5 ways to avoid a phishing attack

Did you know that 90% of modern data breaches now involve a phishing attack?[1]

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

Clicking the wrong link can allow bad actors to install malware, steal login credentials, or gain a foothold into your company's systems.

The best defense? Know what to look for before you click.

Here are five quick ways to spot a hoax:

1 Inspect the sender with care

Phishing emails often spoof familiar names but use suspicious domains. Watch for extra characters, misspellings, or odd addresses (like alerts@amaz0n-support.io).

2 Generic greeting? Be suspicious.

If a company you use refers to you as "Customer" or "Sir/Madam," treat the message with caution. Legitimate brands usually address you by name.

3 Hover but don't click

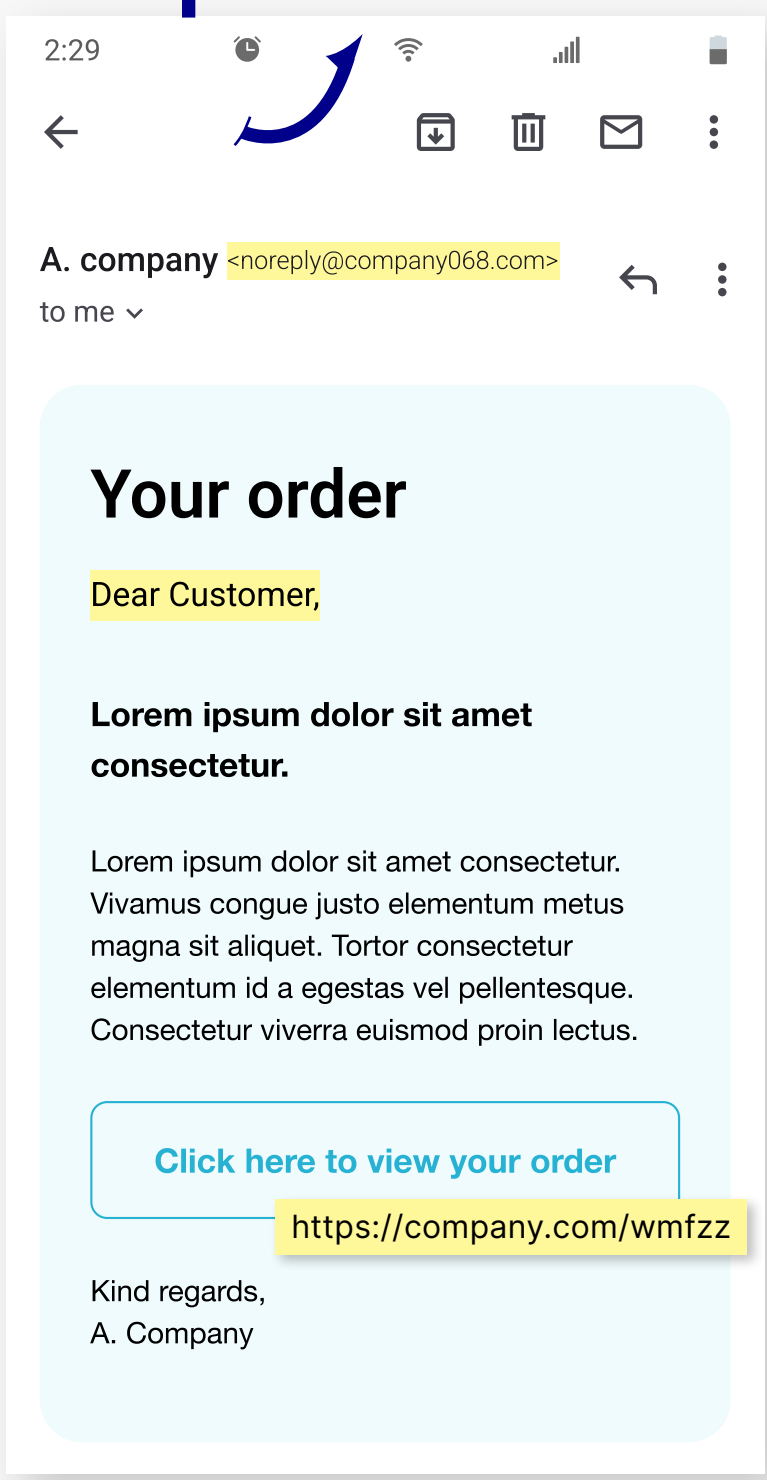
Before you click on a link, hover over it to preview the real URL. If it redirects somewhere sketchy or doesn't match the brand, don't click. Even shortened URLs can be deceptive, so use a URL expander tool if needed.

4 What's in the footer?

No physical address? No unsubscribe option? That's a major red flag. All legitimate marketing emails include this information to comply with anti-spam laws.

5 When in doubt, throw it out

Trust your gut. If anything feels off—even just the tone—delete the email. Phishing relies on urgency and emotion to push you into clicking fast.



cybersecurity.opentext.com

1 OpenText, *2025 Threat Report Nearly 50% of AI-driven phishing attacks bypass basic spam filters*