How to recognize phishing emails

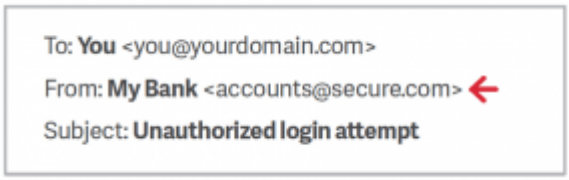
Phishing email messages, websites, and phone calls are designed to steal money, steal data and/or destroy information. Cybercriminals can do this by installing malicious software on your computer or stealing personal information off of your server or computer.

Cybercriminals also use social engineering to convince you to install malicious software or hand over your personal information under false pretenses. They might email you, call you on the phone, or convince you to download something off of a website.

Don't trust the display name

A favorite phishing tactic among cybercriminals is to spoof the display name of an email. Return Path analyzed more than 760,000 email threats targeting 40 of the world's largest brands and found that nearly half of all email threats spoofed the brand in the display name.

Here's how it works: If a fraudster wanted to spoof the hypothetical brand "My Bank," the email may look something like:



Since My Bank doesn't own the domain "secure.com," DMARC will not block this email on My Bank's behalf, even if My Bank has set their DMARC policy for mybank.com to reject messages that fail to authenticate. This fraudulent email, once delivered, appears legitimate because most user inboxes only present the display name. Don't trust the display name. Check the email address in the header from—if looks suspicious, don't open the email.

If you receive an email or even an instant message from someone you don't know directing you to sign in to a website, be wary, especially if that person is urging you to give up your password or social security number. Legitimate companies never ask for this information via instant message or email, so this is a huge red flag. Your bank doesn't need you to send your account number -- they already have that information. Ditto with sending a credit card number or the answer to a security question.

You also should double-check the "From" address of any suspicious email; some phishing attempts use a sender's email address that is similar to, but not the same as, a company's official email address.

How to recognize phishing emails

Look but don't click

Hover your mouse over any links embedded in the body of the email. If the link address looks weird, don't click on it. If you want to test the link, open a new window and type in website address directly rather than clicking on the link from unsolicited emails.

Typically, phishing scams try to convince you to provide your username and password, so they can gain access to your online accounts. From there, they can empty your bank accounts, make unauthorized charges on your credit cards, steal data, read your email and lock you out of your accounts.

Often, they'll include embedded URLs that take you to a different site. At first glance, these URLs can look perfectly valid, but if you hover your cursor over the URL, you can usually see the actual hyperlink. If the hyperlinked address is different than what's displayed, it's probably a phishing attempt and you should not click through.

Another trick phishing scams use is misleading domain names. Most users aren't familiar with the DNS naming structure, and therefore are fooled when they see what looks like a legitimate company name within a URL. Standard DNS naming convention is Child Domain dot Full Domain dot com; for example, info.LegitExampleCorp.com. A link to that site would go to the "Information" page of the Legitimate Example Corporation's web site.

A phishing scam's misleading domain name, however, would be structured differently; it would incorporate the legitimate business name, but it would be placed before the actual, malicious domain to which a target would be directed. For instance, Name of Legit Domain dot Actual Dangerous Domain dot com: LegitExampleCorp.com.MaliciousDomain.com.

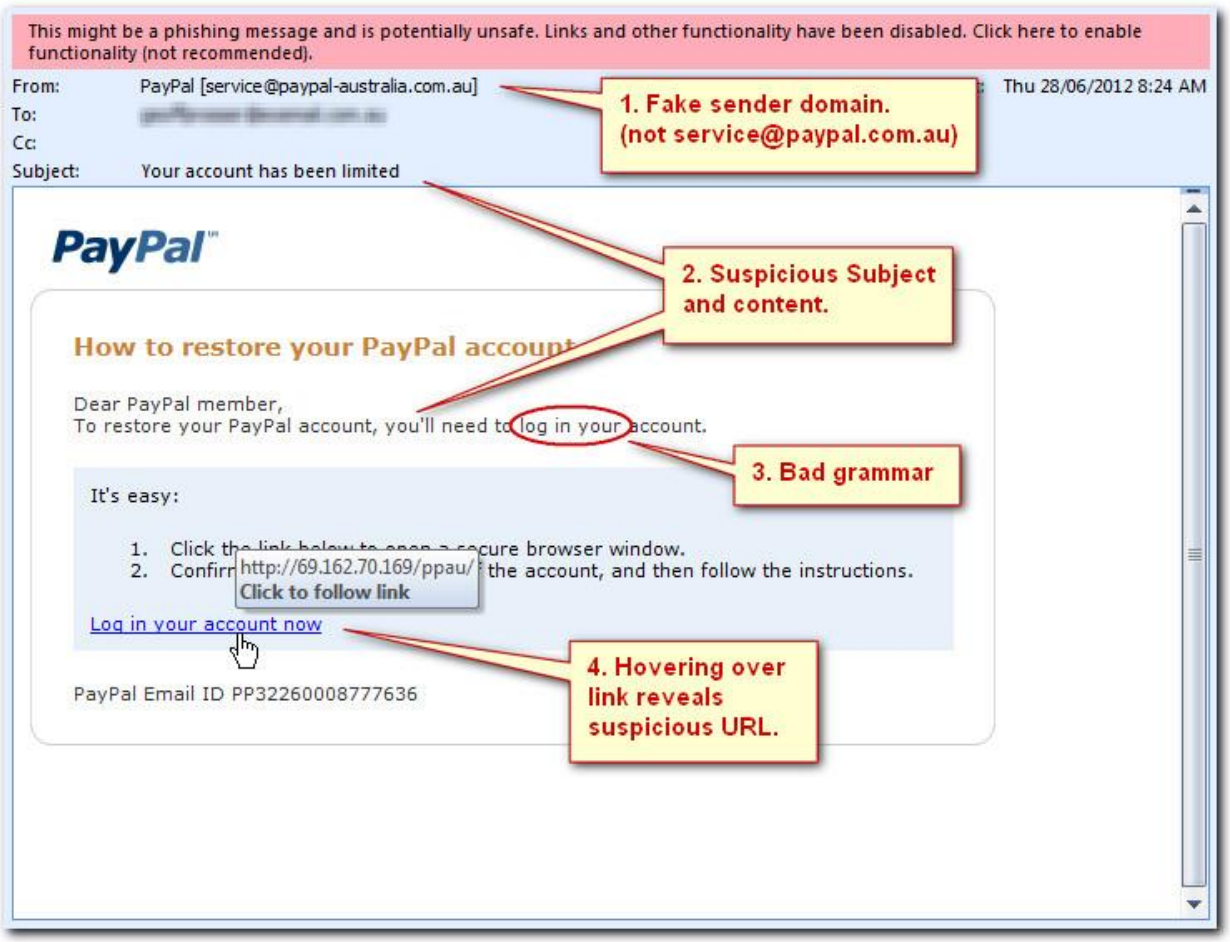
To an average user, simply seeing the legitimate business name anywhere in the URL would reassure them that it was safe to click through. Spoiler alert: it's not.

Check for spelling mistakes

Brands are serious about email. Legitimate messages usually do not have major spelling mistakes or poor grammar. Read your emails carefully and report anything that seems suspicious. It's highly unlikely that a corporate communications department would send messages to its customer base without going through at least a few rounds of spelling and grammar checks, editing and proofreading. If the email you receive is riddled with these errors, it's a scam.

You should also be skeptical of generic greetings like, "Dear Customer" or "Dear Member." These should both raise a red flag because most companies would use your name in their email greetings.

How to recognize phishing emails



Analyze the salutation

Is the email addressed to a vague "Valued Customer?" If so, watch out—legitimate businesses will often use a personal salutation with your first and last name.

Don't give up personal information

Legitimate banks and most other companies will never ask for personal credentials via email. Don't give them up.

Beware of urgent or threatening language in the subject line

Invoking a sense of urgency or fear is a common phishing tactic. Beware of subject lines that claim your "account has been suspended" or your account had an "unauthorized login attempt." "Urgent action required!" "Your account will be closed!" "Your account has been compromised!" These intimidation tactics are becoming more common than the promise of "instant riches"; taking advantage of your anxiety and concern to get you to provide your personal information. Don't hesitate to call your bank or financial institution to confirm if something just doesn't seem right. And scammers aren't just using banks, credit cards and email providers as cover for their scams, many are using the threat of action from

government agencies like the IRS and the FBI to scare unwitting targets into giving up the goods. An important point: government agencies, especially, do not use email as their initial means of communication.

Review the signature

Lack of details about the signer or how you can contact a company strongly suggests a phish. Legitimate businesses always provide contact details.

Don't click on attachments

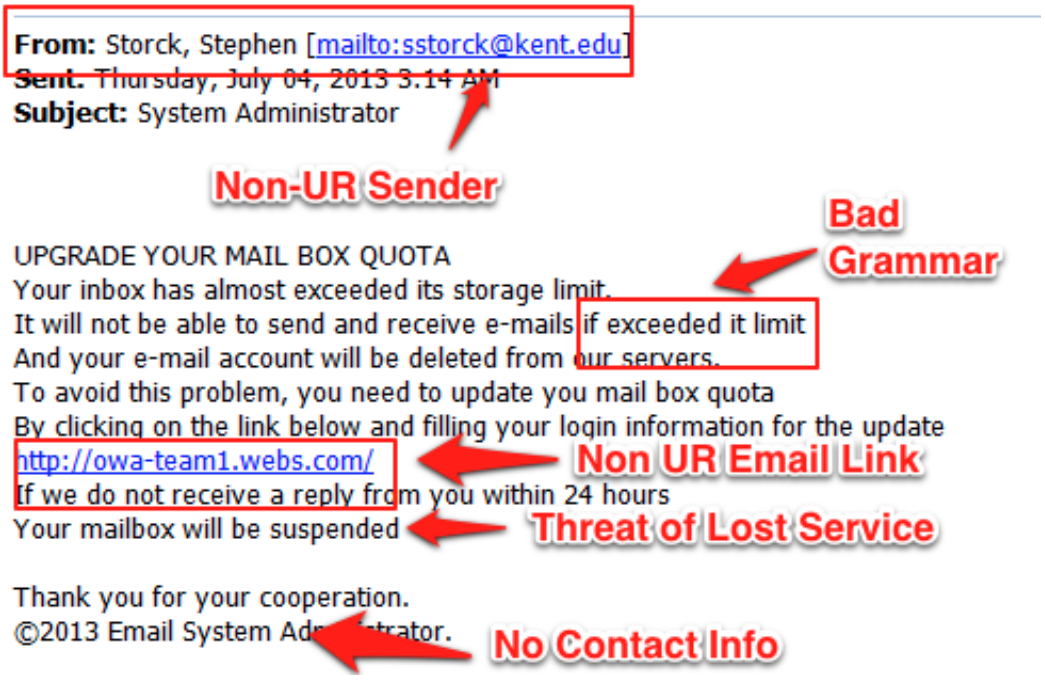
Including malicious attachments that contain viruses and malware is a common phishing tactic. Malware can damage files on your computer, steal your passwords or spy on you without your knowledge. Don't open any email attachments you weren't expecting.

Don't trust the header from email address

Fraudsters not only spoof brands in the display name, but also spoof brands in the header from email address. Return Path found that nearly 30% of more than 760,000 email threats spoofed brands somewhere in the header from email address with more than two thirds spoofing the brand in the email domain alone.

Don't believe everything you see

Phishers are extremely good at what they do. Just because an email has convincing brand logos, language, and a seemingly valid email address, does not mean that it's legitimate. Be skeptical when it comes to your email messages—if it looks even remotely suspicious, don't open it.



How to recognize phishing emails