5-Step Checklist To Prevent Phishing Attacks

CYBERLOGIC
www.cyberlogic.co.za
hello@cyberlogic.co.za
086 111 1202

Simply go through this 5-step checklist every time you receive an email to prevent becoming a potential victim of cyber attackers.

1 Check the FROM address

Attackers often create fake domains which look very similar to the legitimate one - “name@cyberlogic.co.za” is not “name@cybercyber.co.za”. Similarly, “name@cyberlogic.top” is not a trusted mail address.

2 Inspect links

Hover over any links to make sure that it points to a trusted domain. If you are on mobile phone, copy and paste the link into a note application. If the link is shortened (for example “shorturl.at/mruPZ” but points to “www.google.com”), ask your Technical Support team to inspect it.

3 Question attachments

If the email contains an attachment, be sure that the above two actions check out. Cyberlogic offers protection to prevent malware from being transferred via email. But always rather escalate the email to your Technical Support team if you feel something might be suspicious.

4 Look for things that seem off

If your email passes all initial checks but seems strange in nature, reach out to the party via another method such as a phone call to verify the request.

5 Be extremely wary

Attackers like to play on their victim's emotional reactions and construct emails such as winning a competition or potentially missing paychecks due to incorrect filing. Be wary as we often click and skip safety checks due to the sense of urgency.