

Avoiding Scams



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



We Think Digital

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

LESSON 1

Spotting 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.



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.

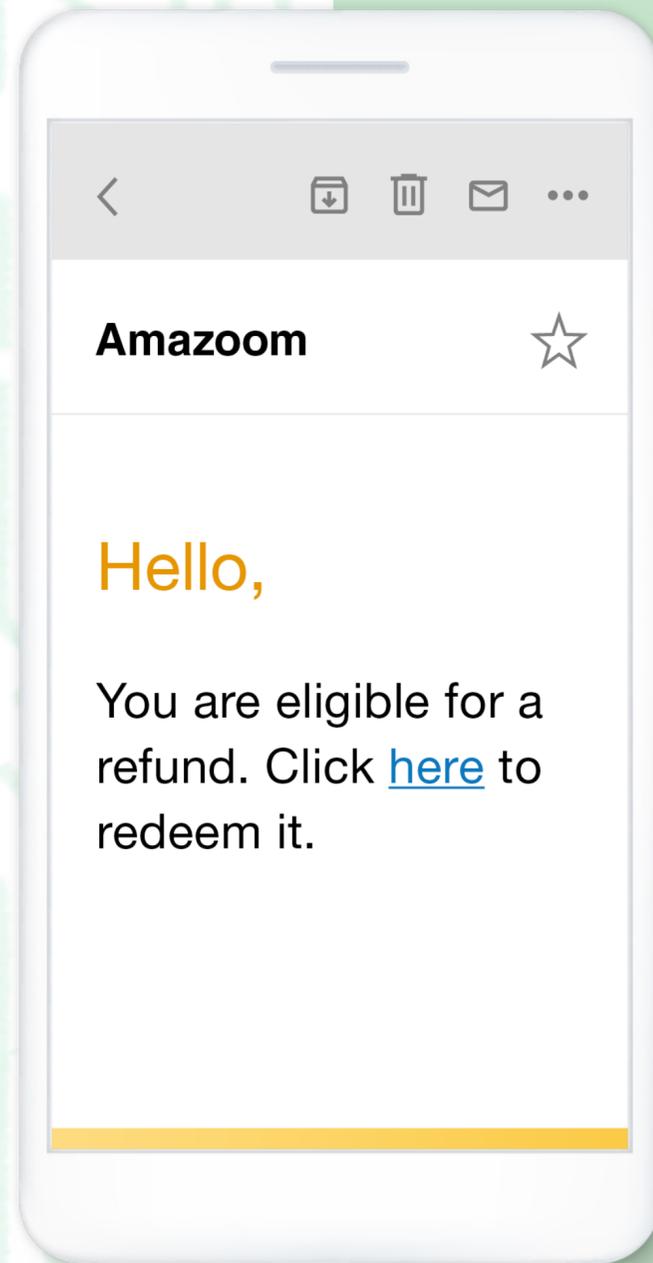




Let's Learn About Common Online Frauds and Meet Some Typical Scamsters



What is Phishing?



- **Phishing** is a type of scam that tricks people into sharing their login or personal information.
- Phishing can come in the form of 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.

Identifying 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.



What is Catfishing?

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

How to Detect Phishing

Some signs that a message might be a phishing scam:

- Anyone asking you to pay a fee in order to apply for a job or get a resume check.
- Messages or posts with poor spelling and grammatical mistakes.
- People asking you for money who you don't know in person.
- People asking you to move your conversation off Facebook to a less public or less secure setting, such as a separate email.

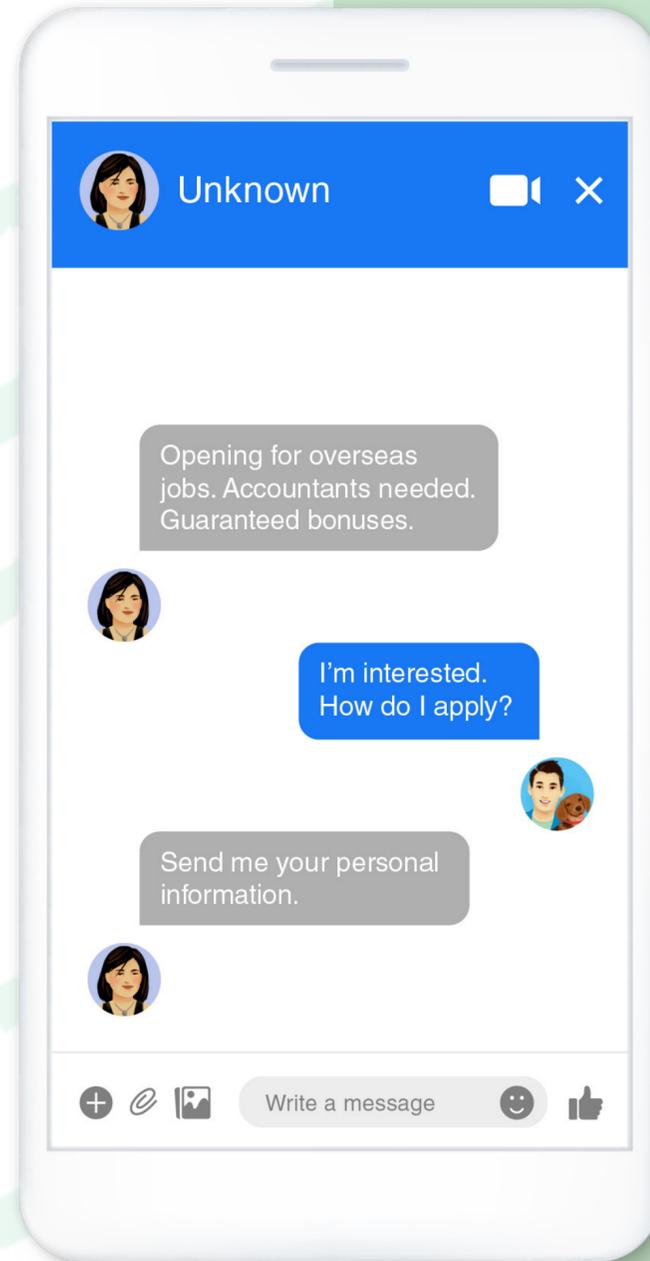
How to Detect Phishing

Some signs that a message might be a phishing scam:

- People asking you to send them money or gift cards to receive a loan, prize, or other winnings.
- People claiming to be a friend or relative in an emergency.
- People or accounts directing you to a separate webpage to claim a prize.
- People who misrepresent where they are located.



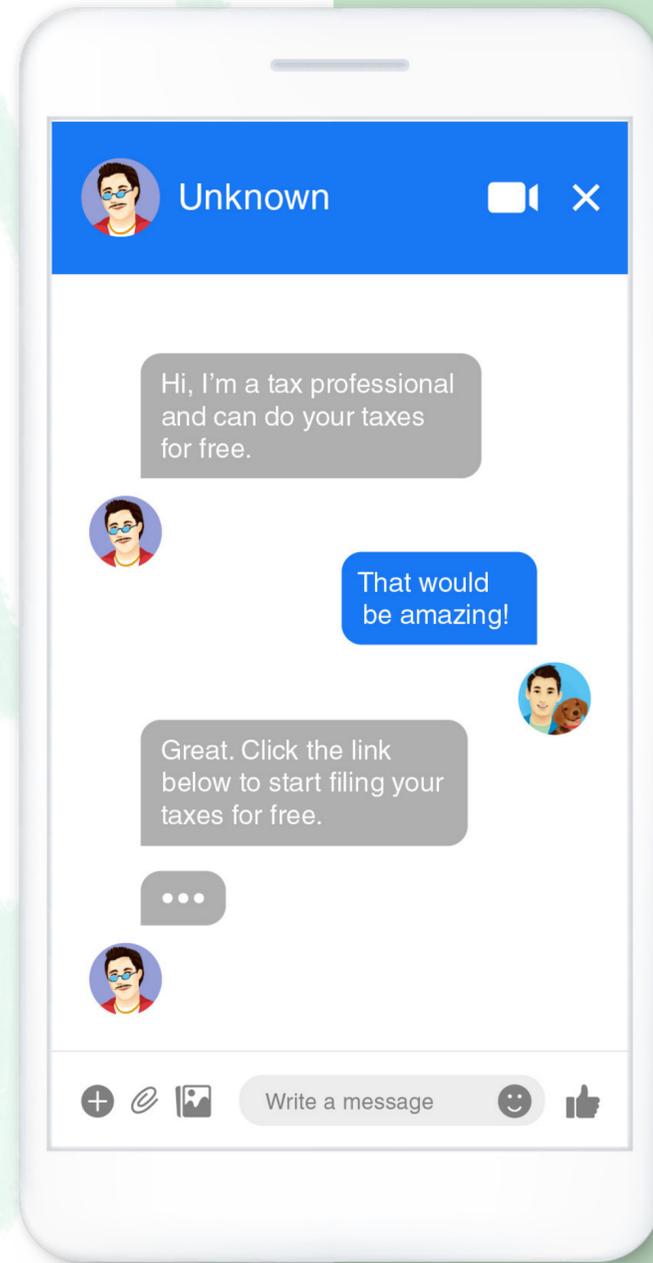
Financial Scams



- 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.



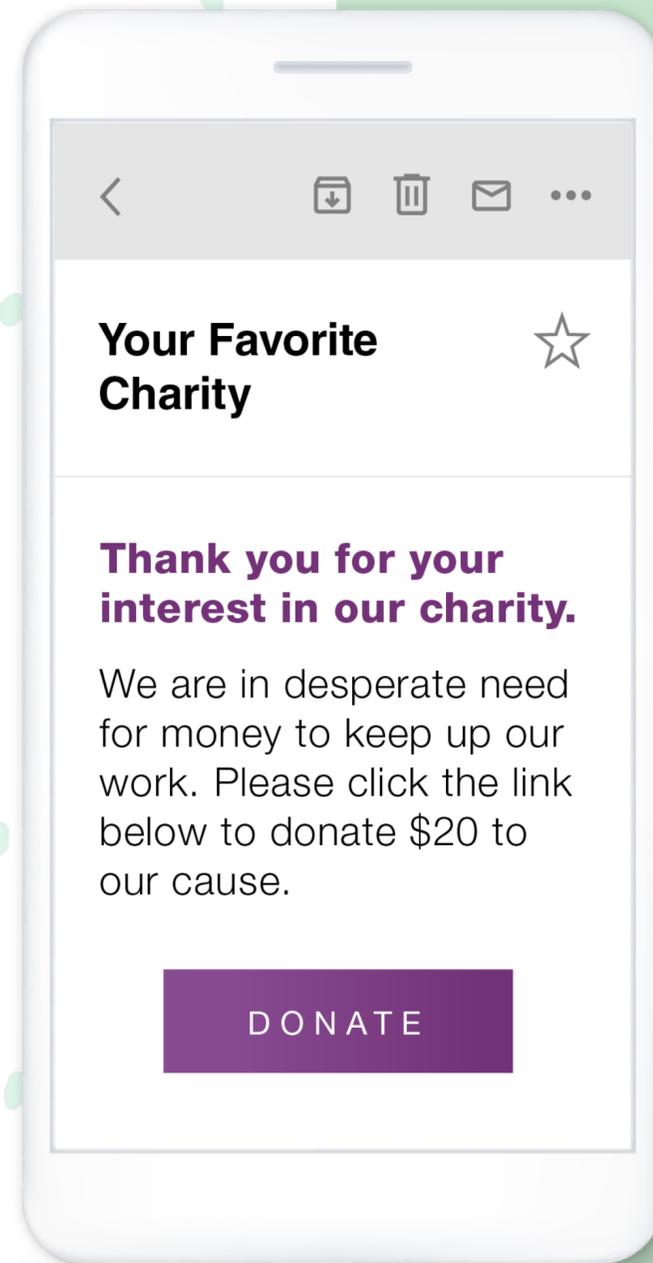
Tax Scams



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



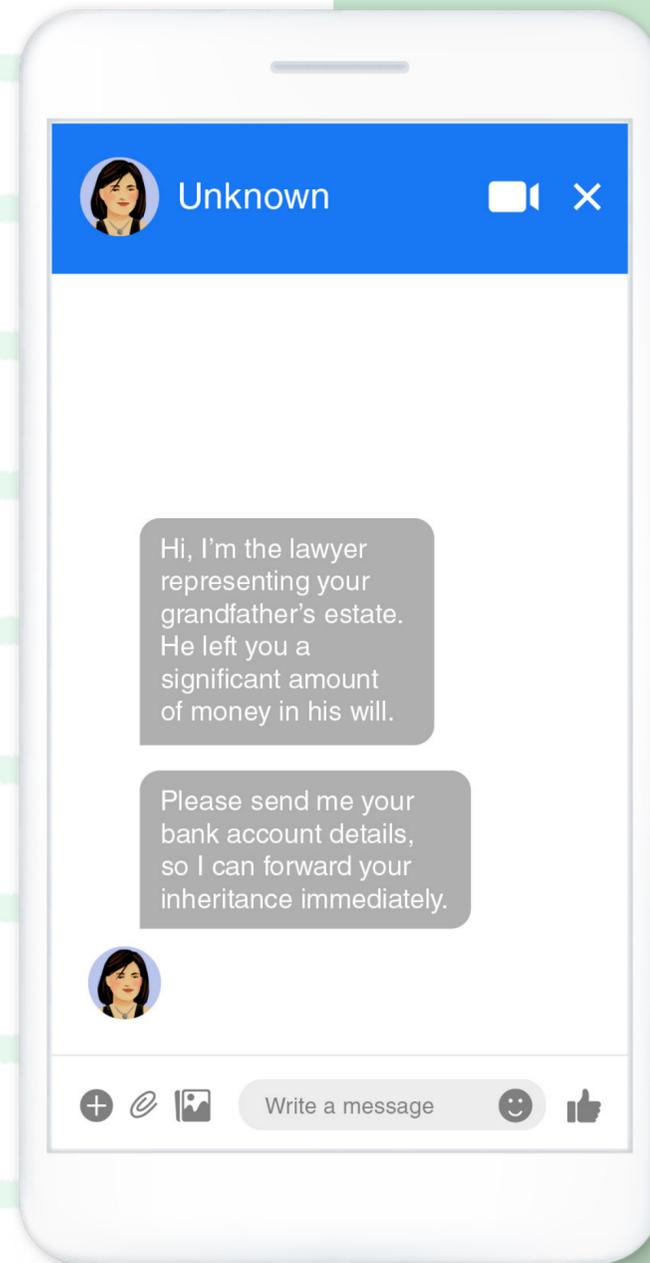
Charity Scams



- Be careful 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](https://www.charitynavigator.org).
 - Make sure that you are going to the charity’s official website before donating.



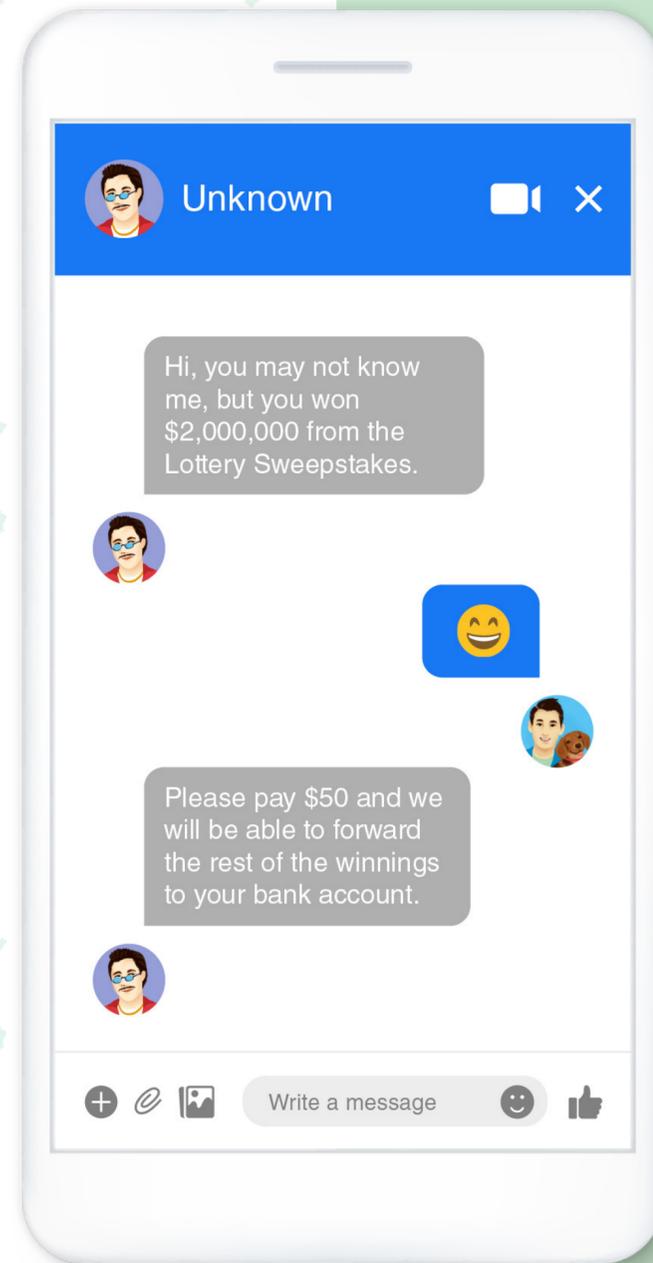
Inheritance Scams



- 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'.



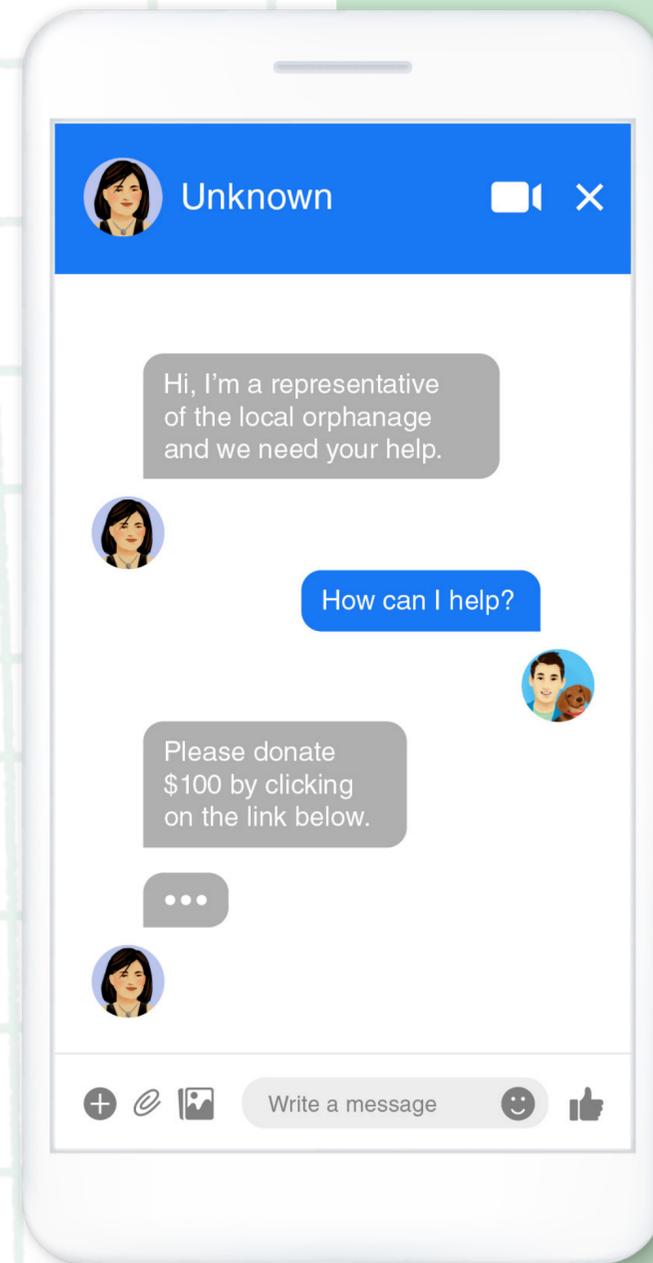
Lottery Scams



- 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.



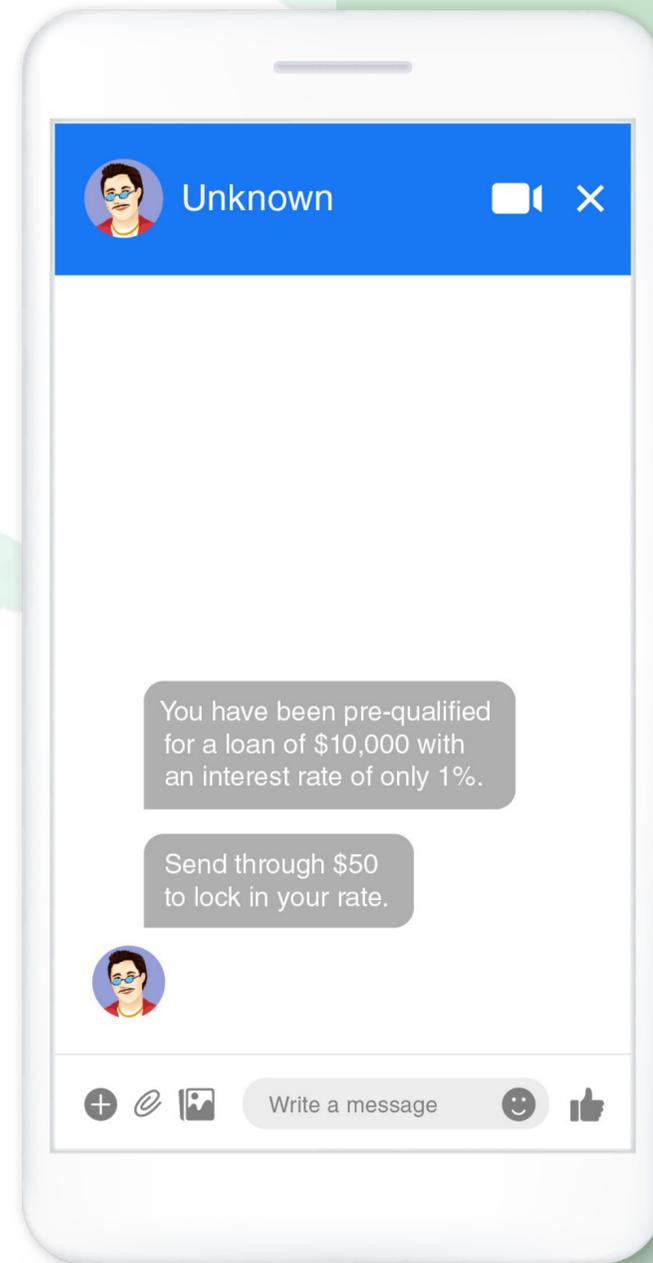
Donation Scams



- 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.



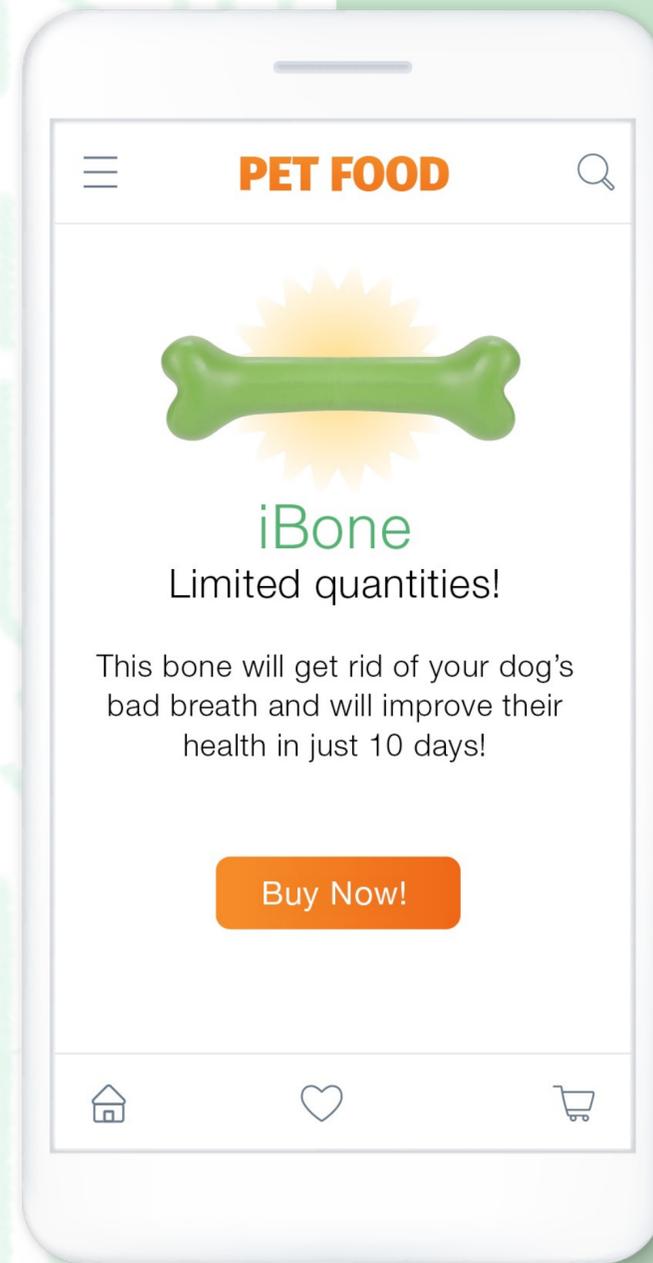
Loan Scams



- 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.



Facebook Commerce Scams



- Always be cautious when using person-to-person transactions to purchase e-commerce items, especially if an item needs to be shipped.

Tips for Buying and Selling Online

- 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.
- Meet in-person.
- Protect your privacy.
- Use online payment methods.
- Verify the item.
- Avoid paying by bank transfer.
- Watch out for counterfeit items.



Local Pickup on Facebook Marketplace



LOCAL PICKUP

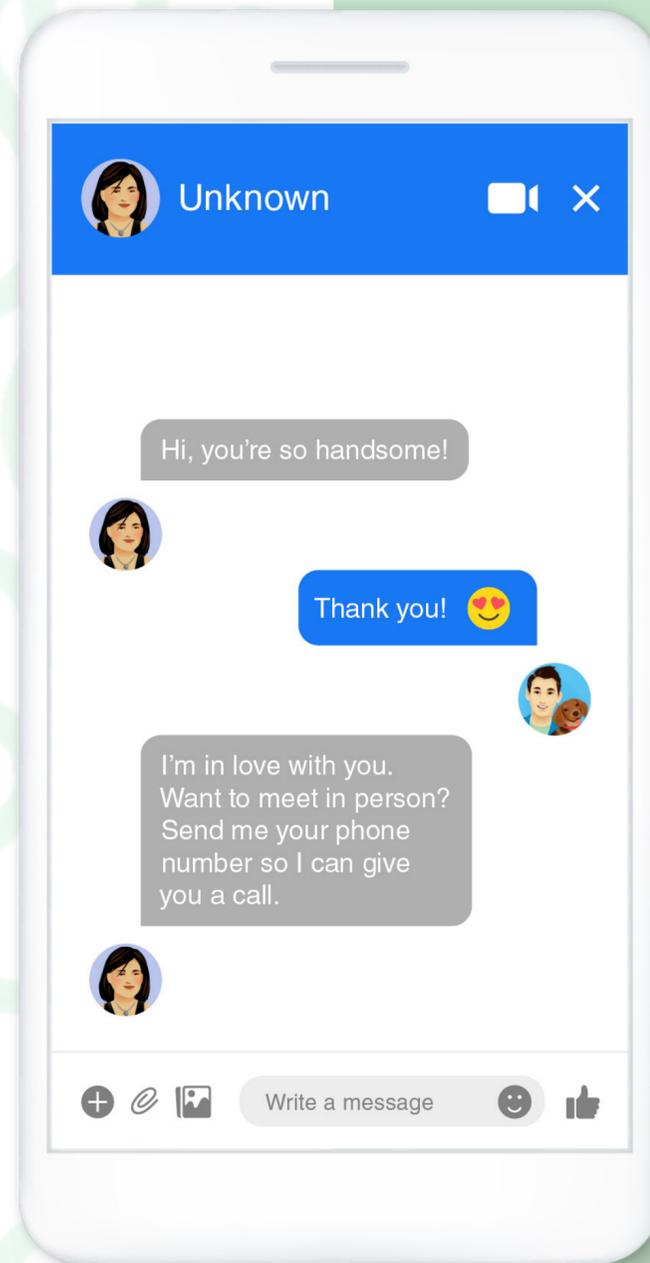
Buyers can message the seller to arrange a transaction. Dropping off or picking up items helps you avoid interacting with people directly. Items purchased with local pickup aren't covered by Purchase Protection.



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



Online Dating or Romance Scams



- 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.

Staying Safe While Online Dating

When meeting someone online:

- Share carefully.
- Keep your identifying information private.
- Conduct a Reverse Image Search.
- Report and block anyone who asks you to share personal information, such as information that could compromise your privacy, safety or security, or anyone who you feel is suspicious.

Online Dating: Common Warning Signs

Common warning signs include when a scammer:

- 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.

Online Dating: Meeting in Person

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

- Tell someone about your plans.
- Share your location.
- 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.

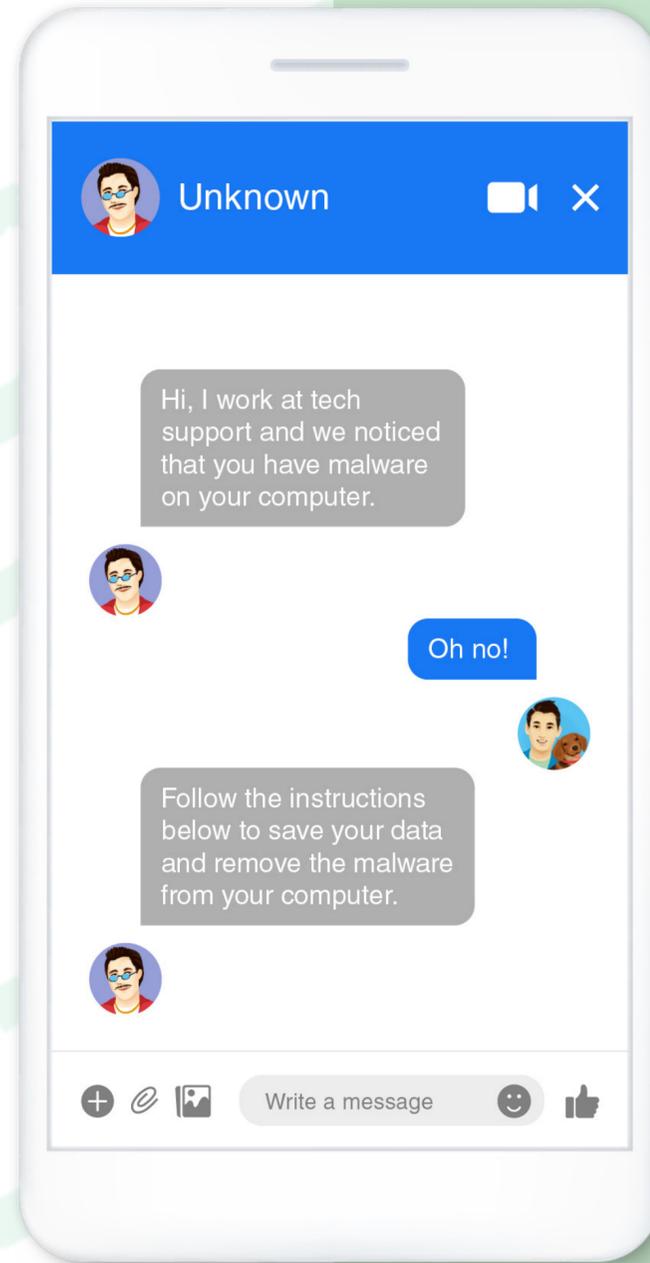
If You Feel Uncomfortable or Unsafe

- 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.





Infected Computer or Tech- Support Scams

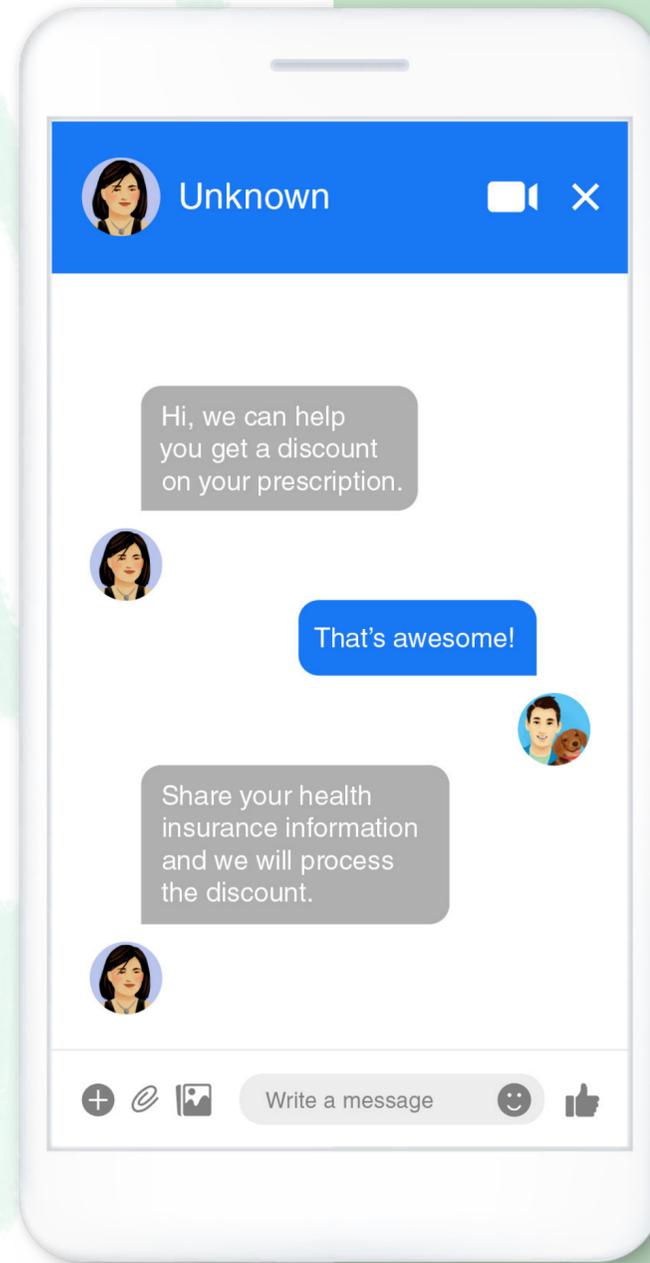


- Someone claiming to be tech support for a real company may say that viruses have been detected on your computer or broadband router.
- Then they may ask you to follow instructions to save your data, or grant them remote access to your computer, which will allow them to install malicious software on 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.



Medical Identity Theft

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

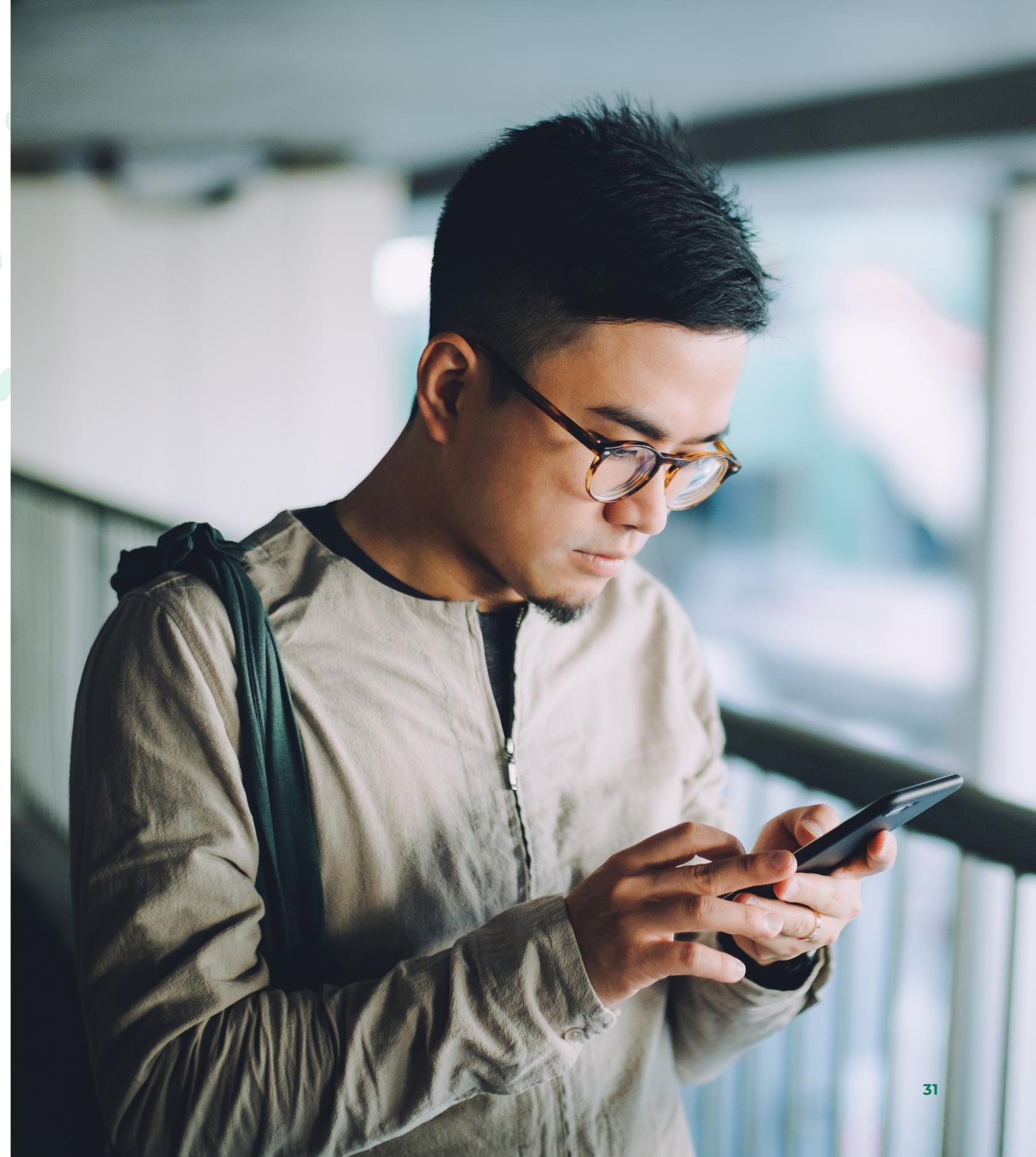


To avoid medical identity theft, keep the following tips in mind:

- 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.

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.





Let's Learn Some Tips for Staying Safe Online

These days,

Additional Strategies for Avoiding Scams

- If an offer looks too good to be true, it probably is.
- If a contest, job, or scholarship asks you to pay money upfront, don't do it.
- Be cautious about giving out personal information to individuals or organizations that you don't know and trust.
- Reach out to the person, organization, or charity offline directly to verify authenticity using the phone number you know to be authentic.

Common Scams on Facebook



**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

Things to Watch Out for While 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.

How to Report Scammers or Suspicious Activity in Facebook Messages

If you encounter scammers or suspicious activity when sending or receiving money in messages, you can report their Facebook account for review.



For more information on how to report scammers or suspicious activity in Facebook messages, visit: [facebook.com/help](https://www.facebook.com/help)



How to Report a Post or Profile on Instagram

REPORT A POST THROUGH THE FEED

1. Tap ⋮ (iPhone) or ⋮ (Android) above the post.
2. Tap Report.
3. Follow the on-screen instructions.

REPORT 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) in the top right of the profile.
3. Tap Report.
4. Follow the on-screen instructions.

REPORT 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



Discussion and Self-Reflection

- Have you encountered any online scams in the past?
- How did you react?
- How would you react now?



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



Activity: Sharing Personal Information

INSERT PHOTO HERE

www.url.com

INSERT PHOTO HERE

www.url.com



Activity: Let's Go Phishing - Spot the Scam

INSERT PHOTO HERE

www.url.com

INSERT PHOTO HERE

www.url.com



Activity: Let's Go Phishing - Spot the Scam Account

INSERT PHOTO HERE

INSERT PHOTO HERE

www.url.com

www.url.com



Activity: Check for Understanding

QUESTION 1

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

SPAMMING

PHARMING

PHISHING

TROLLING



Activity: Check for Understanding

QUESTION 1

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

SPAMMING

PHARMING

PHISHING

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.

CATFISHING

PHARMING

SPAMMING

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.

CATFISHING

PHARMING

SPAMMING

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

Shopping Safely Online

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.



For more information about how web browsers check the security of individual websites, review the following resources from common browsers:

- [Check if a site's connection is secure \(Google Chrome Help\).](#)
- [If Safari says it can't establish a secure connection, or the website is using weak encryption \(Apple Support\).](#)



Discussion and Self-Reflection

- Have you used unencrypted websites in the past?
- What did you use them for?
- Would you still use those same websites now?
- Why or why not?





Why is it Important to Use Encrypted Websites?

Safe Online Shopping

In addition to using encrypted websites, there are other strategies that you can use to stay safe while online shopping:

- Shop only at reputable online stores.
- Pause before you purchase.
- Be proactive.

Online Marketplaces

- The internet can be a great place to connect with people who are buying and selling personal products.
- Many social media sites also include online marketplaces that allow users to buy and sell their own items and products.

Tips for Safely Shopping in Online Marketplaces

- 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.
- Be a critical consumer.
- Watch out for counterfeit and recalled items and compare prices before buying an item.
- Checks can be counterfeit so use online payment methods such as PayPal.

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.
- 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.

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

Steps to Take if You are Disapproved

If your listing has been rejected for violating Facebook's Commerce Policies and you feel it was a mistake, you can request a review by following these steps for:

- **FACEBOOK MARKETPLACE:**
facebook.com/help/2193854224216494
- **INSTAGRAM:**
help.instagram.com/494867298080532





Reporting a Shop or Product on Instagram

TO REPORT A SELLER:

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

TO REPORT A PRODUCT:

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

TO REPORT A POST CONTAINING A TAGGED PRODUCT:

1. Go to the post with a tagged product.
2. Tap **⋮** (iPhone) or **⋮** (Android) in the top right.
3. 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



Discussion and Self-Reflection

- Have you bought things from an online store? How did it go? Would you do anything differently after learning the content in this lesson? Why or why not?
- Have you bought or sold anything in an online marketplace? How did it go? Would you do anything differently after learning the content in this lesson? Why or why not?



Additional Resource:

[Internet Safety: Safe Online Shopping](#) by GCFGlobal



Activity: Online Marketplace Review

www.url.com

www.url.com



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 PADLOCK
ICON

A POP-UP
WINDOW WHEN
YOU FIRST VISIT
THE SITE THAT
SAYS "SECURE"

HTTPS:// AT
THE BEGINNING
OF THE URL

A FIVE-STAR
RATING ON
GOOGLE



Activity: Check for Understanding

QUESTION 2

What are signs of an encrypted website?

Select all that apply

A PADLOCK
ICON

A POP-UP
WINDOW WHEN
YOU FIRST VISIT
THE SITE THAT
SAYS "SECURE"

HTTPS:// AT
THE BEGINNING
OF THE URL

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

Reporting Cyber Crimes and Scams

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.

Spot the Warning Signs

- Messages contain grammatical or spelling errors.
- Messages create a sense of urgency in decision-making.
- Offers or deals 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.

What If I Think 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.](#)

What If I Experience a Scam?

- 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.

Additional Resource:

[How To Recognize and Avoid Phishing Scams](#) by FTC Consumer Information



Activity: How to Report Scams

INSERT PHOTO HERE

www.url.com

INSERT PHOTO HERE

www.url.com

Common Scams on Facebook



**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/1674717642789671

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.

How to Report Scammers or Suspicious Activity in Facebook Messages

If you encounter scammers or suspicious activity when sending or receiving money in messages, you can report their Facebook account for review.



For more information on how to report scammers or suspicious activity in Facebook messages, visit: [facebook.com/help/1004934609532652](https://www.facebook.com/help/1004934609532652)



How to Report a Post or Profile on Instagram

REPORT A POST THROUGH FEED:

1. Tap ⋮ (iPhone) or ⋮ (Android) above the post.
2. Tap Report.
3. Follow the on-screen instructions.

REPORT 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) in the top right of the profile.
3. Tap Report.
4. Follow the on-screen instructions.

REPORT 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



Activity: Check for Understanding

QUESTION 1

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

Select all that apply

**INSTALLING
ANTIMALWARE
AND ANTIVIRUS
SOFTWARE ON
YOUR COMPUTER**

**UPDATING APPS,
SOFTWARE AND
OPERATING
SYSTEMS (OS)
REGULARLY ON
ALL PERSONAL
DEVICES**

**USING MULTI-
FACTOR
AUTHENTICATION
WHEN POSSIBLE**

**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

**INSTALLING
ANTIMALWARE
AND ANTIVIRUS
SOFTWARE ON
YOUR COMPUTER**

**UPDATING APPS,
SOFTWARE AND
OPERATING
SYSTEMS (OS)
REGULARLY ON
ALL PERSONAL
DEVICES**

**USING MULTI-
FACTOR
AUTHENTICATION
WHEN POSSIBLE**

**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.

ANTIVIRUS
SOFTWARE

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.

ANTIVIRUS
SOFTWARE

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

Avoiding Scams



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



We Think Digital