

CLICK WITH CARE

Phishing scams are one of the most common ways for data to be breached. Be wary of any links or attachments sent to you randomly, and ignore urgent requests for money or personal information.

HOW TO IDENTIFY A PHISHING EMAIL



- 1 The sender displays a sense of urgency or uses threatening language.
- 2 The email isn't addressed to you.
- 3 There are spelling and grammar errors.
- 4 It contains a request for money or personal info.
- 5 There's a call to action, such as clicking a link or downloading an attachment.
- 6 It comes from an unusual source.

From: neil.a@trustybank.com
To: you@youreemail.com
Subject: URGENT!!! Account compromised! 1

Dear Sir or Madam, 2

There has been problem identified with your account. Plaese click on the link below to download the appropriate files and return them ASAP. It is very important, as you account has been 3 compromised and time is of the utmose essance. Be prepared to provide proof of your identity. 4

[Click here to download files.](#) 5

Sincerely, 6
Neil A.
Trusty Bank

Being able to identify phishing emails is a great step toward avoiding data breaches. If you come across a phishing email, please report it immediately.

