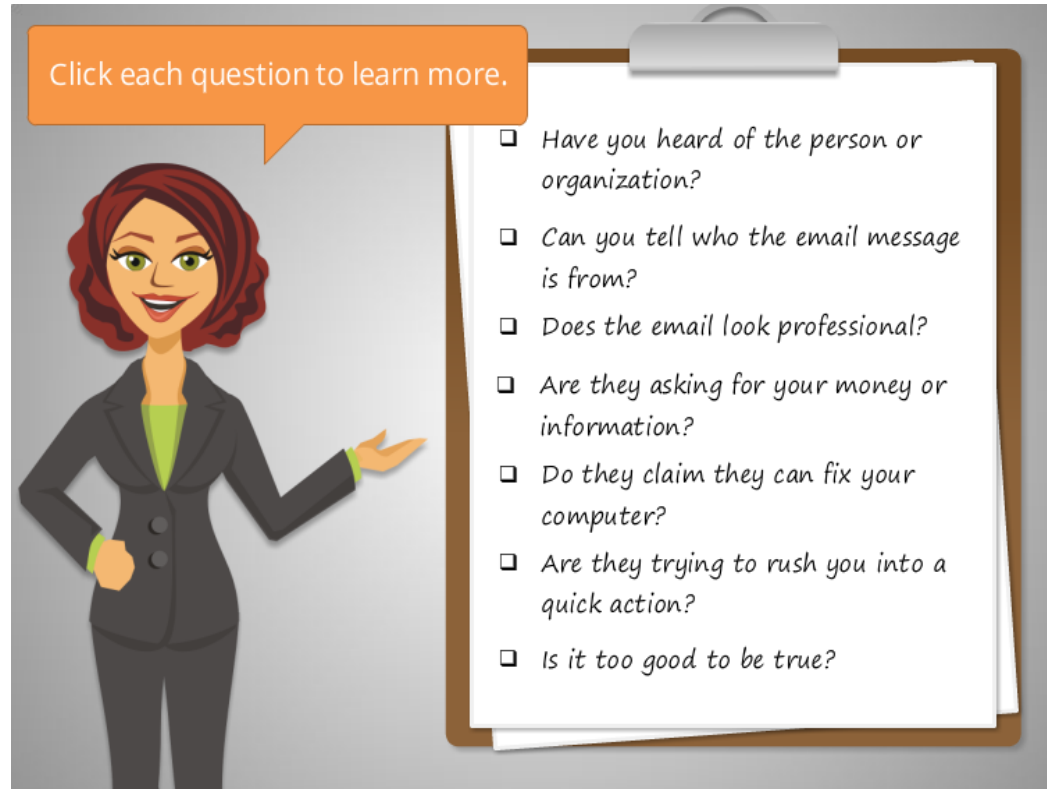


Recognizing Scams



Click each question to learn more.

- Have you heard of the person or organization?
- Can you tell who the email message 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?

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?

The screenshot shows the CVS.com homepage. At the top, a blue banner contains the text "Have you heard of the person or organization?". Below this is the website's navigation bar, which includes the CVS.com logo, links for MinuteClinic, Photo, Optical, and a welcome message. A search bar and a "myCVS Store" selector are also present. A large orange arrow points to the CVS pharmacy logo in the top left. Below the navigation bar are four promotional tiles: "Get your flu shot today.", "all the deals & so much more", "myhealthfinder & MinuteClinic", and "We accept ALL Medicare plans.". At the bottom, there is a newsletter sign-up form and a grid of service categories. A second orange arrow points to the "Questions? Call 1-888-607-4287" link in the bottom left corner.

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.

Can you tell who the email message is from?

Subject: IMPORTANT: UNCLAIMED TAX REFUND EXPIRES IN 3 DAYS

From: IRS Refunds Now <irsrefundsnow@**yahoo.com**>



Dear Sir or Madam,

Your refund of **\$542 Dollars** must be claimed prior to February 11, 2016. We were unable to deliver your refund due to missing information in your account.

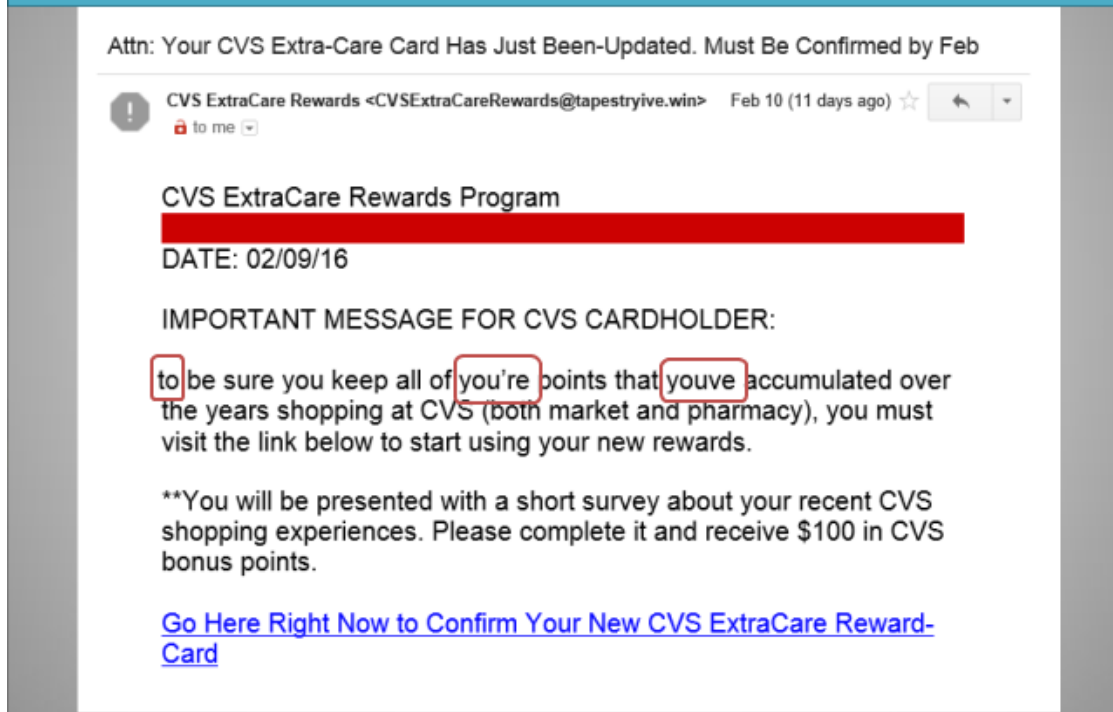
Please [Click Here](#) to confirm your information or your refund will be forfeited.

Sincerely,

Tax Refund Department
Internal Revenue Service

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?



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 money or information?



Monday: February 8, 2016
Case Number: 4391023002

Dear Sir or Madam,

Your refund of **\$542 Dollars** must be claimed prior to February 11, 2016. We were unable to deliver your refund due to missing information in your account.

Please [Click Here](#) to confirm your information or your refund will be forfeited.

Sincerely,

Tax Refund Department
Internal Revenue Service

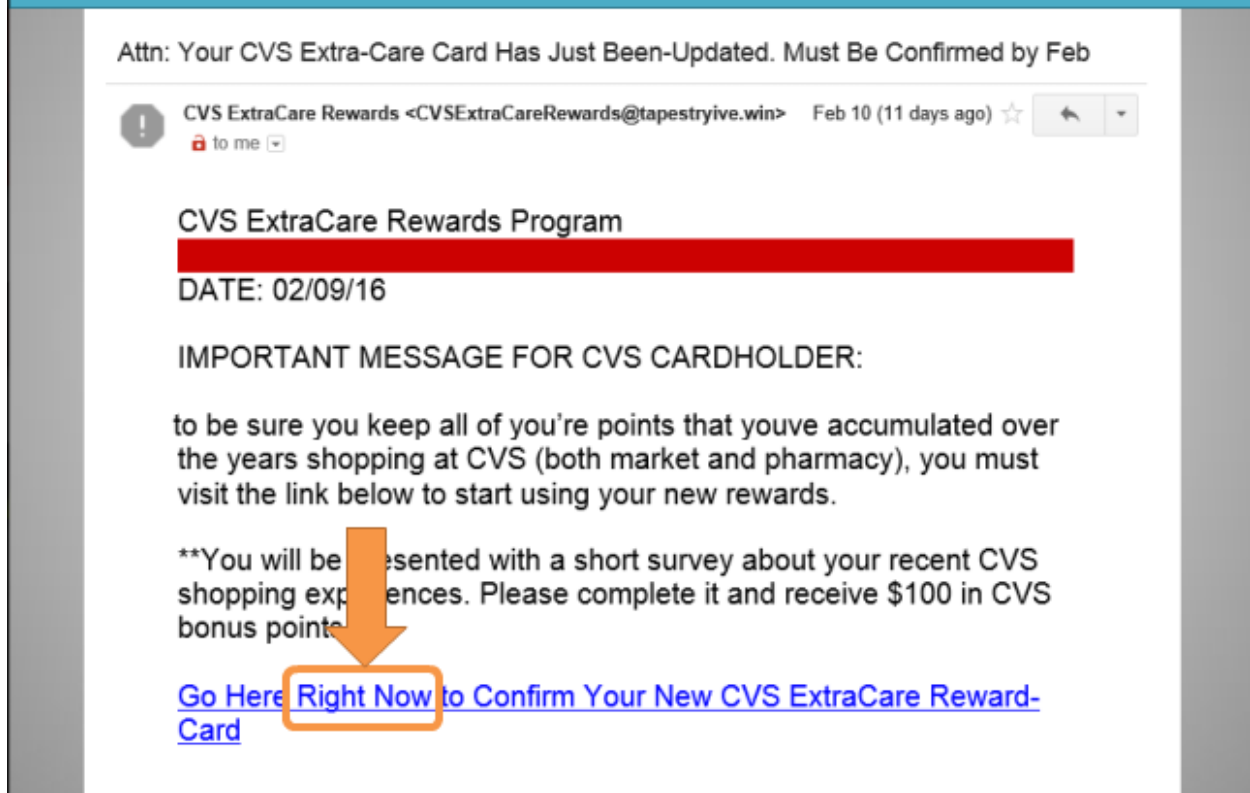
Are they asking for your information? Scammers may claim that they need to verify or update your information. Some scammers will also ask you to wire them money or send a deposit, promising to pay you more in return.

Do they claim they can fix your computer?



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?



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?



Congratulations!

**You have been selected as the
Grand Prize Winner
in our 2016 National Sweepstakes!**

[CLICK HERE](#) to claim your prize!

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?

How can you tell that this is a scam?

Sent from a strange email

Tries to rush you into an action

Asks for your information

Too good to be true

All of the above

Submit

Pickup/confirmation is required for your order

! Walmart Points <WalmartPoints@monstercut.win>
to me

Walmart - Save money. Live better.

Monday: February 8, 2016
Notification #9438

Your accumulated reward points will expire if they are not claimed by the end of the day on 02/11/16.

When you follow the link below, you will be presented with an optional Walmart customer-survey. If you answer the few short questions, \$100 in rewards points will be awarded to you.

[Please Go Here to Confirm Receipt & Claim Your Walmart Reward](#)

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.