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

Be Cautious

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.

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

Verify Links
Phishing attacks may contain links that appear to be legitimate. Double check by simply hovering your mouse over the link to see the actual URL.

"From:" Address
The "From:" address of an email can be forged to appear legitimate. 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.

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.