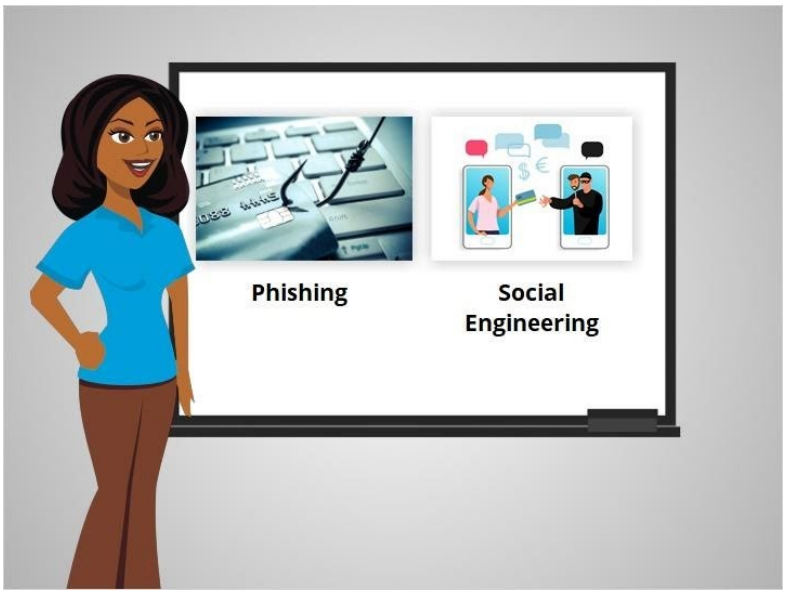
Online Fraud and Scams

Types of Scams

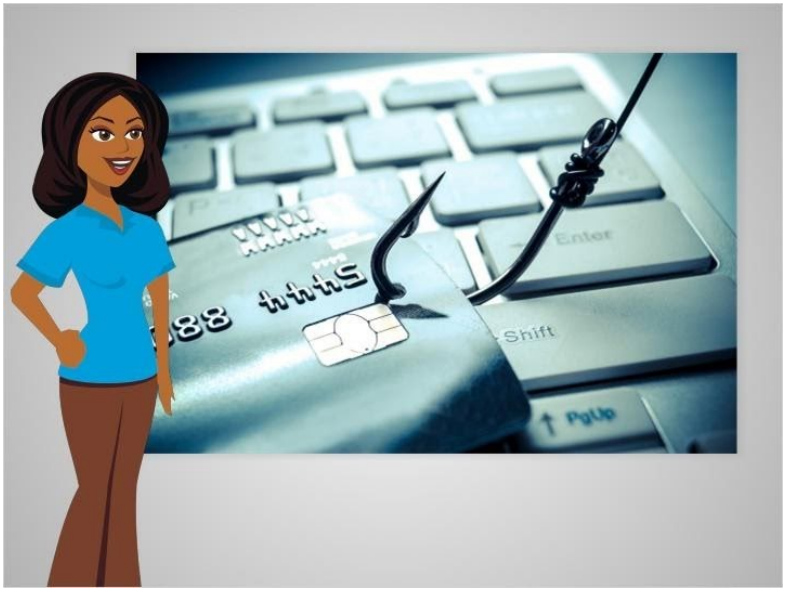
Hi, I'm Belle. There are many things you can do to protect yourself from fraud and keep your accounts and devices safe from online scams. We'll follow along with Albert to learn what types of scams are out there, how to recognize the warning signs, how to respond when you see a scam, and how to report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

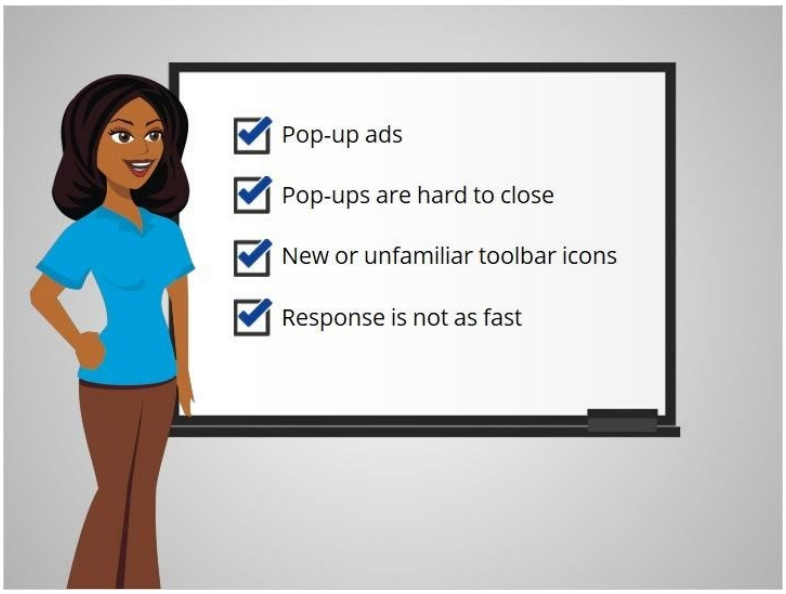
You may encounter these scams on a website, in an email or text message, or even in a pop-up window on your computer.



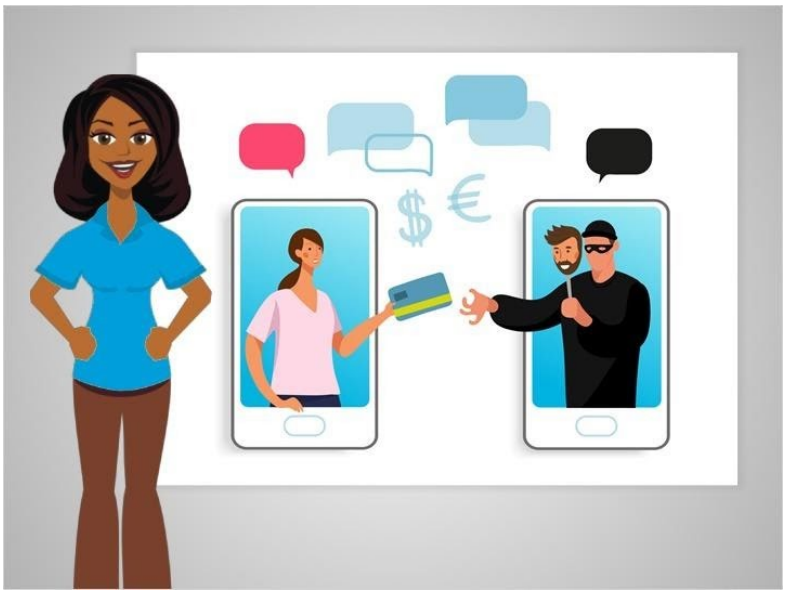
Let's begin by talking about phishing, which is a common type of scam. Phishing is when scammers use fake emails or text messages to "fish" for information.

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.



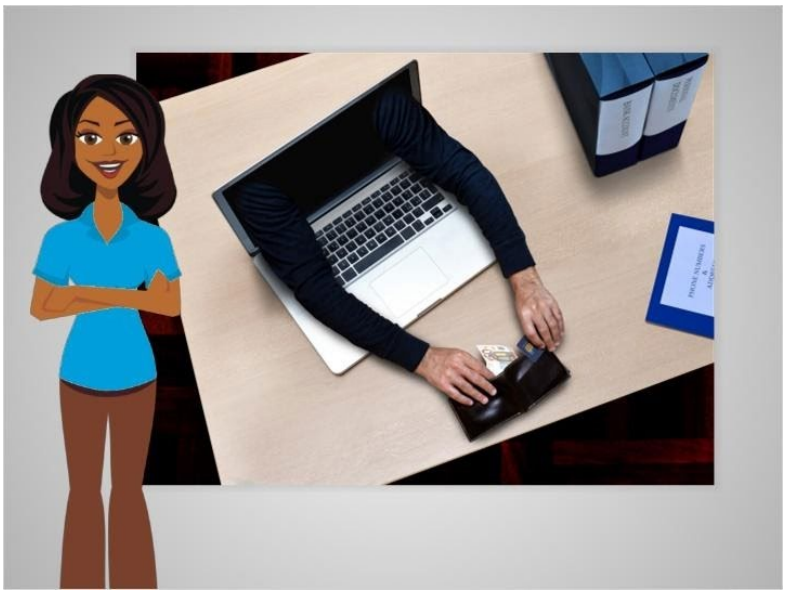
You may be able to tell when malware has been installed on your computer or device if you see these signs: pop-up ads appear and they are hard to close; new or unfamiliar toolbar icons appear on the screen; or your computer or mobile device is not responding as fast as it used to.



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.

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.

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

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.