What make an Email suspicious?

Any email, or a link within an email, that asks you to disclose any of your banking or personal information. Those emails are **Phishing** or **Email Spoofing**.

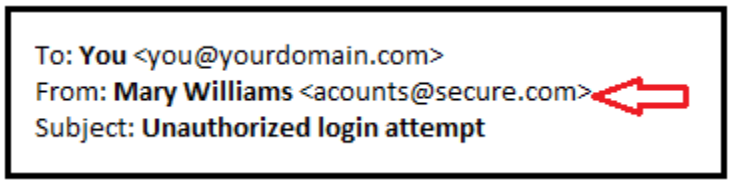
Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Email spoofing is the creation of email messages with a forged sender address.

How to identify a phishing or spoofing email

1. **Don't trust the display name** - A favorite phishing tactic among cybercriminals is to spoof the display name of an email.

   Here is how it works: If a fraudster wanted to spoof the hypothetical "Mary Williams", the email may look something like:

   This fraudulent email, once delivered, appears legitimate because most user inboxes only present the display name. Do not trust the display name. Check the email address in the header from — if looks suspicious, do not open the email, and delete the email.

2. **Look but do not click -** Hover your mouse over any links embedded in the body of the email. If the link address looks weird, do not 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.

3. **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.

4. **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.

5. **Do not give up personal information** - Legitimate banks and most other companies will never ask for personal credentials via email. Do not give them up.

6. **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.”

7. **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.

8. **Do not 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. Do not open any email attachments you were not expecting.

9. **The offer seems too good to be true** - There is an old saying that if something seems too good to be true, it probably is. That holds especially true for email messages. If you receive a message from someone unknown to you who is making big promises, the message is probably a scam.

10. **Don't forward chain email messages** - Not only do you lose control over who sees your email address making your address susceptible to attacks, but you also may be furthering a hoax or aiding in the delivery of a virus.