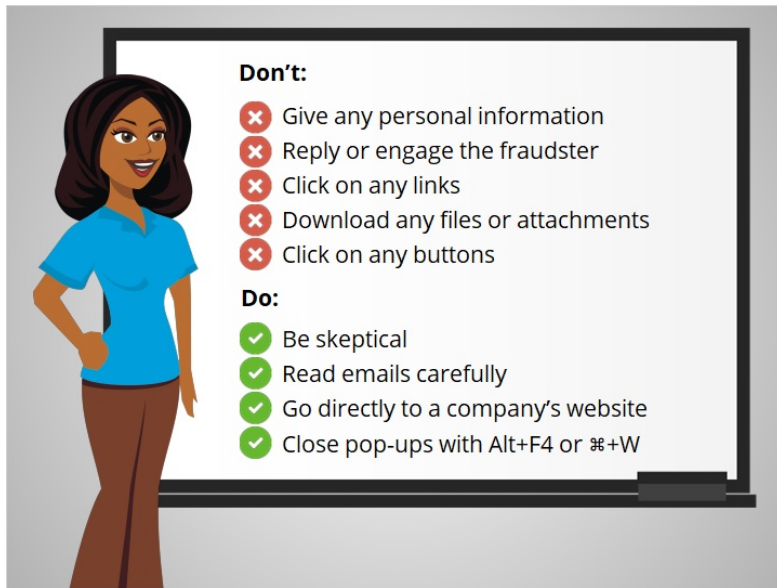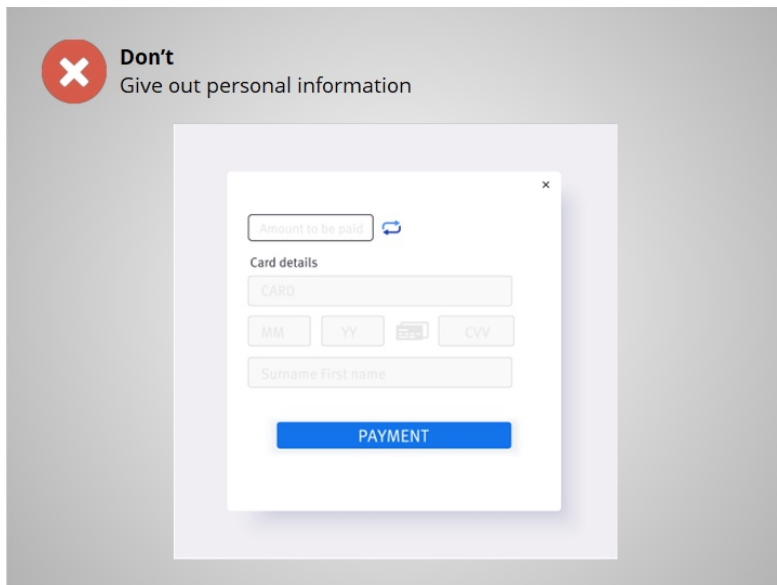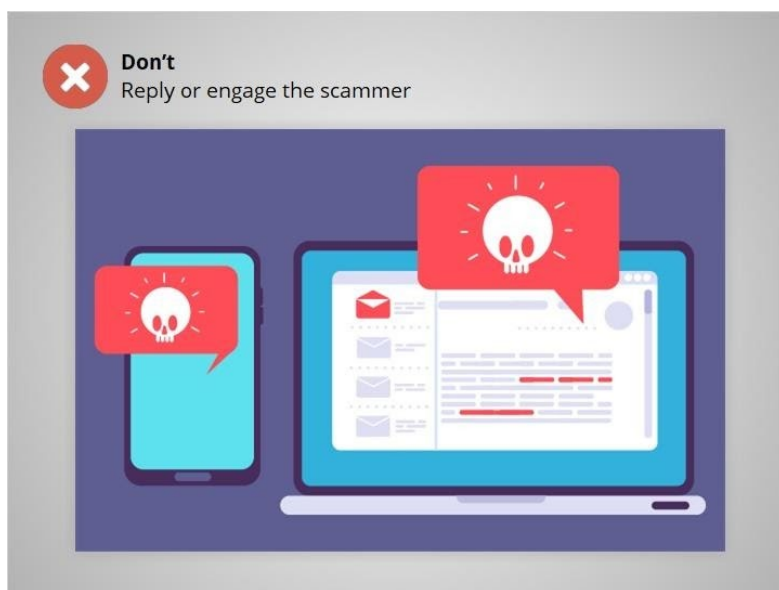# Online Fraud and Scams
What to Do with Scams

Now that Albert has learned how to recognize common frauds and scams, he wants to know what he can do when he encounters one.
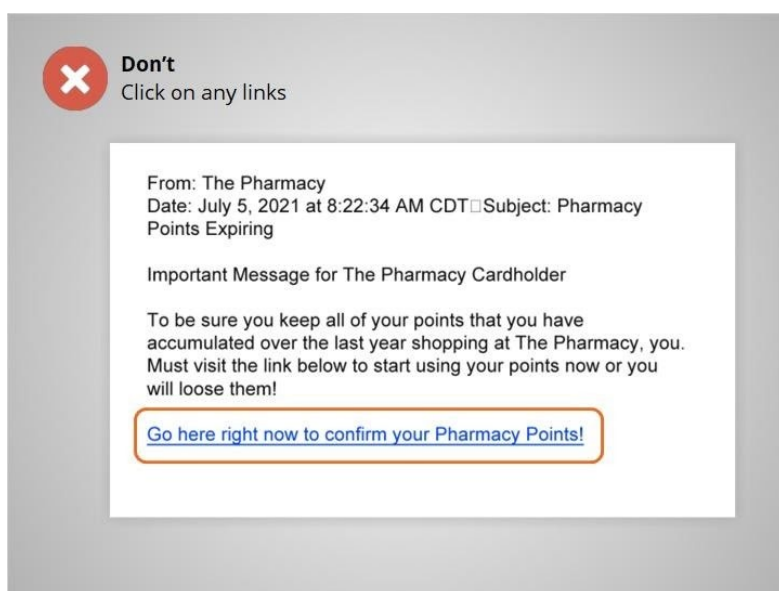
Here are some dos and don'ts. We'll go through each one.

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 only 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 untrustworthy websites.
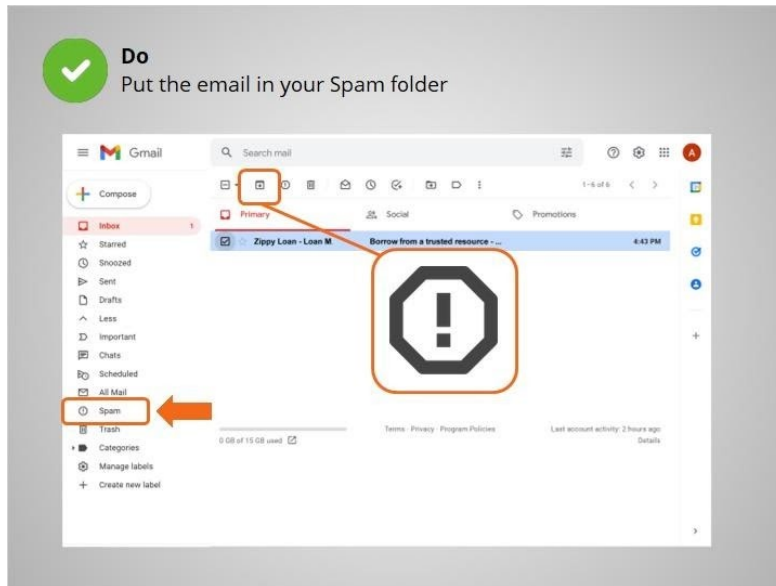
Don't
Download any files or attachments

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
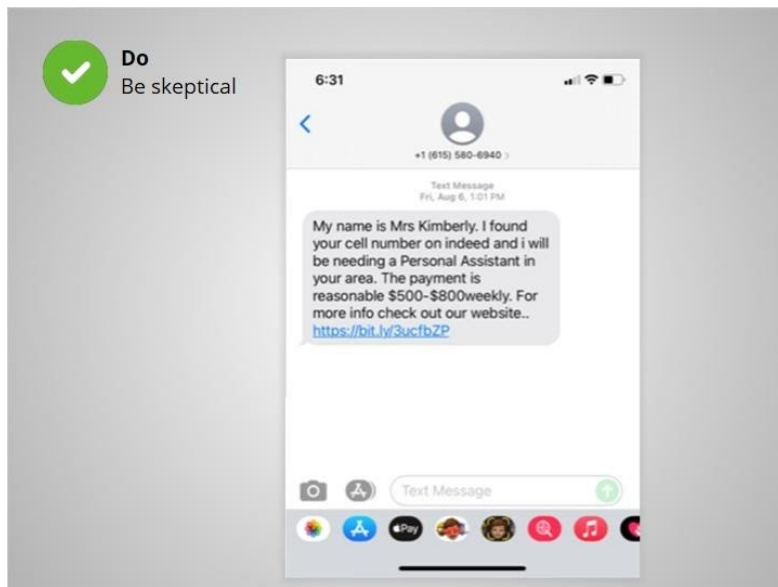
Do be skeptical. If you think something is a scam, it probably is.

Remember to read emails and text messages carefully, checking to make sure you know the sender.

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.
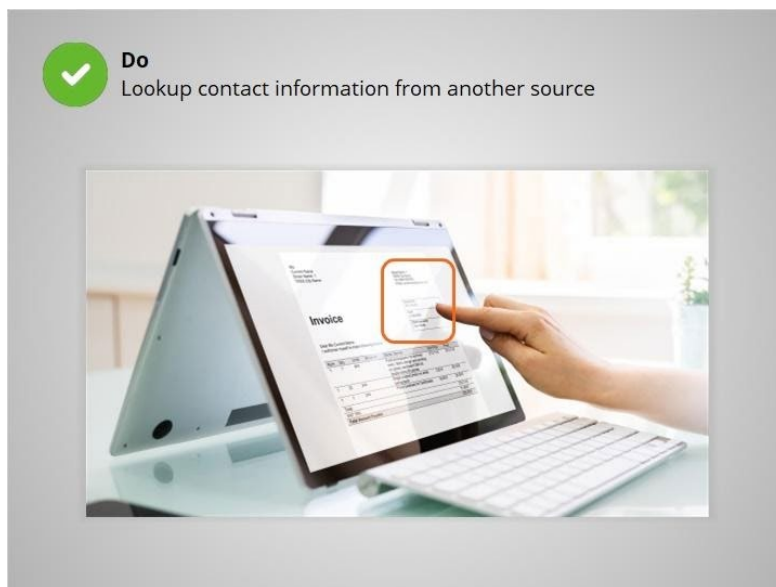
Do look up their contact information on your own, from a statement you've received in the mail or from their official website.
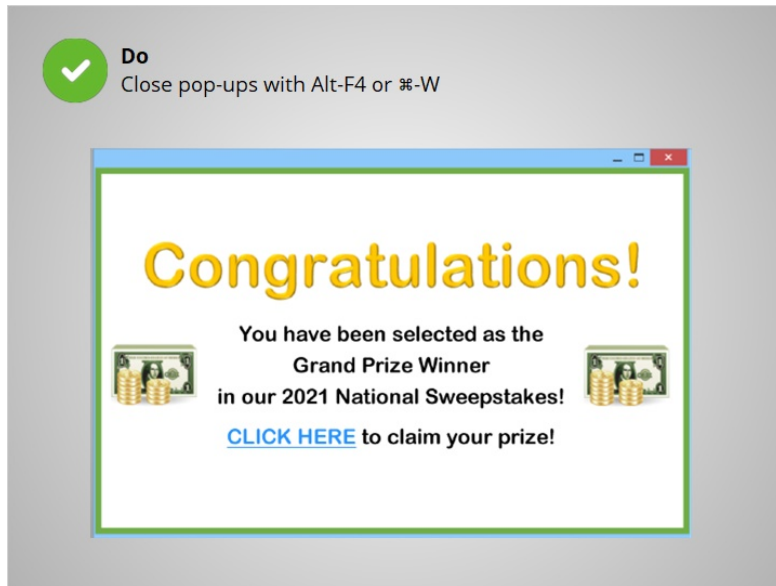
For pop-ups on a website, don't click on any buttons. Sometimes even the X will not close a scam pop-up window and may trigger more pop-ups to open instead.

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 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's won a prize. He thinks it's probably spam. How should Albert react to this scam email? Click the correct answer.

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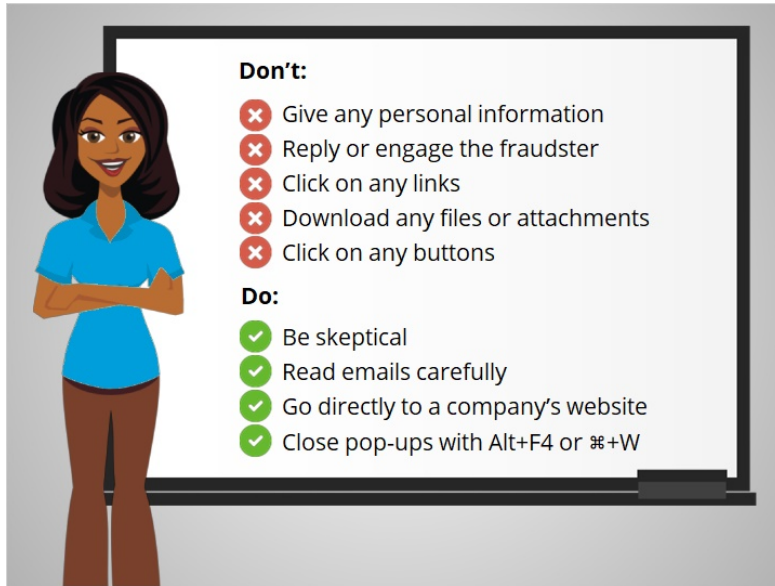
Now Albert knows what he can do when he encounters a scam on a website, in an email, or a text message. When Albert follows these tips, he can stay safe whenever he encounters a scam. In the next lesson, Albert will learn when an dhow to report scams.

Click on the blue button to end this lesson.