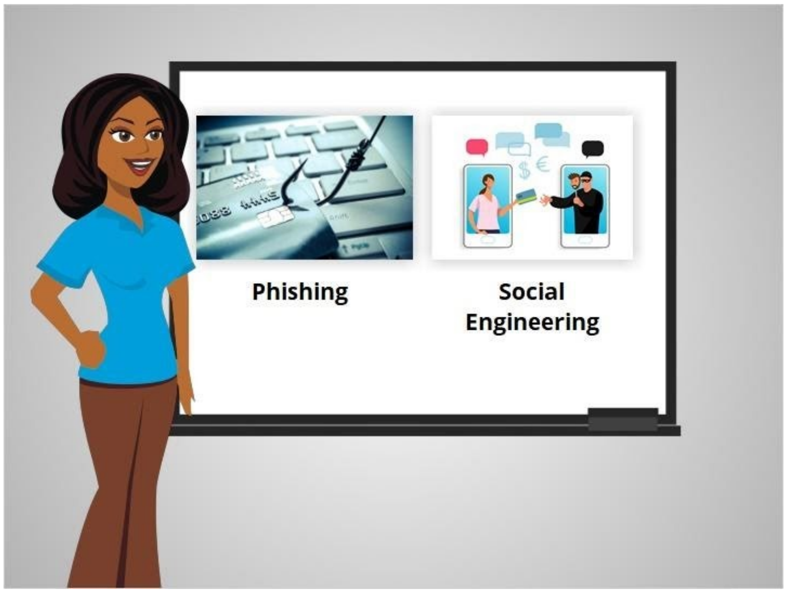
Online Fraud and Scams

Types of Scams

1 Types of scams
2 Recognize warning signs
3 How to respond
4 How to report a scam

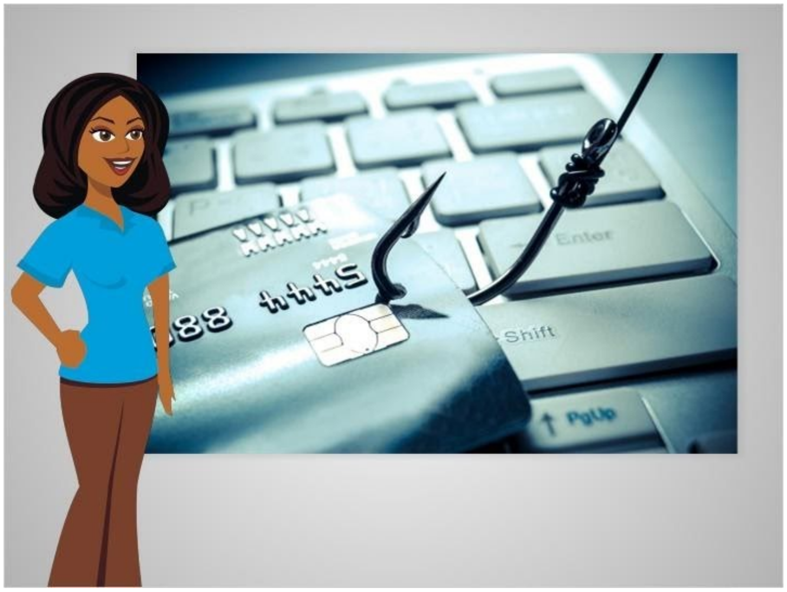
Hi, I'm Belle. There are many things you can do to protect yourself from fraud and keep your accounts and devices safe from online scams. We'll follow along with Albert to learn what types of scams are out there, how to recognize the warning signs, how to respond when you see a scam, and how to report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

Online scams can come in many shapes and 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 or text message, or even in a pop-up window on your computer.



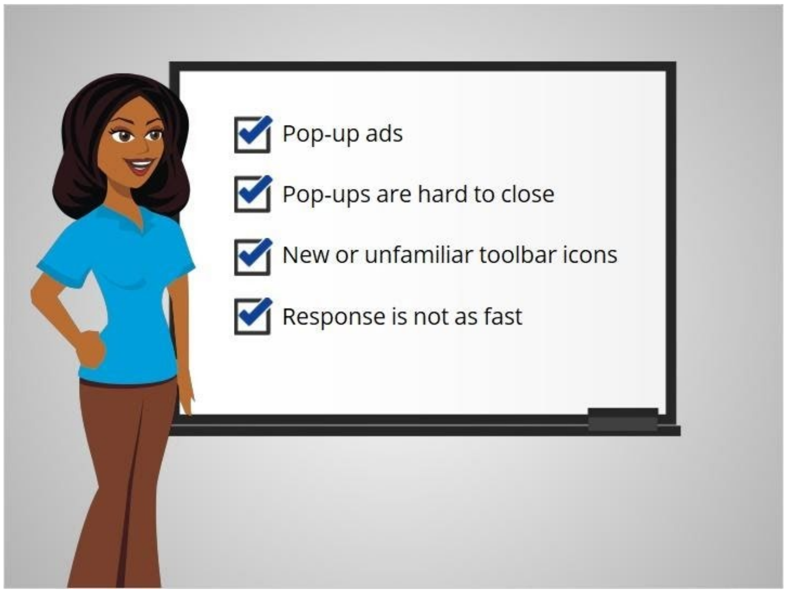
Let’s begin by talking about phishing, which is a common type of scam. Phishing is when scammers use fake emails or text messages to “fish” for information.

Fake Email or Phishing Scams:

- Lead you to fake websites
- Try to win your trust
- Claim to be from a real organization
- Ask for your information

These fake messages can look real, but link to fake websites. The website may look like a trusted, well-known company, organization or government agency, but it's all a trick to get your information – such as your Social Security number or bank number and credit card account numbers.

A fake email can also be used to infect your computer with malicious software, referred to as malware, or a virus as soon as you open the email. Malware is a tool used by scammers that can take many different shapes. For example, malware can lead to viruses that infect your computer or “spyware” that tracks your online activities.



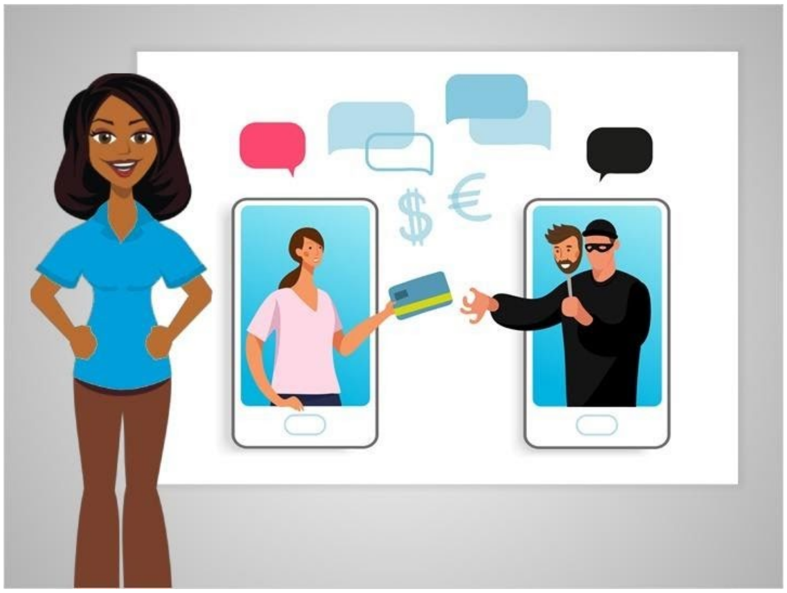
☑ Pop-up ads

☑ Pop-ups are hard to close

☑ New or unfamiliar toolbar icons

☑ Response is not as fast

You may be able to tell when malware has been installed on your computer or device if you see 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.



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, in order to get personal information from you.

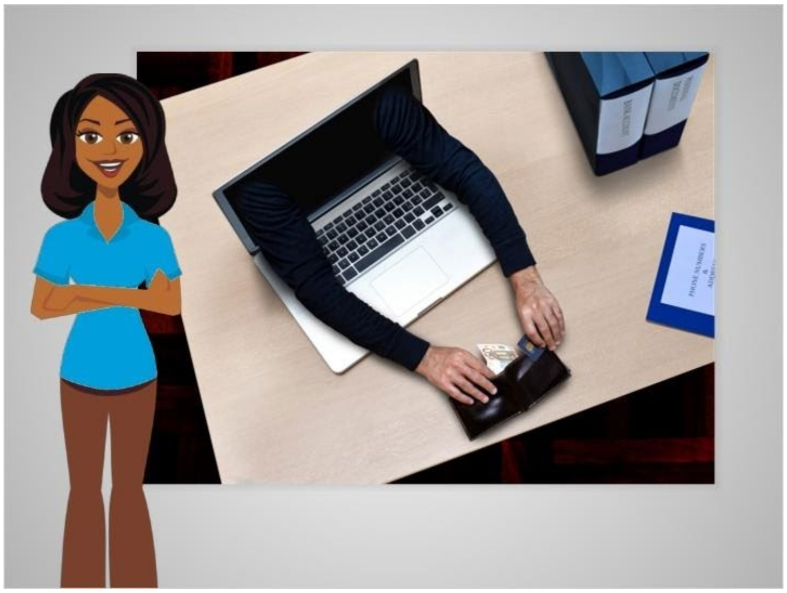
☑ Claim to be family or friend in trouble

☑ Pretend to be company with great offer

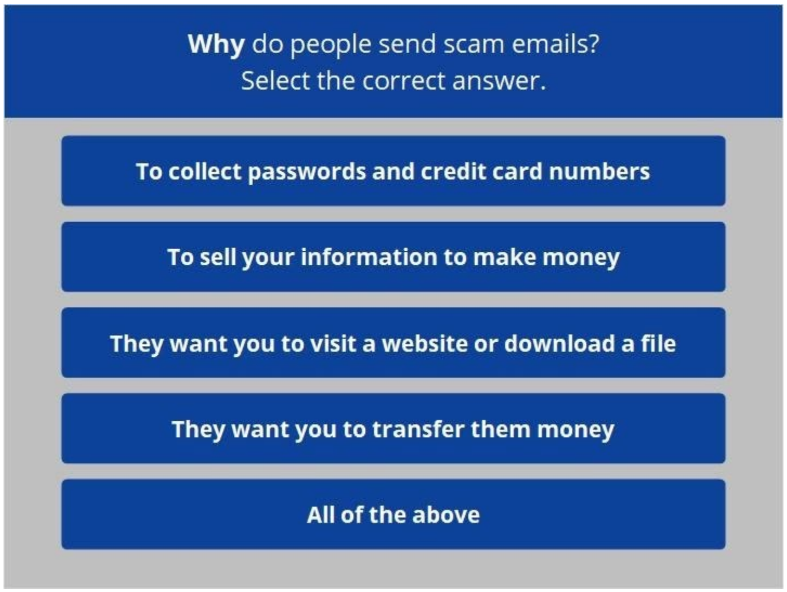
☑ Claim to be working on behalf of government, organization, collections

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.



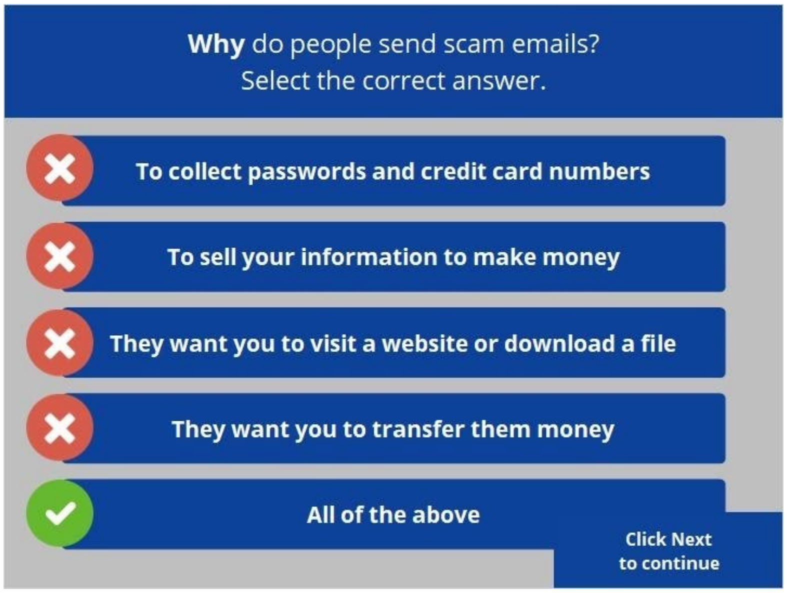
No matter what form a scam takes, fraudsters usually have the same goals: to steal your money or collect information like your passwords or credit card numbers. Scams can also cause problems for your computer by infecting it with viruses or malware.



Why do people send scam emails?
Select the correct answer.

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

Let’s see what you remember about scam emails. Why do people send scam emails? Select the correct answer.



Why do people send scam emails?
Select the correct answer.

☒ To collect passwords and credit card numbers

☒ To sell your information to make money

☒ They want you to visit a website or download a file

☒ They want you to transfer them money

✓ All of the above

The correct answer is all of the above. Scam emails are sent for a variety of reasons. Knowing what to look out for can help you protect yourself from fraud and keep your accounts and devices safe from online scams. Click Next to continue.

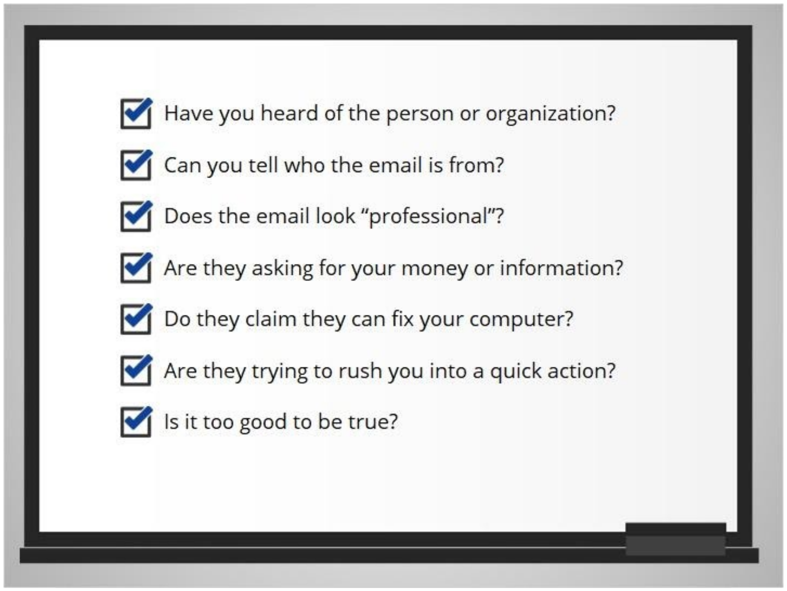
In this lesson, Albert learned about common types of frauds and scams including phishing and social engineering. He learned that he may encounter these scams while searching a website, in an email or text message, or even in a pop-up window on his computer. In the next lesson, Albert will learn a few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

Click on the blue button to end this lesson.

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 his text messages.



☑ Have you heard of the person or organization?

☑ Can you tell who the email is from?

☑ Does the email look “professional”?

☑ Are they asking for your money or information?

☑ Do they claim they can fix your computer?

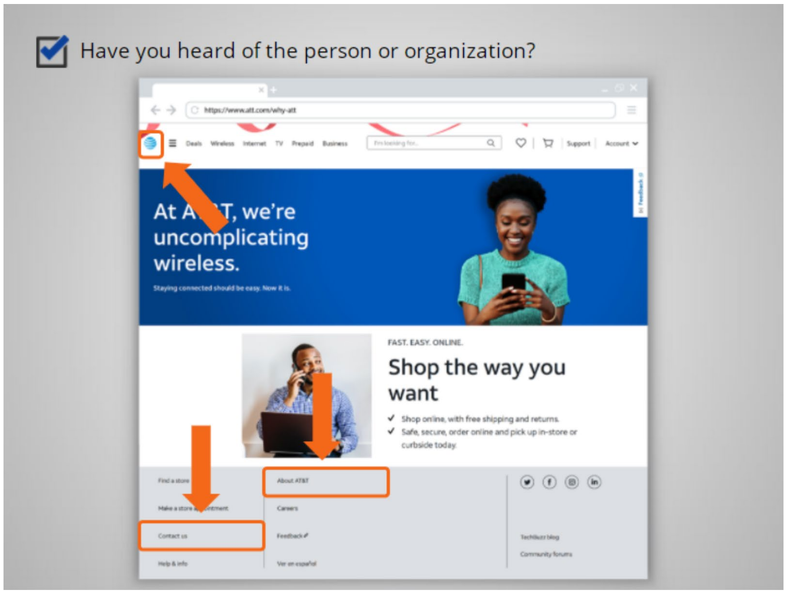
☑ Are they trying to rush you into a quick action?

☑ Is it too good to be true?

Here are some questions to ask yourself if you’re not sure.

- Have you heard of the person or organization?
- Can you tell who the email is from?
- Does the email look professional?
- Are they asking for your money or information?
- Do they claim they can fix your computer?
- Are they trying to rush you into a quick action?
- Is it too good to be true?

We’ll look at them one by one.



☑ Have you heard of the person or organization?

At A T, we're uncomplicating wireless.

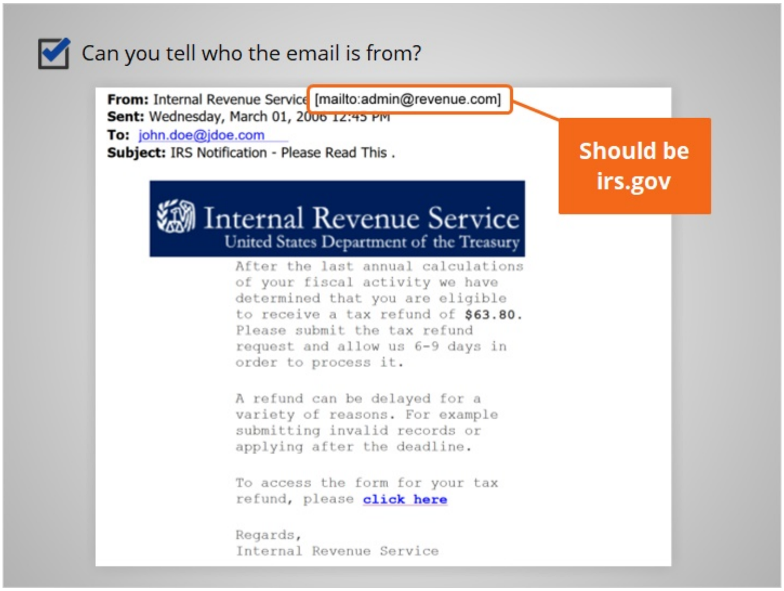
Staying connected should be easy. Now it is.

FAST. EASY. ONLINE.

Shop the way you want

✓ Shop online, with free shipping and returns.
✓ Safe, secure, order online and pick up in-store or curbside today.

Have you heard of the person or organization before? Albert is searching the web for a pharmacy and found this website. In today's lesson, we are using the CVS Pharmacy website to identify key markers of a legitimate corporate 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@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 applying after the deadline.

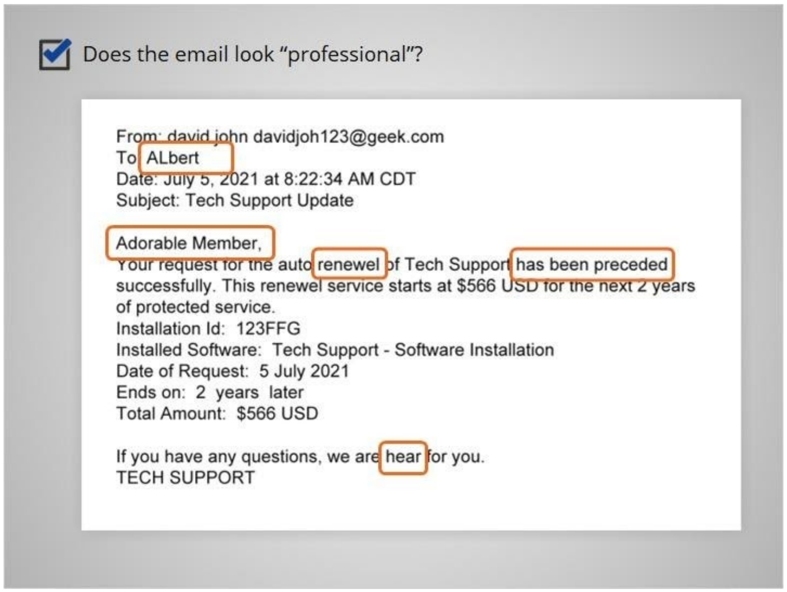
To access the form for your tax refund, please **click here**

Regards,
Internal Revenue Service

Should be irs.gov

Can you tell who the email message is from? Albert received an email that claims to be from the IRS. But the email address ends with an unknown email provider, not irs.gov. This is a sure sign of a phishing 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.



☑ Does the email look “professional”?

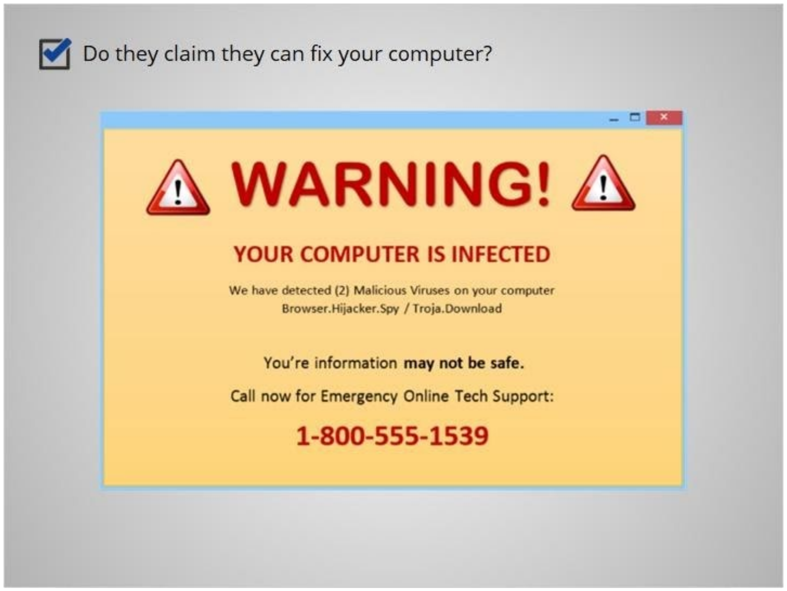
From: david john davidjoh123@geek.com
To ALbert
Date: July 5, 2021 at 8:22:34 AM CDT
Subject: Tech Support Update

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

Does the email look 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 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

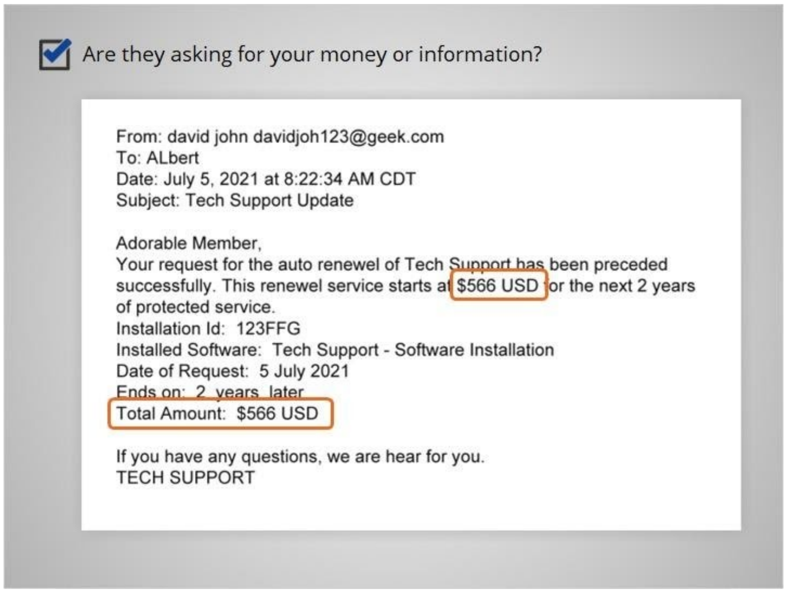
We have detected (2) Malicious Viruses on your computer
Browser.Hijacker.Spy / Troja.Download

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 received a pop-up message. It tells him 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.



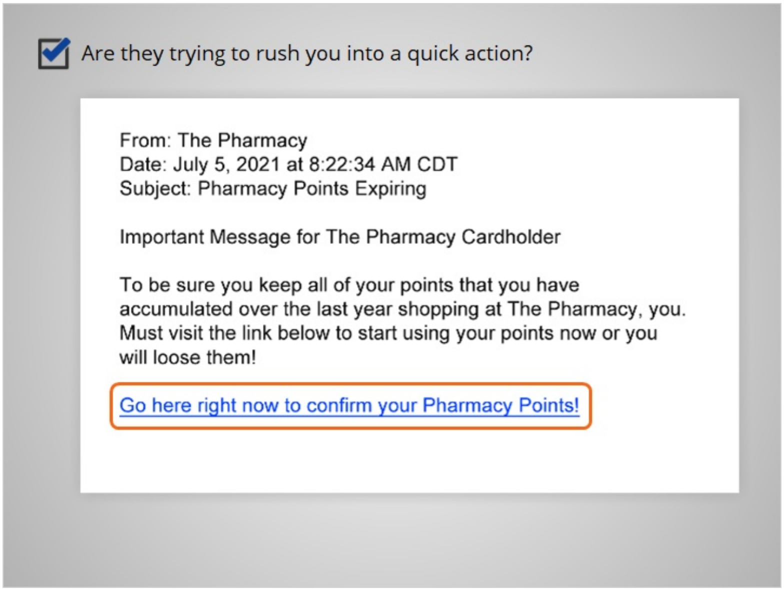
☑ Are they asking for your money or information?

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 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

Are they asking for your 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 loose them!

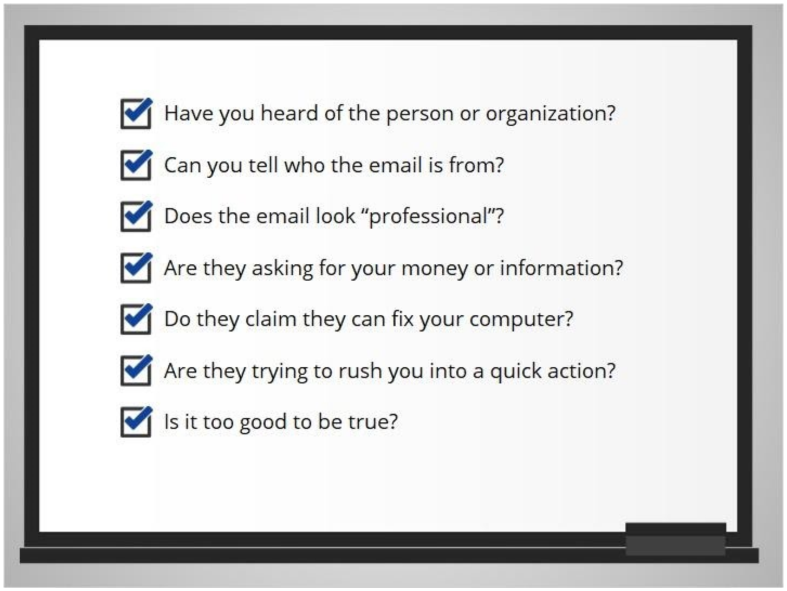
Go here right now to confirm your Pharmacy Points!

Are they trying to rush you into a quick action before taking the 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. Other fraudsters will promise something good, but only if you respond right away.

☑ Is it too good to be true?

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.



☑ Have you heard of the person or organization?

☑ Can you tell who the email is from?

☑ Does the email look “professional”?

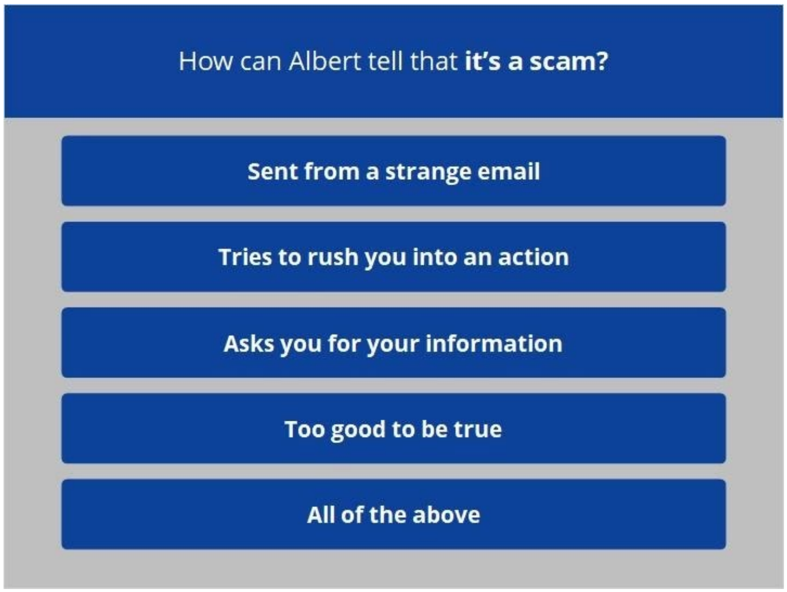
☑ Are they asking for your money or information?

☑ Do they claim they can fix your computer?

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

☑ Is it too good to be true?

Great, we’ve reviewed everything in the list! Let’s see what you remember about recognizing scams.



How can Albert tell that **it’s a scam?**

Sent from a strange email

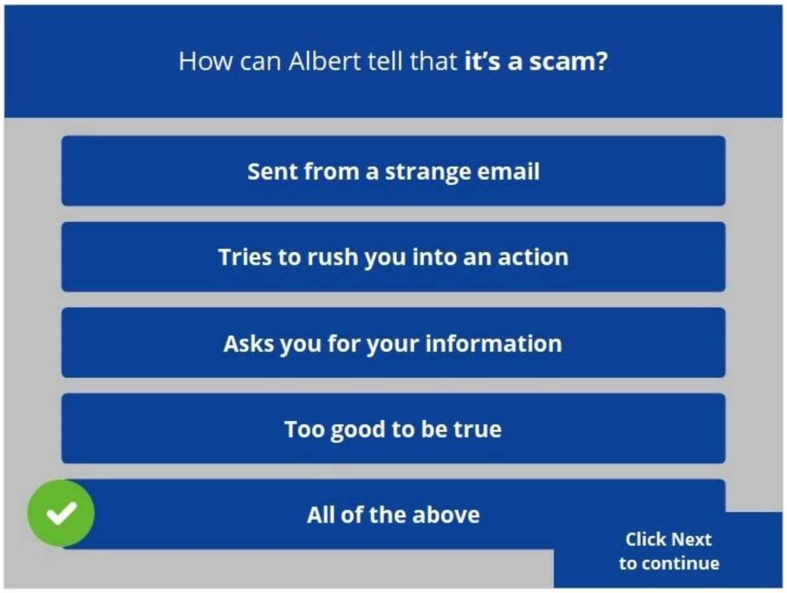
Tries to rush you into an action

Asks you for your information

Too good to be true

All of the above

Albert is looking at an email in his inbox and he is not sure if it’s a scam. How can he tell that it is a scam? Select the correct answer.



How can Albert tell that **it's a scam?**

Sent from a strange email

Tries to rush you into an action

Asks you for your information

Too good to be true

✓ All of the above

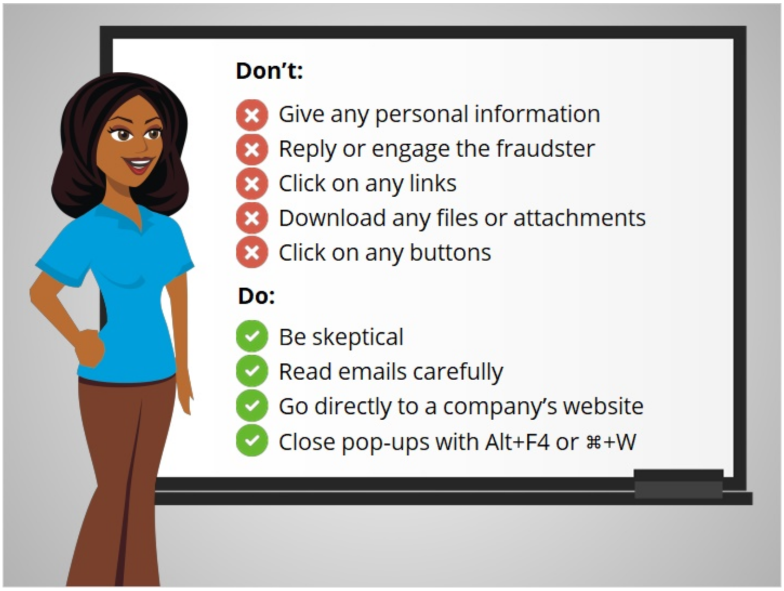
Click Next to continue

The correct answer is all of the above. There are a variety of ways to determine if an email, website or text message 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 online, in his email, on a website and in a text message. In the next lesson, Albert learns what to do with a scam once he has identified it.

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.



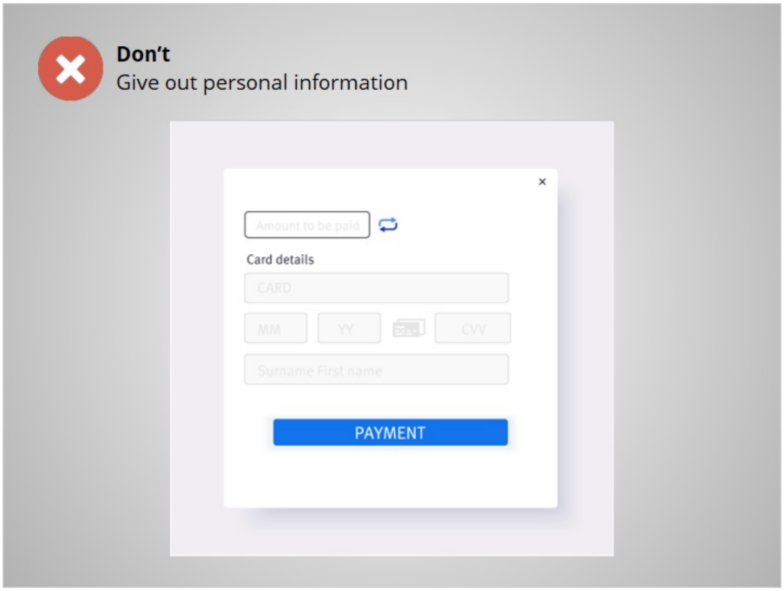
Don't:

- ✗ Give any personal information
- ✗ Reply or engage the fraudster
- ✗ Click on any links
- ✗ Download any files or attachments
- ✗ Click on any buttons

Do:

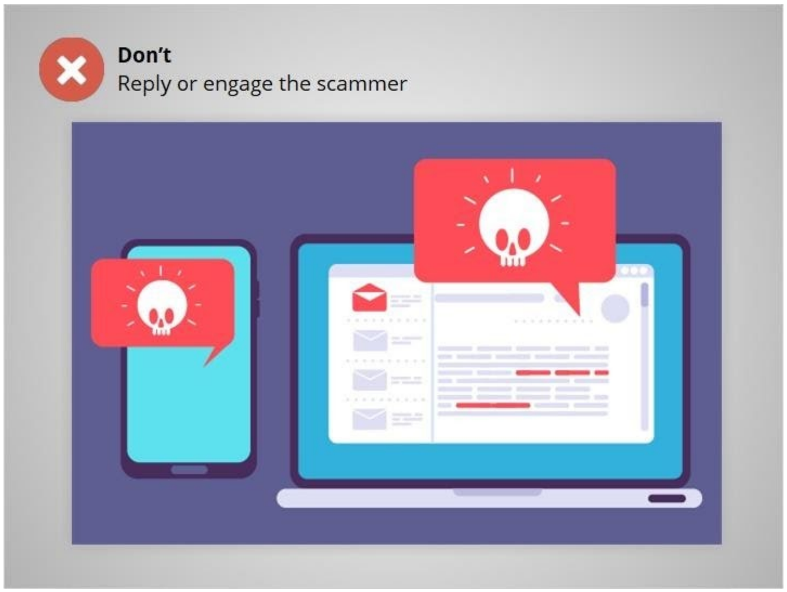
- ✓ Be skeptical
- ✓ Read emails carefully
- ✓ Go directly to a company's website
- ✓ Close pop-ups with Alt+F4 or ⌘+W

Here are some dos and don'ts. We'll go through each one.



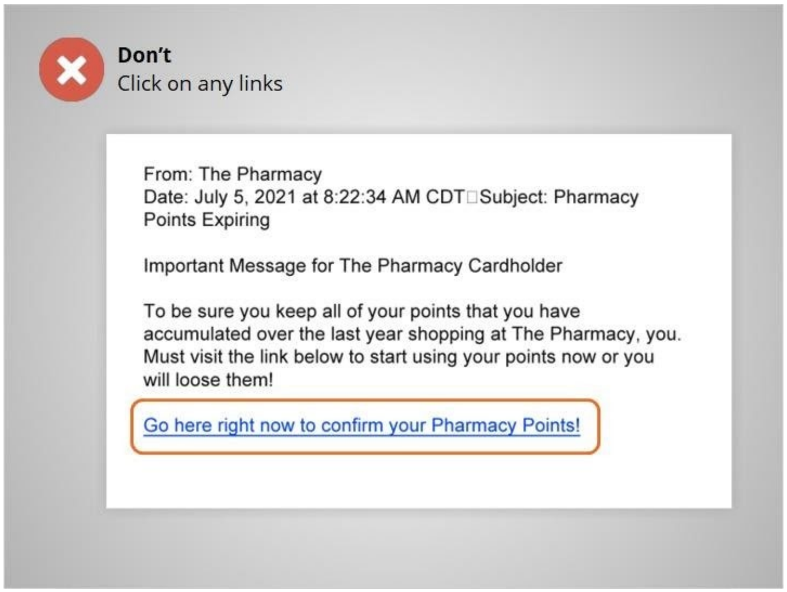
Don't
Give out personal information

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
Reply or engage the scammer

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



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 loose them!

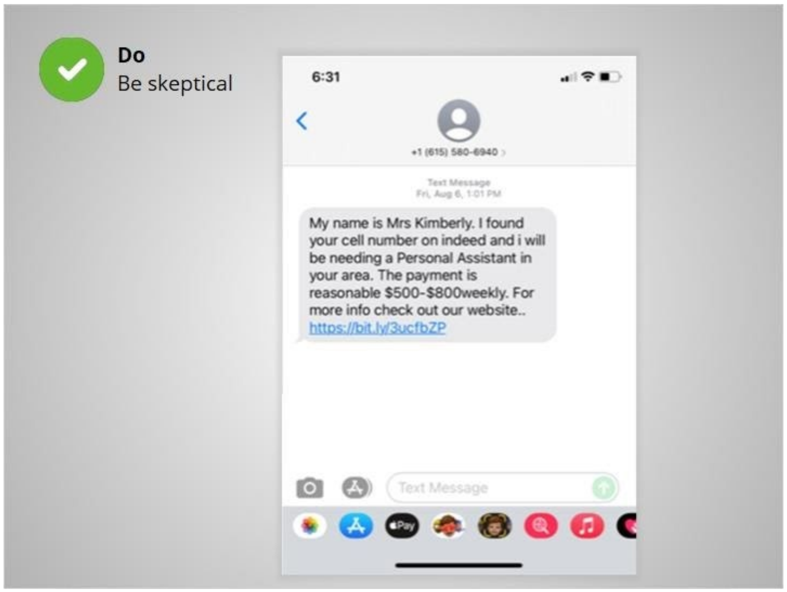
Go here right now to confirm your Pharmacy Points!

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

Don't

Download any files or attachments

Don't download any email attachments or files on an untrustworthy website. They could contain viruses or malware that harm your computer or collect your personal information.



Do
Be skeptical

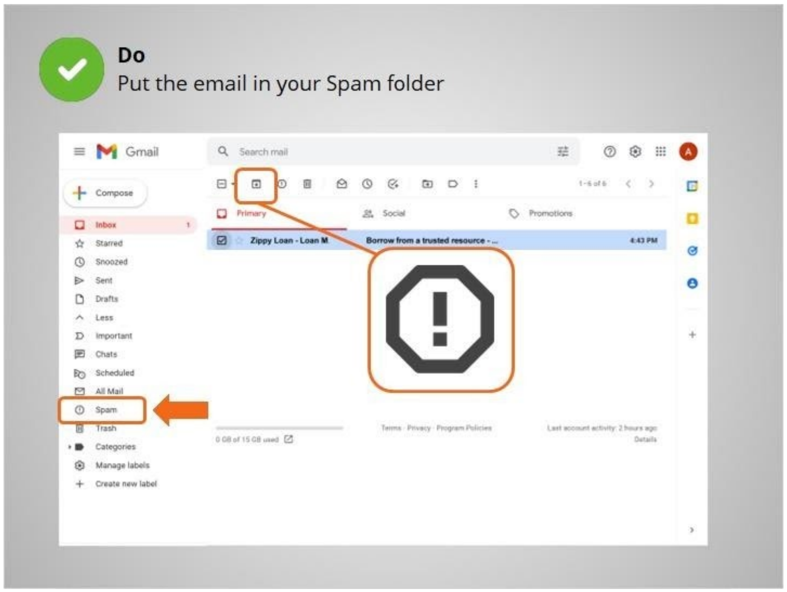
6:31

+1 (615) 580-6940

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 is a scam, it probably is. Remember to read emails and text messages carefully, checking to make sure you know the sender.

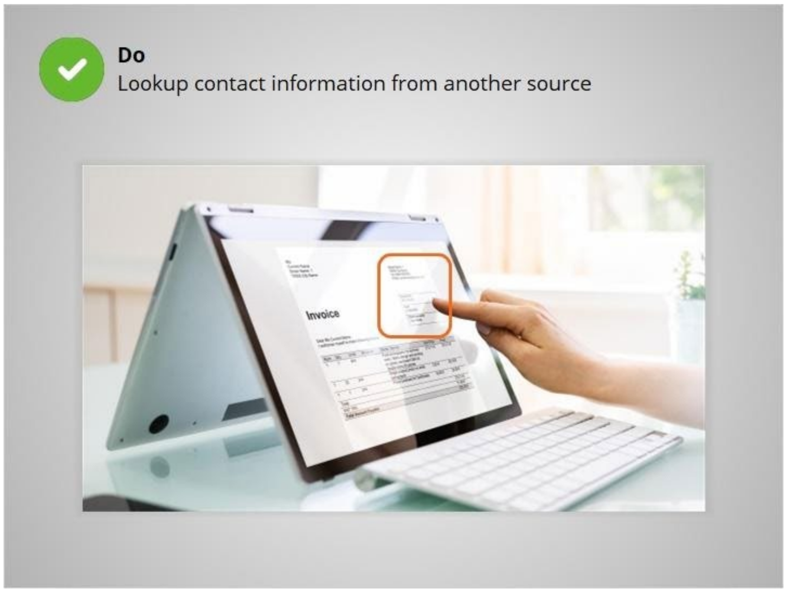


Do
Put the email in your Spam folder

Zippy Loan - Loan M — Borrow from a trusted resource - ... — 4:43 PM

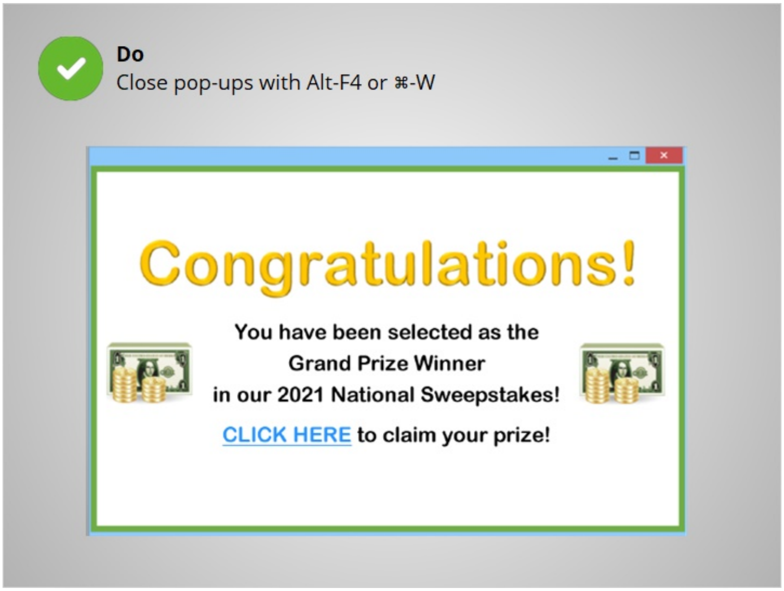
Most email flagged as spam is automatically moved to a spam folder, so you don't see it in the Inbox. This is an example of the spam folder in Gmail. If you do see a spam email in your Inbox, mark the item as spam in your email. Avoid opening the message, clicking on any links, or viewing any pictures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

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**
Lookup contact information from another source

Do look up their contact information on your own, from a statement you've received in the mail or from their official website.



✓ **Do**
Close pop-ups with Alt-F4 or ⌘-W

Congratulations!

You have been selected as the
Grand Prize Winner
in our 2021 National Sweepstakes!

CLICK HERE to claim your prize!

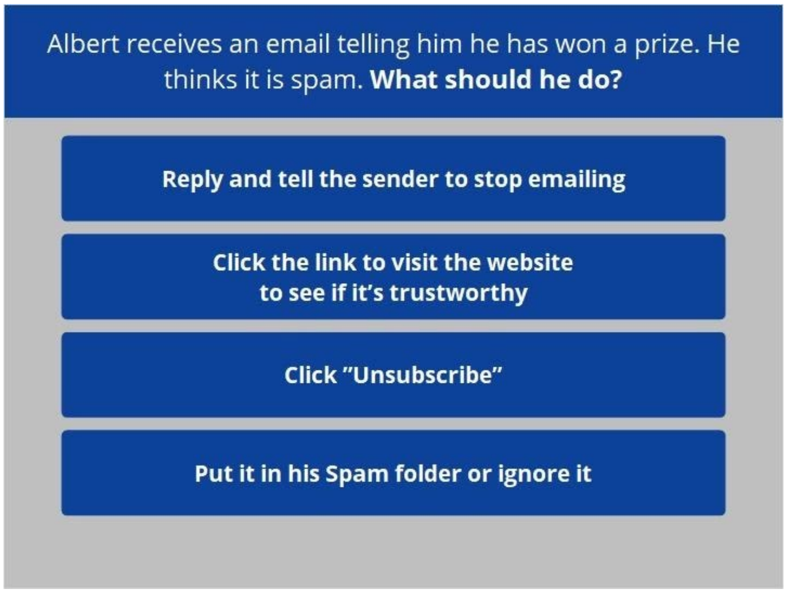
For pop-ups on a website, don't click on any buttons. Sometimes even the X will not close a scam pop-up window and may trigger more pop-ups to open instead.

✓ **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.

Now, let's check-in 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?**

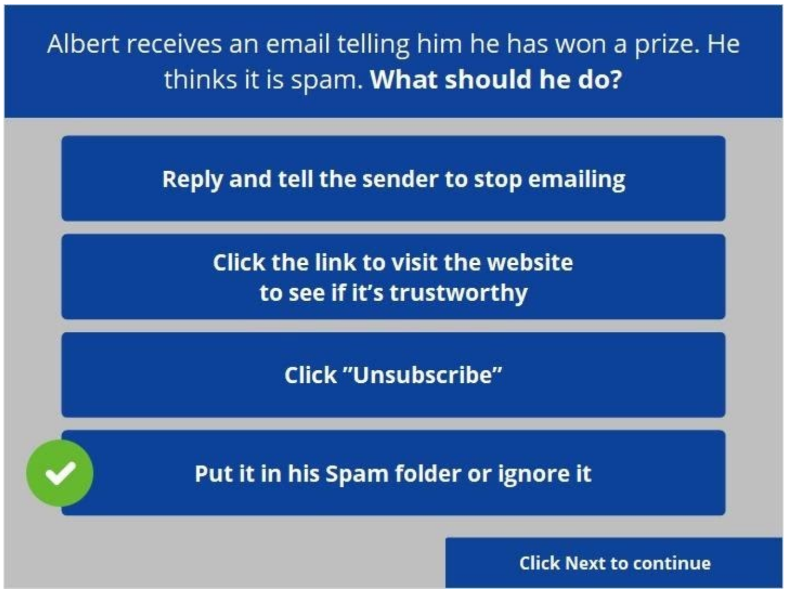
Reply and tell the sender to stop emailing

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

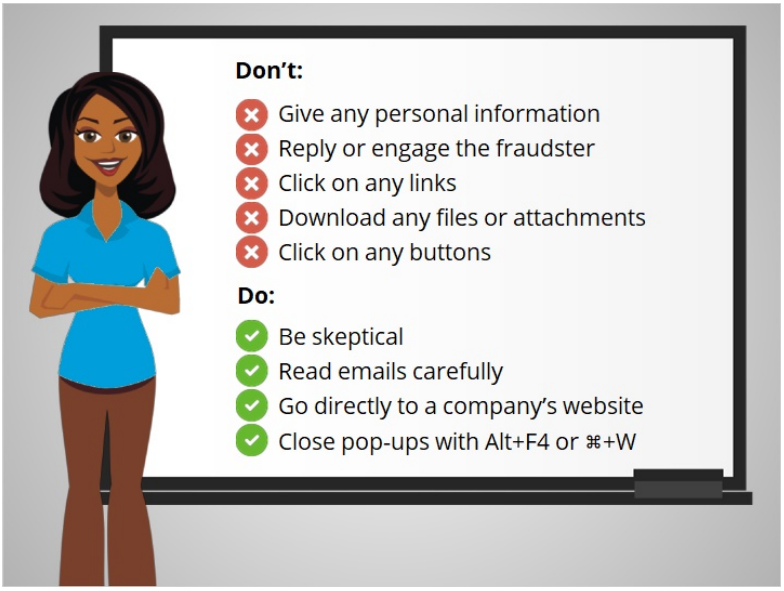
Click the link to visit the website to see if it's trustworthy

Click "Unsubscribe"

✓ Put it in his Spam folder or ignore it

Click Next to continue

That is correct! Engaging the sender can result in getting more spam. Clicking on any link in a scam email can result in getting more spam and lead to unsafe websites.



Don’t:

- ✗ Give any personal information
- ✗ Reply or engage the fraudster
- ✗ Click on any links
- ✗ Download any files or attachments
- ✗ Click on any buttons

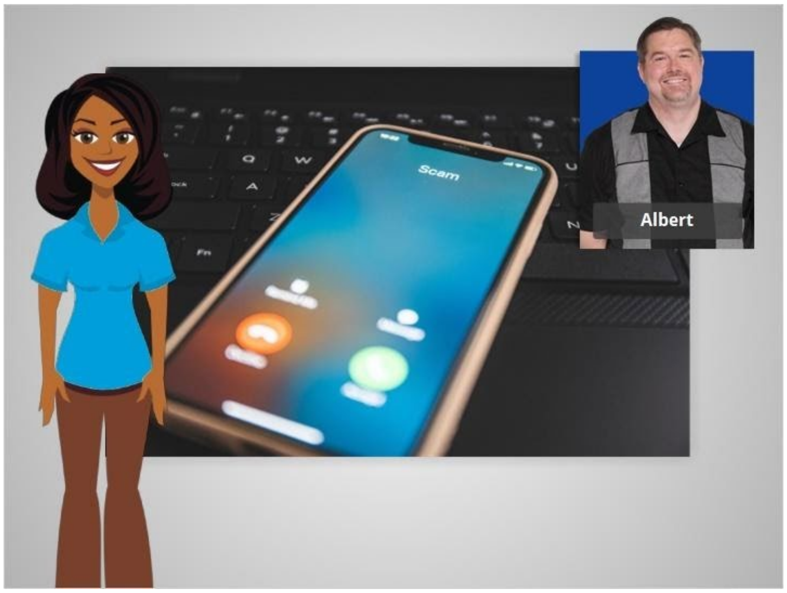
Do:

- ✓ Be skeptical
- ✓ Read emails carefully
- ✓ Go directly to a company’s website
- ✓ Close pop-ups with Alt+F4 or ⌘+W

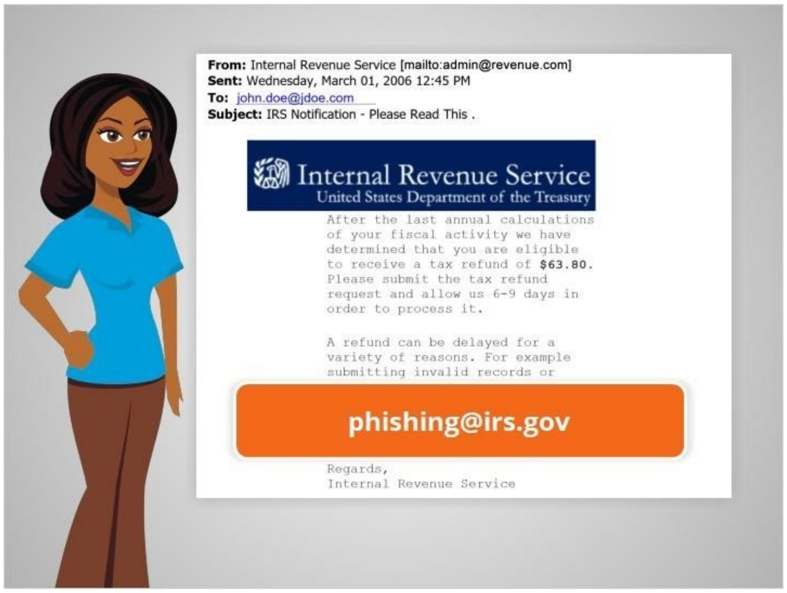
Now Albert knows what he can do when he encounters a scam on a website, in an email, or a text message. When Albert follows these tips, he can stay safe whenever he encounters a scam. In the next lesson, Albert will learn when and how to report scams.

Click on the blue button to end this lesson.

Reporting Scams



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 to help protect others from falling for the same fraud or scam. In this lesson, Albert will learn when and how to report scams.



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

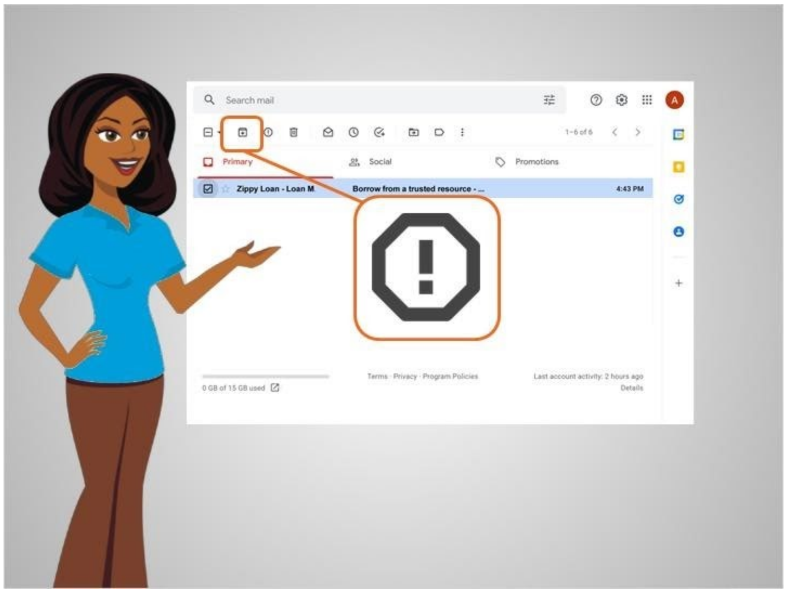
phishing@irs.gov

Regards,
Internal Revenue Service

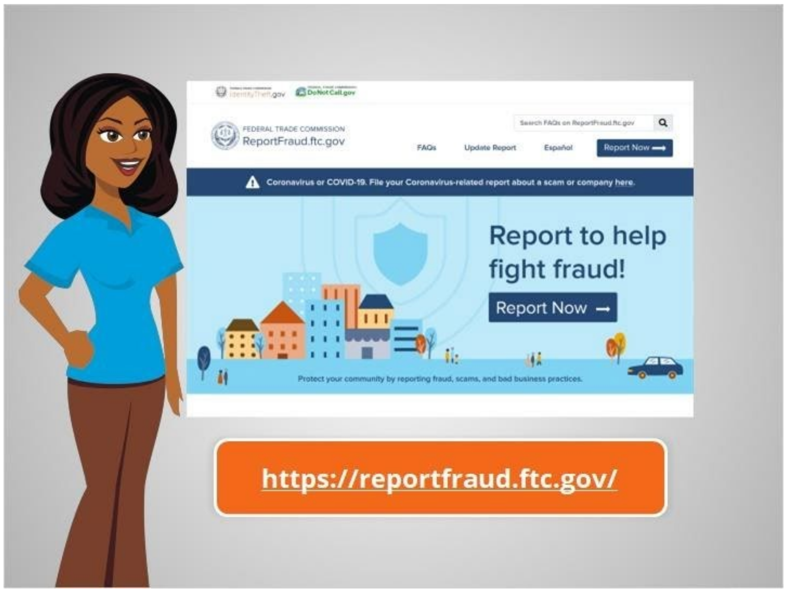
If you encounter a phishing scam imitating an organization you know, you can contact that organization.

But remember not to use the contact information in the 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.


Search mail
1–6 of 6
Primary
Social
Promotions
Zippy Loan - Loan M
Borrow from a trusted resource - ...
4:43 PM
0 GB of 15 GB used
Terms · Privacy · Program Policies
Last account activity: 2 hours ago
Details

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.



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

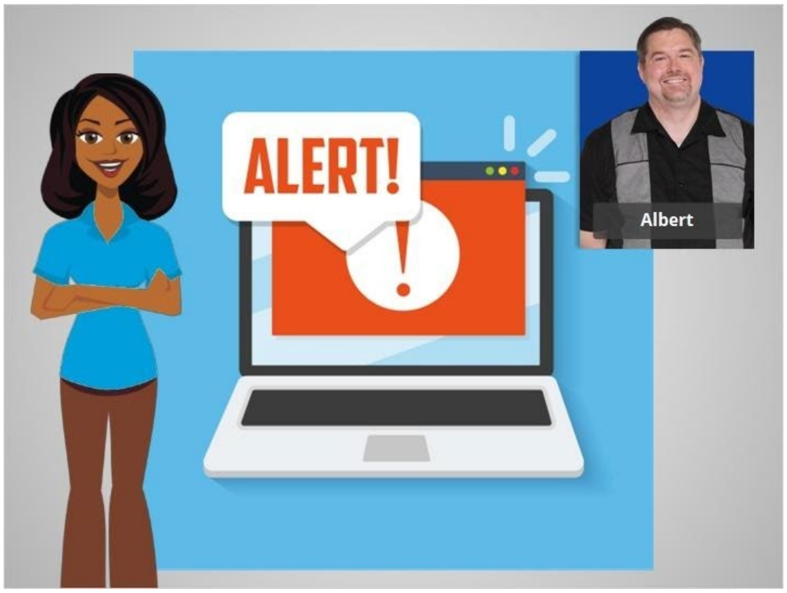
Report to help fight fraud!

Report Now

Protect your community by reporting fraud, scams, and bad business practices.

https://reportfraud.ftc.gov/

You can also file official complaints with the Federal Trade Commission by visiting their website at reportfraud.ftc.gov.



In this class, we learned along with Albert 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.

Click on the blue button to end this course.