How to Protect Your Data from Email Phishing Attacks

There are many different types of phishing scams, but email remains the most common of them all. Responding to a sender, clicking on a link, or downloading a file that may not be trustworthy can lead to data corruption, leaked confidential information, and infected devices or networks.

Here is how to avoid becoming a phishing victim:

1

INSPECT THE SENDER'S EMAIL ADDRESS
Phishing involves using email addresses that contain suspicious elements to target victims, even sometimes spoofing a well-known site or brand. Be on the lookout for changed or added words or characters, as well as misspelled words within a domain name.

2

EXAMINE THE MESSAGE'S GREETING AND TONE
Be wary of emails that utilize a generic greeting and an urgent tone. Phishing emails target many people at once and implore the recipient to take immediate action, usually without a personalized opening line.

3

LOOK FOR VERIFIABLE SENDER CONTACT INFORMATION
Avoid responding to emails that don't contain any return contact information for the sender, such as a phone number, email address, or office location.

4

DON'T SEND SENSITIVE INFORMATION VIA EMAIL
Even if the email has an urgent tone, never divulge confidential information in reply to an email. Cyber criminals leverage social engineering techniques to obtain personal data like names, addresses, banking information, and more that can be used for fraudulent activity.

5

AVOID CLICKING ON UNEXPECTED LINKS
Don't click on links that come from unfamiliar email senders or organizations. You may be redirected to a website or start a download that can compromise your data or infect your device.

6

AVOID OPENING UNTRUSTWORTHY EMAIL ATTACHMENTS
Avoid opening email attachments from untrustworthy senders or simply to satisfy your curiosity. Suspicious attachments can be carriers of malware and ransomware payloads that can corrupt your data and harm your device.

7

INSTALL A PHISHING FILTER FOR YOUR EMAIL CLIENT
Ensure that you have a phishing filter that works with your desktop email software of choice. You can also install one for use in your browser. While it won't keep out all phishing messages, it will greatly reduce the number of attempts that show up in your inbox.