

Checklist for Identifying Phishing and Spam Emails

This checklist will provide insights on how to identify phishing and spam emails.

Indicators of a Phishing and Spam Email	
<input type="checkbox"/>	Check for unexpected attachments from unknown users, clients, vendors, or peers
<input type="checkbox"/>	Attachments with unusual or unrecognized formats
<input type="checkbox"/>	Identify the differences in the email ID of the sender and display names
<input type="checkbox"/>	Check for incomplete or incorrect email IDs or organization names or that use numbers in place of letters in the name
<input type="checkbox"/>	Check for generic greetings such as “Dear users” or “Dear customers”
<input type="checkbox"/>	Check links that display a different website or URL when hovered on or have a URL with an incorrect name or domain
<input type="checkbox"/>	Check for emails presenting offers that are too attractive to believe, such as the user winning a lottery, a competition, or a free subscription or vacation, and job offers
<input type="checkbox"/>	Check for emails that do not have a complete signature and contact details of the sender
<input type="checkbox"/>	Check for obvious misspellings and strange uses of punctuation
<input type="checkbox"/>	Verify messages asking for charity donations can be suspicious and need verification
<input type="checkbox"/>	Be careful with emails that appear to be from the bank, financial institution, organization, service provider, or other associates, asking to reveal sensitive information

<input type="checkbox"/>	Check for spoofed sender names and email addresses to make victims believe that mail originated from the actual senders
<input type="checkbox"/>	When the sender's name and email address appear from the actual sender, the format of the email must be verified with old emails received from that sender.
<input type="checkbox"/>	Verify the complete address of the links provided in the email to ensure that the links are not redirected to malicious websites.
<input type="checkbox"/>	Verify the images and signatures in the email as attackers do not focus on using high-quality pictures most of the time.
<input type="checkbox"/>	Scan all attachments in the email before opening them, even though the sender's name, email address, and email format are correct.
<input type="checkbox"/>	Verify the links to shared drives such as Google Suite, Dropbox, and Office 365 before clicking.
<input type="checkbox"/>	Verify the email header for the true source of the sender
<input type="checkbox"/>	Verify the IP addresses of attackers/campaigns