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?
- 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?
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 money or 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.