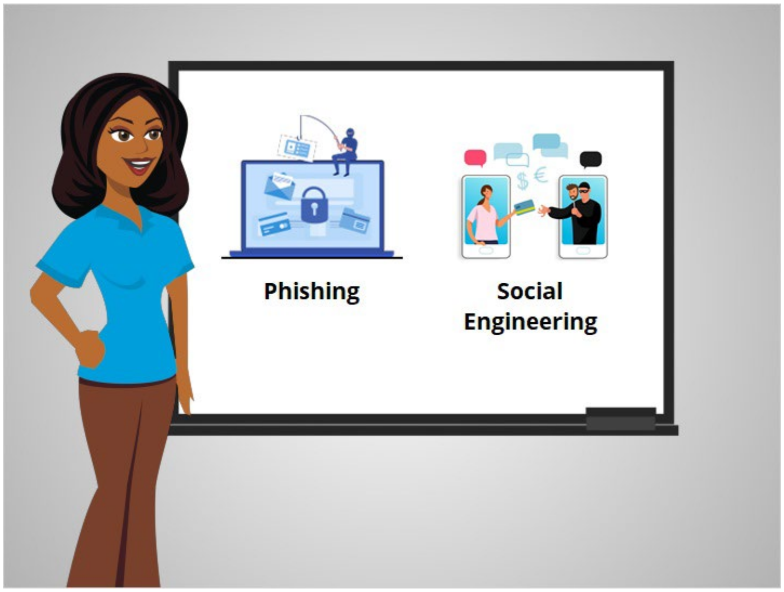
Online Fraud and Scams

Activity 1: Types of Scams

1. Types of online scams
2. Recognize online scams
3. How to respond
4. Reporting a scam

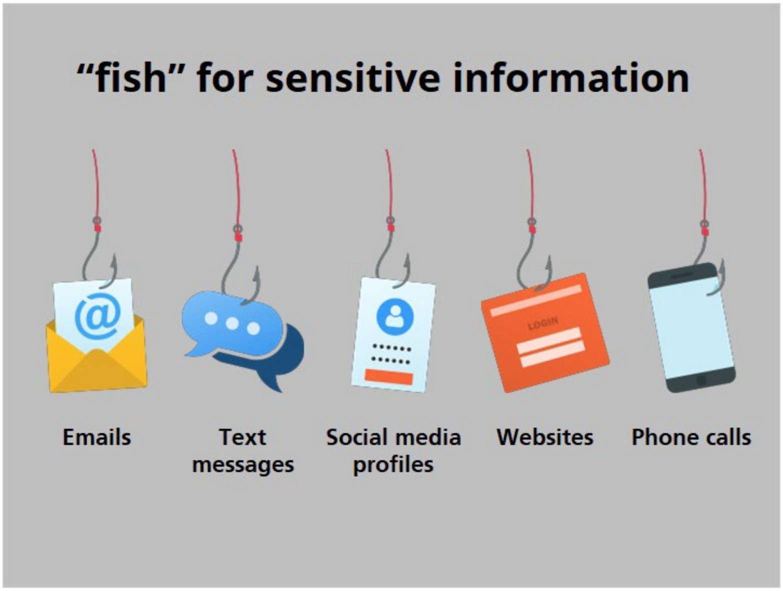
Hi, I'm Belle! There are many things you can do to protect yourself from fraud and keep your accounts and devices safe from online scams. We'll follow along with Albert to learn what types of scams are out there, how to recognize the warning signs, how to respond when you see a scam, and how to report a scam.



Online scams can take many forms. We're going to help Albert learn how to recognize and avoid the most common types of fraud and scams when he is online.
Some of the most common types include phishing and social engineering.
You may encounter these scams on a website, in an email, text message, or phone call, in an online game, or even in a pop-up window on your computer.

Let's begin by talking about phishing, which is a common type of scam.

None of the other companies whose names or logos appear in these educational materials have been involved in the creation of these materials, or approve, sponsor, or are affiliated in any way with these materials.



“fish” for sensitive information

Phishing occurs when fraudsters or scammers use fake emails, text messages, social media profiles, websites, or phone calls to fish for sensitive information like passwords, Social Security Numbers, credit card and bank account details, or personal data. The scammers can use this information to gain access to your money or steal your identity.

Phishing Scams:

☑ Try to win your trust

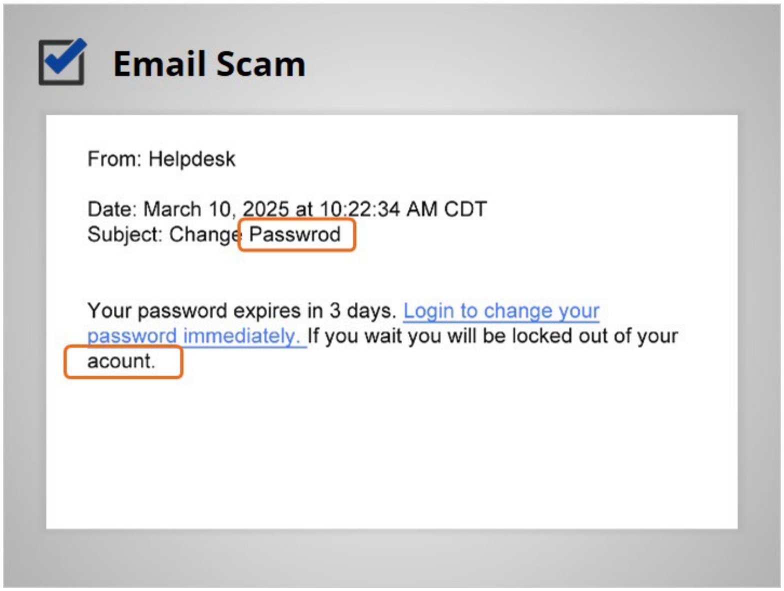
☑ Claim to be from a real organization

☑ Ask for your personal or financial information

☑ Steal money or identity

These messages can look real, but when you dig deeper, you find it’s fake. Phishing scams try to win your trust, by pretending to be a trusted person or organization. The fraudster wants you to share personal information about yourself that you would not normally share with a stranger. The fraudster then uses this personal information to gain access to your finances or steal your identity.

Let’s explore some examples of phishing scams that Albert may experience when he uses his smartphone, computer or tablet.



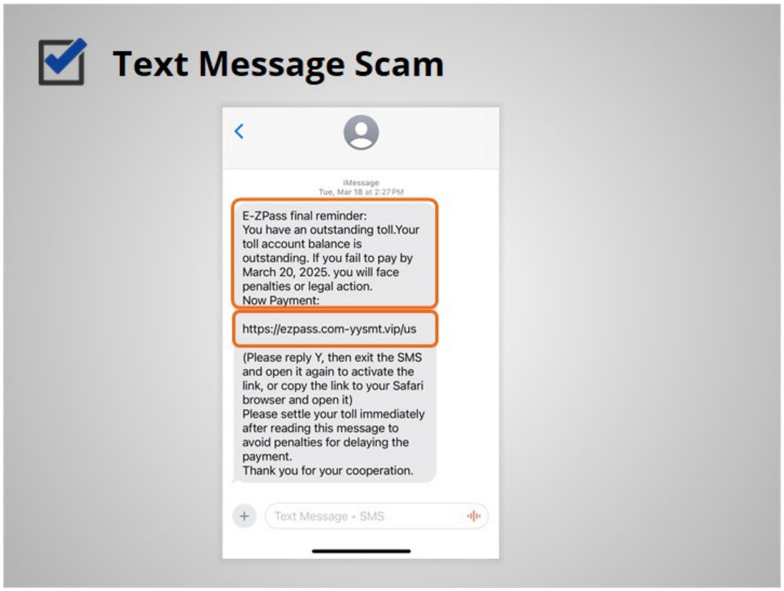
Email Scam

From: Helpdesk

Date: March 10, 2025 at 10:22:34 AM CDT
Subject: Change Passwrod

Your password expires in 3 days. Login to change your password immediately. If you wait you will be locked out of your acount.

Albert recently received an email that appeared to be from his employer's helpdesk, requesting he log into a website to update his password. Upon closer inspection, Albert notices misspellings and found the email suspicious. In this example a fraudster is pretending to work at the same organization to access personal information. If Albert had filled out the form, the fraudster could have used his account to access his employer's systems.



Text Message Scam

iMessage
Tue, Mar 18 at 2:27 PM

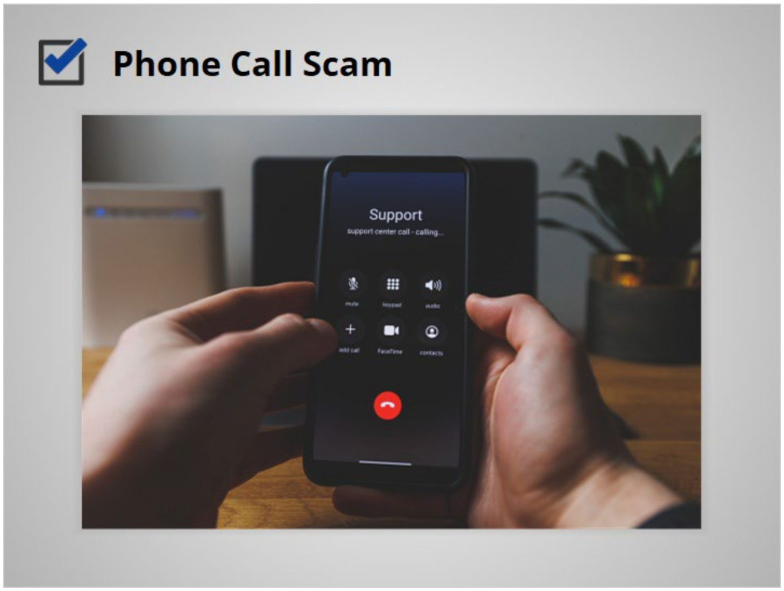
E-ZPass final reminder:
You have an outstanding toll.Your toll account balance is outstanding. If you fail to pay by March 20, 2025. you will face penalties or legal action.
Now Payment:

https://ezpass.com-yysmt.vip/us

(Please reply Y, then exit the SMS and open it again to activate the link, or copy the link to your Safari browser and open it)
Please settle your toll immediately after reading this message to avoid penalties for delaying the payment.
Thank you for your cooperation.

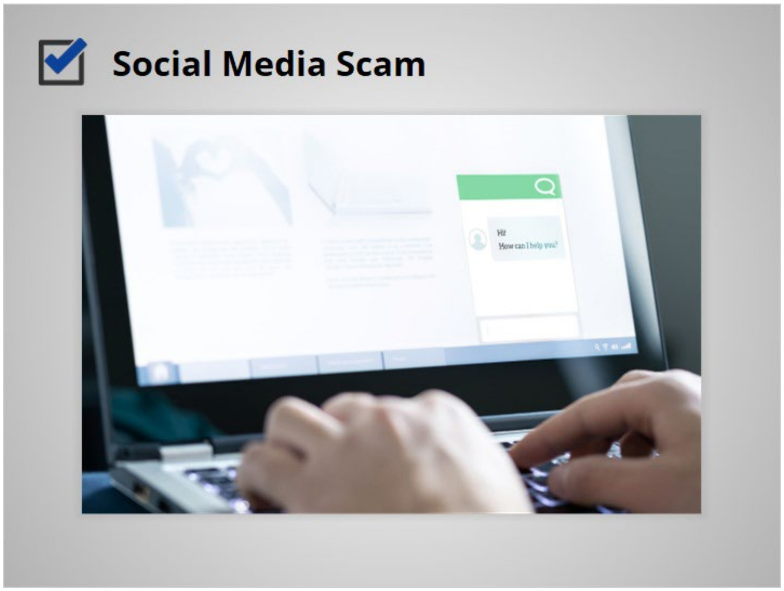
Recently, Albert received an urgent text message that appeared to be from a state agency asking him to pay an unpaid toll immediately. Like the email phishing example, text message scams try to trick people into sharing personal information. Albert does not drive, so he did not click the link to pay the bill, but had he done so, he might have unwittingly provided his financial information to a fraudster.

Albert received a call from someone who claimed to be from his health insurance company. The caller asked for Albert's personal information and claimed they needed credit card information for a medical device that would be shipped. Albert became suspicious, because his doctor didn't prescribe this device. What Albert experienced is a phone call phishing attack. With this scam, a caller impersonates someone from an organization you trust, like a government agency, bank, or insurance company, to gain your trust and access to your personal information. In this example, the fraudster wanted Albert’s credit card information to pay for a device he didn't need and wouldn't actually receive.



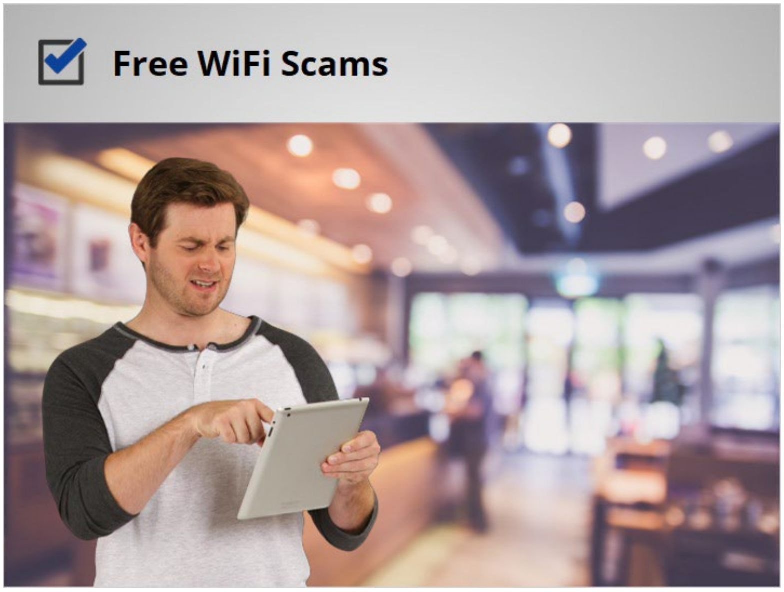
☑ Phone Call Scam

Beware that fraudsters can spoof Caller ID to make it appear that a trusted organization is making the call, even when it isn't.



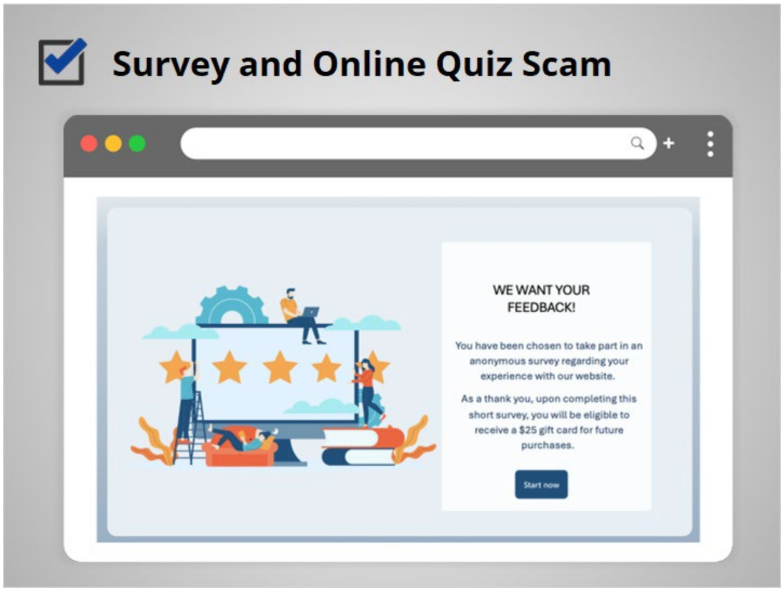
☑ Social Media Scam

There are also scammers on social media platforms. They may trick you into sharing personal information by impersonating an individual or organization. Last week, Albert left a complaint about a product on a company's social media page. The next time he visited his social media account, Albert was contacted by someone who claimed to be with the company and promised to address his complaint. When the person asked for his login credentials, Albert knew this person wasn't trying to help him, they were trying to scam him.



☑ Free WiFi Scams

Albert is at the coffee shop and wants to pay some bills while he's there. But not all free Wi-Fi networks are safe. A fraudster may set up a free Wi-Fi hotspot that looks legitimate. When a customer connects to the unofficial Wi-Fi network, the fraudster can see and track everything they do on the internet. If Albert logs into his bank account or credit card company portal, the fraudster can see his login details and use them to gain access to his accounts in the future.



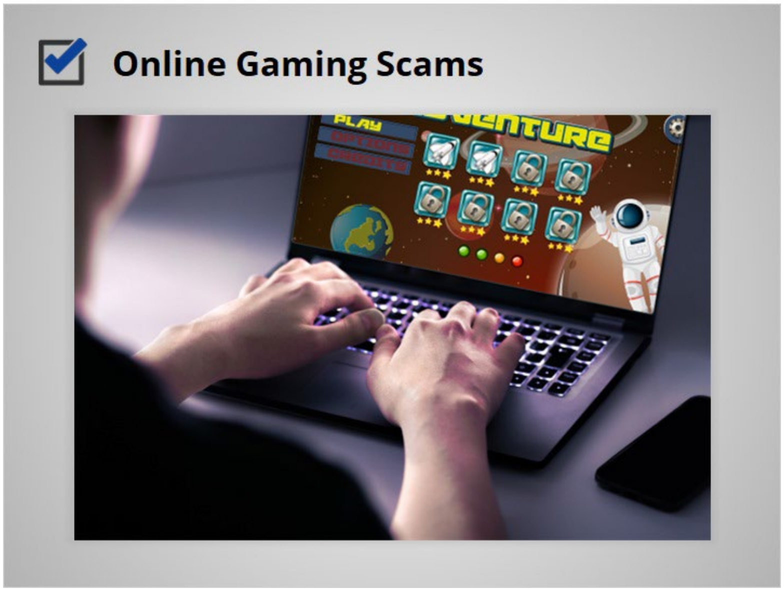
Survey and Online Quiz Scam

WE WANT YOUR FEEDBACK!

You have been chosen to take part in an anonymous survey regarding your experience with our website.

As a thank you, upon completing this short survey, you will be eligible to receive a $25 gift card for future purchases.

Beware of surveys and online quizzes found in online ads, social media, mobile games, email, or text messages. Fraudsters can use surveys and quizzes to gather sensitive information about you, which they can later use to steal your identity or gain access to your bank account or credit card information. Don't provide your usernames, passwords, Social Security number, credit card details, or any other personal information used to answer online security questions. While the promise of a gift certificate or the chance to win a vacation can be enticing, it's not worth the potential harm of sharing personal information.



☑ Online Gaming Scams

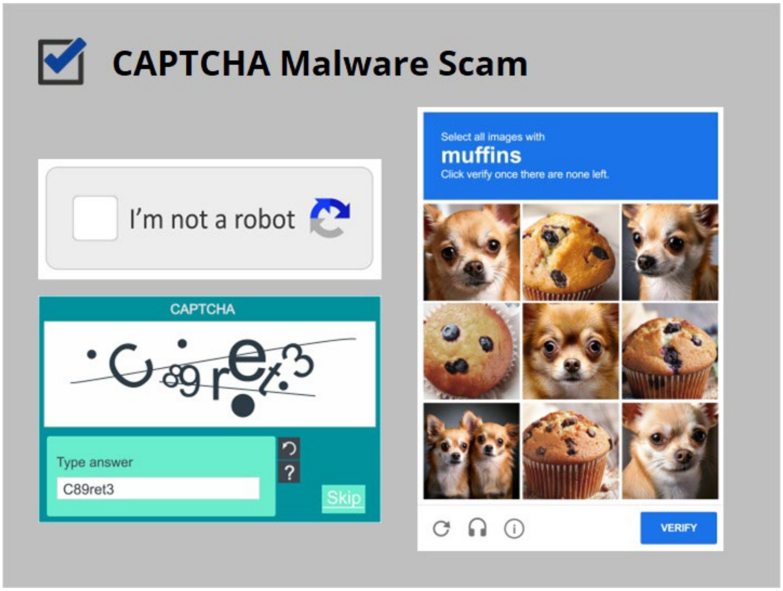
Fraudsters will also use online or mobile games to access personal information. Albert likes to play games online and, on his phone, to relax, but he knows he needs to remain vigilant. When you create a gaming account or communicate with other players, do not share private information – fraudsters can exploit that information to attempt to steal your identity.

☑ Malware Downloads
SPACE VENTURE
DOWNLOAD
Free space games!
FREE DOWNLOAD

Advertisements may appear to promote a new game or application. Albert was playing a game online when a pop up advertisement appeared. If you click on an ad and download the game, you may also install malware onto your device. Malware shares your personal information with a fraudster.

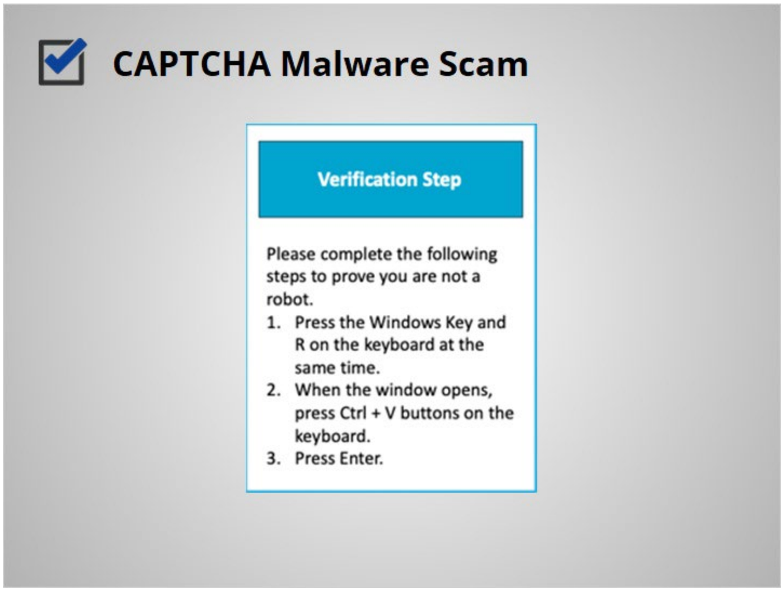
http://www.
Virus Alert!
Warning! Threat detected!
A malicious item has been detected!

Malware, also known as malicious software, is a virus created to harm a computing device. Fraudsters and scammers use malware to steal sensitive information, such as your identity, money from your accounts, or other information you do not want to share with others. Use caution when downloading software or clicking on links from sources you do not know.



CAPTCHA Malware Scam

Another malware scam involves the CAPTCHA verification tool. A CAPTCHA is a checkbox or puzzle that websites use to verify that the person using the website is a human and not a bot. However, some bad actors now use fraudulent CAPTCHAs to install malware on your computer. It starts out working just like a real CAPTCHA. You visit a website and are asked to click a checkbox that you are not a robot, type the letters you see on the screen into the textbox or select all of the pictures that match the prompt. The scam begins after you complete the first step.



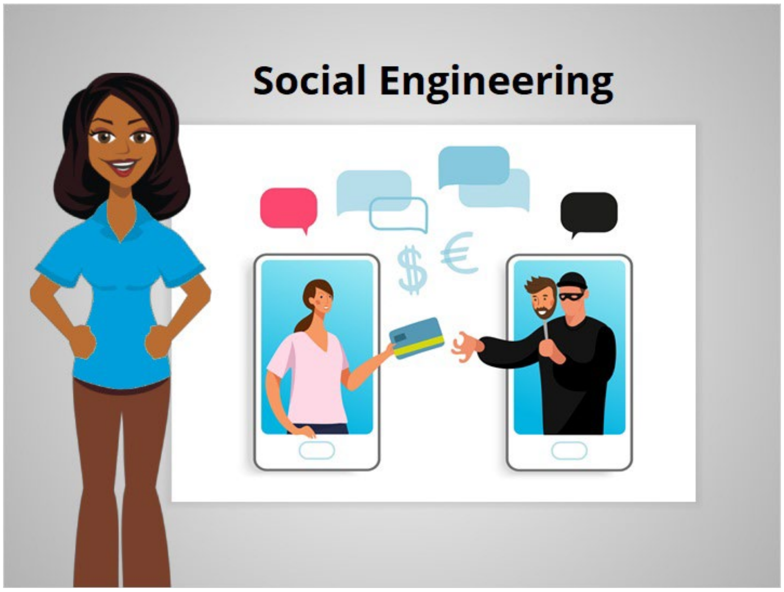
☑ CAPTCHA Malware Scam

Verification Step

Please complete the following steps to prove you are not a robot.

1. Press the Windows Key and R on the keyboard at the same time.
2. When the window opens, press Ctrl + V buttons on the keyboard.
3. Press Enter.

Another screen appears asking you to take an additional step to verify you are a human. When you complete this task, like pressing the Windows Key + R on your keyboard, it will download malware onto your device and try to install it. Valid CAPTCHAs will not ask you to take additional steps that require downloading applications onto your device.



Social Engineering

Social engineering is another common type of scam. It's a new name for an old con-artist trick. In this scam, a fraudster tries to gain your trust by convincing you they are someone they are not, to get personal information from you.

☑ Claim to be friend or family in trouble

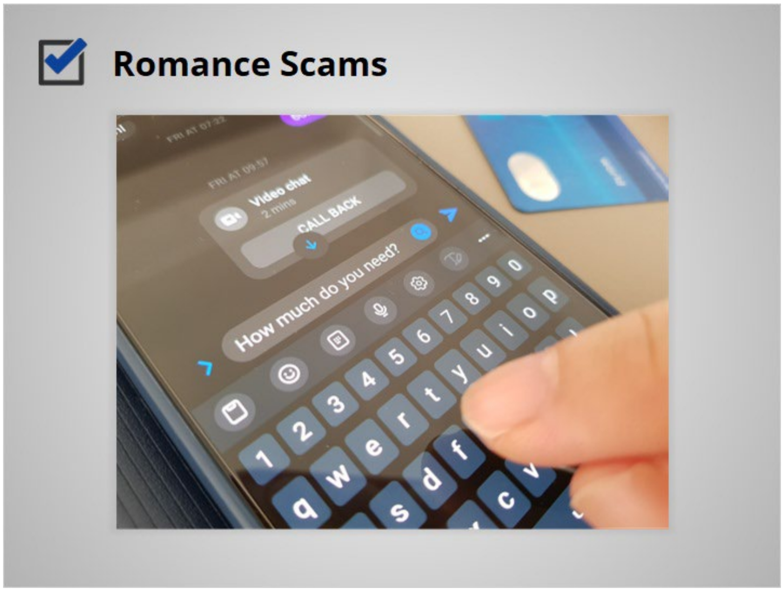
☑ Pretend to be a company with great offer

☑ Claim to be working on behalf of government, organization, collections

For example, the person may claim to be a friend or family member in trouble, pretend to be a company with a great discount or offer, or claim to be working on behalf of a government agency, organization or collection agency.
These fraudsters can approach you by phone, email, text or social media.
Let’s explore some examples of social engineering.

☑ **Family or Grandparent Emergency Scam**

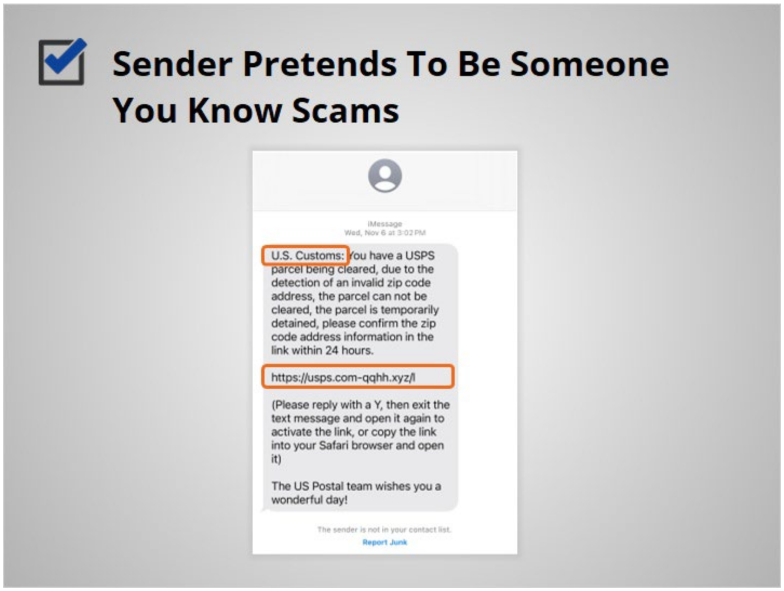
Fraudsters may impersonate a family member, like a grandchild, in urgent need, claiming a fake emergency such as bail, medical expenses, a car accident, or a stolen credit card and ask you to transfer money to them as soon as possible!



☑ Romance Scams

How much do you need?

Beware of romance scams. Fraudsters create fictional personas with fake online profiles on social media or dating apps. Over time, the criminal gains your trust only to take advantage of the relationship, tricking the victim into giving them money and sharing personal information.



☑ Sender Pretends To Be Someone You Know Scams

iMessage
Wed, Nov 6 at 3:02 PM

U.S. Customs: You have a USPS parcel being cleared, due to the detection of an invalid zip code address, the parcel can not be cleared, the parcel is temporarily detained, please confirm the zip code address information in the link within 24 hours.

https://usps.com-qqhh.xyz/l

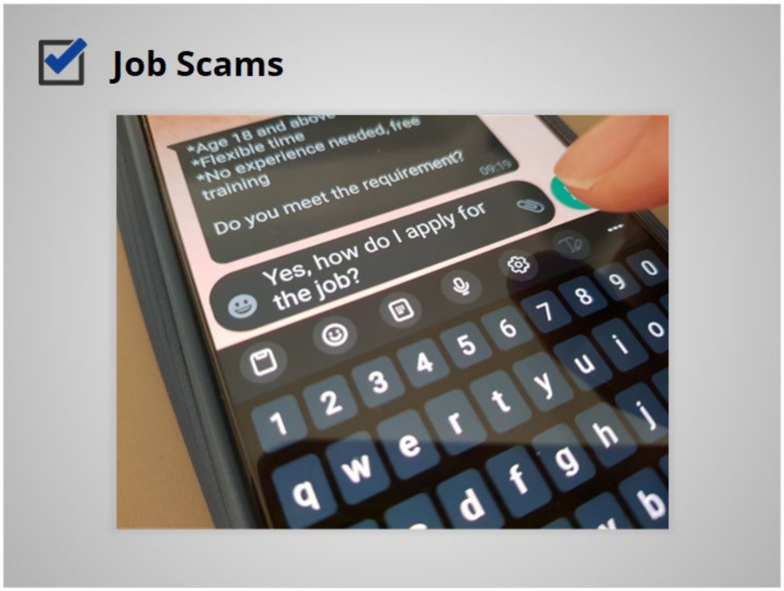
(Please reply with a Y, then exit the text message and open it again to activate the link, or copy the link into your Safari browser and open it)

The US Postal team wishes you a wonderful day!

The sender is not in your contact list.
Report Junk

You may also be contacted by email, text message, or on social media by a person pretending to be someone you know, like a co-worker, police officer, delivery person, or government representative.

This text message claims to come from US Customs, but uses a fraudulent US Postal Service link to try to get personal information from you.



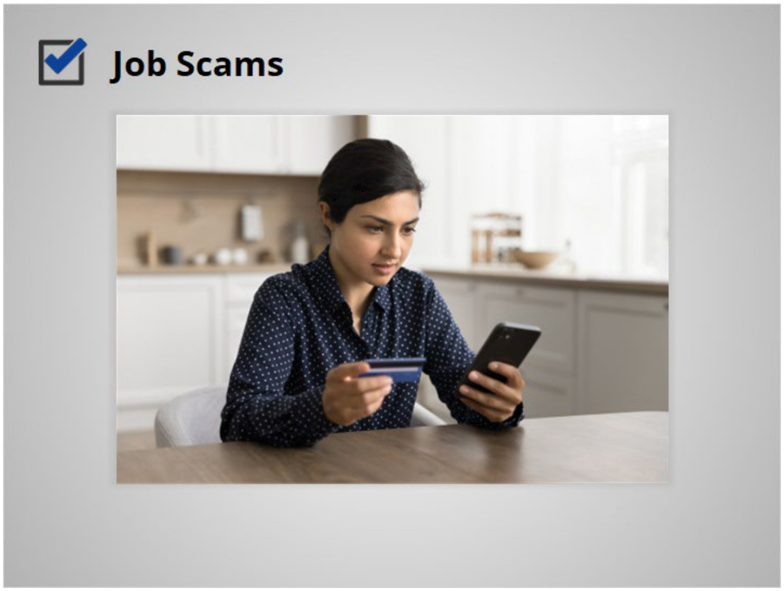
☑ Job Scams

*Age 18 and above
*Flexible time
*No experience needed, free training

Do you meet the requirement?

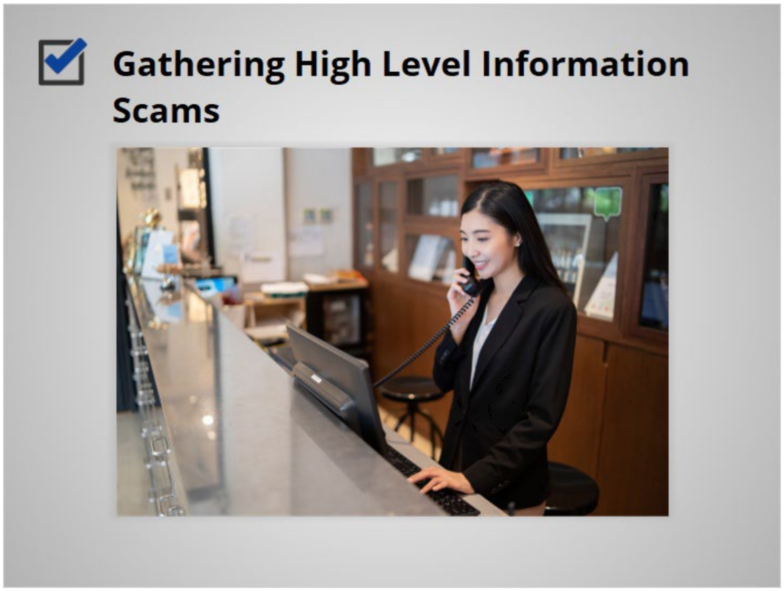
Yes, how do I apply for the job?

Fraudsters can also pose as employers who are hiring but are actually using the hiring process to scam job seekers. For example, a potential employer reaches out about a job. After a few emails, they offer you the position and send paperwork that requires your personal information, such as your Social Security Number and bank account details. Once you submit this paperwork, you never hear from them again and they now have your personal information.



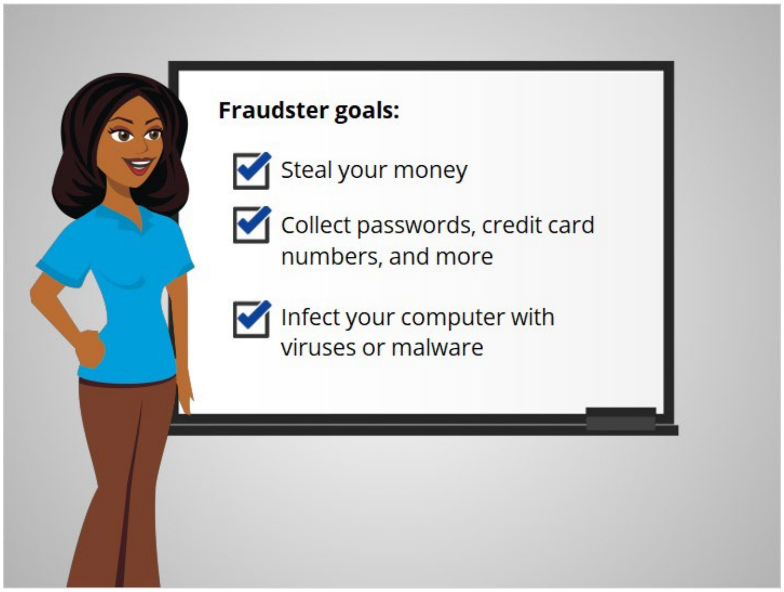
☑ Job Scams

Another employment scam involves offering jobs that require an upfront payment for training or equipment. The employer promises to reimburse you once you begin, but after they receive your money, you never hear from them again.



☑ Gathering High Level Information Scams

This type of scam typically targets high-ranking people within an organization, or influential people in a community. A fraudster will begin by contacting lower level staff members at a company, or by contacting friends or associates of someone of influence. During the contact, the fraudster will attempt to lure sensitive data, such as personal or company financial information, passwords, trade secrets, or other confidential information that could harm the organization.



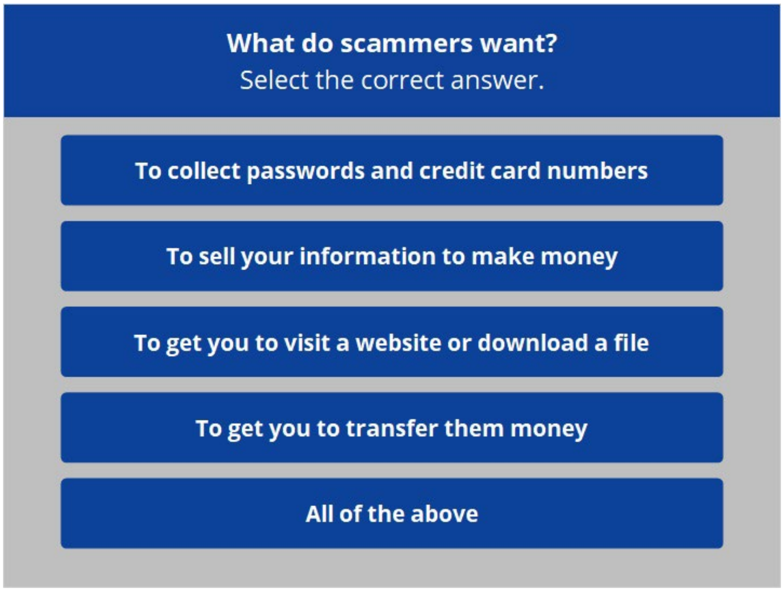
Fraudster goals:

☑ Steal your money

☑ Collect passwords, credit card numbers, and more

☑ Infect your computer with viruses or malware

No matter what form a scam takes, fraudsters usually have the same goals: to steal your money or collect information like your passwords or credit card numbers. Scams can also cause problems for your computer by infecting it with viruses or malware.

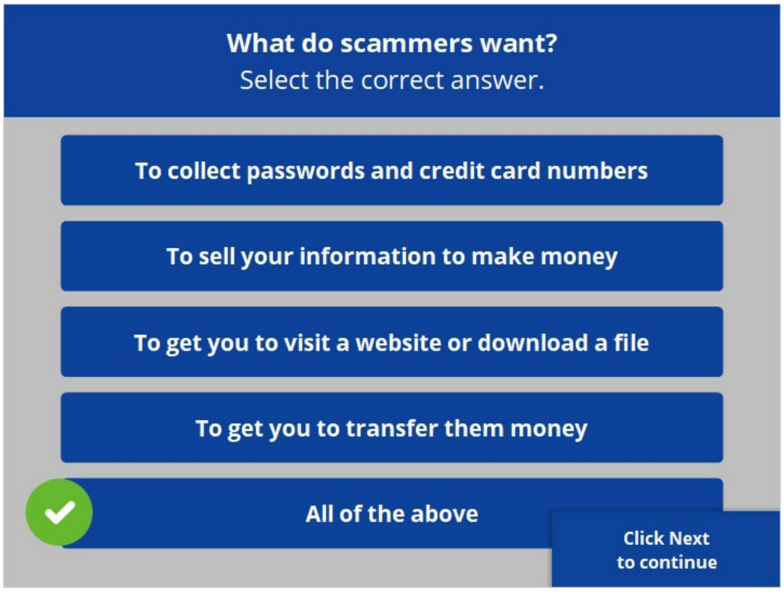


What do scammers want?
Select the correct answer.

- To collect passwords and credit card numbers
- To sell your information to make money
- To get you to visit a website or download a file
- To get you to transfer them money
- All of the above

Let’s see what you remember about the scams we covered today.

What do scammers want? Select the correct answer.



What do scammers want?
Select the correct answer.

- To collect passwords and credit card numbers
- To sell your information to make money
- To get you to visit a website or download a file
- To get you to transfer them money
- ✓ All of the above

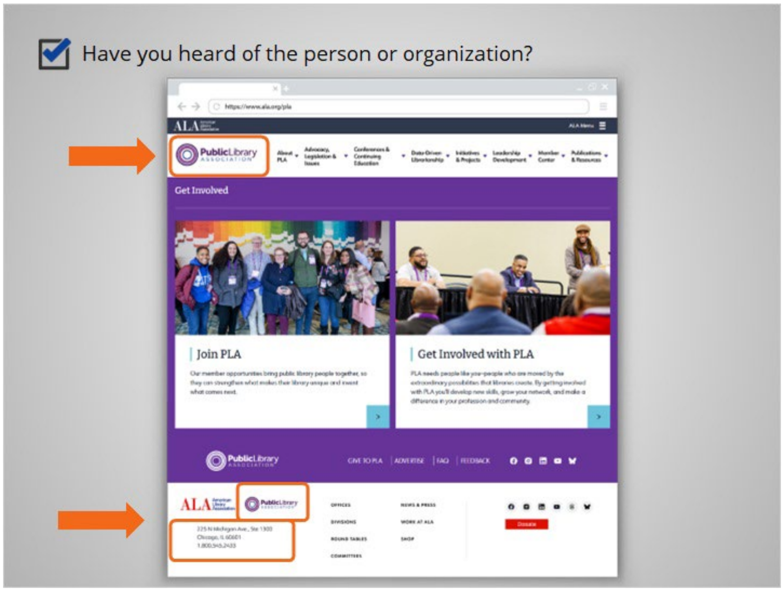
The correct answer is all of the above. Knowing what scammers want can help you protect yourself from fraud and keep your accounts and devices safe from online scams. Click Next to continue.

In this lesson, Albert learned about common types of fraud and scams, including phishing and social engineering. He learned that he may encounter these scams while browsing a website, receiving a phone call, in an email, text message, online game, or even in a pop-up window on his computer. In the next lesson, Albert will learn a few tips to help him identify online scams.

Activity 2: Recognizing Scams

How can you tell if something is a scam or a fraud?

In this lesson, Albert will learn several tips to help him identify scams online, in his email, and in text messages.



☑ Have you heard of the person or organization?

https://www.ala.org/pla

ALA Menu

About PLA · Advocacy, Legislation & Issues · Conferences & Continuing Education · Data-Driven Librarianship · Initiatives & Projects · Leadership Development · Member Center · Publications & Resources

Get Involved

Join PLA

Our member opportunities bring public library people together, so they can strengthen what makes their library unique and invent what comes next.

Get Involved with PLA

PLA needs people like you–people who are moved by the extraordinary possibilities that libraries create. By getting involved with PLA you'll develop new skills, grow your network, and make a difference in your profession and community.

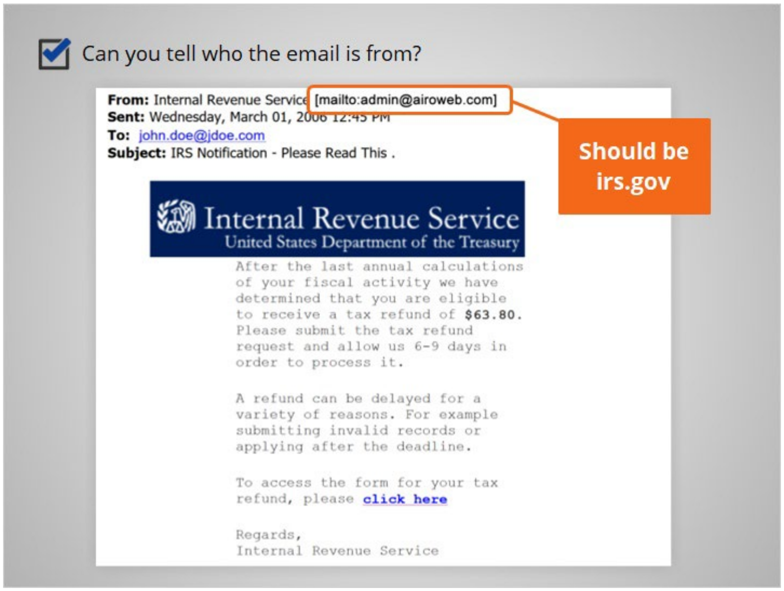
GIVE TO PLA | ADVERTISE | FAQ | FEEDBACK

225 N Michigan Ave., Ste 1300
Chicago, IL 60601
1.800.545.2433

OFFICES · DIVISIONS · ROUND TABLES · COMMITTEES · NEWS & PRESS · WORK AT ALA · SHOP

Donate

Have you heard of the person or organization before? In this example, we are using the Public Library Association website to identify key features of a legitimate organization's website. If it's a legitimate business, like this example, their official logo, address, and contact information should be posted on their website.



☑ Can you tell who the email is from?

From: Internal Revenue Service [mailto:admin@airoweb.com]
Sent: Wednesday, March 01, 2006 12:45 PM
To: john.doe@jdoe.com
Subject: IRS Notification - Please Read This .

Internal Revenue Service
United States Department of the Treasury

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of **$63.80**. Please submit the tax refund request and allow us 6-9 days in order to process it.

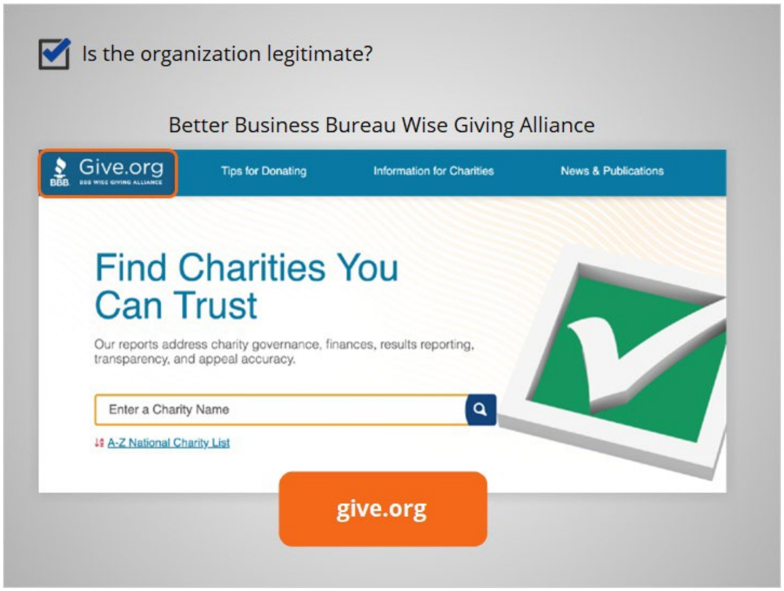
A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please **click here**

Regards,
Internal Revenue Service

Should be irs.gov

Can you tell who it's from? Albert received an email that claimed to be from the IRS. But when he looked closely, he noticed that the address was not from irs.gov and was sent from someone he did not know or recognize. This is a sure sign of a phishing scam. If you can’t see the actual email address from the sender, you can roll over the email name, or tap on the email name on a mobile device, to see the sender’s email address.



☑ Is the organization legitimate?

Better Business Bureau Wise Giving Alliance

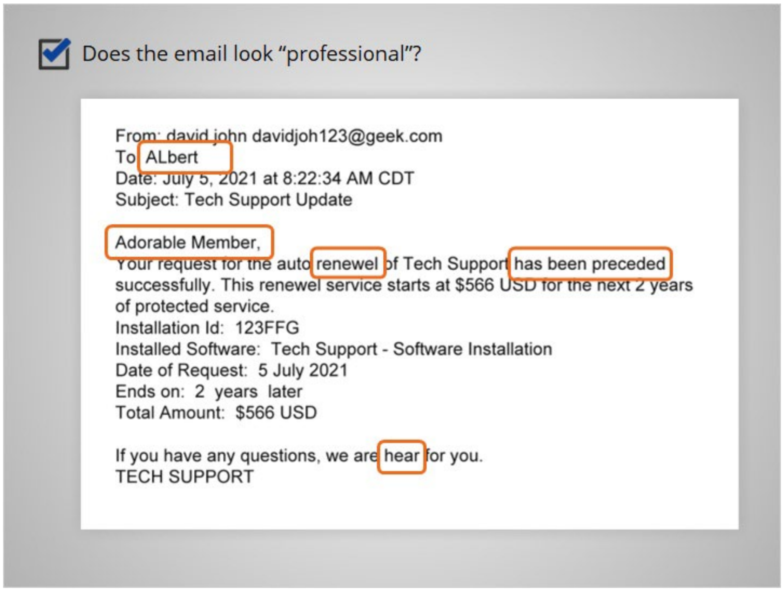
BBB Give.org BBB WISE GIVING ALLIANCE
Tips for Donating
Information for Charities
News & Publications

Find Charities You Can Trust

Our reports address charity governance, finances, results reporting, transparency, and appeal accuracy.

Enter a Charity Name
A-Z National Charity List
give.org

Is the organization legitimate? Use caution when you're contacted by a charity on the phone, text, email or online. To learn more about a charity asking for money check the BBB Wise Giving Alliance website to see reports and ratings about how charitable organizations spend donations.



☑ Does the email look “professional”?

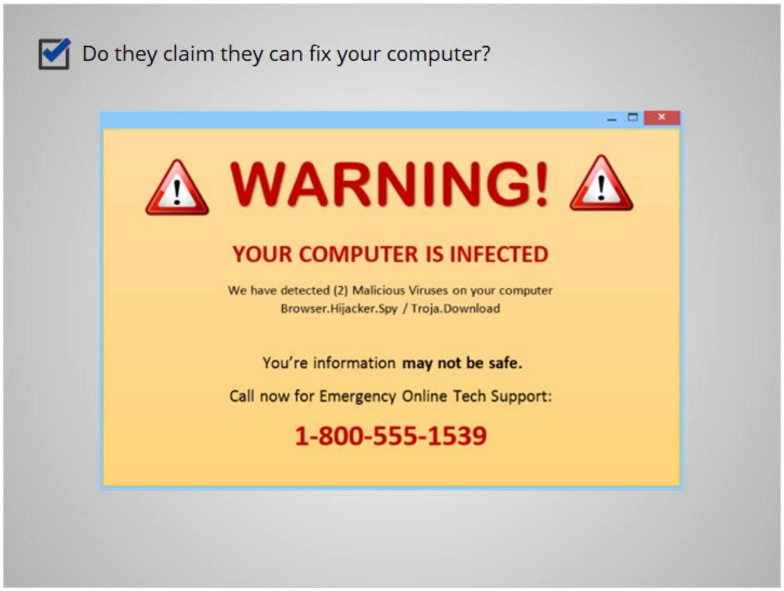
From: david john davidjoh123@geek.com
To ALbert
Date: July 5, 2021 at 8:22:34 AM CDT
Subject: Tech Support Update

Adorable Member,
Your request for the auto renewel of Tech Support has been preceded successfully. This renewel service starts at $566 USD for the next 2 years of protected service.
Installation Id: 123FFG
Installed Software: Tech Support - Software Installation
Date of Request: 5 July 2021
Ends on: 2 years later
Total Amount: $566 USD

If you have any questions, we are hear for you.
TECH SUPPORT

Is the message professional? Albert has received an email from a company he has an account with. But when he receives other emails from companies, he has an account with, they normally include his name. This one just says, “Adorable Member”.

Albert also notices that there are spelling errors and grammar mistakes in the email. If the email is from a legitimate business, it wouldn’t include those mistakes.



☑ Do they claim they can fix your computer?

WARNING!

YOUR COMPUTER IS INFECTED

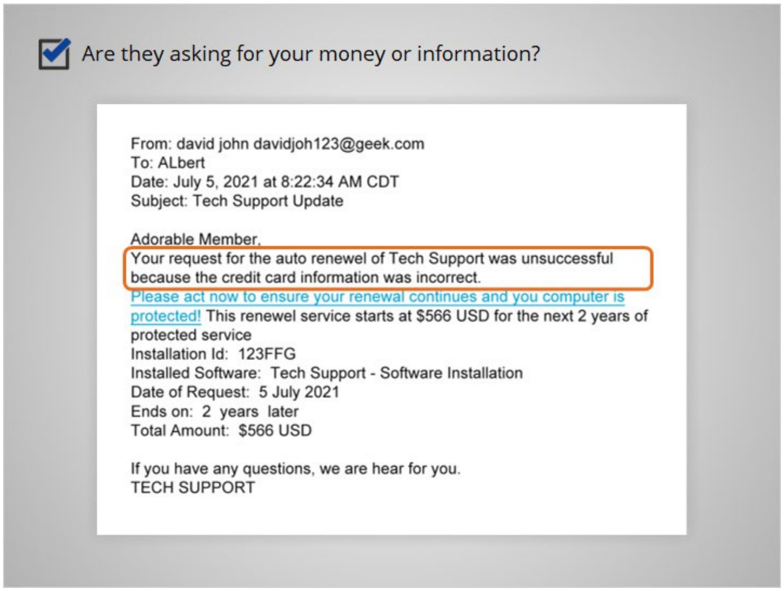
We have detected (2) Malicious Viruses on your computer
Browser.Hijacker.Spy / Troja.Download

You're information **may not be safe.**

Call now for Emergency Online Tech Support:

1-800-555-1539

Do they claim that they can fix your computer? Albert was searching the web and this pop-up message displayed. It claims his computer is infected and that he should click on a link or call a number so it can be fixed. Legitimate companies will never solicit you to fix your computer in this way.



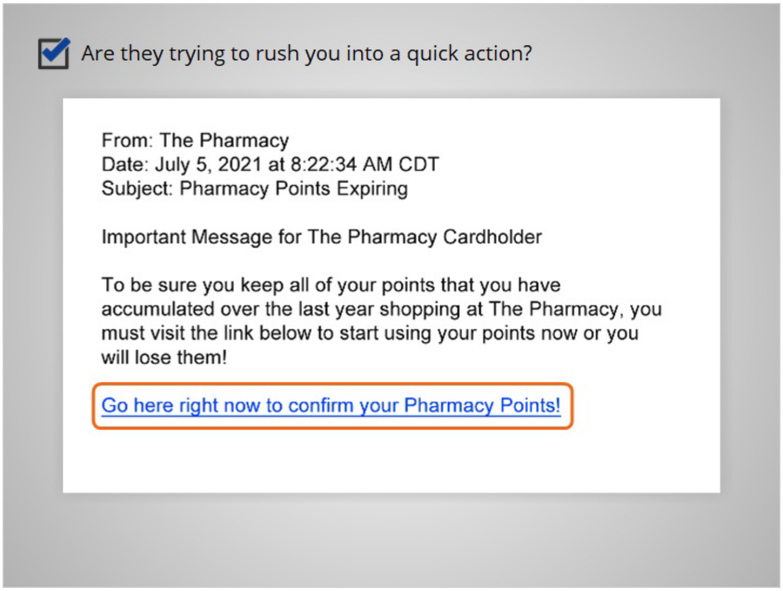
☑ Are they asking for your money or information?

From: david john davidjoh123@geek.com
To: ALbert
Date: July 5, 2021 at 8:22:34 AM CDT
Subject: Tech Support Update

Adorable Member,
Your request for the auto renewel of Tech Support was unsuccessful because the credit card information was incorrect.
Please act now to ensure your renewal continues and you computer is protected! This renewel service starts at $566 USD for the next 2 years of protected service
Installation Id: 123FFG
Installed Software: Tech Support - Software Installation
Date of Request: 5 July 2021
Ends on: 2 years later
Total Amount: $566 USD

If you have any questions, we are hear for you.
TECH SUPPORT

Are they asking for your money or information? In this email that Albert received, the fraudster is asking for his credit card information. Fraudsters may claim that they need to verify or update your information. Some fraudsters will also ask you to wire them money or send a deposit, promising to pay you more in return.



☑ Are they trying to rush you into a quick action?

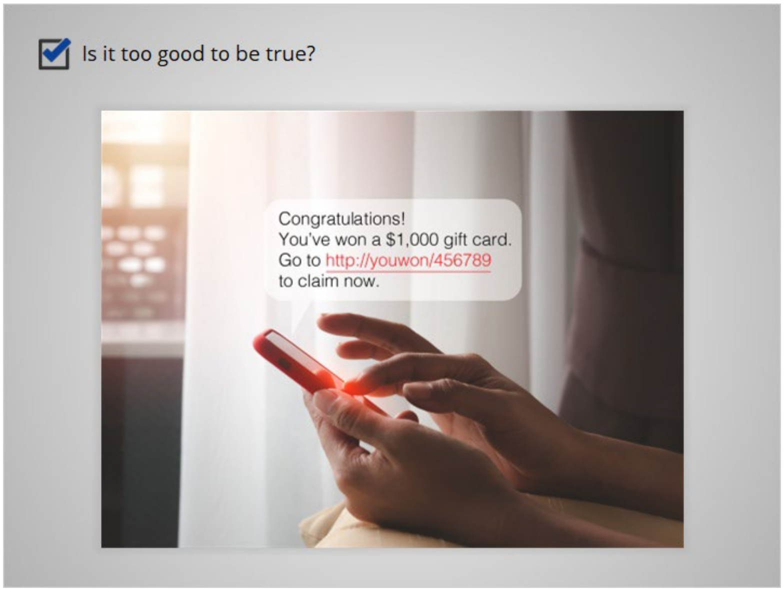
From: The Pharmacy
Date: July 5, 2021 at 8:22:34 AM CDT
Subject: Pharmacy Points Expiring

Important Message for The Pharmacy Cardholder

To be sure you keep all of your points that you have accumulated over the last year shopping at The Pharmacy, you must visit the link below to start using your points now or you will lose them!

Go here right now to confirm your Pharmacy Points!

Are they trying to rush you into a quick action before you have time to think about it? Albert has received this message about his pharmacy points expiring. Some fraudsters try to scare you into acting fast, threatening that something bad will happen, like an account will be closed if you don't act now.

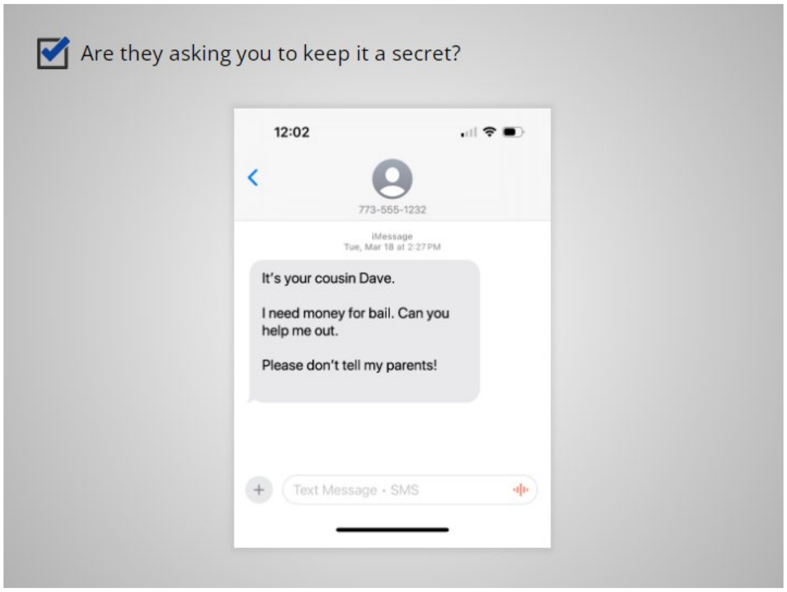


☑ Is it too good to be true?

Congratulations!
You've won a $1,000 gift card.
Go to http://youwon/456789
to claim now.

Is it too good to be true, like winning the prize for a contest that you don't remember entering? If it sounds too good to be true, it probably is.

None of the other companies whose names or logos appear in these educational materials have been involved in the creation of these materials, or approve, sponsor, or are affiliated in any way with these materials.



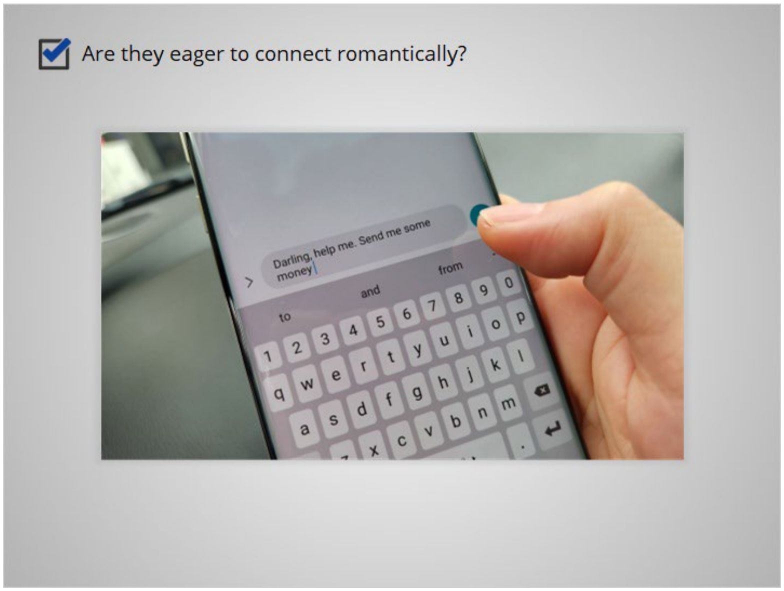
☑ Are they asking you to keep it a secret?

It's your cousin Dave.

I need money for bail. Can you help me out.

Please don't tell my parents!

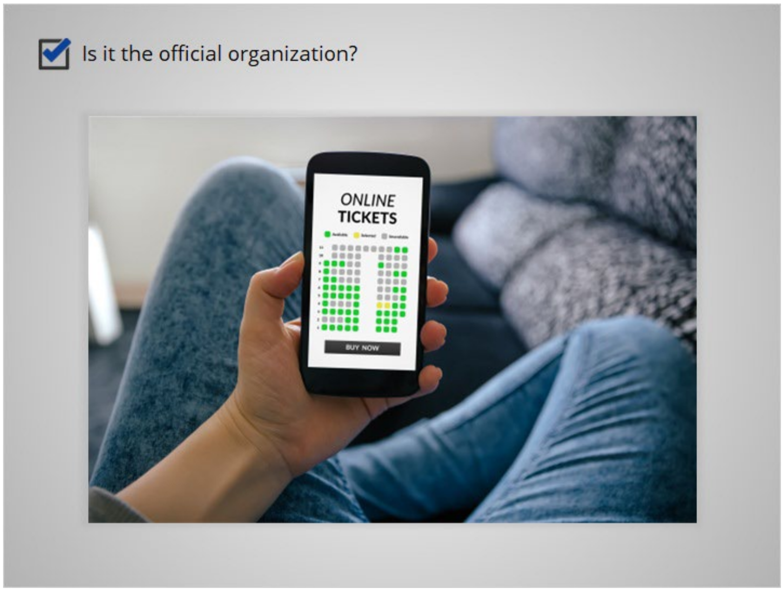
Is the sender asking you to keep it secret? Albert received this text from his cousin. When he looked at the message more closely, he realized it did not come from his cousin's phone number. Another variation on this scam is that the person claims they are using a friend's phone. Scammers try to pressure you into sending money or information before you have time to check if the emergency is real. If someone you know says they are in trouble, contact them using the information you have, not the contact information or link from the person who reaches out to you.



☑ Are they eager to connect romantically?

Darling, help me. Send me some money

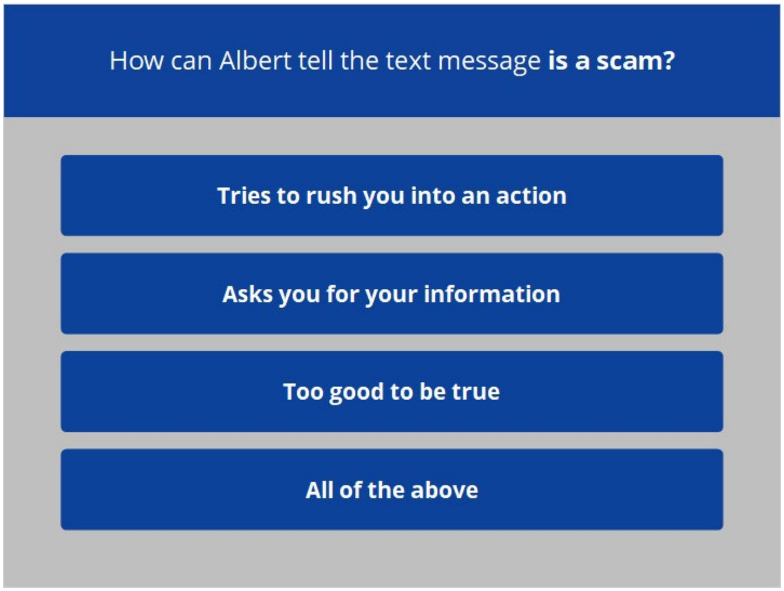
Has someone tried to connect with you romantically online? You may have met them on a dating app or your favorite social media platform. It starts slow, but over time, the conversation becomes more personal. Then they start asking for money or gifts, or they need help with an unexpected bill, or they would love to come see you but they need you to pay for the plane ticket. Scammers create fake profiles using stolen photos to build personal relationships.



☑ Is it the official organization?

Are you working with the organization you thought you were? Some organizations will provide the goods or service you requested but will charge large service fees – fees that you would not have paid if you had purchased from the original provider. For instance, Albert wanted to purchase tickets to a hockey game. He searched online, clicked the first link, which was an advertisement for a ticket reseller, and purchased the tickets. However, he later found out that he paid a significant fee for the tickets that he would not have paid if he had bought them directly from the hockey arena. If you are not sure if the link is an advertisement, look for the word SPONSORED in your search results. Sponsored indicates the link in the result list is a paid advertisement.

Albert has learned how to identify scams online, in his email, and in text messages. Let’s see what you remember about recognizing scams.

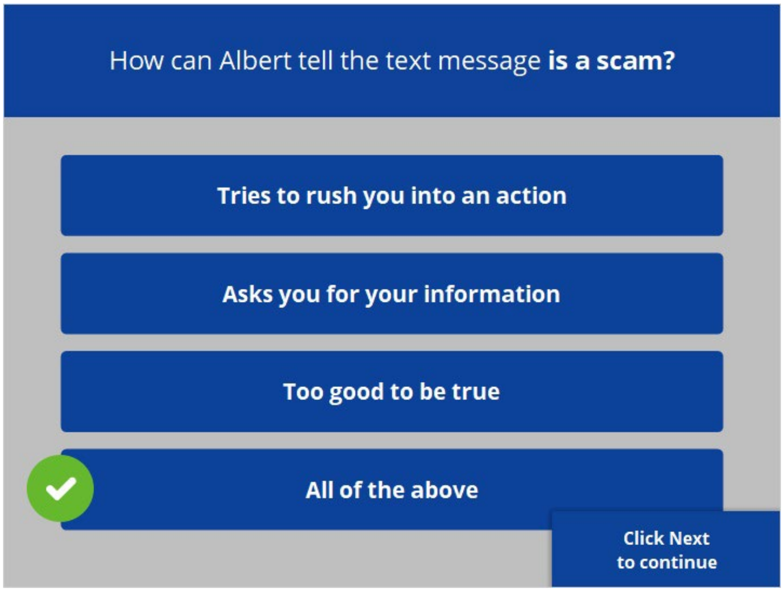


How can Albert tell the text message **is a scam?**

Tries to rush you into an action
Asks you for your information
Too good to be true
All of the above

Albert is looking at a text message and he is not sure it is a scam. How can he tell that it’s a scam? Select the correct answer.

None of the other companies whose names or logos appear in these educational materials have been involved in the creation of these materials, or approve, sponsor, or are affiliated in any way with these materials.



How can Albert tell the text message **is a scam?**

Tries to rush you into an action

Asks you for your information

Too good to be true

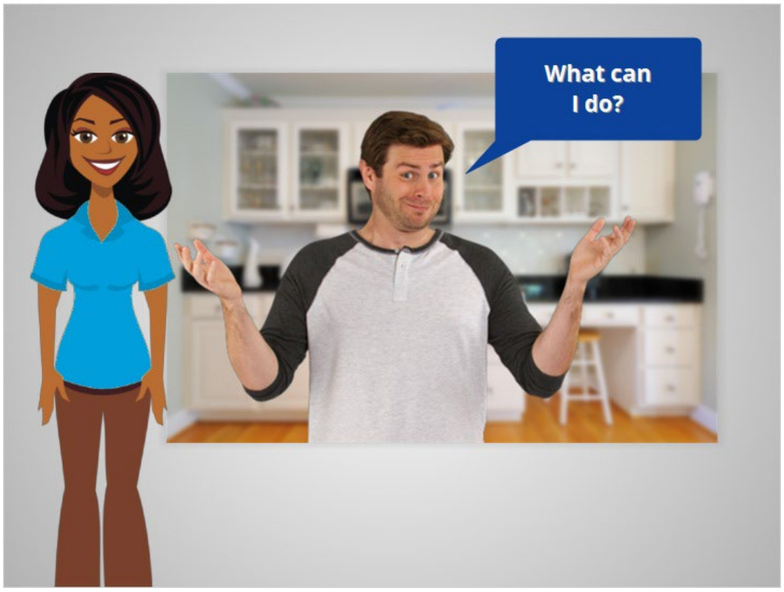
✓ All of the above

Click Next to continue

The correct answer is all of the above. There are a variety of ways to determine if a text message, website or email is a scam. Knowing how to identify a scam can help you protect yourself from fraud and keep your accounts and devices safe. Click Next to continue.

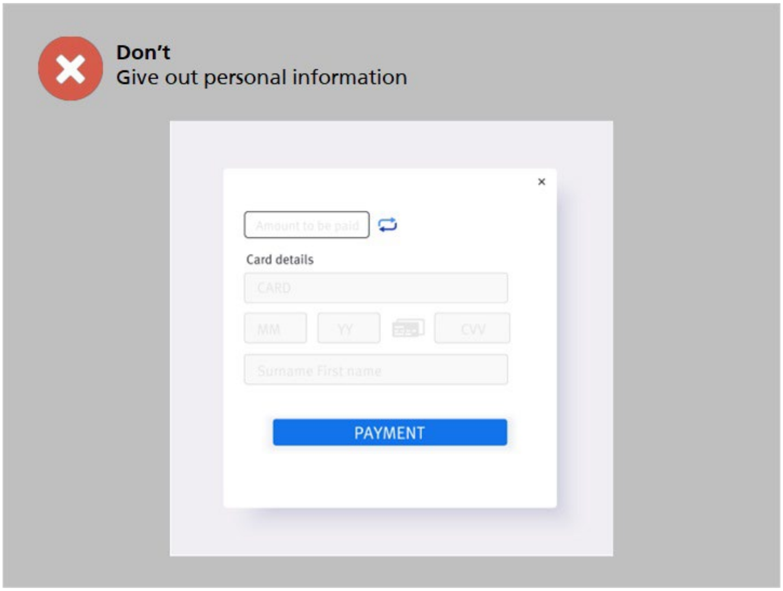
In this lesson, Albert learned tips that will help him identify scams while browsing a website, receiving a phone call, in an email, text message, or online game. In the next lesson, Albert learns what to do with a scam once he has identified it.

Activity 3: What to Do with Scams



Now that Albert has learned how to recognize common frauds and scams, he wants to know what he can do when he encounters one. In this lesson Albert will learn what he should and should not do when he encounters a scam on a website, in an email, text message or on a phone call.

First let's start with things Albert should not do.

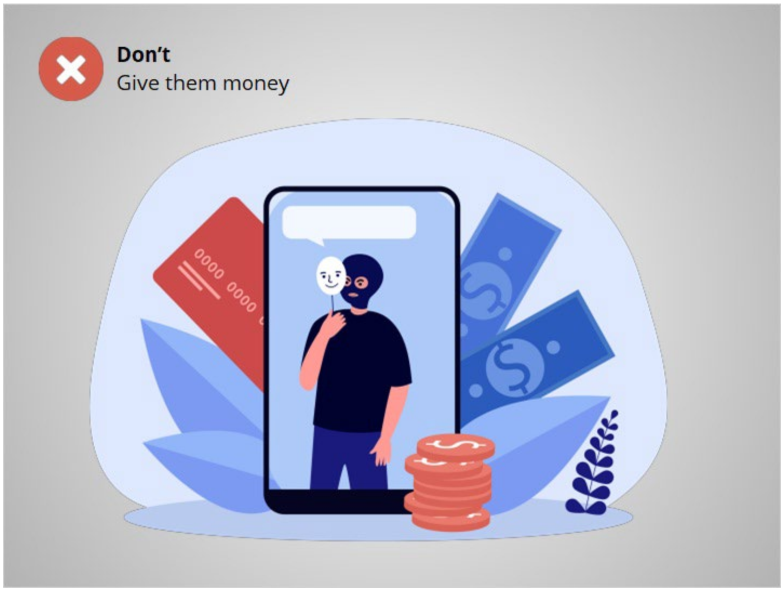


Don’t
Give out personal information

Don’t give out personal information to something that could be a scam. This includes name, email address, credit card number, or password.

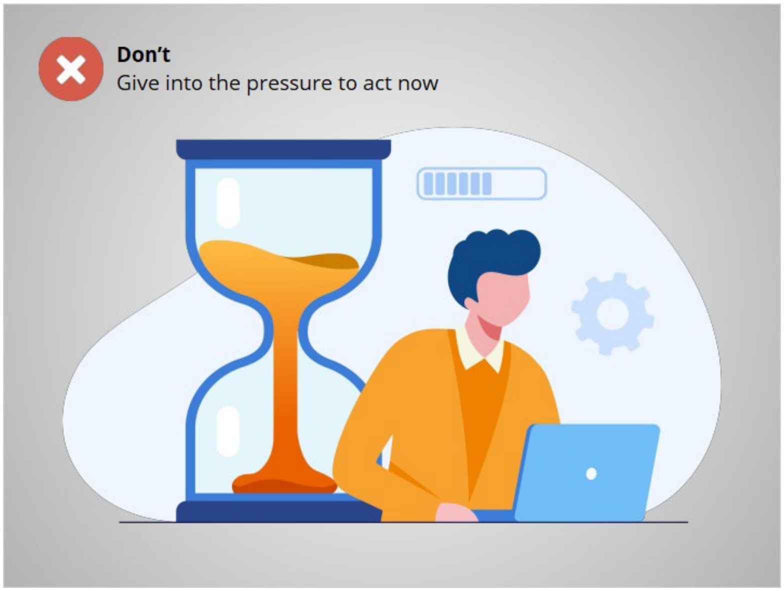
Don’t
Share your personal PIN, password, or passcode

Never share the PIN, passwords, or passcodes associated with your accounts.



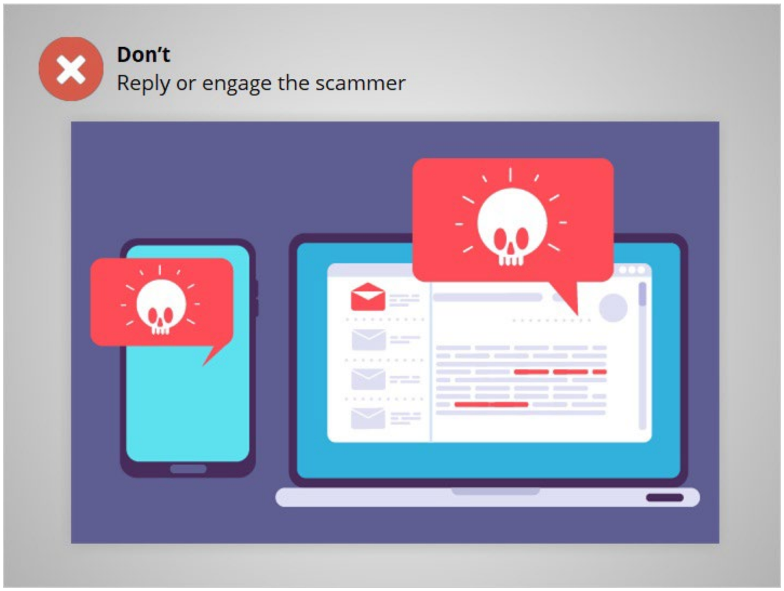
Don't
Give them money

Do not send money, gift cards, prepaid debit cards, or transfer money to someone you have not met in person. If you're shopping on a social media marketplace or another local buy and sell marketplace, don't send money before you see the item in person.



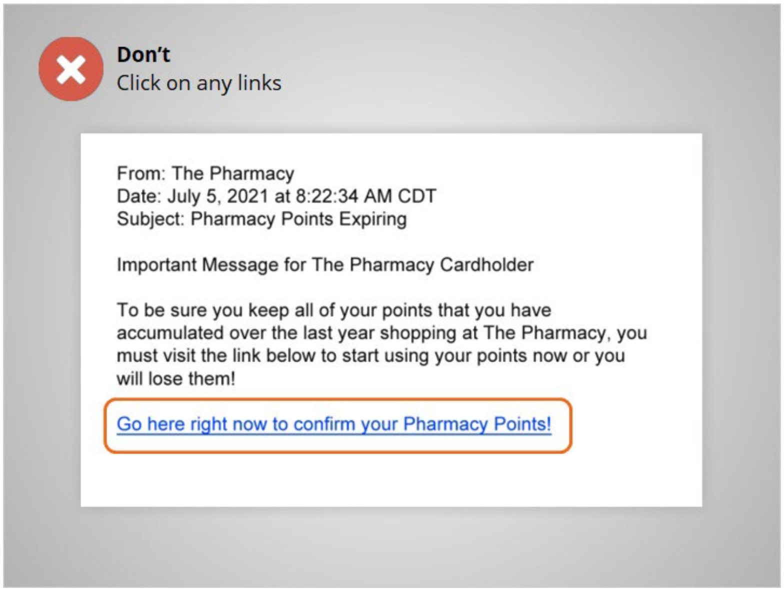
Don't
Give into the pressure to act now

Don't give into the pressure to act now. Scammers try to create a sense of urgency so that you act quickly. Take the time you need to verify the request.



Don't
Reply or engage the scammer

Don't reply or engage them. This can notify the scammer that they've reached a real person, which can result in more scam emails, phone calls or text messages.



Don't
Click on any links

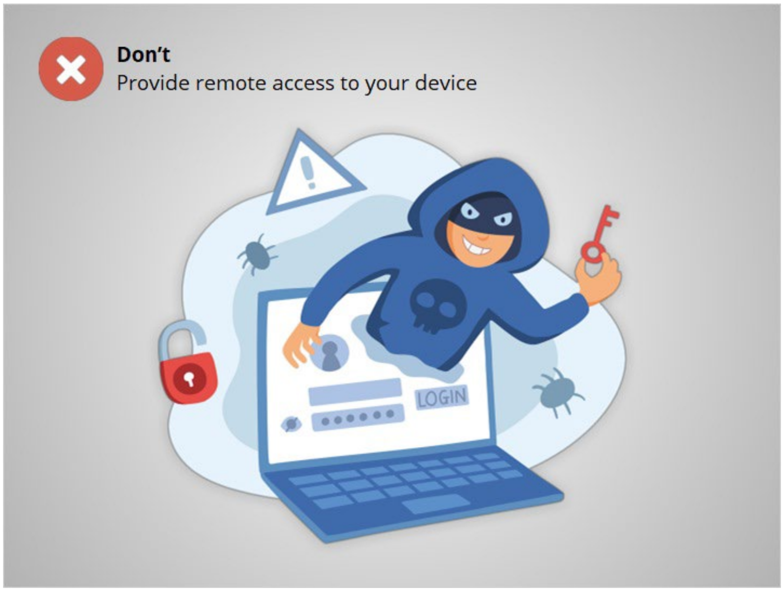
From: The Pharmacy
Date: July 5, 2021 at 8:22:34 AM CDT
Subject: Pharmacy Points Expiring

Important Message for The Pharmacy Cardholder

To be sure you keep all of your points that you have accumulated over the last year shopping at The Pharmacy, you must visit the link below to start using your points now or you will lose them!

Go here right now to confirm your Pharmacy Points!

Don't click on any links in a scam email or text message. This can take you to untrustworthy websites.



Don’t

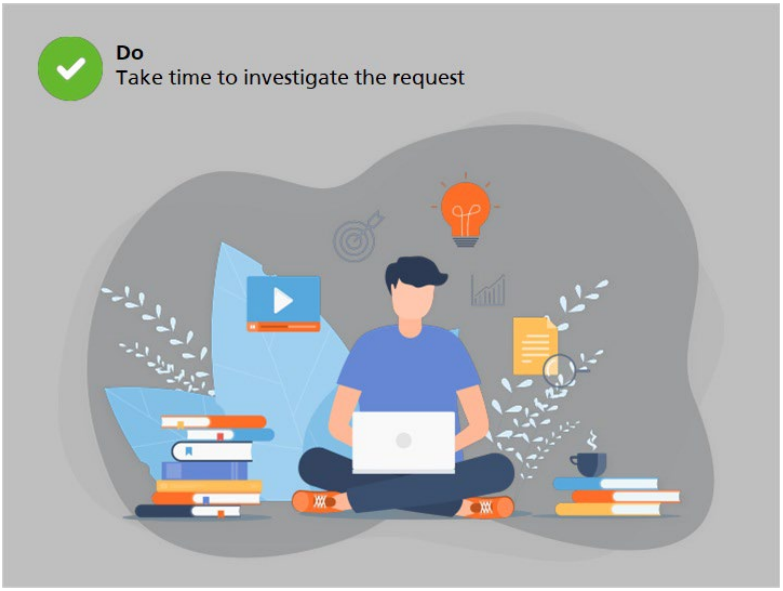
Provide remote access to your device

Never give anyone you don’t trust access to your device. Just by installing software you can give someone remote access to your device.

Don’t

Download any files or attachments

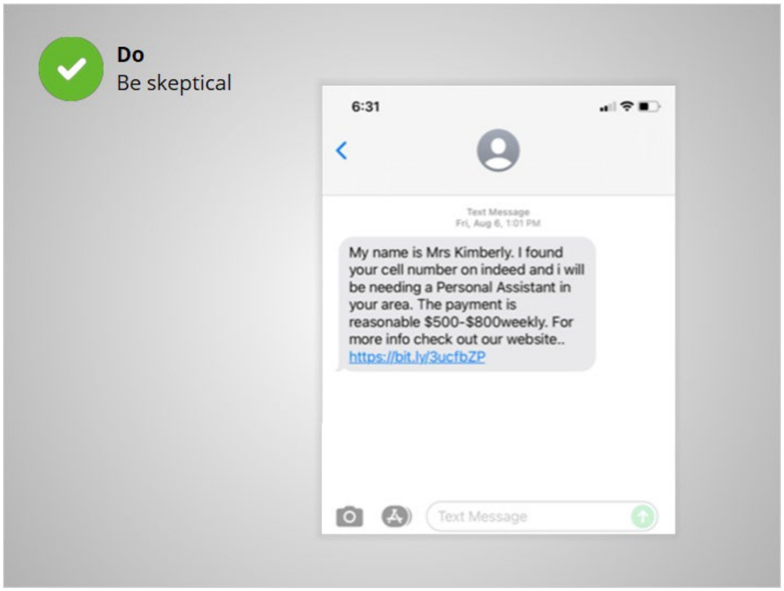
Don’t download any attachments from emails or text messages or files on an untrustworthy website. They could contain viruses or malware that could harm your computer or collect your personal information.



Do

Take time to investigate the request

If you think something might be a scam, check with a trusted person to verify if it's safe. If someone reports that a family member is in trouble, contact that person to check. If someone reports a problem with your bank account, contact your bank using information from their official website or bank statement – do not use the contact information or link from the person who contacts you.



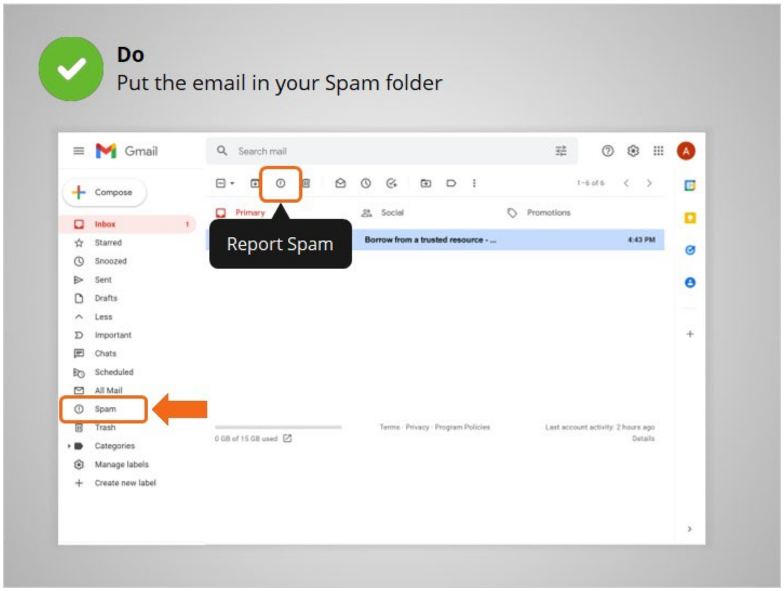
Do
Be skeptical

6:31

Text Message
Fri, Aug 6, 1:01 PM

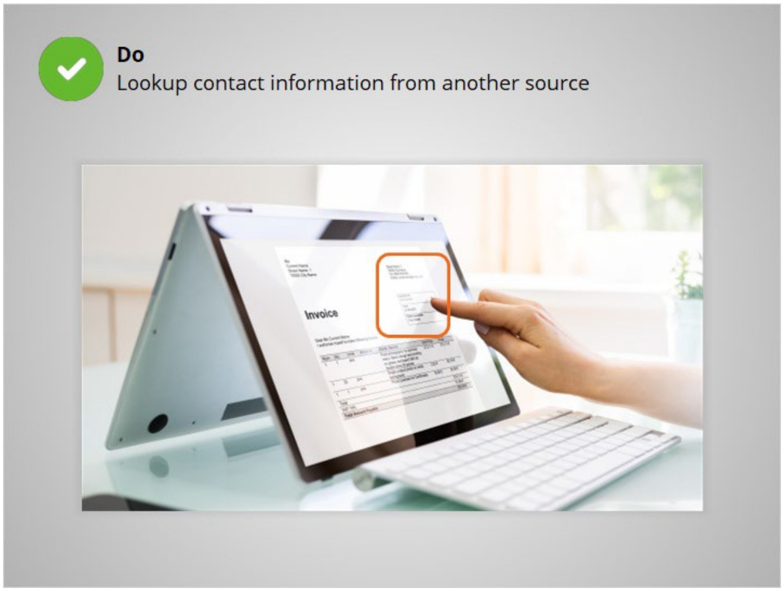
My name is Mrs Kimberly. I found your cell number on indeed and i will be needing a Personal Assistant in your area. The payment is reasonable $500-$800weekly. For more info check out our website.. https://bit.ly/3ucfbZP

Do be skeptical. If you think something may be a scam, it probably is. Remember to read emails and text messages carefully, checking to make sure you know the sender.



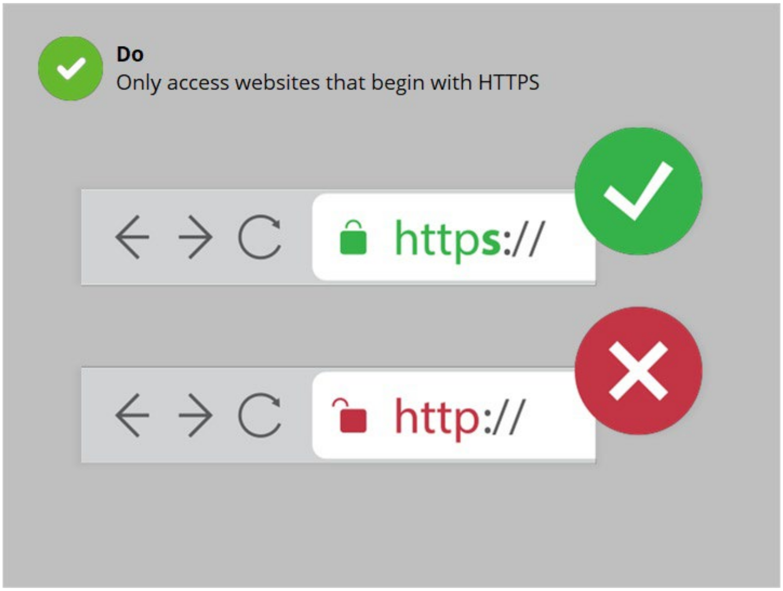
Do
Put the email in your Spam folder

Most email flagged as spam is automatically moved to a spam folder, so you don't see it in the Inbox. This is an example of the spam folder in Gmail. If you do see a spam email in your Inbox, mark the item as spam. Avoid opening the message, clicking on any links, or viewing any pictures in the message.



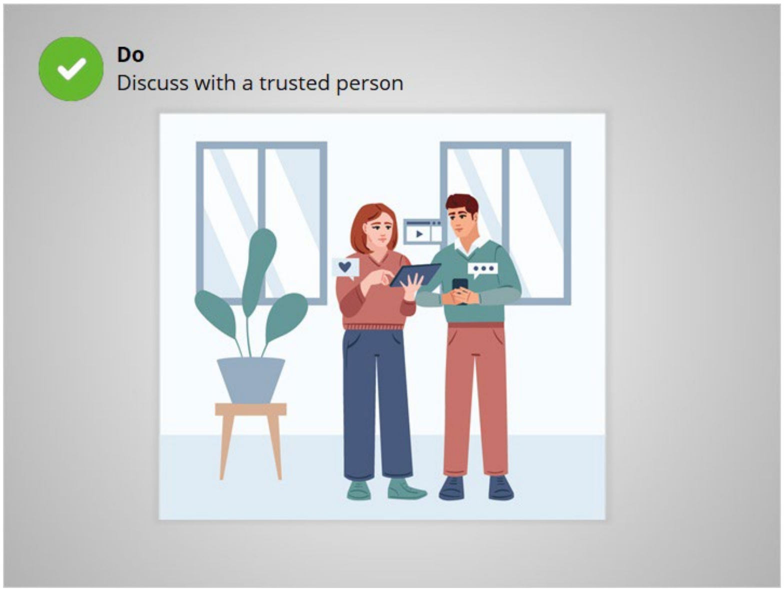
Do
Lookup contact information from another source

Do confirm the contact information is correct by checking a statement you received in the mail or the official website of the company.



Do
Only access websites that begin with HTTPS

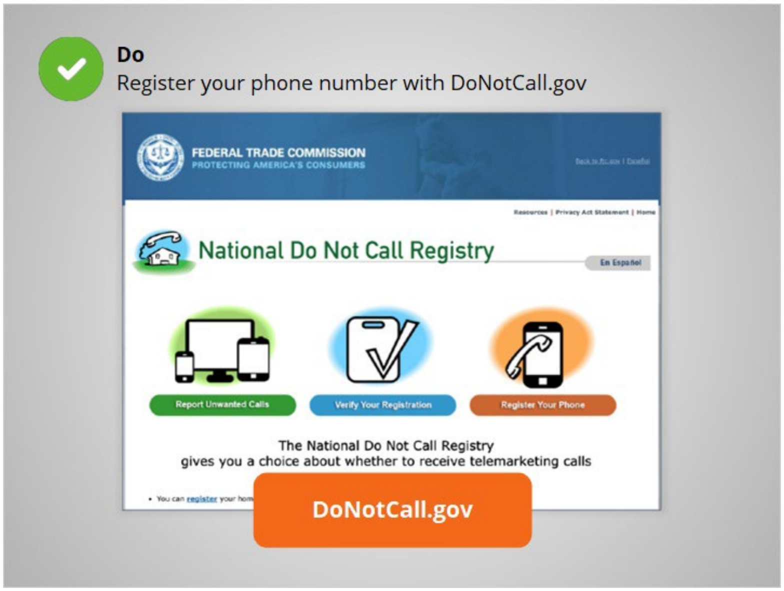
Only click on links to websites that begin with HTTPS.



Do

Discuss with a trusted person

If you are unsure about the request you receive in a text, email, phone call, or online, talk to someone you trust, like a friend or family member. Scammers are trying to get you to act quickly – don't let them rush you into making a quick decision.



Do

Register your phone number with DoNotCall.gov

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

National Do Not Call Registry

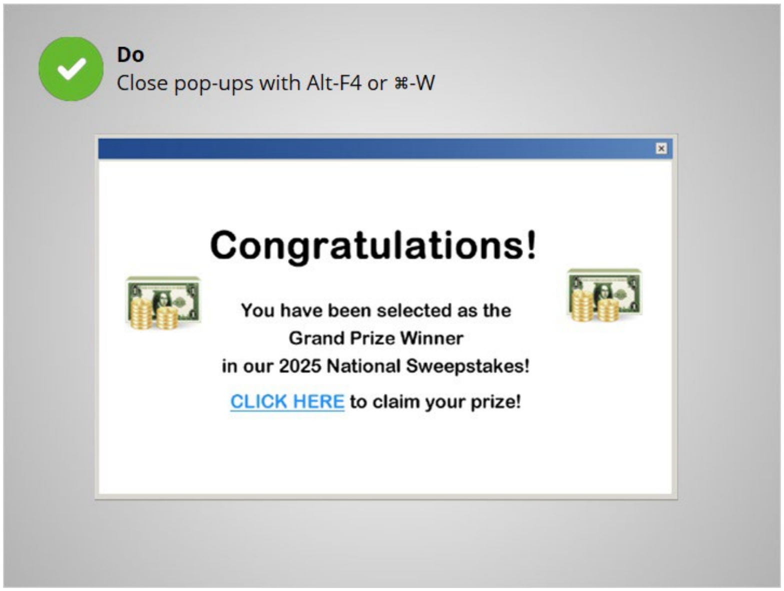
The National Do Not Call Registry
gives you a choice about whether to receive telemarketing calls

- You can register your hom

DoNotCall.gov

Register your phone number with the National Do Not Call Registry and request that telemarketers not call you.

None of the other companies whose names or logos appear in these educational materials have been involved in the creation of these materials, or approve, sponsor, or are affiliated in any way with these materials.



Do

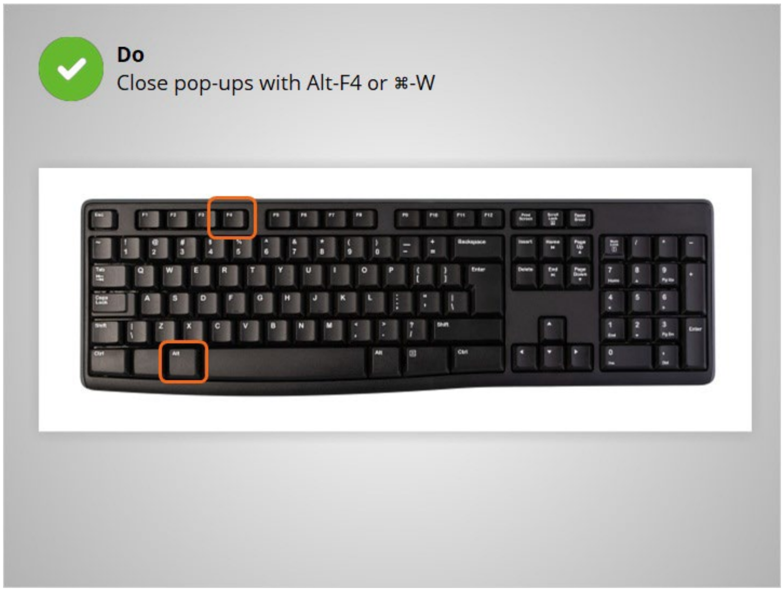
Close pop-ups with Alt-F4 or ⌘-W

Congratulations!

You have been selected as the Grand Prize Winner in our 2025 National Sweepstakes!

CLICK HERE to claim your prize!

For pop-ups on a website, don't click on any buttons. Sometimes even the X will not close a scam pop-up window and may trigger more pop-ups to open instead.

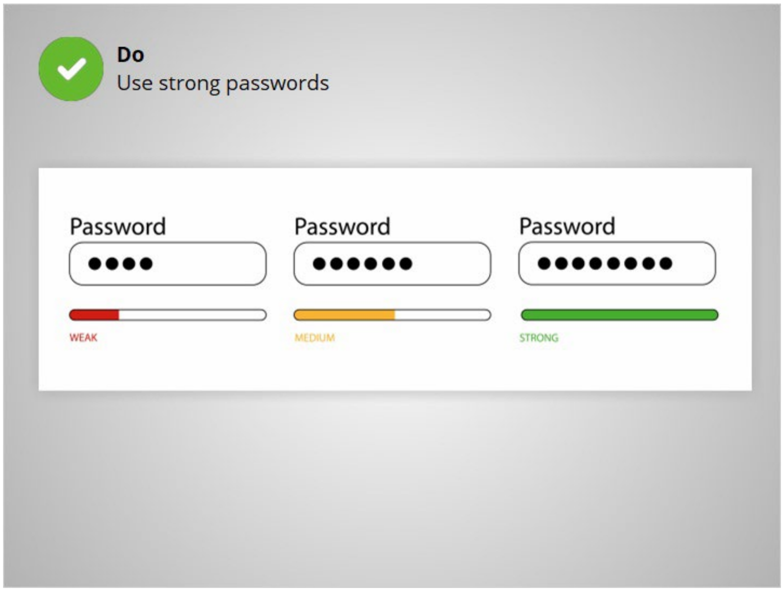


Do

Close pop-ups with Alt-F4 or ⌘-W

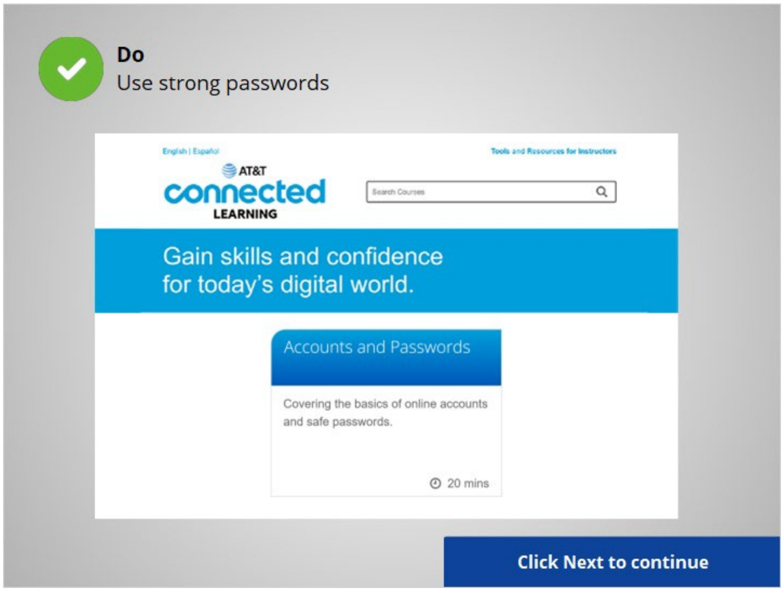
Do try using another method to close the pop-up window. One way to close it is to hold down the Alt key while you press F4 on a PC and Command-W on a Mac. This will close the window. If all else fails, restart your computer, or turn it off and back on again. This is better than being stuck inside a scam.

None of the other companies whose names or logos appear in these educational materials have been involved in the creation of these materials, or approve, sponsor, or are affiliated in any way with these materials.



Do
Use strong passwords

Make sure you use strong passwords that combine upper and lowercase letters, numbers, and special characters. You can also make it stronger by creating a longer password.



Do
Use strong passwords

Gain skills and confidence for today's digital world.

Accounts and Passwords

Covering the basics of online accounts and safe passwords.

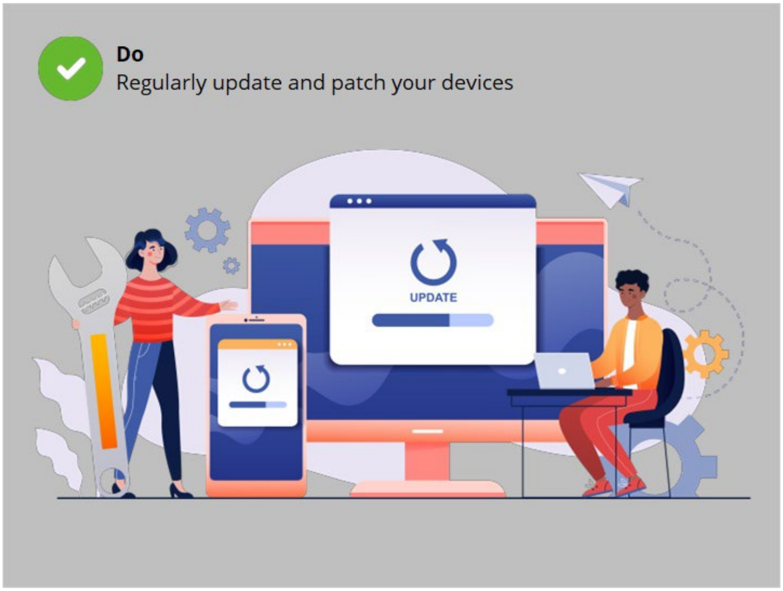
20 mins

Click Next to continue

You can learn more about creating secure passwords and how to keep your online accounts secure by watching the course Accounts and Passwords. To open this course, click on the course title.

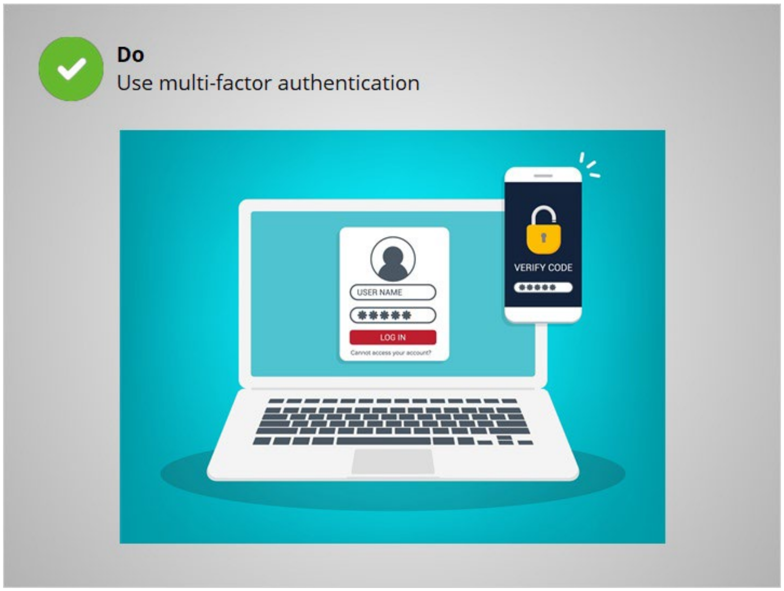
Click Next to continue.

None of the other companies whose names or logos appear in these educational materials have been involved in the creation of these materials, or approve, sponsor, or are affiliated in any way with these materials.



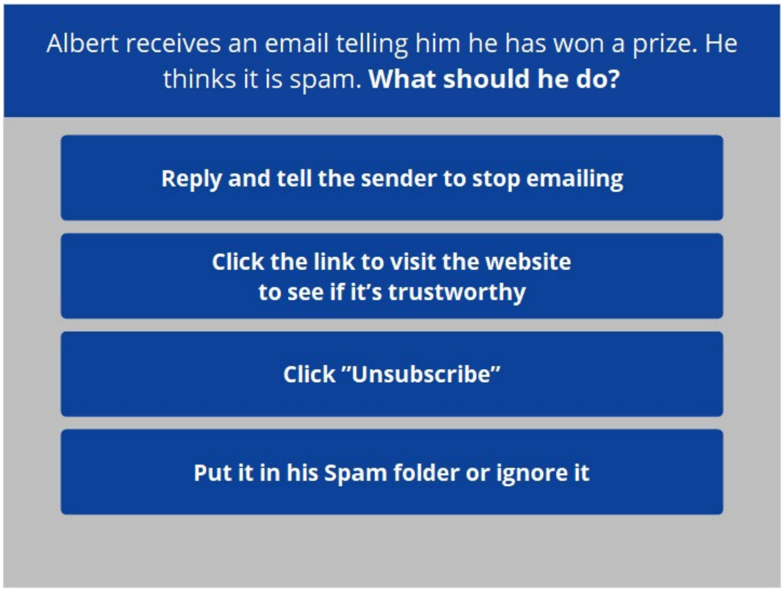
Do
Regularly update and patch your devices

Make sure your device’s operating system and applications are up to date to ensure you have the latest security updates installed.



Do
Use multi-factor authentication

Do use multi-factor authentication, which uses two methods to verify access to your account. It usually includes entering a username and password and one other method, which could be a code sent to your email or phone or your fingerprint. Multi-factor authentication is not always available but is quickly becoming an option on websites and apps. Now let’s check to see what you remember.



Albert receives an email telling him he has won a prize. He thinks it is spam. **What should he do?**

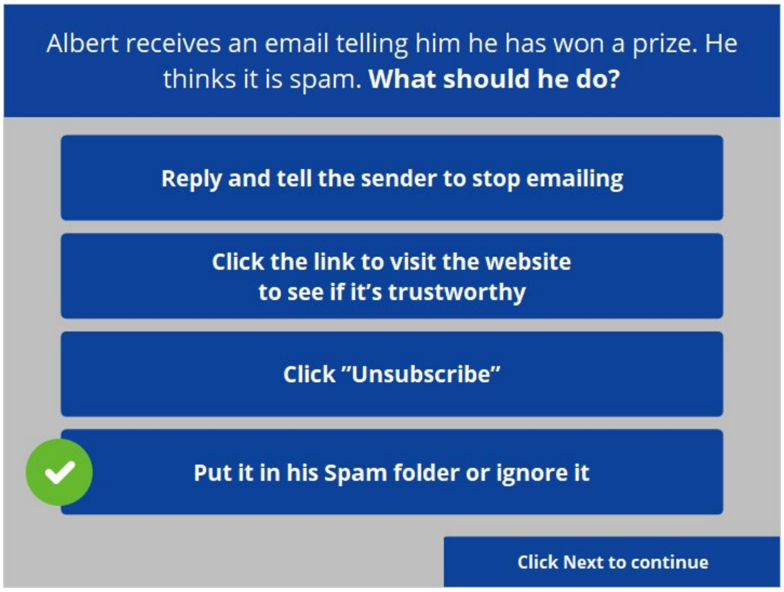
Reply and tell the sender to stop emailing

Click the link to visit the website to see if it's trustworthy

Click "Unsubscribe"

Put it in his Spam folder or ignore it

Albert receives an email telling him he's won a prize. He thinks it's probably spam. How should Albert react to this scam email? Click the correct answer.



Albert receives an email telling him he has won a prize. He thinks it is spam. **What should he do?**

Reply and tell the sender to stop emailing

Click the link to visit the website to see if it's trustworthy

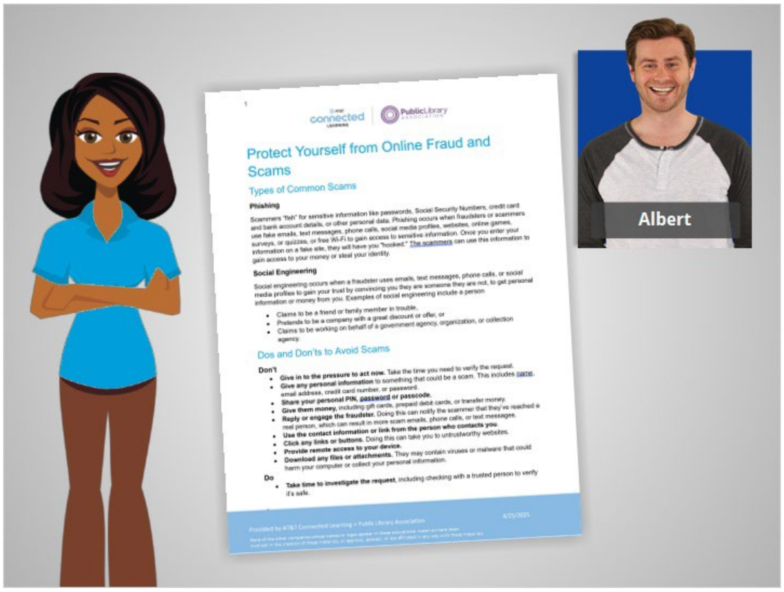
Click "Unsubscribe"

✓ Put it in his Spam folder or ignore it

Click Next to continue

That is correct!

Click Next to continue.



1

Protect Yourself from Online Fraud and Scams

Types of Common Scams

Phishing

Scammers "fish" for sensitive information like passwords, Social Security Numbers, credit card and bank account details, or other personal data. Phishing occurs when fraudsters or scammers use fake emails, text messages, phone calls, social media profiles, websites, online games, surveys, or quizzes, or free Wi-Fi to gain access to sensitive information. Once you enter your information on a fake site, they will have you "hooked." The scammers can use this information to gain access to your money or steal your identity.

Social Engineering

Social engineering occurs when a fraudster uses emails, text messages, phone calls, or social media profiles to gain your trust by convincing you they are someone they are not, to get personal information or money from you. Examples of social engineering include a person

- Claims to be a friend or family member in trouble,
- Pretends to be a company with a great discount or offer, or
- Claims to be working on behalf of a government agency, organization, or collection agency.

Dos and Don'ts to Avoid Scams

Don't

- **Give in to the pressure to act now.** Take the time you need to verify the request.
- **Give any personal information** to something that could be a scam. This includes name, email address, credit card number, or password.
- **Share your personal PIN, password or passcode.**
- **Give them money,** including gift cards, prepaid debit cards, or transfer money.
- **Reply or engage the fraudster.** Doing this can notify the scammer that they've reached a real person, which can result in more scam emails, phone calls, or text messages.
- **Use the contact information or link from the person who contacts you.**
- **Click any links or buttons.** Doing this can take you to untrustworthy websites.
- **Provide remote access to your device.**
- **Download any files or attachments.** They may contain viruses or malware that could harm your computer or collect your personal information.

Do

- **Take time to investigate the request,** including checking with a trusted person to verify it's safe.

Provided by AT&T Connected Learning + Public Library Association 4/25/2025

[illegible]

Albert knows what he should and should not do and when he encounters a scam on a website, in an email, or a text message. When Albert follows these tips, he can stay safe whenever he encounters a scam. If you would like to review these tips please see the handout in the Additional Resources section.

In the next lesson, Albert will learn when and how to report scams.

Activity 4: Reporting Scams

In the previous lesson, Albert learned what he should and should not do when encountering a scam. However, even if you remain vigilant, you may still fall for a scam.

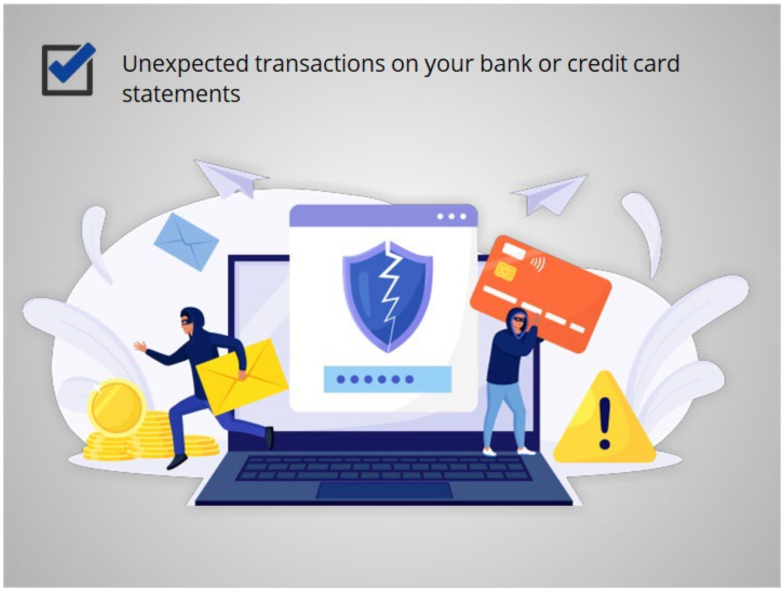
How to identify if you have been scammed

How to report scams

SCAM
Report

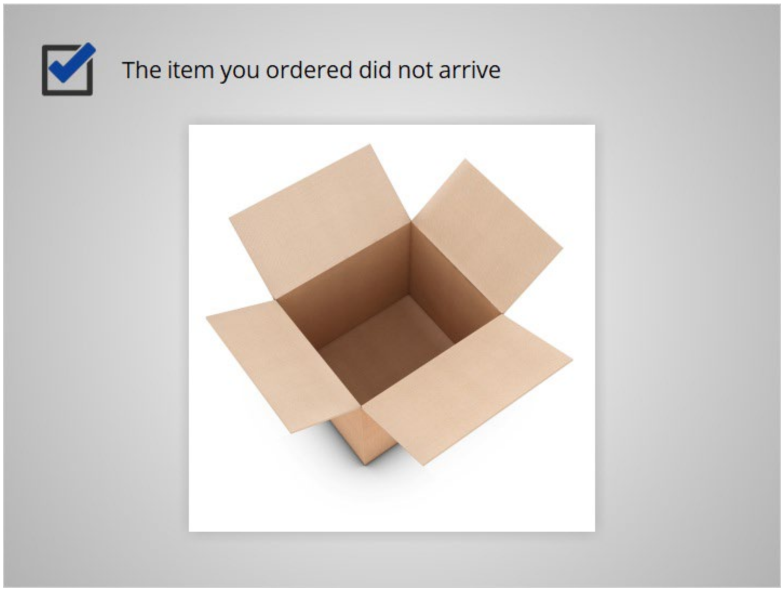
In this lesson, Albert will learn how to identify if he has been scammed and how to report scams.

Here are some examples to help you identify if you’ve been scammed.



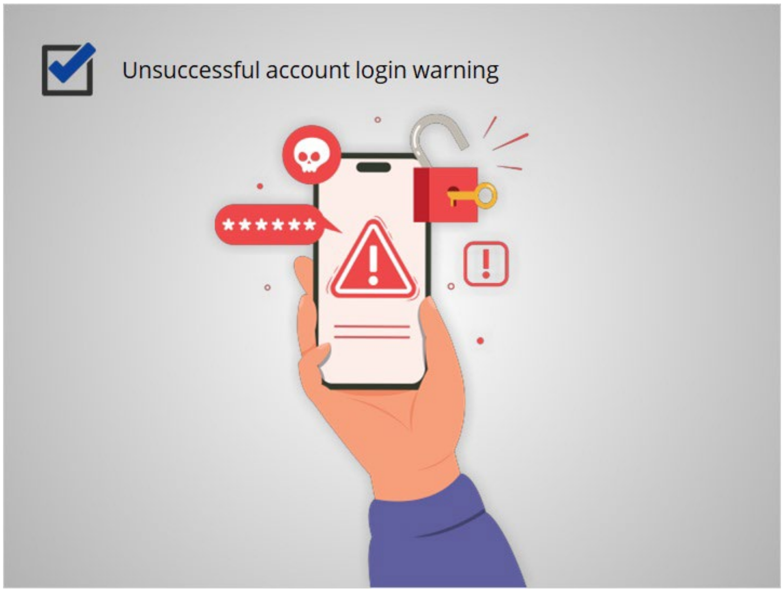
☑ Unexpected transactions on your bank or credit card statements

You see transactions that you did not make on your bank statement or credit report.



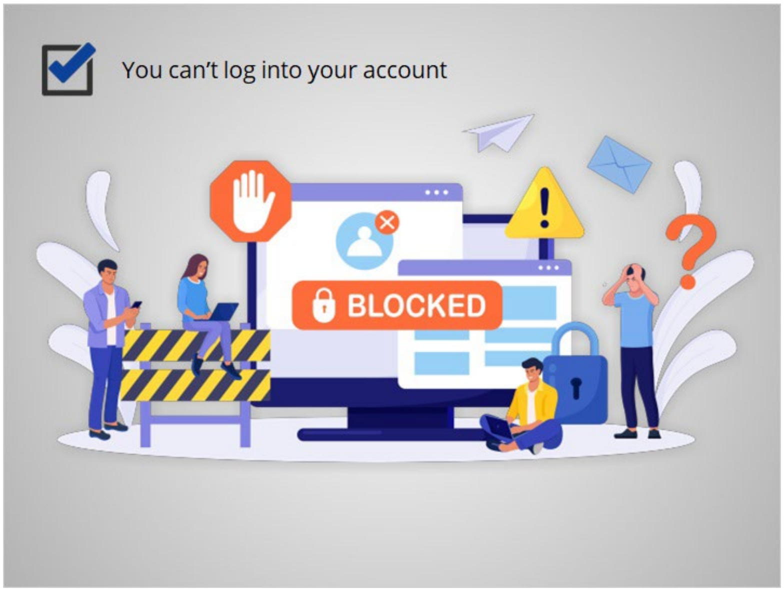
☑ The item you ordered did not arrive

You purchased an item but it did not arrive. When you try to report the issue to the seller, you do not get a response.



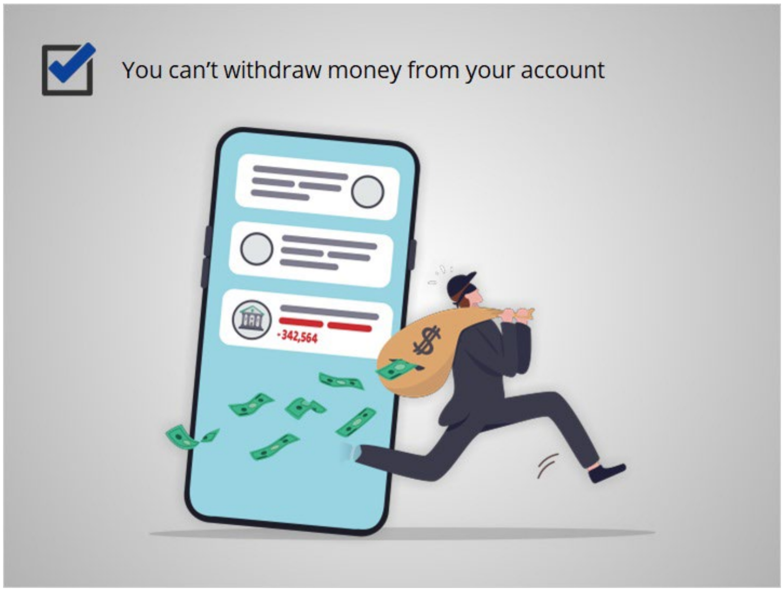
☑ Unsuccessful account login warning

You receive an email that there have been an unusual number of unsuccessful sign-in attempts for one of your accounts, but you have not tried to log in. This could mean someone is trying to access your account.



☑ You can't log into your account

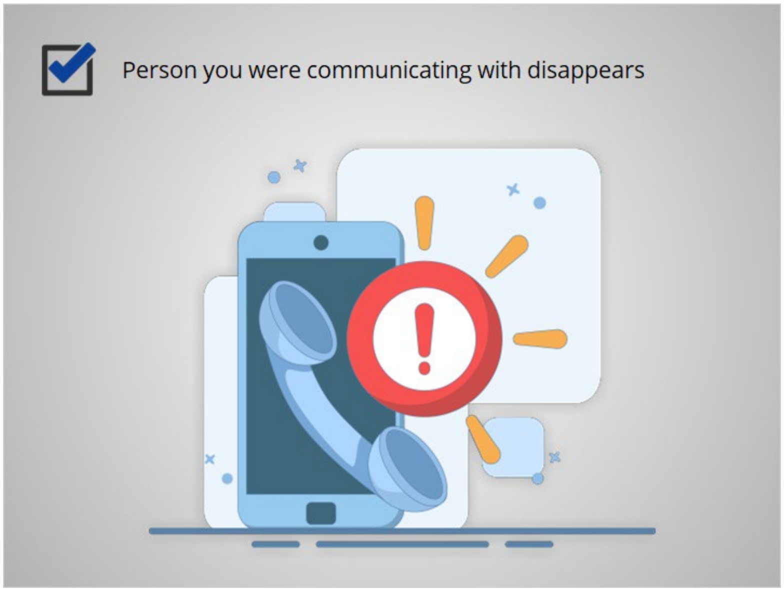
You can no longer log into your account and are unable to reset the password; someone may have taken over your account.



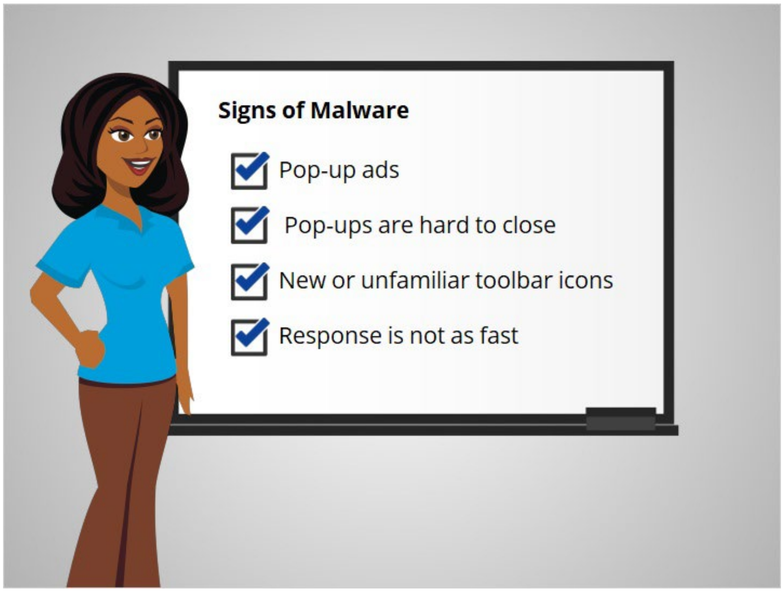
☑ You can't withdraw money from your account

You can't withdraw money from your account and when you log into your bank account, the balance is zero, or it has been closed.

None of the other companies whose names or logos appear in these educational materials have been involved in the creation of these materials, or approve, sponsor, or are affiliated in any way with these materials.


☑ Person you were communicating with disappears

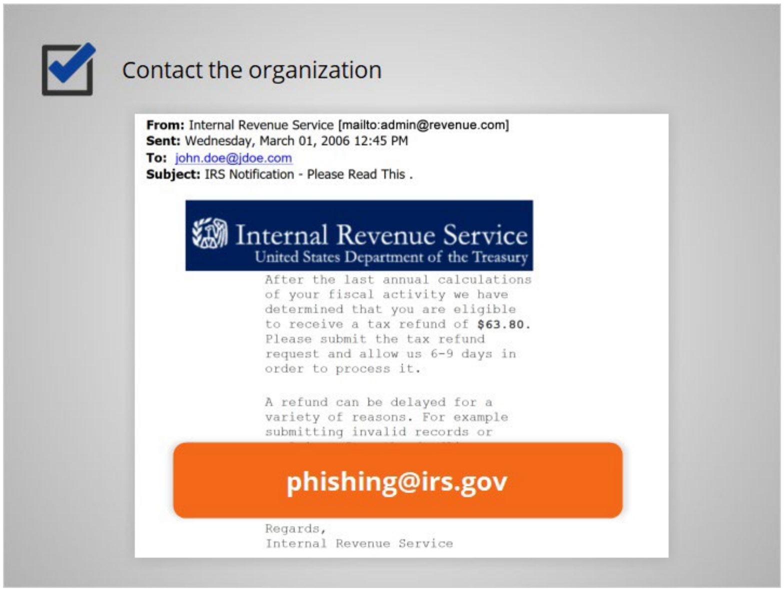
Sometimes, a person may just disappear. You reach out to them via email, text, or social media, but they no longer respond, or you can't locate their online profiles anymore.


Signs of Malware

☑ Pop-up ads
☑ Pop-ups are hard to close
☑ New or unfamiliar toolbar icons
☑ Response is not as fast

You encounter one or more of these signs: Pop-up ads appear and they are hard to close; new or unfamiliar toolbar icons appear on the screen; or your computer or mobile device is not responding as fast as it used to. Your device may be infected with malware.

Online scams can originate from anywhere in the world. This makes it very difficult or even impossible to track down the fraudsters that are behind them. However, there are a few actions you can take if you identify or fall victim to a scam.



Contact the organization

From: Internal Revenue Service [mailto:admin@revenue.com]
Sent: Wednesday, March 01, 2006 12:45 PM
To: john.doe@jdoe.com
Subject: IRS Notification - Please Read This .

Internal Revenue Service
United States Department of the Treasury

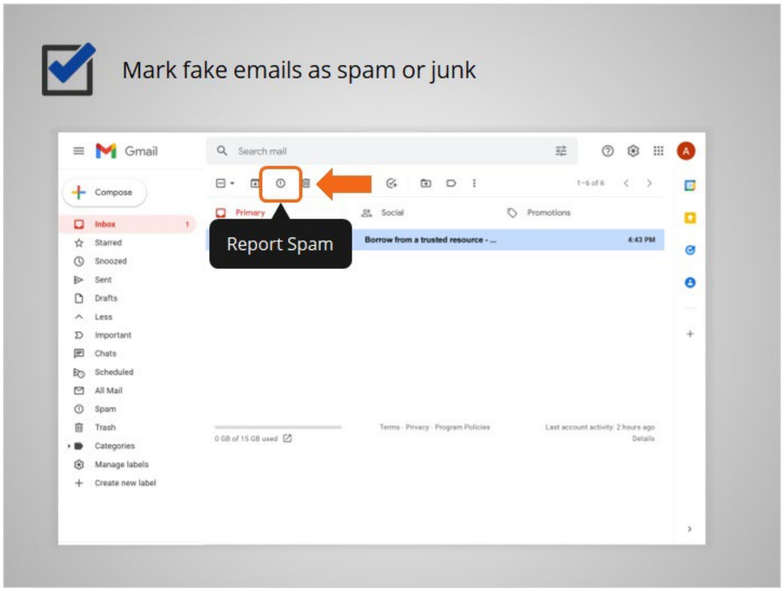
After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of **$63.80.** Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or

phishing@irs.gov

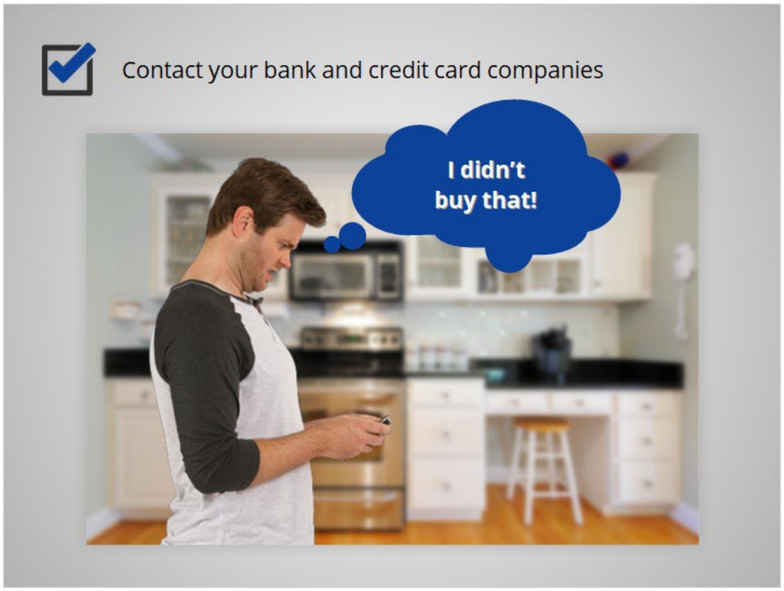
Regards,
Internal Revenue Service

If you encounter a phishing scam imitating an organization you know, you can contact that organization. But remember not to use the contact information in the suspicious email. Look up their information from a different source. For example, Albert received this suspicious email claiming to be from the IRS. With his research, Albert finds that the IRS has a process for reporting these types of scams so Albert forwards it to phishing@irs.gov.



Mark fake emails as spam or junk

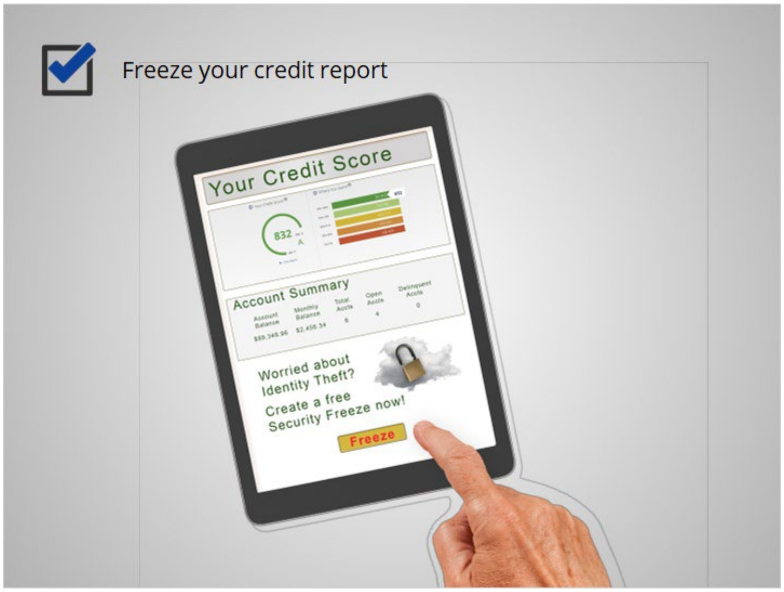
When Albert receives a fake email, he puts the message in his spam or junk folder. In this example, Albert is using Gmail. This helps email providers identify and prevent scams.



Contact your bank and credit card companies

Albert noticed some transactions on his bank account statement that he did not make, so he contacted his bank immediately to report the problem!

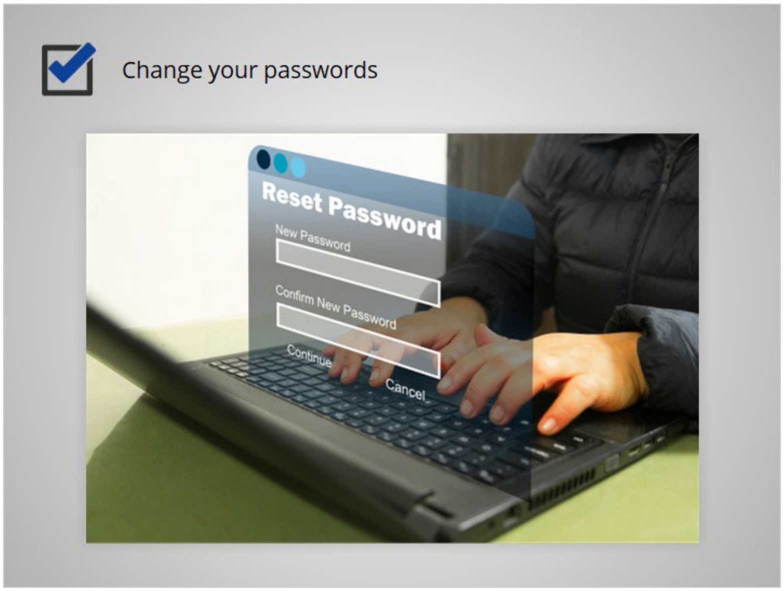
None of the other companies whose names or logos appear in these educational materials have been involved in the creation of these materials, or approve, sponsor, or are affiliated in any way with these materials.



☑ Freeze your credit report

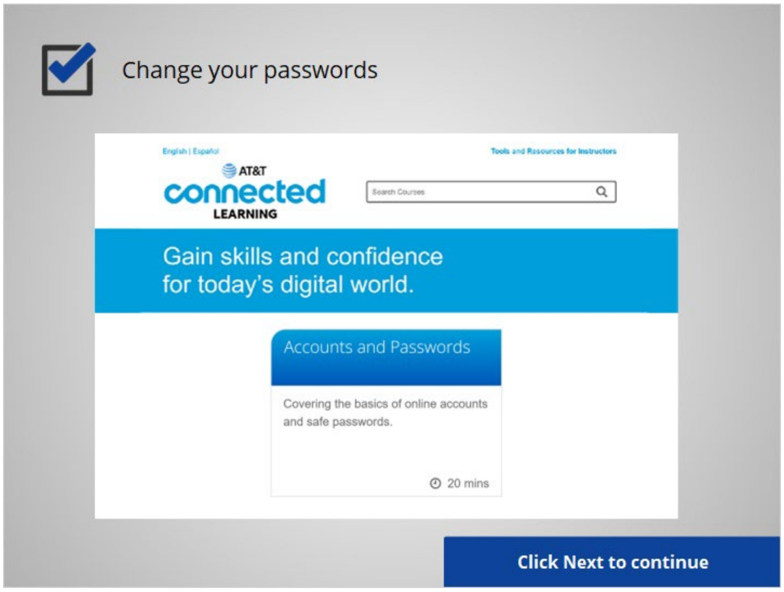
Your Credit Score
832
Account Summary
Worried about Identity Theft?
Create a free Security Freeze now!
Freeze

If you are a victim of identity theft, a data breach or want to be extra cautious, you can freeze your credit report to prevent someone else from applying for credit cards or loans under your name.



☑ Change your passwords

When Albert received an email that someone was trying to access his account, he logged in and changed his password immediately. If you give your password to a scammer or you think someone may have access to your password through a data breach, unsecured internet hotspot, malware, or phishing attempt, change your password.



☑ Change your passwords

Gain skills and confidence for today's digital world.

Accounts and Passwords

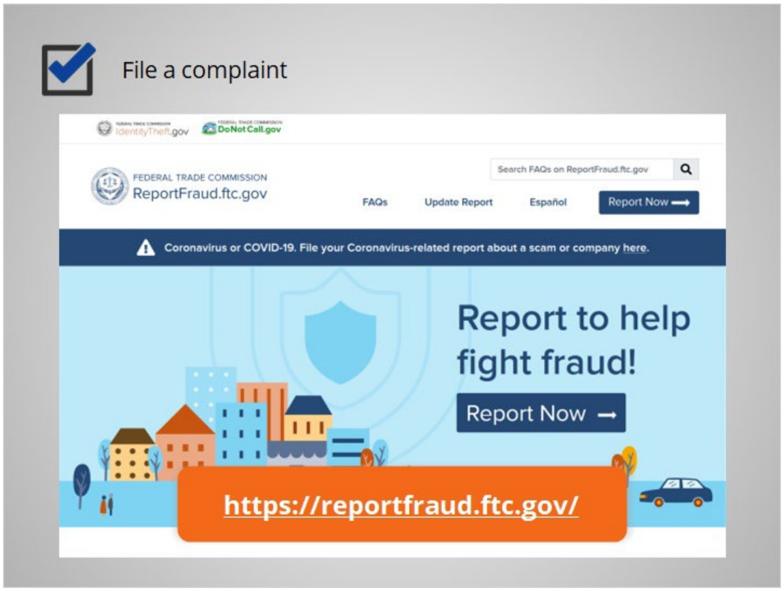
Covering the basics of online accounts and safe passwords.

20 mins

Click Next to continue

Watch the course Accounts and Passwords to learn more about creating strong passwords and keeping your online accounts secure.

To open this course, click on the course title. Click Next to continue.



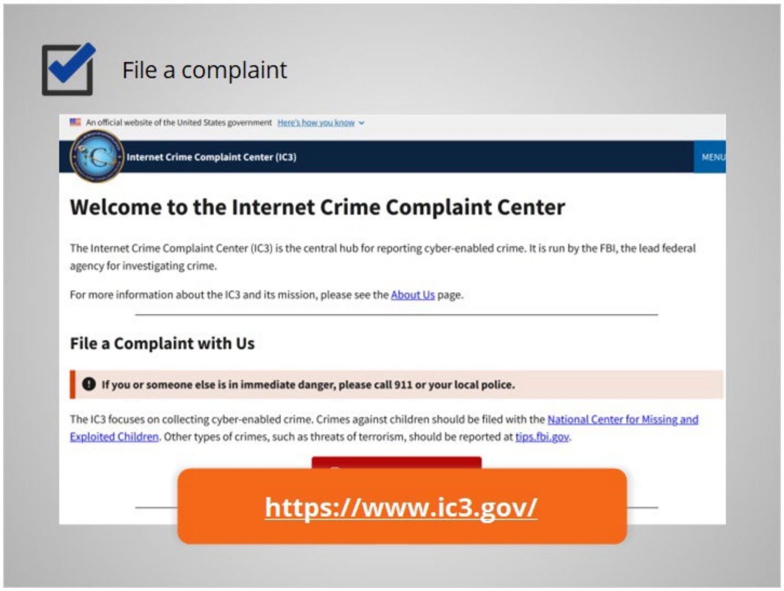
☑ File a complaint

Coronavirus or COVID-19. File your Coronavirus-related report about a scam or company here.

Report to help fight fraud!

https://reportfraud.ftc.gov/

If you have been scammed there are multiple ways to report an incident. You can file official complaints with the Federal Trade Commission by visiting their website at reportfraud.ftc.gov,



File a complaint

An official website of the United States government Here's how you know
Internet Crime Complaint Center (IC3)
MENU

Welcome to the Internet Crime Complaint Center

The Internet Crime Complaint Center (IC3) is the central hub for reporting cyber-enabled crime. It is run by the FBI, the lead federal agency for investigating crime.

For more information about the IC3 and its mission, please see the About Us page.

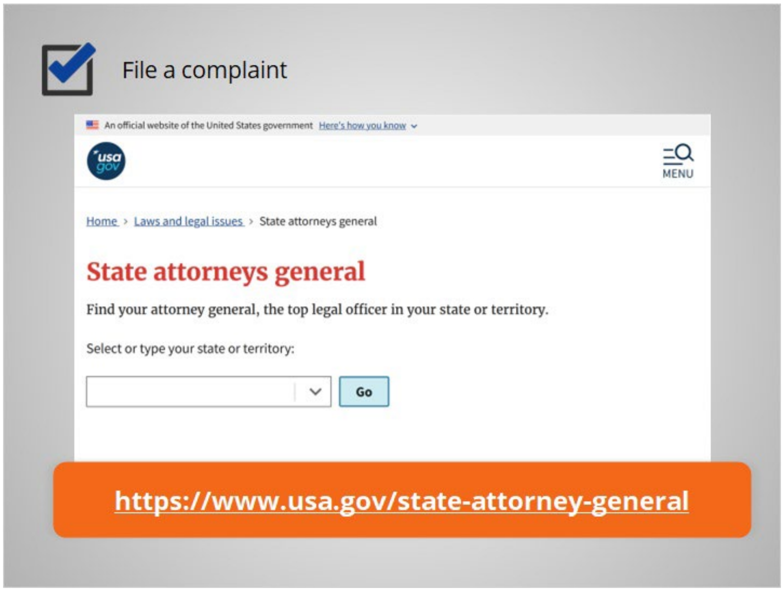
File a Complaint with Us

If you or someone else is in immediate danger, please call 911 or your local police.

The IC3 focuses on collecting cyber-enabled crime. Crimes against children should be filed with the National Center for Missing and Exploited Children. Other types of crimes, such as threats of terrorism, should be reported at tips.fbi.gov.

https://www.ic3.gov/

or the Federal Bureau of Investigation's Internet Crime Complaint Center at www.ic3.gov,



File a complaint

An official website of the United States government Here's how you know
usa gov
MENU
Home > Laws and legal issues > State attorneys general

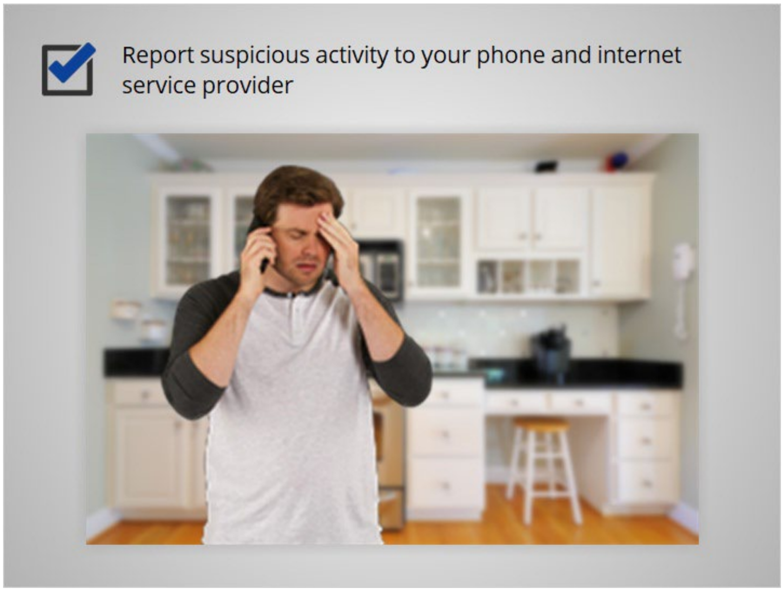
State attorneys general

Find your attorney general, the top legal officer in your state or territory.

Select or type your state or territory:

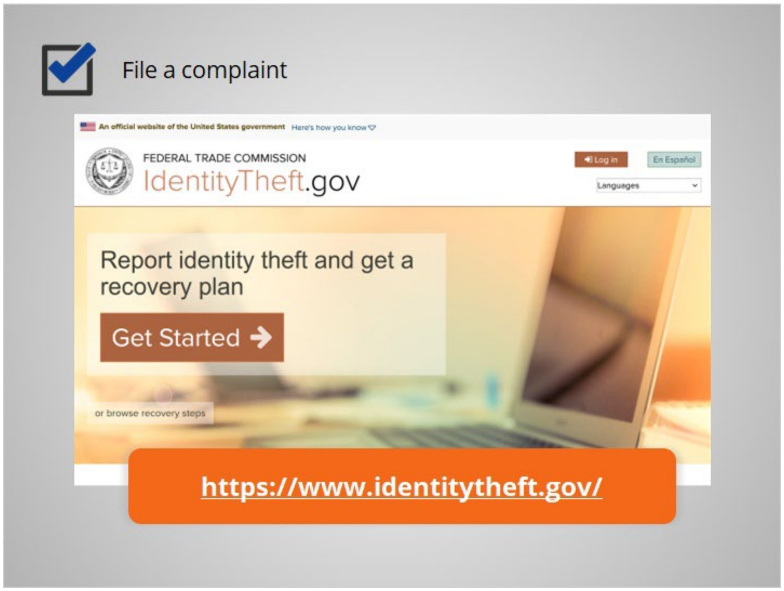
https://www.usa.gov/state-attorney-general

or your state’s attorney general. You can find your state’s attorney general contact information at usa.gov/state-attorney-general.



☑ Report suspicious activity to your phone and internet service provider

For suspicious phone calls, texts or online scams, you can make a report with your telephone company or internet service provider.



☑ File a complaint

An official website of the United States government Here's how you know

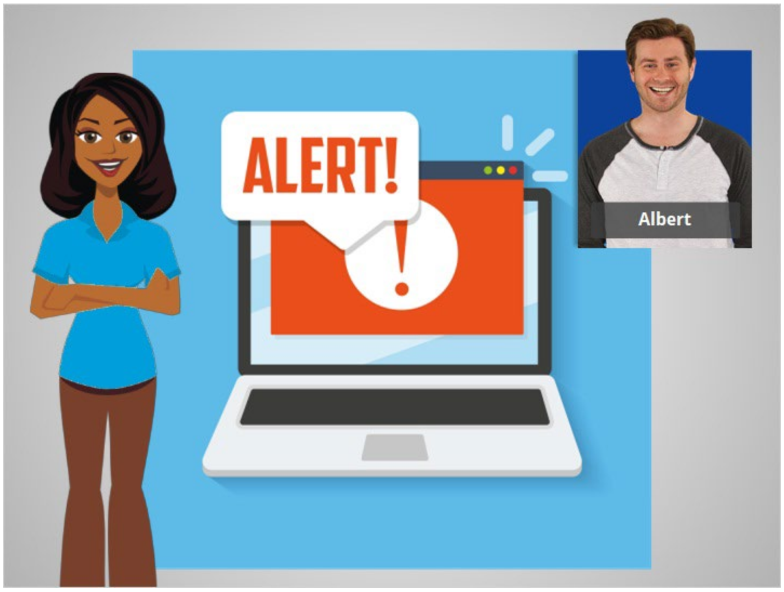
FEDERAL TRADE COMMISSION
IdentityTheft.gov

Report identity theft and get a recovery plan

https://www.identitytheft.gov/

If your identity was stolen, you suspect someone may have stolen your identity, or your information was exposed in a data breach, check the IdentifyTheft.gov website to explore your options, report the theft, and create a recovery plan.

None of the other companies whose names or logos appear in these educational materials have been involved in the creation of these materials, or approve, sponsor, or are affiliated in any way with these materials.



In this course, we learned along with Albert about what types of scams are out there, how to recognize the warning signs, how to respond when you see a scam, and how to report a scam.

Remember the warning signs you've learned in this course in order to protect yourself and your devices from online fraud and scams.