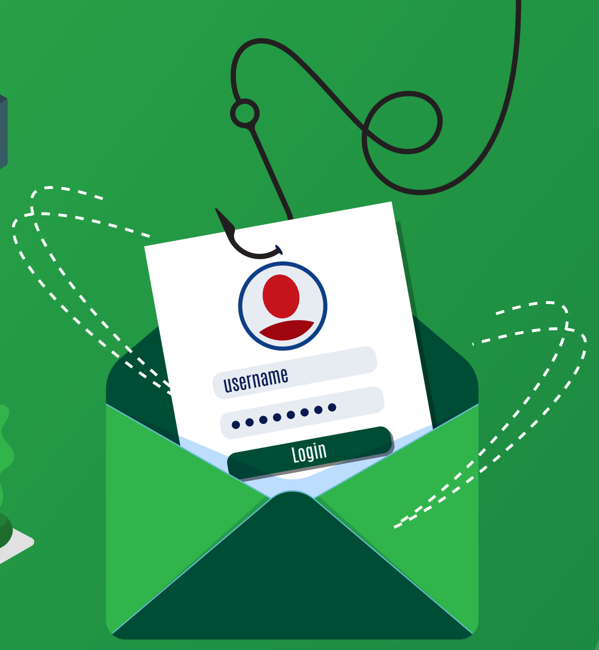

SPOT PHISHING EMAILS

01

Be Cautious

Always be careful when using email. Follow the necessary precautions before clicking links or opening attachments.

02

Spelling Errors

Spelling errors and typos are another indication. Many phishing emails contain strange phrasing and poor grammar. Attackers will often hastily send emails to numerous recipients, hoping to "cast a wide net" and trick an unsuspecting person.

03

Urgent Action

Watch out for calls to action with a deadline or a suggested consequence aimed at creating panic. Attachers use time sensitive and threatening language to increase the chance of clicking.

04

Verify Links

Phishing atttacks may contain links that appears to be lengitimate. Double check by simply havering your mouse over the link to see the actual URL.

05

From :

"From :" Address

The "From :" address of an email can be forged to appear legtimate. Attackers can slip a small typo into an email address to make it look like it's from a legitimate source, such as a CEO or your bank.

06

Personal Information

Emails requesting personal information are always suspect. Follow the previous steps before providing usernames, passwords or other personal information.

Follow these general steps every time you receive an email to prevent being hooked by a phishing scheme.