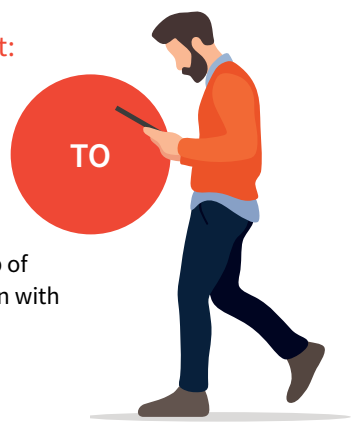
PHISHING

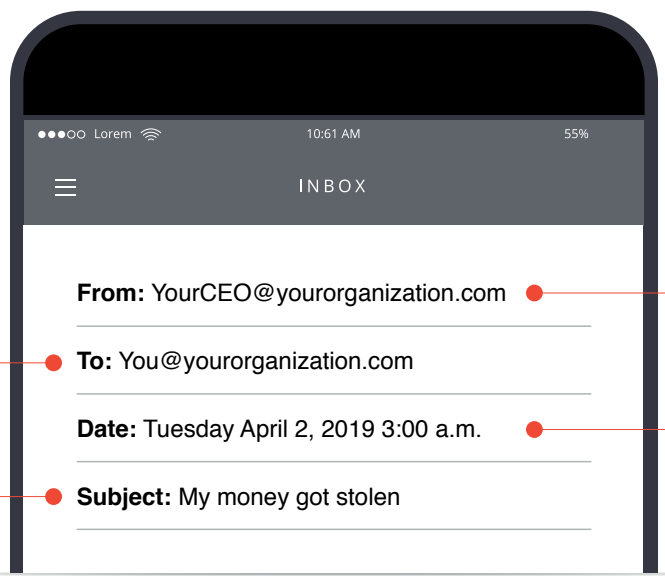
Look before you click.

Learn how to recognize nefarious emails.

Look twice if the recipient list:



- features a group of people, in addition to you, but you don't know the other people personally
- includes an unusal mix of people—such as a random group of people with last names that begin with the same letter



Be cautious if the sender:

- is not someone you ordinarily communicate with, know personally, or can be vouched for by someone you trust
- may be a customer, vendor, or partner—or even someone in your organization—but the email's content is very unusual, out of character, or not related to your job responsibilities
- has an email address with a suspicious domain, such as: microsoft-support.com

Be careful if the time sent:

- does not align with your collegues' normal communication patterns; for example, an email sent at 3:00 a.m. may be suspect

Take note if the subject:

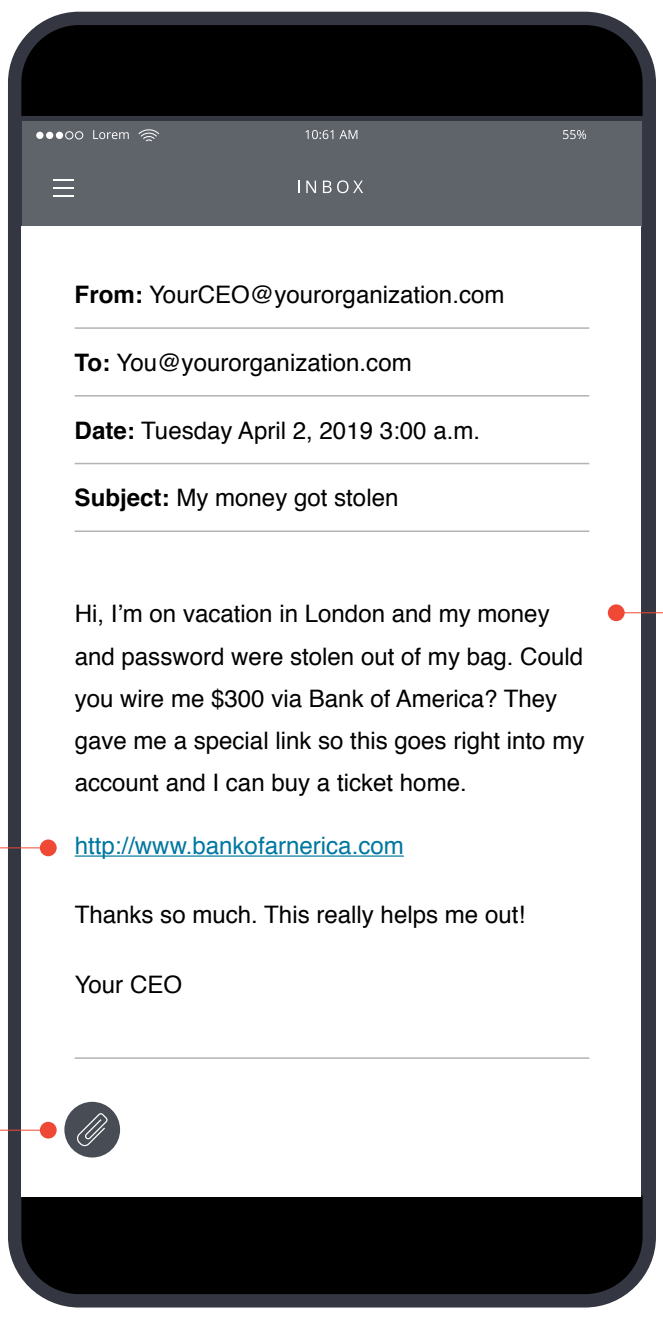
- is irrelevant or does not match the content
- is a reply to something you never sent or requested

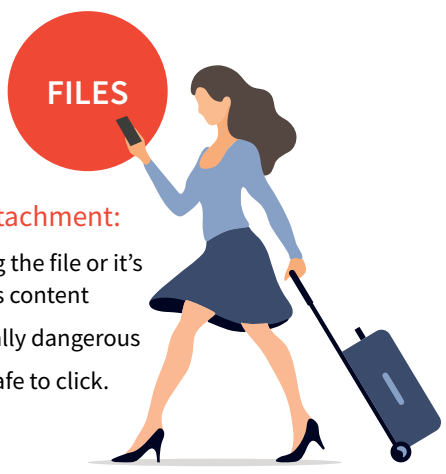
Don't engage if the email:

- is out of the ordinary, written oddly, or has unusual spelling errors
- requests that you click a link or open an attachment to avoid a negative consequence, gain something of value, view a compromising or embarrassing picture of you or someone you know

Don't click a hyperlink:

- if it resembles a known website, but is actually spelled slightly differently
- if it's long, and it's the only content displayed in the email



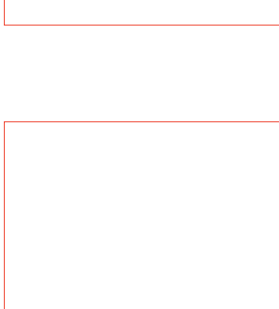


Don't download an attachment:

- if you were not expecting the file or it's not related to the email's content
- if the file type is potentially dangerous

Only .txt files are always safe to click.

Quick Tips



Take a moment

Study sender and subject line

Inspect content for peculiarities

Click or download with care

Content Source: Social Engineering Red Flags, KnowBe4