7 Key Ways to Spot Malicious Emails

#1 Beware the display name

Hackers who are phishing for entry into your email networks often spoof the display name on an email. For example, “From: Your Bank <accountmanagers@secure.com>

Since most inboxes only present the display name, “Your Bank,” users won’t see the fraudulent tail of “secure.com,” which the bank doesn’t own. If you’re in doubt, check the email address in the header form in full. If it looks suspicious, don’t open.

#2 Check for spelling mistakes

Companies are pretty serious about email, so you can expect error-proof copy. Poor grammar and spelling mistakes signal something is amiss. Report anything suspicious.

#3 Analyze the greeting

Companies love to personalize emails these days. A salutation like “Dear Valued Customer” could be the giveaway you're dealing with a hacker.

#4 Beware of urgent, threatening language in subject line

Scare tactics are the territory of malicious emails. Fear makes a great phishing tactic; however, anytime you see something along the lines of an “unauthorized sign on attempt,” be suspicious.

#5 Inspect the signature

Lack of details about the signer suggests a phishing email. Legitimate emails provide contact details.

#6 Avoid clicking attachments

Malicious attachments and malware in attachments is a common phishing tactic. Don’t open yourself to malware which will spy on your usage, steal passwords and damage your files.

#7 Suspect images

Expect professional email phishers to place brand logos, specific language and a seemingly valid email address in attempts to appear valid. If anything - at all - looks off, don’t open.