

How to Detect a phishing E-mail

With the recent increase in Ransomware infections instigated through phishing emails, it is critical to take proactive measures to protect yourself and your organization's security. Vigilance in detecting phishing emails and educating your employees to be proactive and recognize risk is a crucial step in protecting your organization.

Don't trust the display name

Just because an email says it's coming from the name of a person you know or trust, doesn't mean that it truly is. Be sure to look at the email address to confirm the true sender. Better yet, give the person a quick phone call - particularly when sending or receiving money.

Look, don't click

Don't click links within an e-mail that you are at all suspicious of. The objective of a phishing attack is usually to get you to download an attachment or to click on a link. When in doubt, hover your mouse over the text of the hyperlink to see the full URL.

Be wary of attachments

Often phishing emails are ones with malicious attachments which are infected with viruses or other malware. These attachments may be disguised as an invoice, a delivery note, or something else that is designed to encourage you to open it.

Consider the salutation

Is the message addressed to a generic recipient, such as "Valued customer" or "Sir/Madam?" If so, it's likely spam. Legitimate businesses are much more likely to use your real first and last name, particularly if you have established a relationship.

Protect your personal information

Watch for messages asking for personal information such as account numbers, log in credentials, Social Security numbers, or other personal information. Legitimate companies will never ask for these details over email.

Be aware of urgency

Be suspicious of emails that claim you must click, call, or open an attachment immediately. Often, they'll claim you have to act now to claim a reward or avoid a penalty. Creating a false sense of urgency is a common trick of phishing attacks and scams.

Check the email signature

Most legitimate senders will include a full signature block at the bottom of their emails. Phishing emails often leave out important information in the signature, so be cautious of signature details that are incomplete or inaccurate.

Check for spelling errors

While legitimate companies are very strict about emails they send out, Phishing emails often contain poor spelling or grammar.

It looks familiar or expected

Watch out for messages disguised as something expected, like a shipment, password reset, or payment notification. These emails often contain links to malware sites that request your log in credentials or personal information.

Stay vigilant and double-check

Trust your instincts, even if something seems slightly out of the norm, it's better to be safe than sorry. When in doubt, reach out to your I.T. Provider. Quickly double checking the legitimacy of a sender or email could prevent a costly mistake.