5 WAYS TO AVOID A PHISHING ATTACK

A **phishing attack** is a fake email designed by malicious hackers and thieves to look like it's coming from a trusted brand or institution–including your employer. The goal is to get you to click on the links and/or open an attachment.

Once you lower your guard and give up your personal information, financial data, or account logins, this information can be used to breach your employer's systems or compromise your identity.

The best way to defend yourself against phishing attacks is to **identify them before you can become a victim**. Here are five quick ways to identify and avoid a phishing attack in your inbox.

1 Who is the real sender?

Does the organization the email is supposed to be from match the address inside the "< >s"? Most phishing attacks are sent from an individual email account that has nothing to do with the organization, or it's close to the real thing...but not close enough [amaz0n.com vs. amazon.com]

FROM
John Doe <avnet.secure@malware.com>

TO
You <your-email@avnet.com>

2 Check the salutation

If the email comes from a brand or institution you do business with, **your name should always appear in the first line** of the email itself. If it says "Dear customer," or something equally impersonal, that's a warning sign.

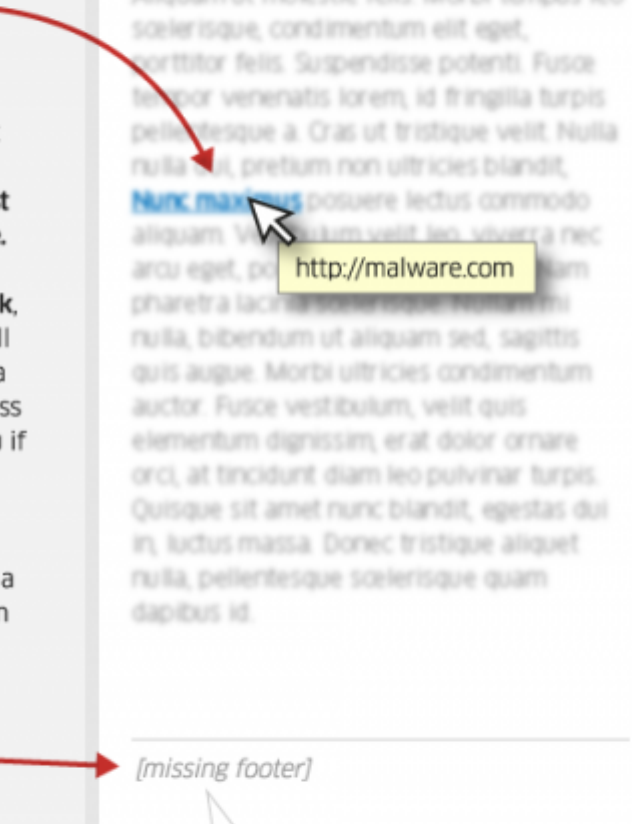
Dear customer,

3 Use your "mouse hover"

The most effective tool we have to defend ourselves against phishing attacks is the mouse hover. It tells us where any hyperlink or button in an email wants to take you without having to click the link. **To use it, just hover over any email links with your mouse.**

CAUTION: Do not click the link, just hover over it, and you'll see a bubble pop up with a URL in it. That is the address where the link will take you if you click on it.

If the destination address in the bubble doesn't lead to a site you'd expect, it's likely a phishing attack. Hover over the other links in the email. If it's a phishing attack, they'll all have the same destination.



4 What's in the footer?

The footer of any legitimate email should contain, at a minimum:

- **A physical address for the institution or brand**
- **An unsubscribe option**

If it lacks either of these items, it's probably fake.

[missing footer]

TrustedCorp • 1st Street, Phoenix AZ 85001

To stop receiving these emails, unsubscribe now.

5 When in doubt, delete

If you don't know the sender or if you are not sure if an email is authentic, delete it. Don't underestimate your instincts. If something feels wrong, it probably is. If it's legitimate, they will make sure to get in contact you another way or send the message again.

Trash Reply