

8 Ways to Recognize a Phishing Attack



Unsolicited Email

Be cautious of
EXTERNAL EMAIL
This is an email outside
UTSA

Sender Address

Check to see if the sender
email address is UTSA.EDU

Attachments

Do not open attachments
in emails or enable
macros/remote content in
documents you weren't
expecting.

Email Tone

If the email claims to be
from a familiar person or
organization, be wary if the
tone seems inconsistent or
unfamiliar

Bad Spelling or Grammar

Phishing messages
often contain
misspelled words

Suspicious Links

Beware of links that can
lead to fake websites or
download malicious files
to your computer. Check
the links by hovering over
the link before clicking.

Email Signature

Check for a signature block
that is overly generic or
doesn't match the
company template.

"Urgent" or Threatening Requests

Phishing emails may
provide a strict deadline for
performing actions or be
threatening in nature.