Online Scams

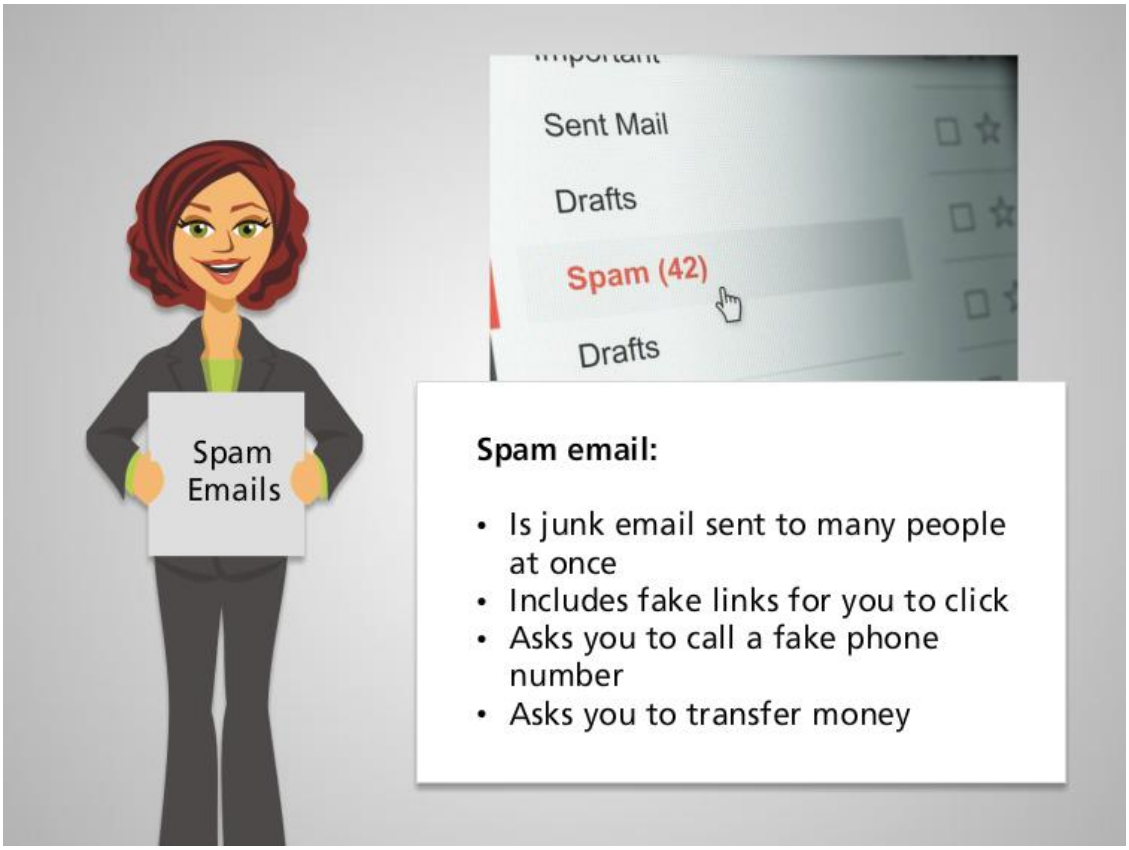
Hi, I'm Kate. We're here to learn how to protect ourselves from online scams. We'll follow along with Kevin to learn what types of scams are out there, how to recognize the warning signs, how to respond when you see a scam, and how to report a scam.

Ready to get started? Click on the green button to continue.

Online scams can come in many shapes and forms. You may encounter them on a website, in an email message, including a type of scam called phishing, or in a pop up window. Let's look at some examples. Click on each button to learn more.

Website Scams

Many websites are not trustworthy. They may try to infect your computer with a virus or lure you into giving them money or personal information. Others may simply try to convince you to click on ads, or give information that is not accurate.

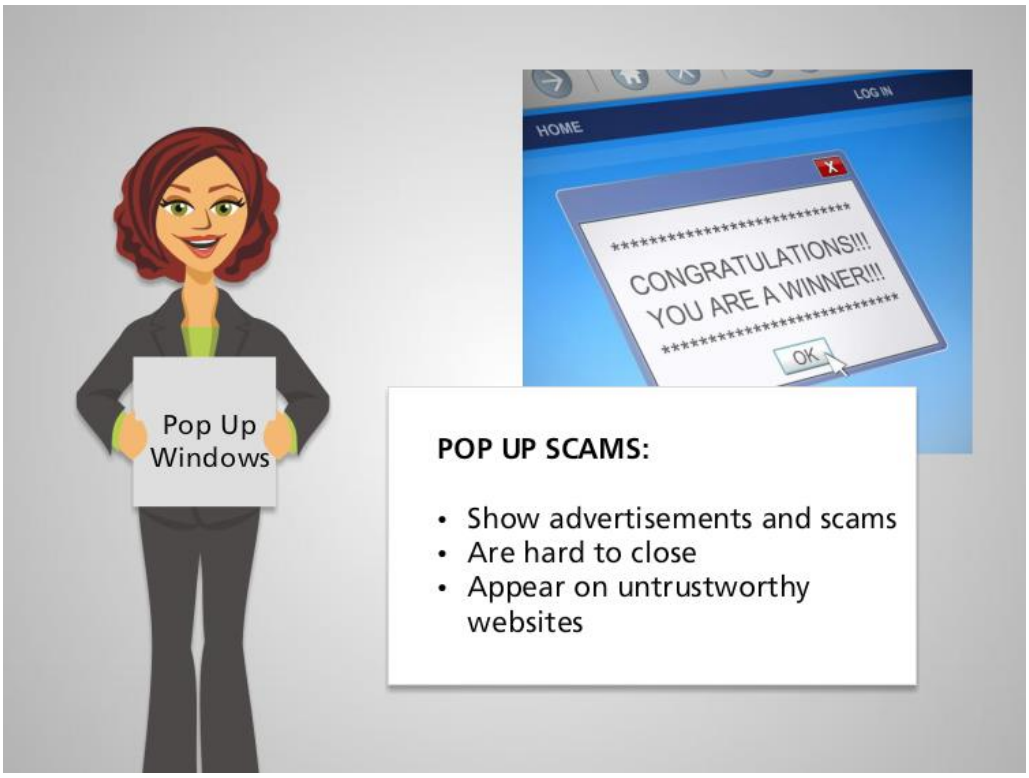


Spam Emails

Junk email, or spam, is almost always fraudulent. These emails are sent to thousands of people at the same time. They try to lure people into clicking on links in the messages, calling a fake number, or even transferring money to the sender.

Phishing

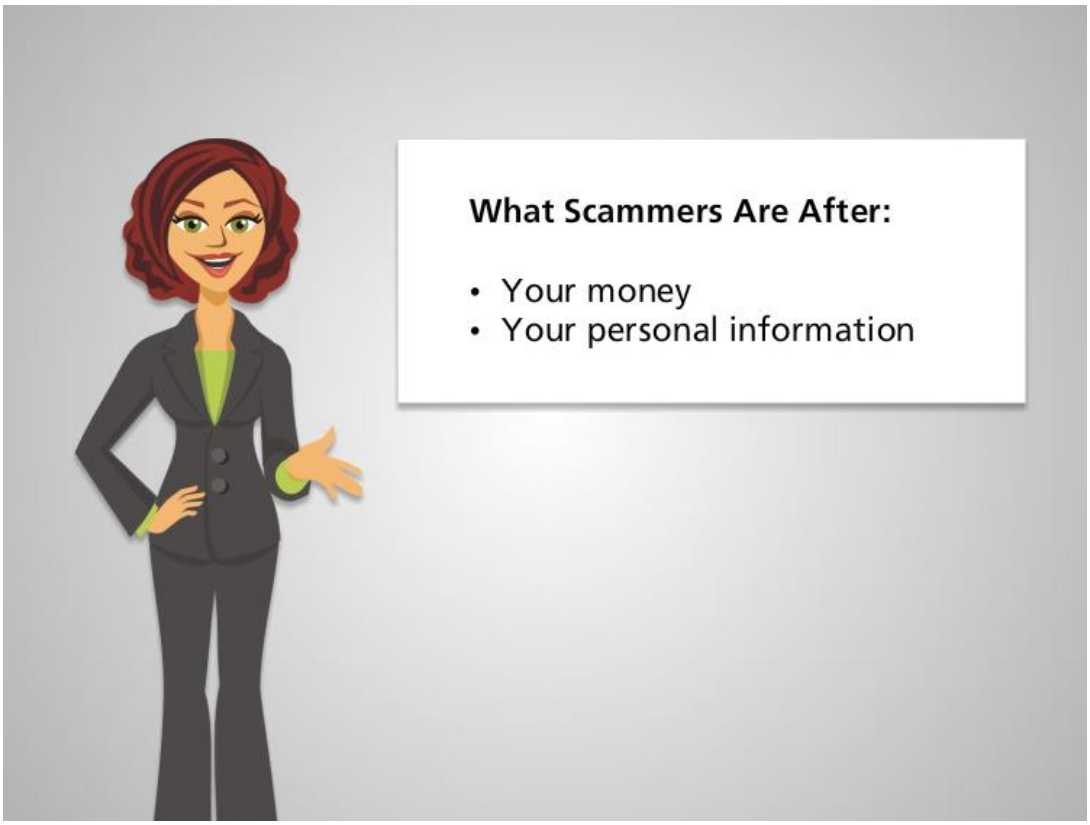
Phishing is a common type of scam. This is when a website or email claims to be a real organization, like the IRS or a bank. Scammers pretend to be an organization that you've heard of to win your trust. Then they ask you for your personal information, or try to get you to visit a fraudulent website.



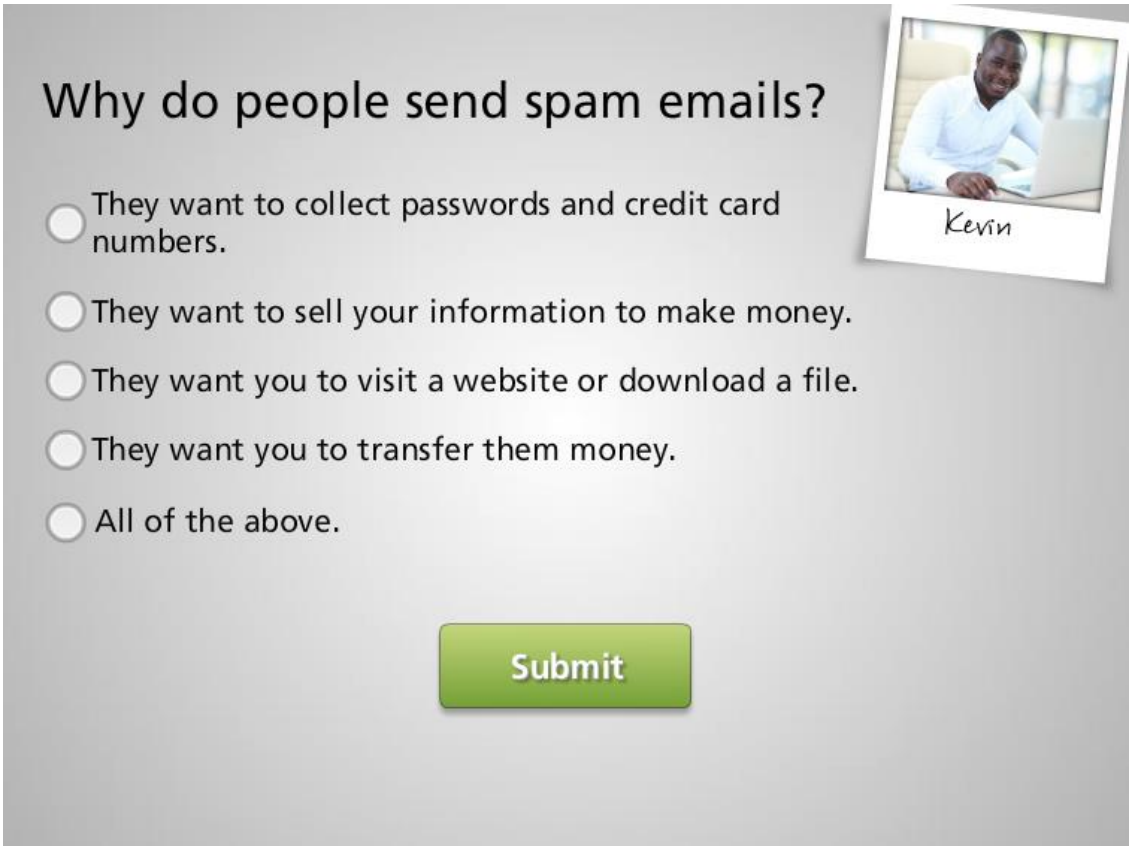
Pop-Up Windows

Some websites will open pop-up advertisements that are hard to close. This is a sure sign that the website is not to be trusted.

Great! Now that you've learned about these four types of scams, click the green button to continue.



No matter what form a scam takes, scams 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 spam emails?

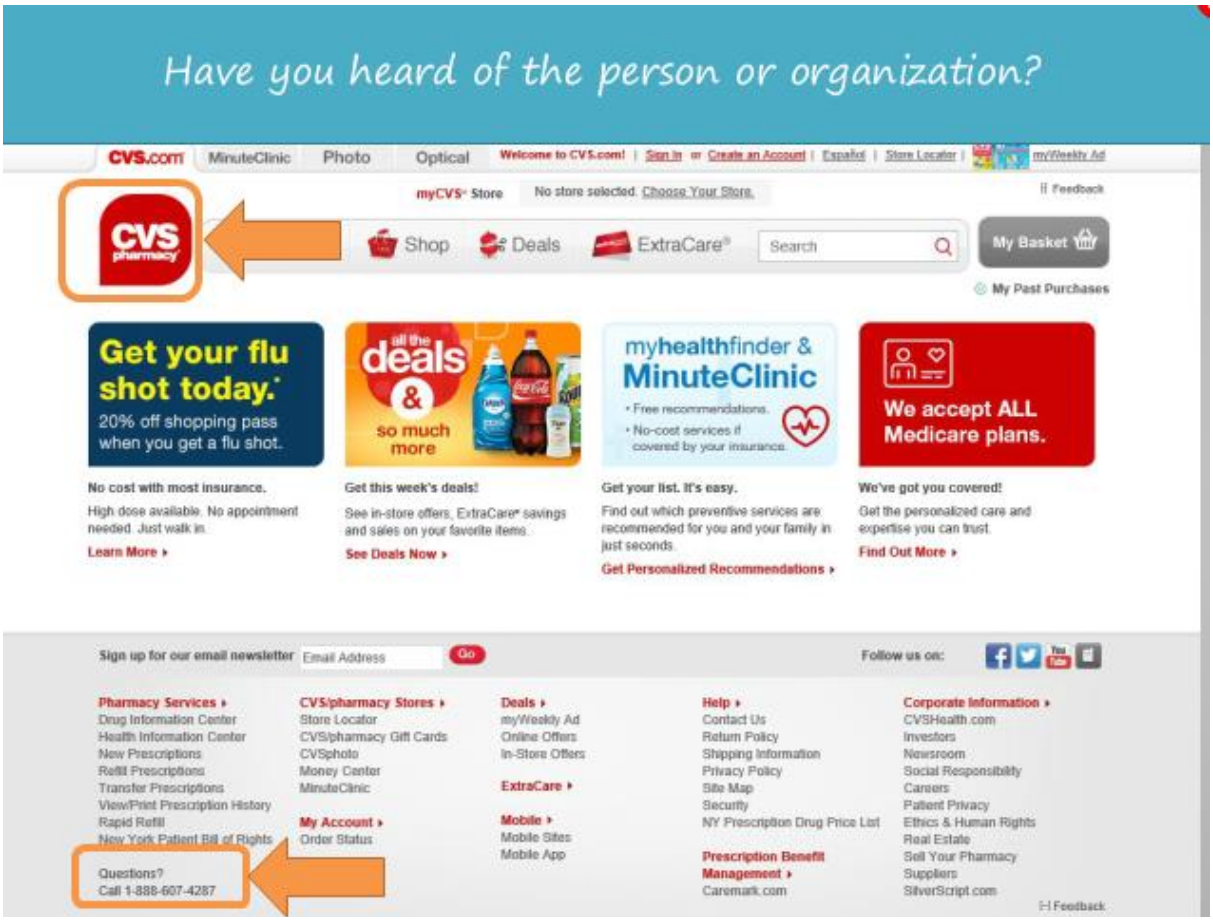
1. They want to collect passwords and credit card numbers.
2. They want to sell your information to make money?
3. They want you to visit a website or download a file.
4. They want you to transfer them money.
5. All of the above.

The correct answer is All of the Above.

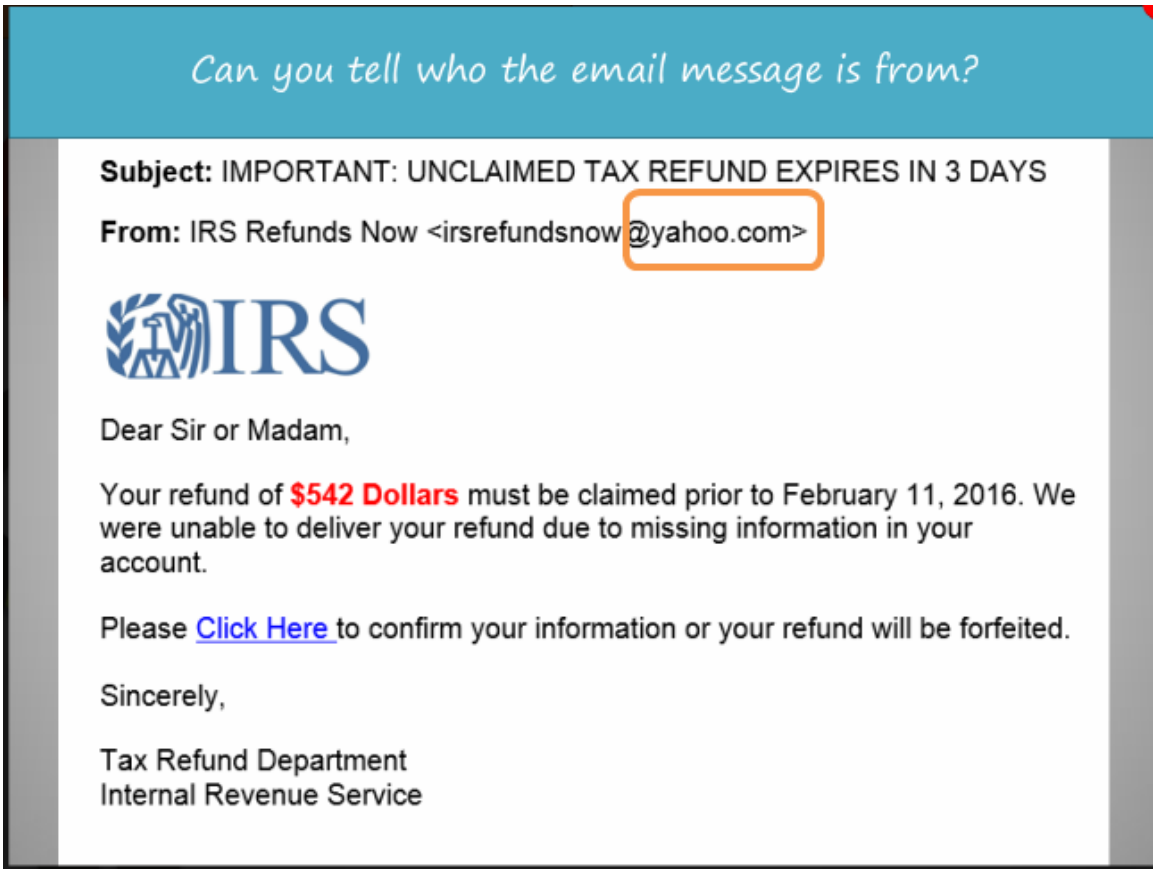
That's right! It's important to guard against scams to keep your information safe.

Recognizing Scams

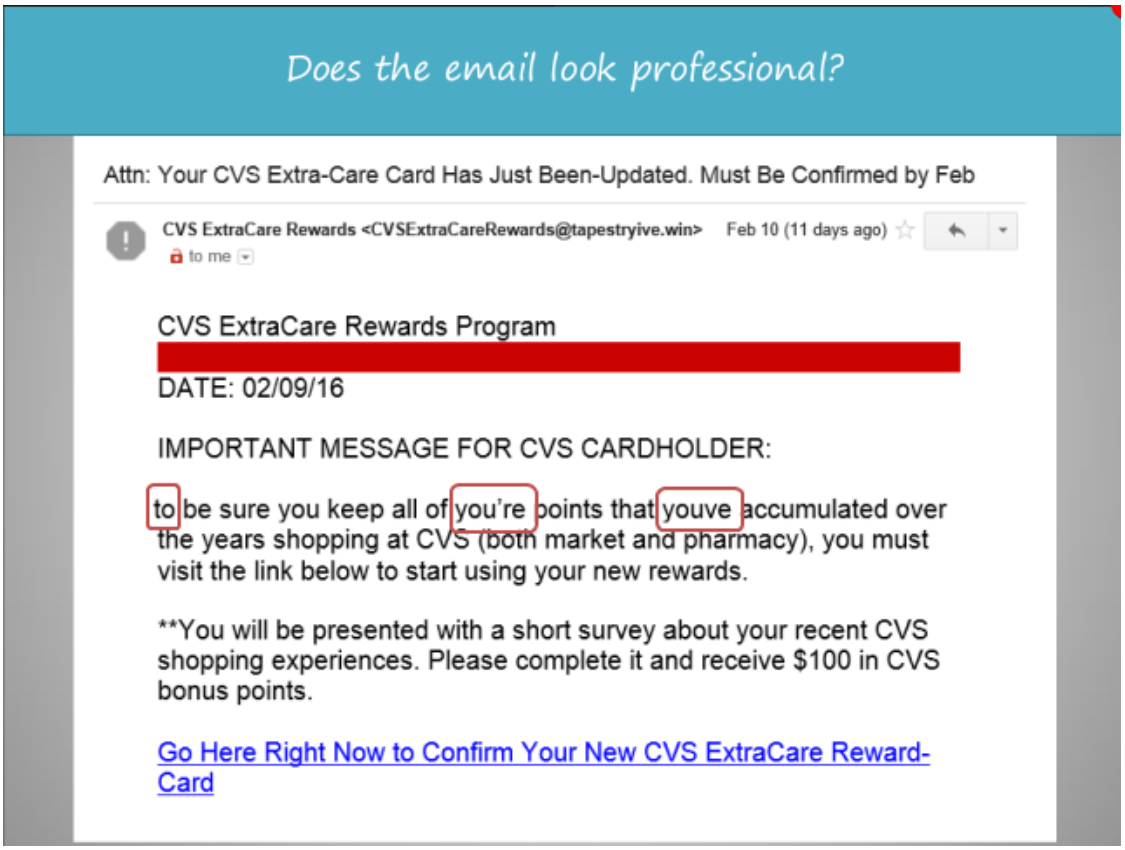
How can you tell if something is a scam? Here are some questions to ask yourself if you're not sure. We'll look at them one by one. Click each question in the list to learn more.



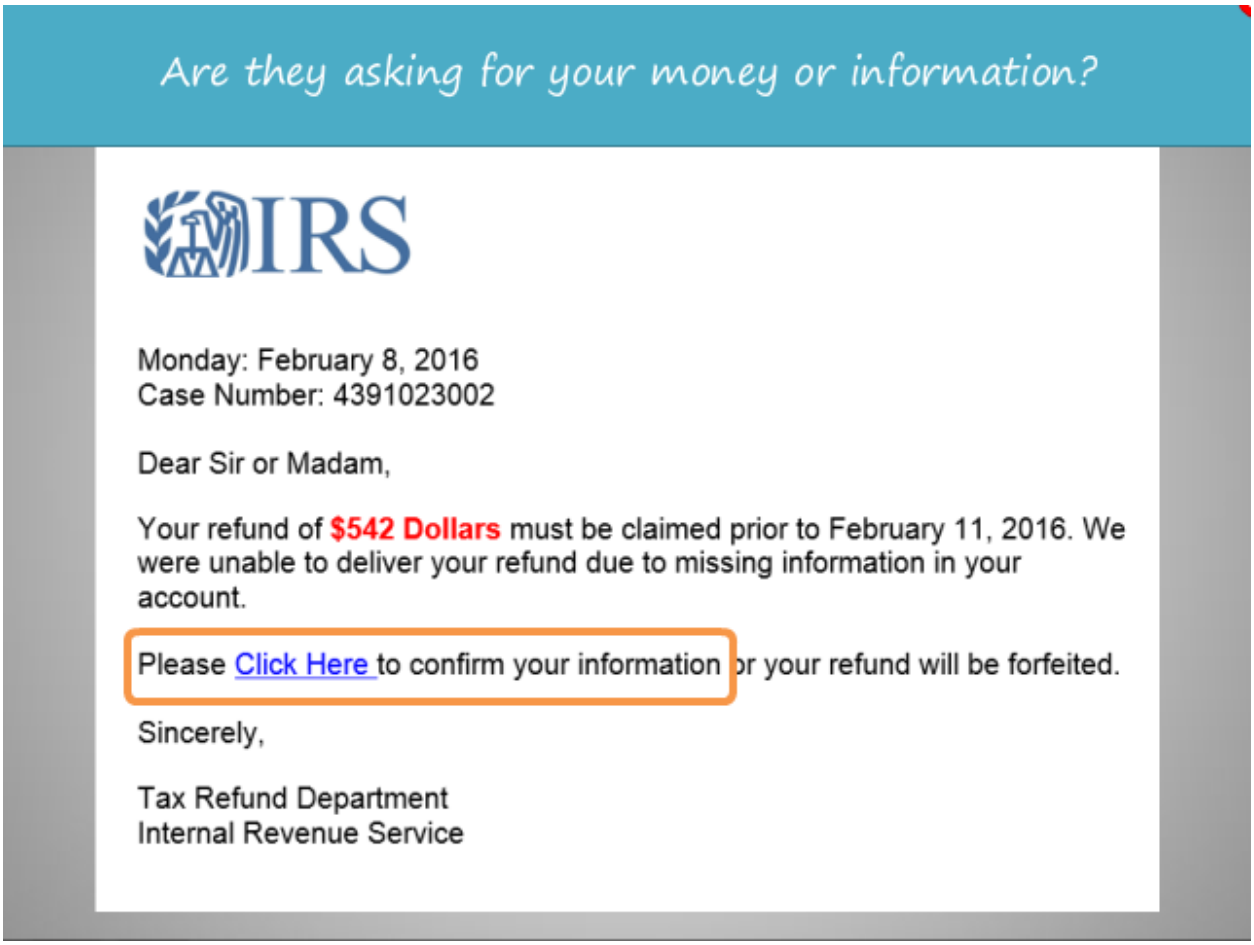
Have you heard of the person or organization before? If not, do some research before responding. If it's a legitimate business, their official logo, address, and contact information should be posted on their website.



On an email message, can you tell who it is from? Look at the address to see if it makes sense. This one claims to be from the IRS, but the email address ends with yahoo.com instead of irs.gov. This is a sure sign of a phishing scam.

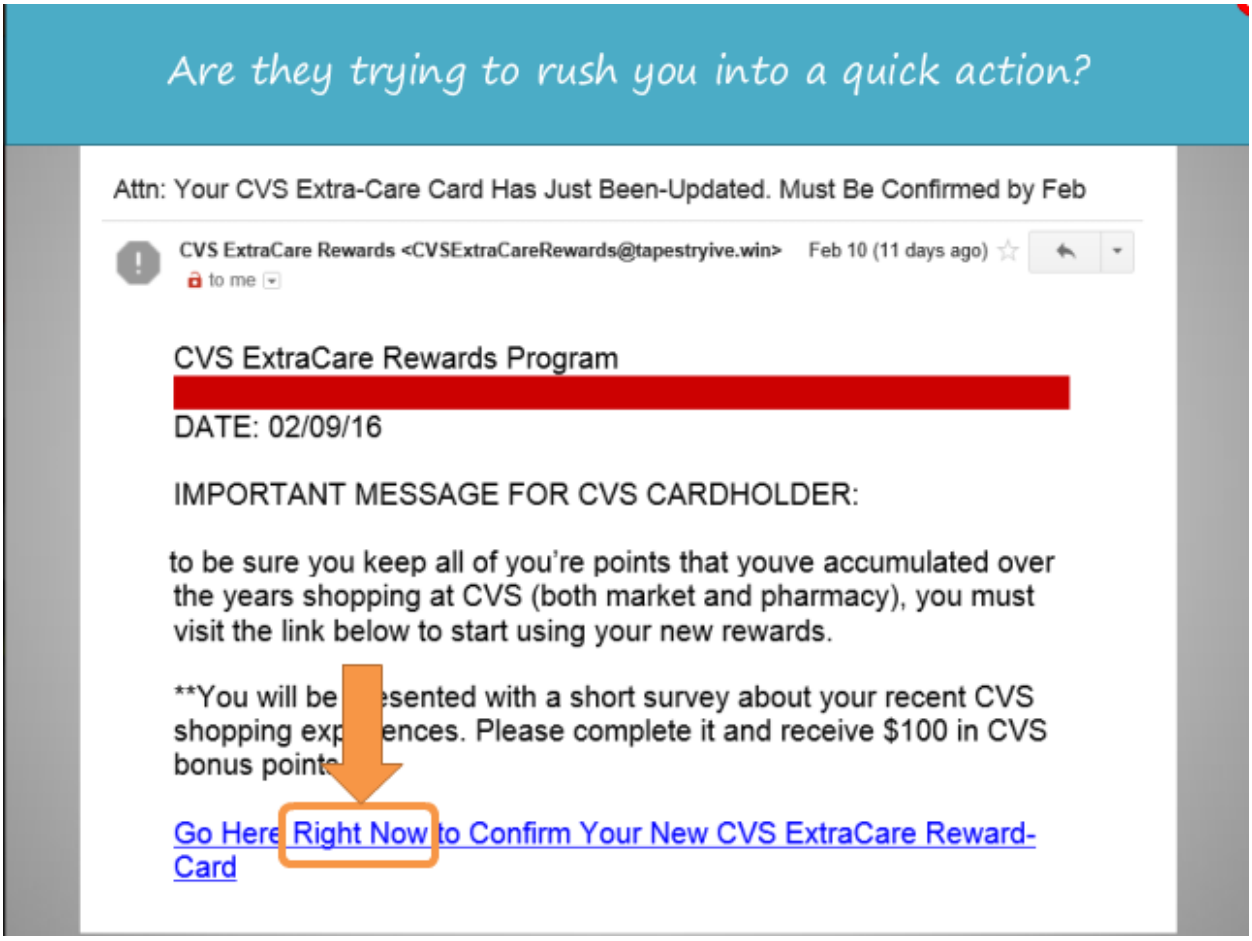


Does the email look professional? If it's a company that you have an account with, they normally include your name. This one just says "Cardholder." If it's from a business, there shouldn't be any spelling or grammar mistakes like this one.

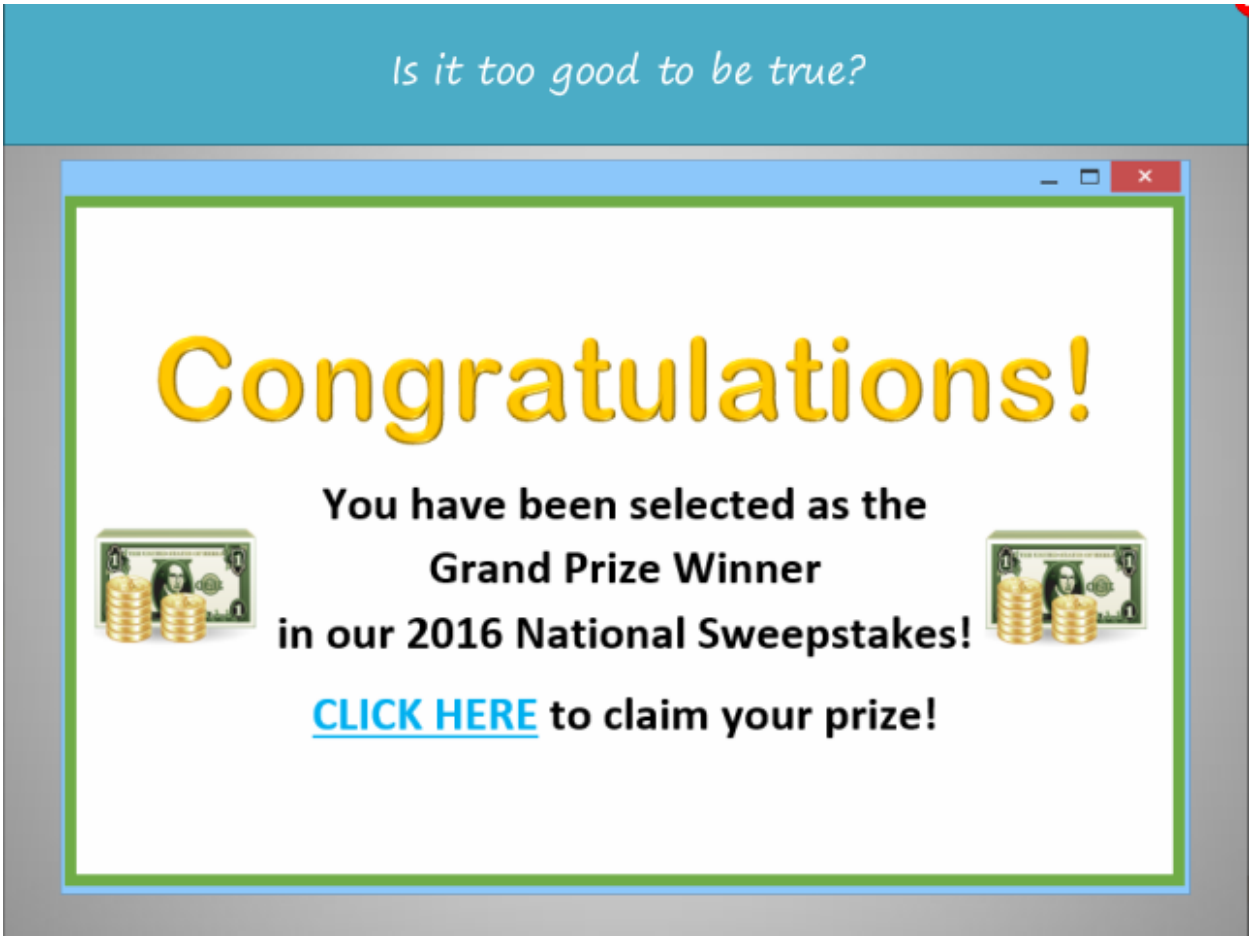


Are they asking for your information? Scammers may claim that they need to verify or update your information. Some scammers will also ask you to wire them money or send a deposit, promising to pay you more in return.

Do they claim that they can fix your computer? Some pop-up scams will say that your computer is infected and tell you to call a number so that they can fix it. Legitimate computer companies like Microsoft will never solicit you to fix your computer in this way.

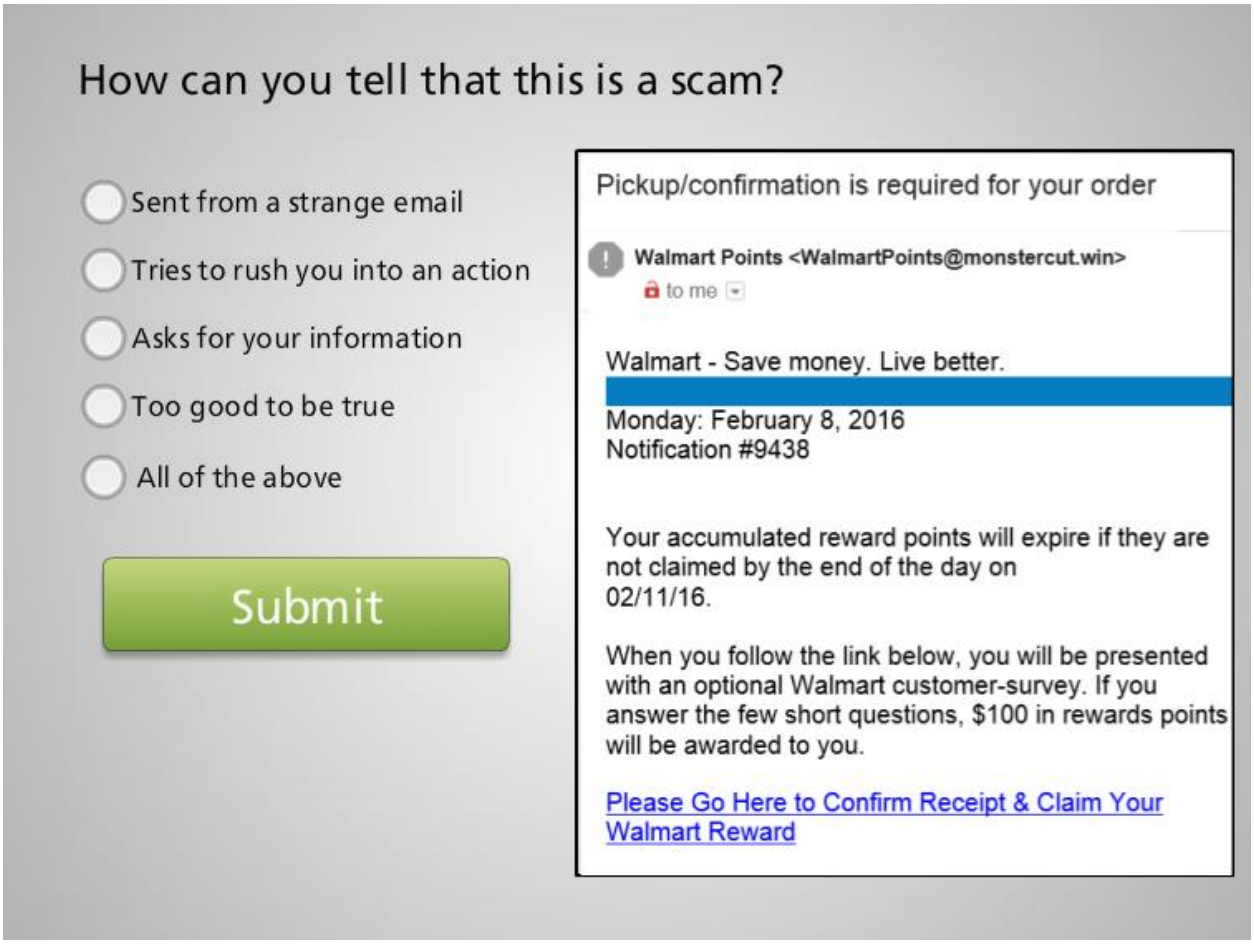


Are they trying to rush you into a quick action before taking the time to think about it? Some scammers try to scare you into acting fast, threatening that something bad will happen, like an account will be closed. Other scammers will promise something good, but only if you respond right away.



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.

Take a look at this example. How can you tell that it's a scam?

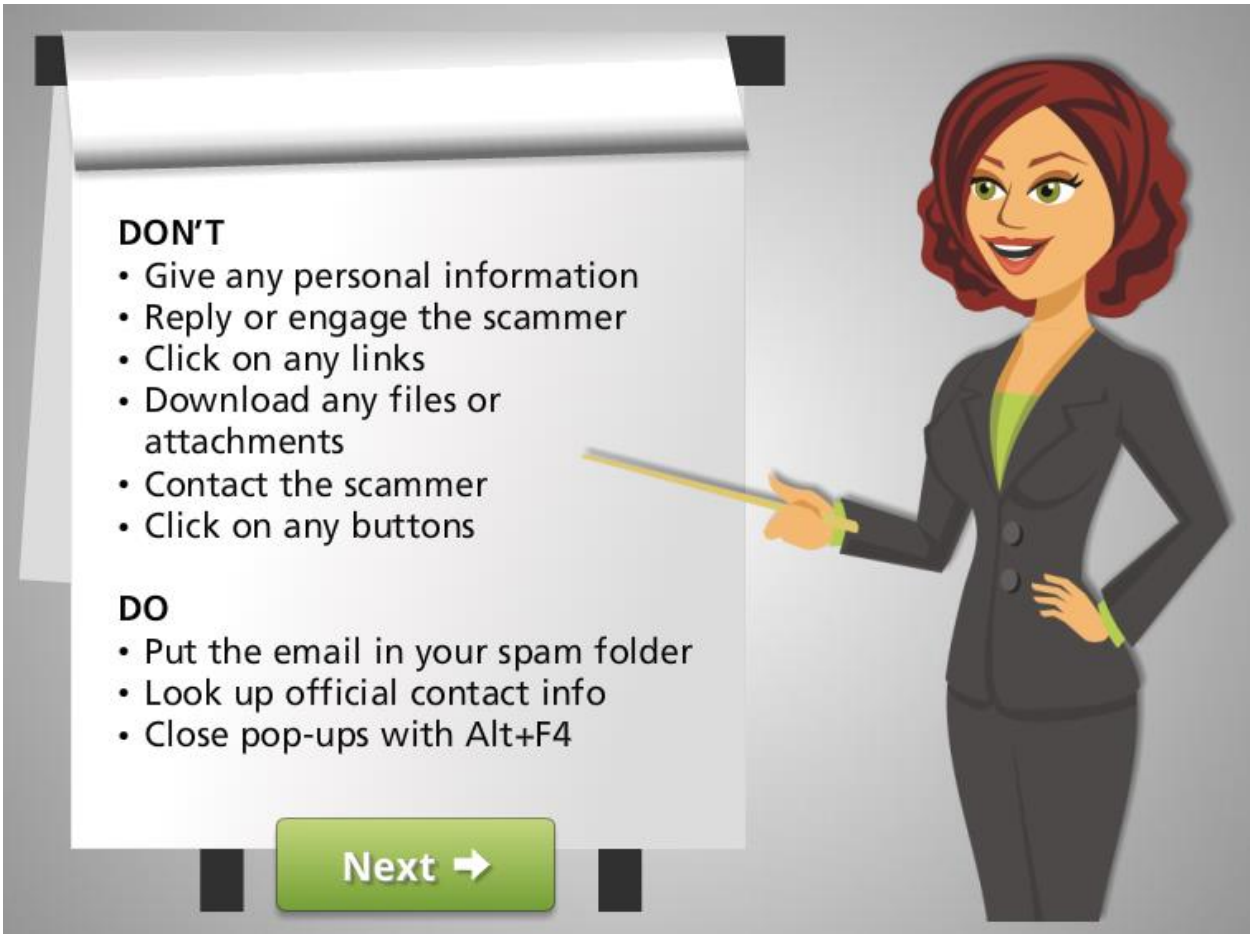


1. Sent from a strange email
2. Tries to rush you into an action
3. Asks for your information
4. Too good to be true
5. All of the Above

The correct answer is All of the Above.

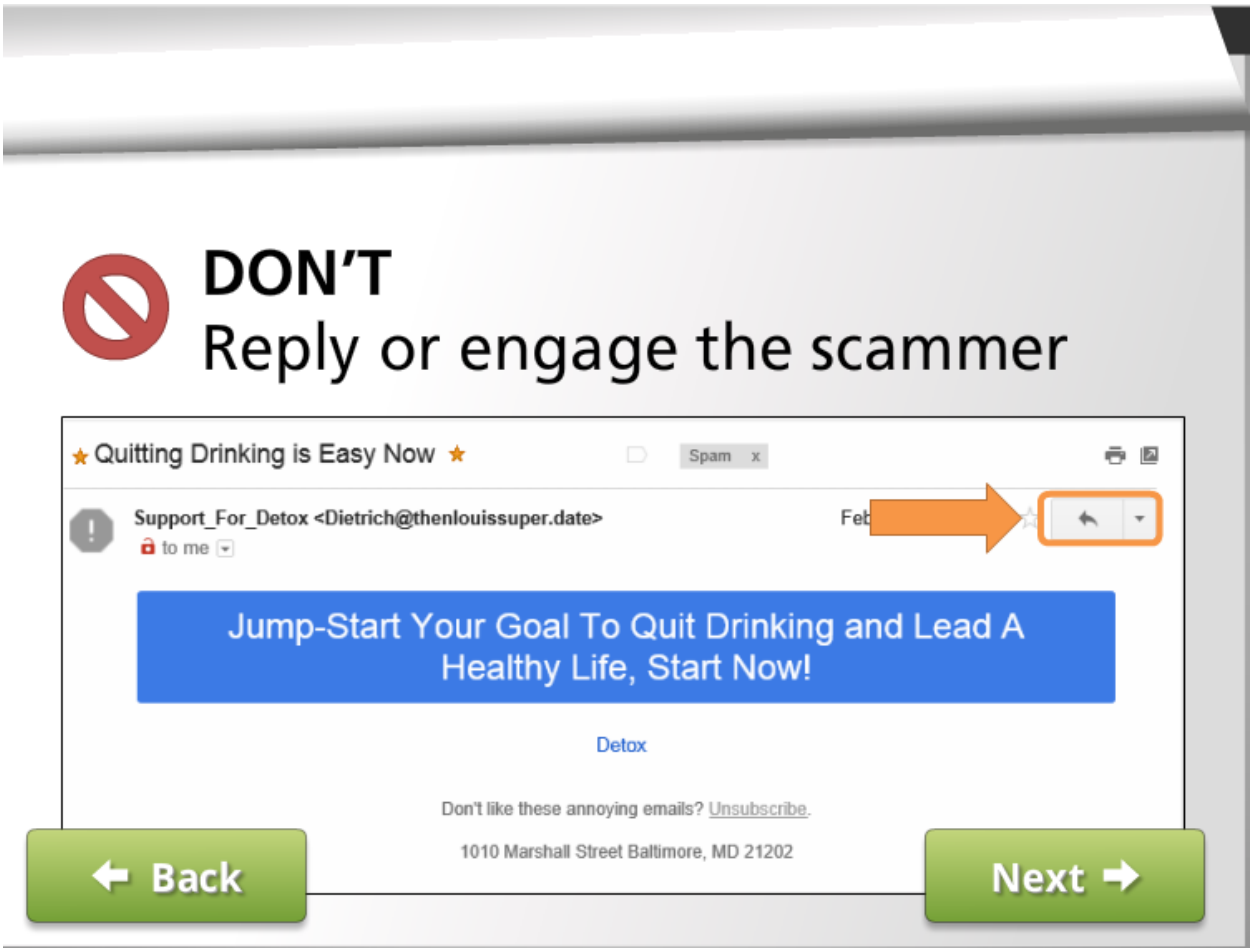
That's right! This email shows several signs of being a scam. We'll learn what to do with emails like this one in the next lesson.

What to Do with Scams



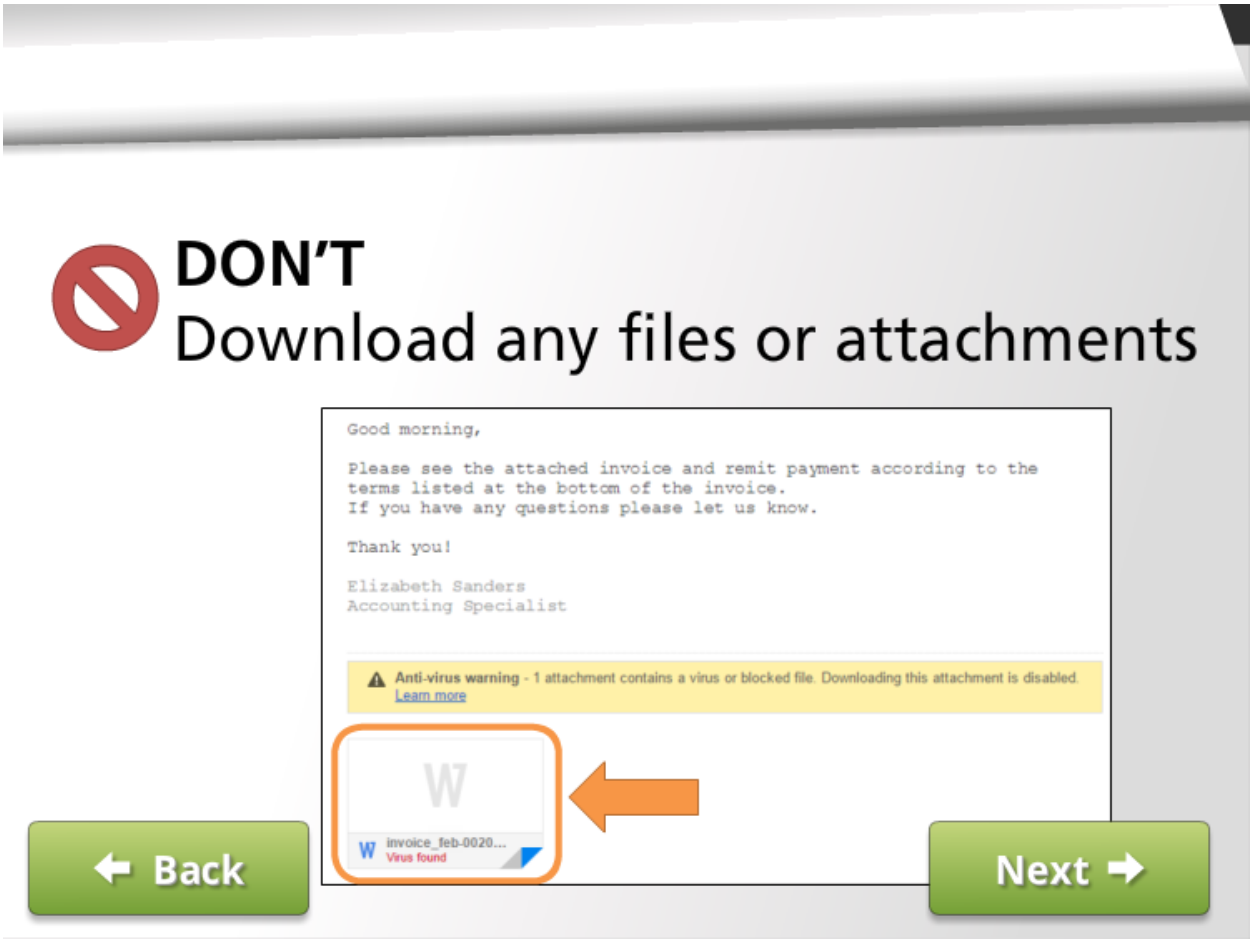
Let's look at the best course of actions to take when you encounter a scam. Here are some do's and don'ts. Use the green buttons to view each of the tips in this list.

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

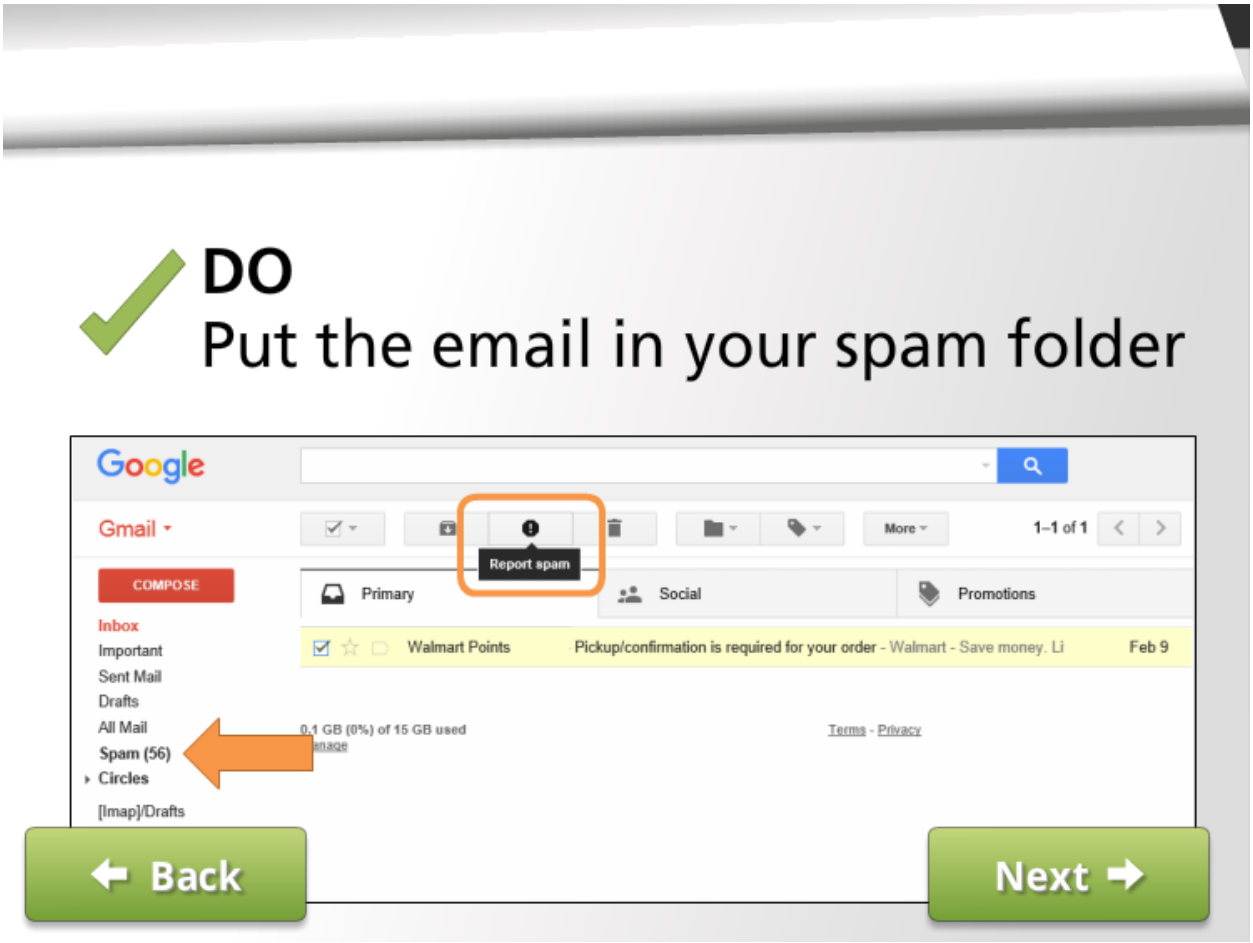


Don't reply or engage them. This can notify the scammer that they've reached a real person, which can result in more scam emails.

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

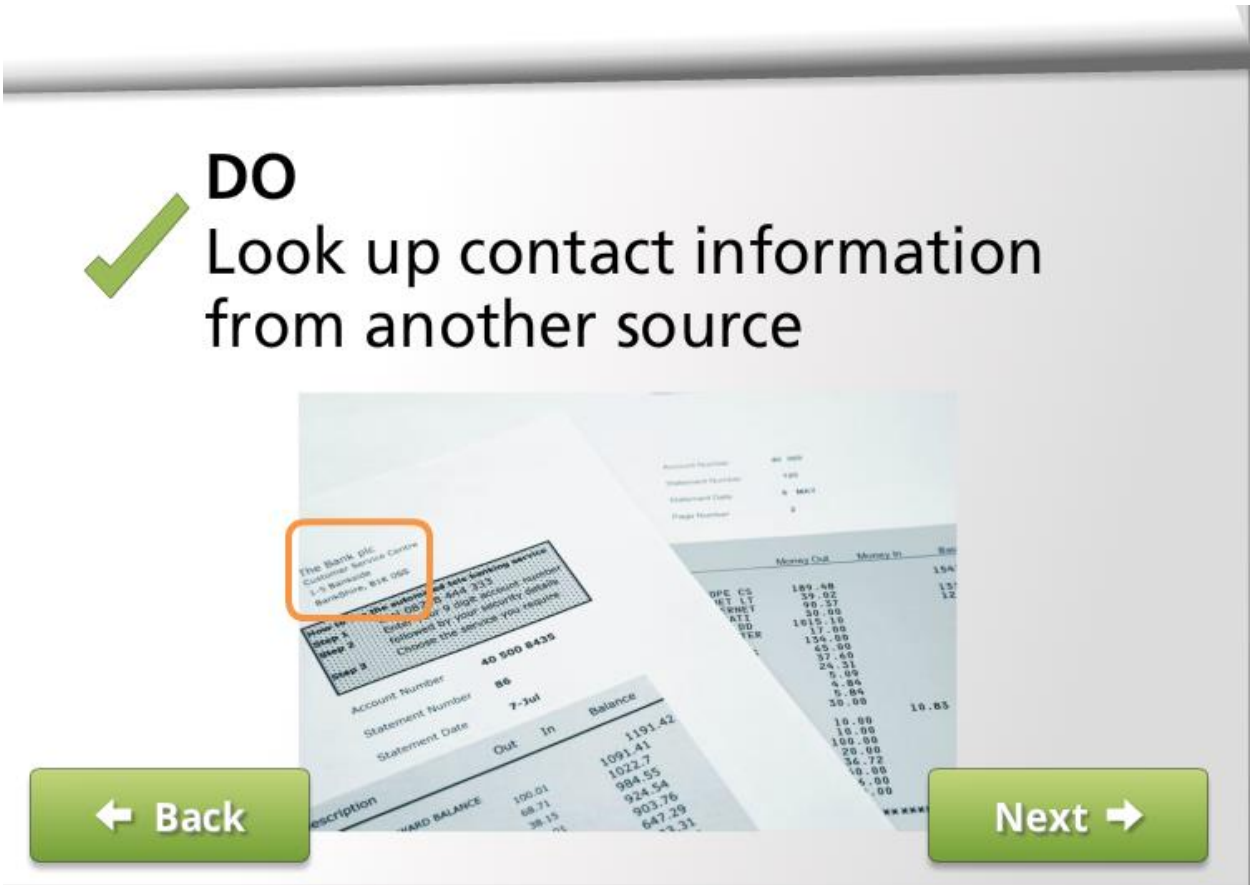


Don't download any email attachments or files on an untrustworthy website. They could contain viruses or malware that harm your computer, or collect your personal information.

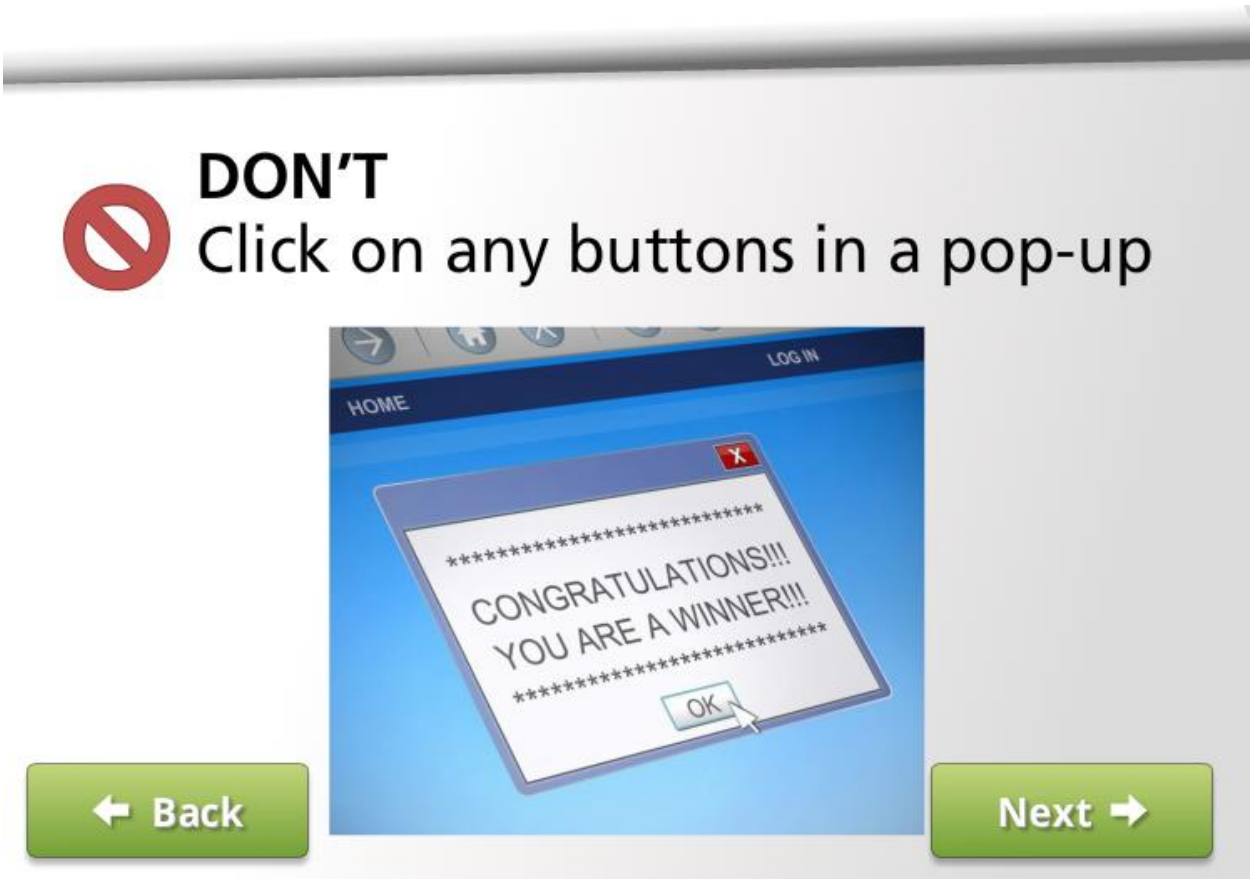


Do put the email message in your spam folder. This will help your email provider alert other people that this is a scam.

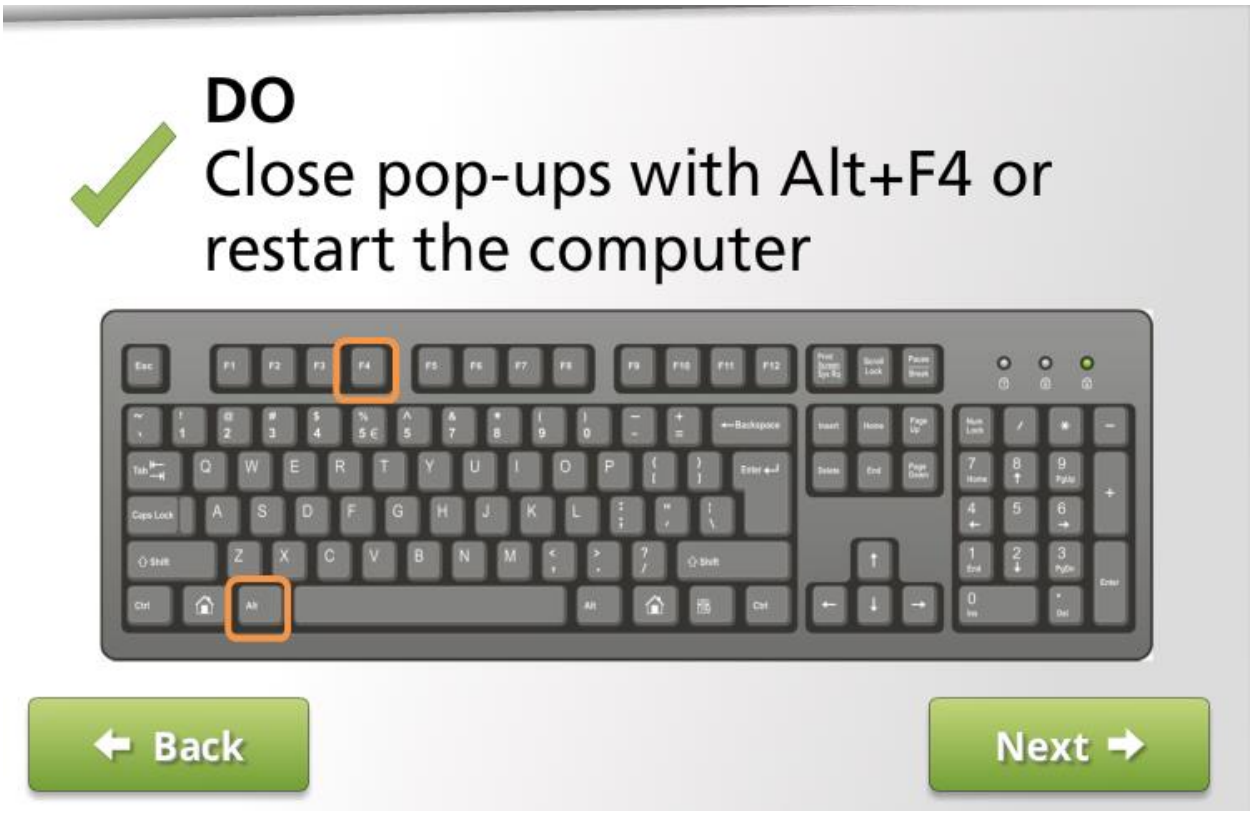
If you suspect something is a phishing scam imitating a real company you trust, don't contact using the email or phone number they gave you.



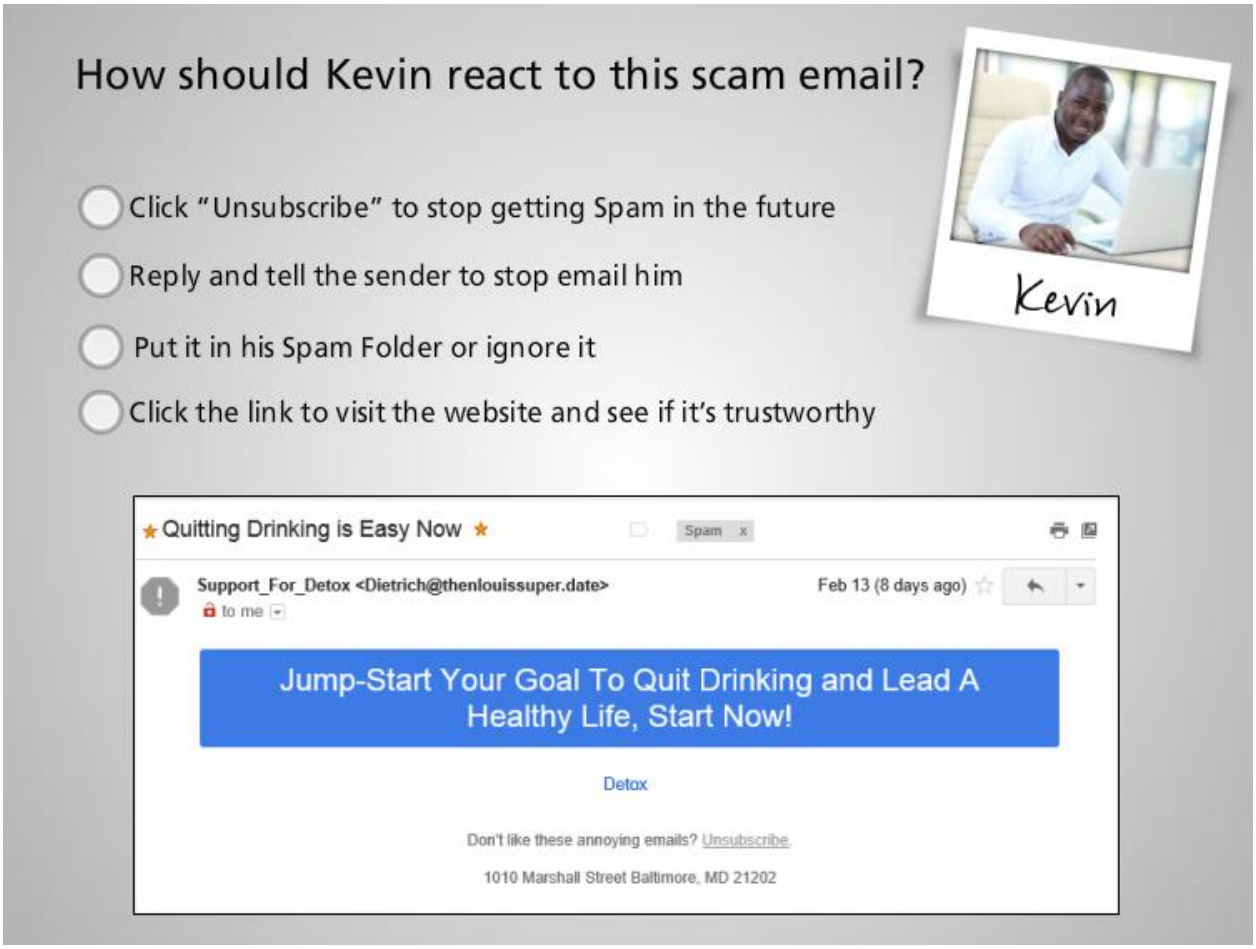
Do look up their contact information on your own, from a statement you've received in the mail or from their official website.



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 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. 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.



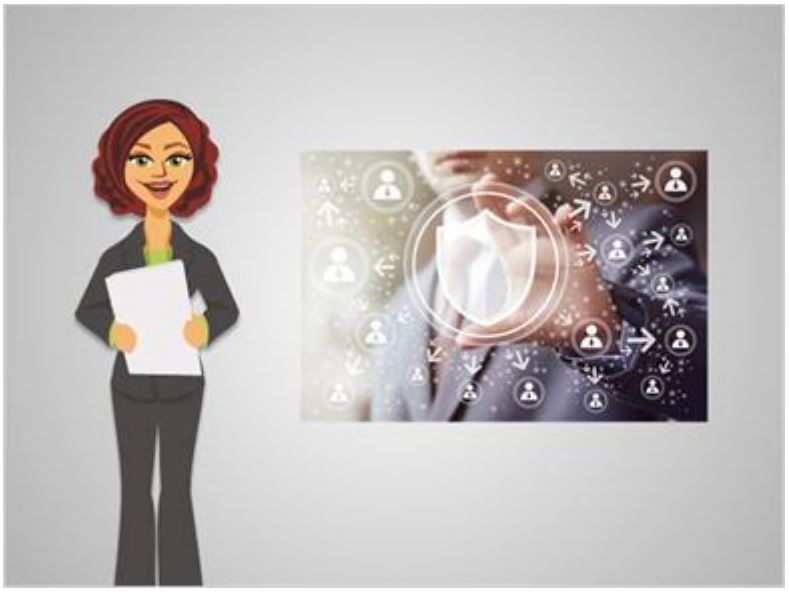
See if you can help Kevin address this scam. What is the best course of action?

1. Click "Unsubscribe" to stop getting Spam in the future
2. Reply and tell the sender to stop emailing him
3. Put it in his Spam Folder or ignore it
4. Click the link to visit the website and see if it's trustworthy

The correct answer is Put it in his Spam folder or ignore it.

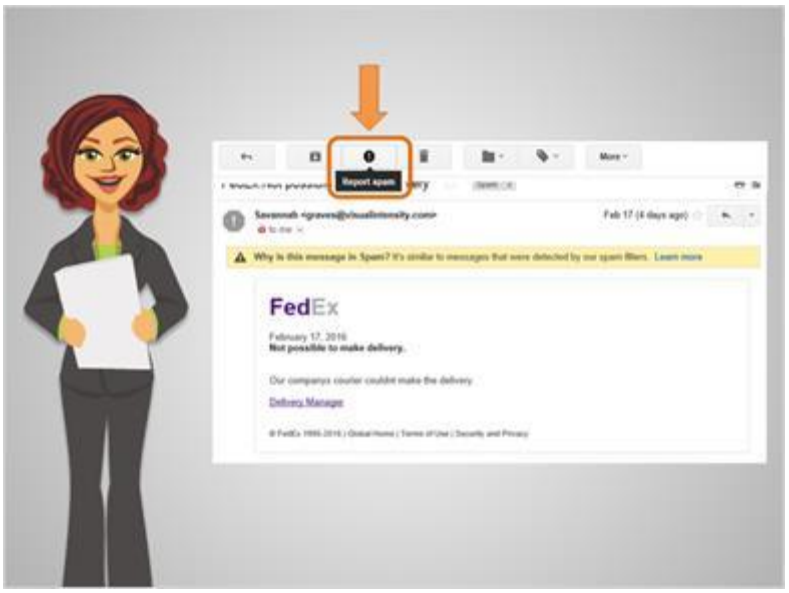
Good job. Follow these tips to stay safe whenever you

Reporting a Scam



Online scams can originate from anywhere in the world. This makes it very difficult or even impossible to track down who is really behind them. However, there are a few actions you can take to help protect others from falling for the same scam.

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. Then, they can warn their other customers about it.
For example, if you see an email imitating the IRS, you can forward it to phishing@irs.gov.



If you receive an email scam, put the message in your spam or junk folder. This helps email providers like Gmail and Yahoo warn others who receive the same email.

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

Remember the warning signs you've learned in this course in order to protect yourself from scams any time that you browse the web or use email.