understanding

QUESTION 2

App and software updates are not important to keep your devices secure.

TRUE

FALSE

Activity: Check for Understanding

QUESTION 3

_____ is a way to protect your online accounts by requiring additional information to log in to an account.

A. Antivirus software

B. Multi-factor authentication

Activity: Check for Understanding

QUESTION 3

_____ is a way to protect your online accounts by requiring additional information to log in to an account.

A. Antivirus software

B. Multi-factor authentication

Activity: Check for Understanding

QUESTION 4

If a scammer makes fraudulent credit card purchases, you will never get the money back.

TRUE

FALSE

Activity: Check for Understanding

QUESTION 4

If a scammer makes fraudulent credit card purchases, you will never get the money back.

TRUE

FALSE

Good job!

You have leveled up
in your online safety!

LEARNING MODULE

You have 15 minutes to apply the tips to your accounts and devices!

This module was reviewed by Get Safe Online.
To learn more about this partner, visit getsafeonline.org

Meta | Digital Tayo

LEARNING MODULE

What did you apply already during those 15 minutes?

This module was reviewed by Get Safe Online.
To learn more about this partner, visit getsafeonline.org

Meta | Digital Tayo

Key Summary Points

Scams happen when people create fake accounts or hack into existing accounts or pages. These fake or compromised accounts to trick you into giving them money or personal information.

Different types of scams include phishing, catfishing, financial, identity theft, romance, and commerce scams, among others.

Check important details like the sender, the message, and sketchy links when you receive unknown messages to avoid phishing scams

Key Summary Points

Check common warning signs especially when asked to meet in person, for dating and commerce scams.

Protect yourselves from fraud through different measures like antivirus/antimalware, 2FA or Multiple-Factor Authentication, among others.

Review your platforms' commerce policies and other risk mitigating actions (e.g., reporting a product, shop, page, etc.).

LEARNING MODULE

What are your Top 3 KEY TAKEAWAYS?

Share it with 3 people after this.

This module was reviewed by Get Safe Online.
To learn more about this partner, visit getsafeonline.org

Meta | Digital Tayo

Spot the Warning Signs

- Be sure to review product-specific guidelines about what is allowed on the marketplace.
- Protect your privacy and be mindful of sharing personal details and information.
- Be wary of gift card scams and deals that seem too good to be true.
- You are being asked to click on a link, open an attachment, or enter personal information into an unknown or untrusted external website.

Things to Watch Out for When Shopping Online

- People asking you for money.
- People asking you to send them money or gift cards to receive a loan, prize, or other winnings.
- Anyone asking you to pay a fee in order to apply for a job.
- Pages representing large companies, organizations, or public figures that are not verified.
- People asking you to move your conversation off the platform.
- People claiming to be a friend or relative in an emergency.
- People who misrepresent where they are located.
- Messages or posts with poor spelling and grammatical mistakes.
- People or accounts directing you to a Page to claim a prize.

What if my computer has a virus?

- Run a system scan using trusted antimalware and antivirus software.
- If your software recommends taking action, follow the recommended steps.

For more information on what to do if your computer gets a virus, visit the following resource from **GCFGlobal: Internet Safety: What To Do if Your Computer Gets a Virus.**

Additional Resources:

- The Senior's Guide to Online Safety by ConnectSafely
- BBB Scam Tips by Better Business Bureau
- Fraud.org by the National Consumers League
- Report Phishing by the Internal Revenue Service
- How To Recognize and Avoid Phishing Scams by the Federal Trade Commission Consumer Information

MODULE 7

Avoiding Scams

This module was reviewed by Get Safe Online.
To learn more about this partner, visit getsafeonline.org

Meta | Digital Tayo