

How to Spot a Phishing Email

What Is Phishing?

Phishing is a tactic used by cybercriminals to steal information or gain unauthorized access by posing as a trusted person or organization. These attacks commonly occur by email, leading to data breaches, service disruptions, identity theft, and more.

Signs of a Phishing Email

Suspicious Sender:

Be careful if you don't recognize the sender. Phishing attempts often have altered email addresses that don't match who they say they are.

Generic Greetings:

Phishing emails sometimes use generic greetings like "Dear User" or "Hello [Username]" instead of your actual name.

Spelling and Formatting:

Official communications are typically well-written and free of noticeable errors.

Urgent or Threatening:

Phishing attempts often use urgency or threats. Don't let them pressure you into a hasty decision.

Unusual URLs:

Before clicking a link, hover your mouse over it to ensure the URL matches what it says. Avoid following links that seem unrelated or suspicious.

Unexpected Attachments:

Be cautious with unexpected attachments, especially from an unknown sender. They may contain malware.

Information Requests:

Avoid sharing sensitive information with untrusted sources. Instead, contact the person or organization directly to verify the request.

Suspect Phishing? What to Do Next



Do Not Click

Avoid clicking links or attachments, and do not reply to the message



Send to IT

Forward the email to your IT security team and note that it's phishing.



Mark as Spam

Flag the message as spam to alert the IT team and to help protect others.



Delete Message

Once forwarded to IT and marked as spam, delete it. Do not keep it.



Stay Alert

Watch for any other unusual activity, whether via email, text, or phone call.