Did you know that 90% of modern data breaches now involve a phishing attack?

These attacks usually consist of fake emails designed to look like they’re coming from a brand or institution that you trust.

Their goal is to entice you to click a link or download an attachment, which, in turn, puts malicious files on your computer. This can enable hackers to steal your identity, breach your employer’s systems, and more.

The best way to defend yourself against phishing attacks is to identify phony emails before you click on them.

WAYS TO AVOID A PHISHING ATTACK

From: trusted-brand@domain.com
To: your-email@domain.com

1. Who’s the real sender?
   Make sure the organization name in the “From” field matches the address between the brackets. Watch out for addresses that contain typos in the organization name (think amaz0n.com).

2. Check the salutation
   If you do business with an organization, the first line of the email should always contain your name. Don’t trust impersonal introductions like “Dear Customer.”

3. Use your mouse hover
   Hover over an email link to see the full URL it will direct you to. Do NOT click the link—just hover. If the address isn’t where you’d expect to go, don’t click it. Check all the links—if the URLs are all the same, it’s likely a phishing email.

4. What’s in the footer?
   The footer of any legitimate email should contain, at minimum:
   • A physical address for the brand or institution
   • An unsubscribe button
   If either of these items are missing, it’s probably fake.

5. When in doubt, delete
   If you don’t know the sender, or even if something seems off, delete the email. If it’s not fake, the sender will contact you another way or send the message again.