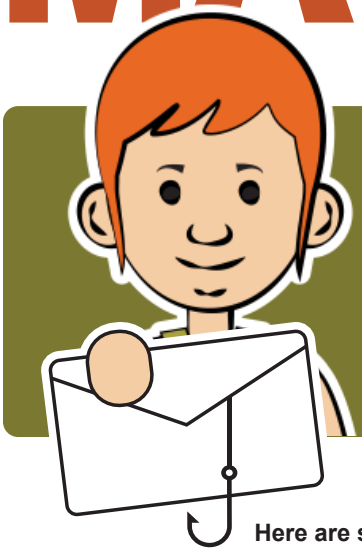
HOW DO YOU KNOW IF A LINK IS MALICIOUS?



Cybercriminals use links in phishing emails to try to trick you into sharing sensitive information.

These fraudulent links, disguised as trustworthy, lead to malicious websites that can trick you into sharing sensitive information like your password or initiate malicious software (malware) downloads when you interact with them.

Here are some things to look out for when you receive a message with a link:

Full Stops

Full stops split domain names and, in the example **"know.be4.com"**, direct you to a potentially different website like "**be4.com**".

Shortened Links

Shortened links, such as "**https://bit.ly/49Pd3MK**," can mask the actual destination, potentially leading to malicious sites. Copy and paste the link into a link expander tool to show you where it will direct you before interacting.

Numbers

Numbers preceding a domain could be a warning sign for phishing or a malicious site. The intention is to obscure the destination with numbers.

Hyphens

A hyphen would change the domain, sending you to "**secure-knowbe4.com**" rather than the intended "**knowbe4.com**."

Spelling Errors

Minor spelling mistakes or omissions, like "**https://knowb4.com**," can deceive you into believing you're visiting the intended, legitimate site.

If you receive a link in an email, you should:

- Hover over a link to check the actual destination
- Type in the address manually - don't interact with a link sent to you
- Report the email immediately if you are unsure or suspicious

When you receive links on your phone, wait until you return to your computer before acting on it. It's easier to make mistakes on mobile devices.

Remain vigilant against phishing links; caution is your best defence in protecting your online information and you are the last line of defence against these attacks.

Popcorn Training
a KnowBe4 company