How to Spot an Email Phishing Scam

Countless scam emails are being circulated throughout the web everyday in the hopes of catching an unsuspecting victim. A phishing email is an email message that seeks to obtain important information about you by impersonating a legitimate company, organization or someone familiar to you.

For example, you may receive an email from Amazon stating that there is a problem with your recent order and you will need to log in to view and resolve the issue. A link to log in will be provided in the email for your "convenience", however instead of going to Amazon.com, you are directed to a fake login page where the email scammer can obtain your login credentials, and then ask to verify your credit card number or any other type of valuable information they want from you.

There are a number of tactics these phishing emails use to fool you, however with a bit of knowledge and careful inspection you can learn to identify most common ones and keep your sensitive information out of the wrong hands. Here are some ways to spot a phishing email:

1. Email sender and domain are mismatched
   Continuing with our Amazon email example, the email you

receive says it's from Amazon Customer Service, however the email address next to it says help@amzn.biz or some domain that looks similar to but is not amazon.com. Another tactic is to use the name amazon.com as a child domain to an entirely different parent domain. A child domain is placed on the left side of a parent domain, so for example amazon.com can be placed on the left side of maliciousdomain.com to form amazon.com.maliciousdomain.com. Although amazon.com is found in the email domain, it has no relationship to it whatsoever and can mislead you if you don't look closely at the full address.

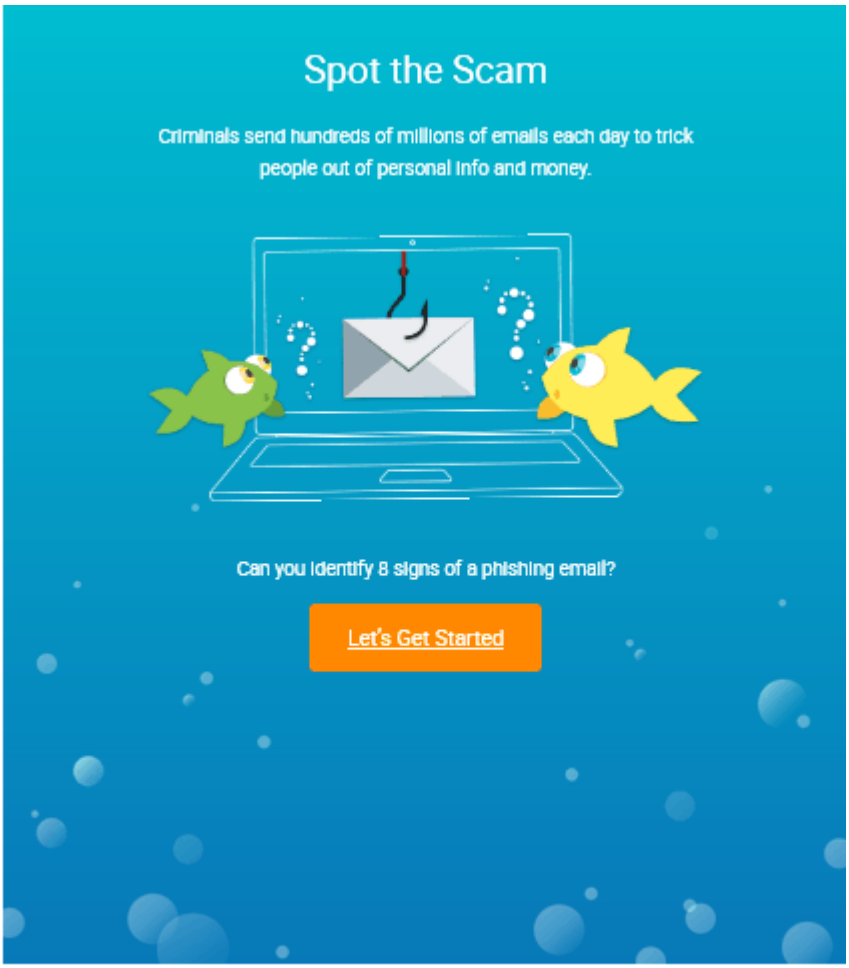
2. Link text in email and link address is mismatched
   A phishing email will often have a link to a open a web address in your browser called a hyperlink. The link text in the email may say Amazon.com login, which appears to look OK, however the actual address that is linked to the text but not immediately visible may be pointing at amzn.biz. The way to identify the hyperlink in the email is to hover your mouse pointer over it, which will usually cause the full web address beginning with http:// to appear down at the bottom of the email window or off to the side. As a general rule of safety, it is best to have a policy of not clicking on links in emails at all, but rather to visit the website manually in your browser if you do believe you have received a legitimate email requiring your attention.
3. You have no relationship with the sender
   This may sound obvious, but if you haven't ordered anything from Amazon.com, at least not recently, then clearly the email is a scam. Phishing attacks count on at least some recipients having a connection with the purported organization which lures them in.
4. Emails from the government or a financial institution asking for sensitive information
   In general, government agencies and financial institutions do not ask for important information in an

email. For example, phishing emails will often pose as being from the FBI, IRS or your local bank to scare you into thinking it's serious business that must be attended to. Such agencies will not use the email system to correspond with you about important matters requiring your immediate attention. If you are unsure, log into your bank or government website in your web browser the usual way you do to see if there is something important for you to respond to, or contact them directly by telephone and verify whether the email is from them or not.

5. It just doesn't look right, or looks too good to be true
   Emails making exaggerated claims such as "You won the lottery!", or that your grandson is stuck in London without his passport and needs a $2000 money wire immediately should be viewed with suspicion. Always follow your gut when something doesn't look right.
6. Poor spelling and grammar
   Emails from reputable companies and organizations are not going to be laden with spelling and grammatical errors and are an immediate tip off.
7. Email contains attachments
   An email from a known company or organization will usually not have an attached document unless you specifically requested it from someone. Never open an email attachment that you aren't expecting from someone, as many kinds of viruses and malware are circulated this way.

For additional insight and to practice spotting a phishing scam, AVG Technologies posted an exercise on their website called Spot the Scam! , which will help you spot phishing clues in an interactive environment. Give it a try!

•



Signal ⟩ Security ⟩ Trends ⟩ Spot the Scam!

~Ted Eiler