9 Common Signs of a Phishing Email

1. An Unfamiliar Tone or Greeting

The first thing that usually arouses suspicion when reading a phishing message is that the language isn't quite right – for example, a colleague is suddenly over familiar, or a family member is a little more formal. If a message seems strange, it's worth looking for other indicators that this could be a phishing email.

2. Grammar and Spelling Errors

One of the more common signs of a phishing email is bad spelling and the incorrect use of grammar. Most businesses have the spell check feature on their email client turned on for outbound emails. It is also possible to apply autocorrect or highlight features on most web browsers. Therefore, you would expect emails originating from a professional source to be free of grammar and spelling errors.

3. Inconsistencies in Email Addresses, Links & Domain Names

Another simple way to identify a potential phishing attack is to look for discrepancies in email addresses, links and domain names. For example, it is worth checking against previous correspondence that originating email addresses match. If a link is embedded in the email, hover the pointer over the link to verify what 'pops up'. If the email is allegedly from PayPal, but the domain of the link does not include "paypal.com," that's a huge giveaway. If the domain names don't match, don't click.

4. Threats or a Sense of Urgency

Emails that threaten negative consequences should always be treated with suspicion. Another tactic is to use a sense of urgency to encourage, or even demand, immediate action in a bid to fluster the receiver. The scammer hopes that by reading the email in haste, the content might not be examined thoroughly so other inconsistencies associated with a phishing campaign may pass undetected.

5. Suspicious Attachments

If an email with an attached file is received from an unfamiliar source, or if the recipient did not request or expect to receive a file from the sender of the email, the attachment should be opened with caution. If the attached file has an extension commonly associated with malware downloads (.zip, .exe, .scr, etc.) – or has an unfamiliar extension – recipients should flag the file to be virus-scanned before opening.

6. Unusual Request

If the email is asking for something to be done that is not the norm, then that too is an indicator that the message is potentially malicious. For example, if an email claims to be from the IT team asking for a program to be installed, or a link to patch the PC followed, yet this type of activity is typically handled centrally, that's a big clue that you have received a phishing email and you should not follow the instructions.

7. Short and Sweet

While many phishing emails will be stuffed with details designed to offer a false security, some phishing messages have also been sparse in information hoping to trade on their ambiguity. For example, a scammer that spoofs an email from Jane at a company that is a preferred vendor emailing the company once or twice weekly, has the vague message 'here's what you requested' and an attachment titled 'additional information' in hopes they'll get lucky.

8. Recipient Did Not Initiate the Conversation

Because phishing emails are unsolicited, an often-used hook is to inform the recipient he or she has won a prize, will qualify for a prize if they reply to the email, or will benefit from a discount by clicking on a link or opening an attachment. In cases where the recipient did not initiate the conversation by opting in to receive marketing material or newsletters, there is a high probability that the email is suspect.

9. Request for Credentials, Payment Information or Other Personal Details

One of the most sophisticated types of phishing emails is when an attacker has created a fake landing page that recipients are directed to by a link in an official looking email. The fake landing page will have a login box or request that a payment is made to resolve an outstanding issue. If the email was unexpected, recipients should visit the website from which the email has supposedly come by typing in the URL – rather than clicking on a link – to avoid entering their login credentials of the fake site or making a payment to the attacker.