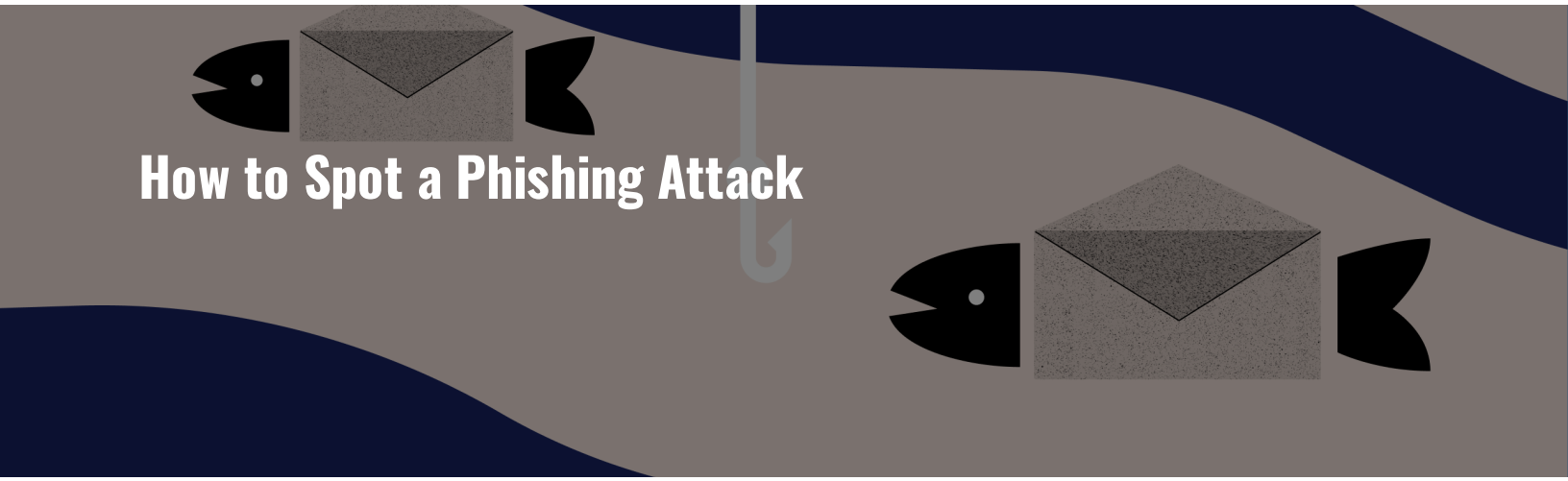


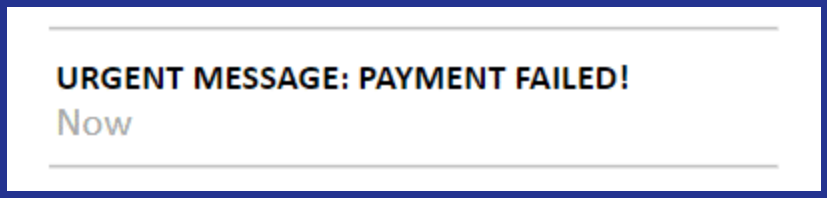
How to Spot a Phishing Attack

Phishing emails — fraudulent correspondence designed to trick people into divulging personal information — are the most common type of online attack.

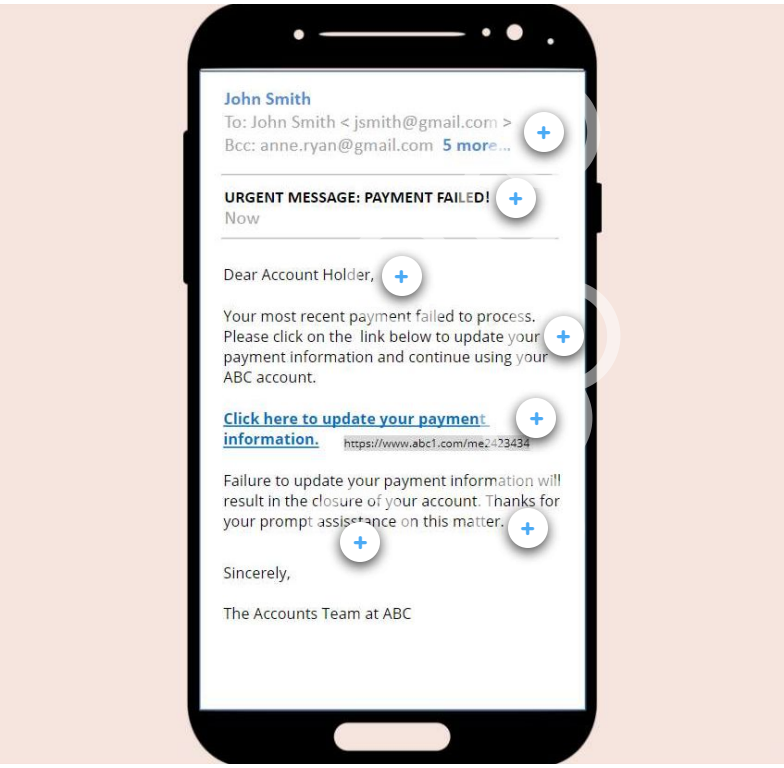
Some Phishing Facts

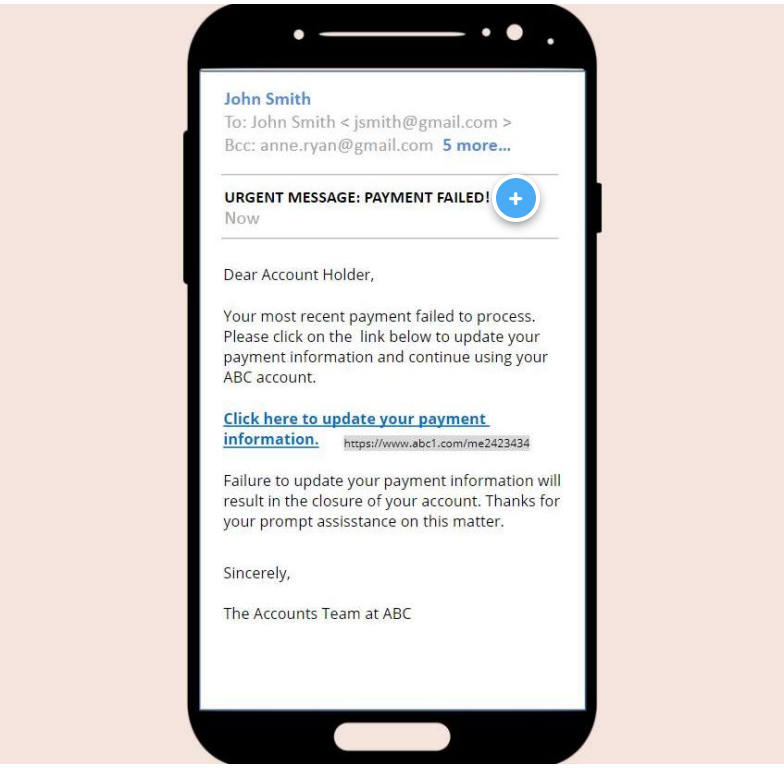
- **Nearly half** of all emails sent are phishing attempts.
- **90%** of successful data breaches begin with a phishing email.
- If you haven't received a phishing email, **it's only a matter of time!**

You've got mail!



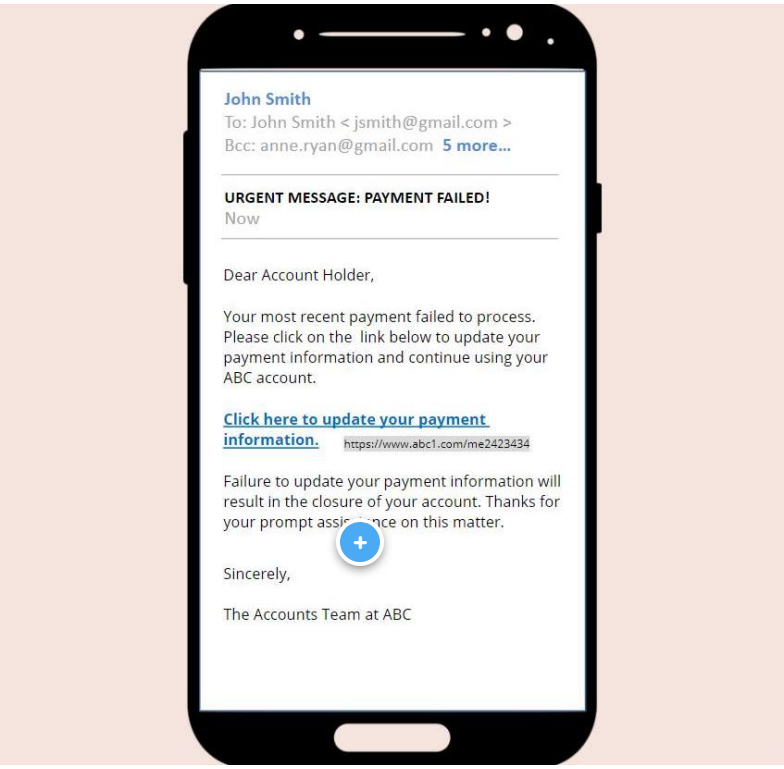
Oh, no! It looks like your payment to ABC Ltd. was declined... *or was it?* Examine the message more closely by tapping the icons on the next screen.


John Smith
To: John Smith < jsmith@gmail.com >
Bcc: anne.ryan@gmail.com 5 more...
URGENT MESSAGE: PAYMENT FAILED!
Now
Dear Account Holder,
Your most recent payment failed to process. Please click on the link below to update your payment information and continue using your ABC account.
Click here to update your payment information.
https://www.abc1.com/me2423434
Failure to update your payment information will result in the closure of your account. Thanks for your prompt assistance on this matter.
Sincerely,
The Accounts Team at ABC



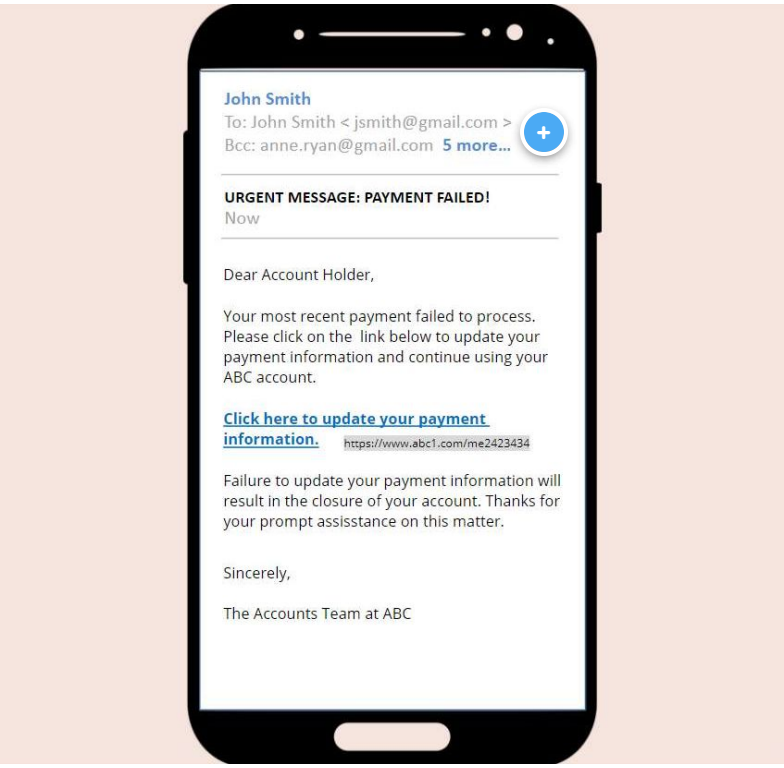
Sense of Urgency

Cybercriminals create a sense of urgency in phishing emails to move you to action.



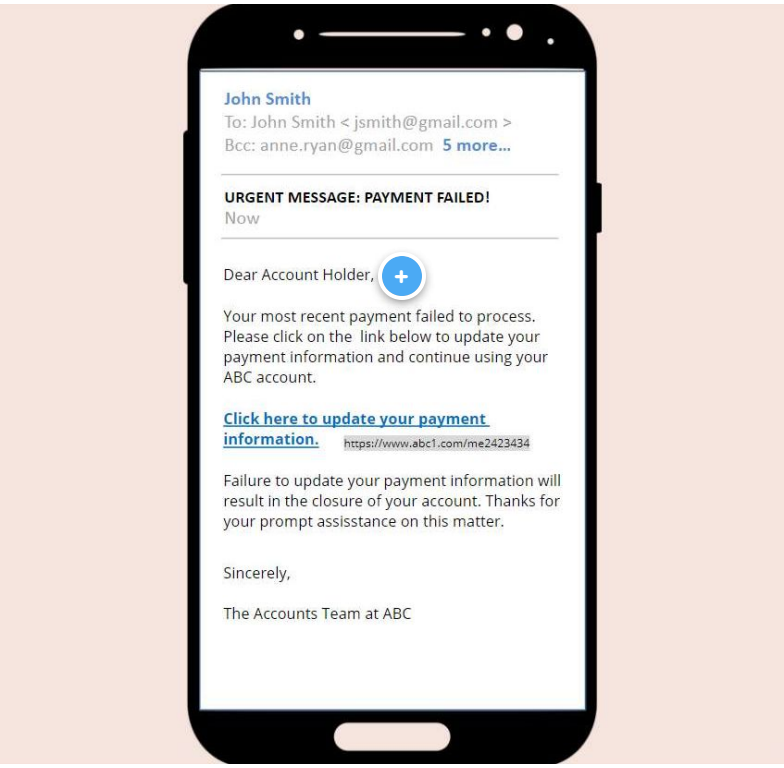
Typos and Mistakes

Misspellings, grammatical errors, and incorrect or strange phrasing are hallmarks of phishing emails.



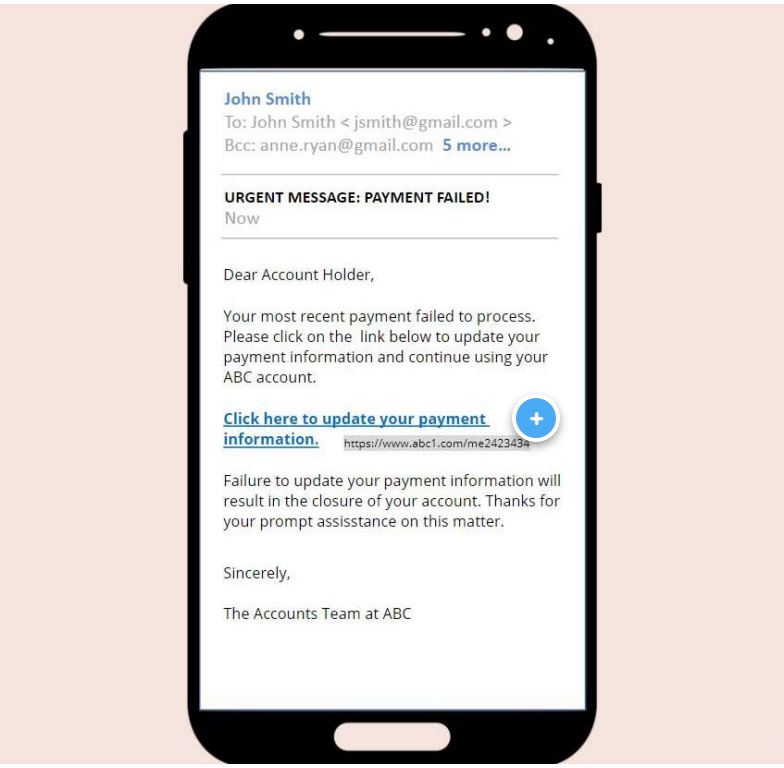
Unfamiliar Recipients

Phishing attempts will sometimes include other unknown recipients in the "To:" and "Cc:" fields.



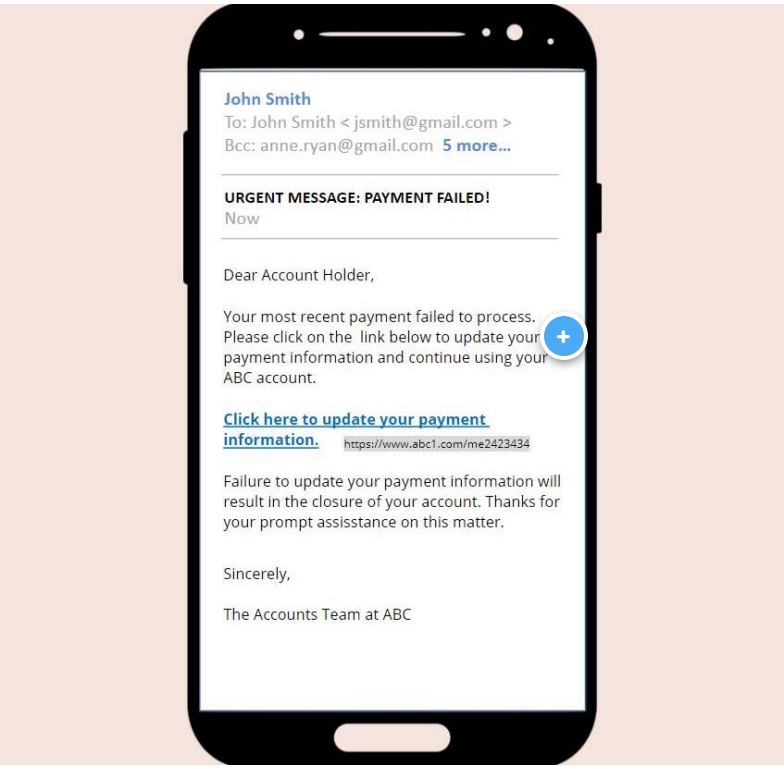
Generic Greeting

Scammers don't take time to personalize emails. Be wary of vague greetings like "Dear Customer" or "Dear Subscriber."



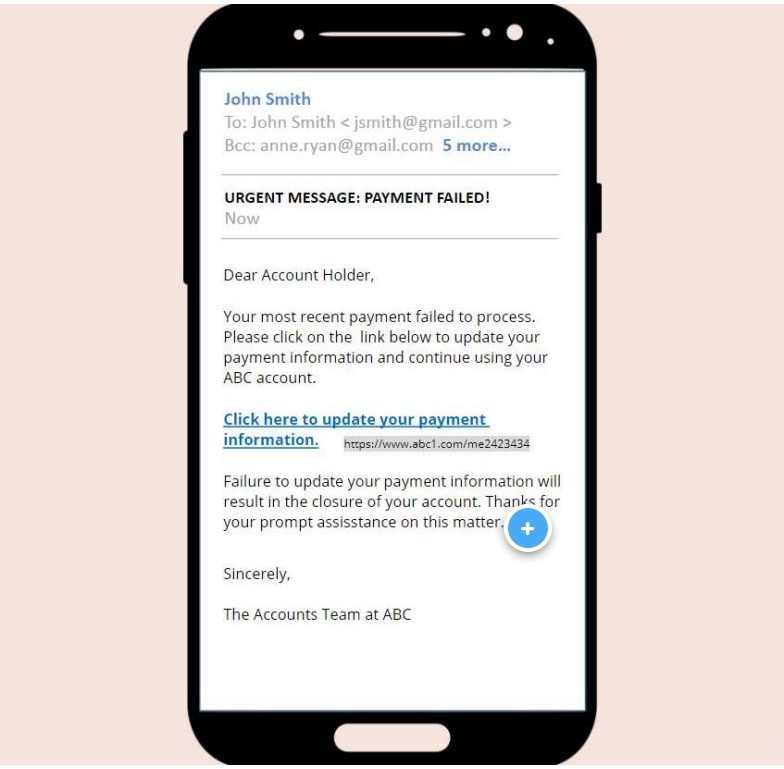
Deceptive Links

Calls to click a link is a common phishing hallmark. Never click a link from an email. Note how this trickster swapped an "i" for a "1" in the company URL.



Request for Personal Information

Many phishing emails want you to enter a password or account number to "fix" a problem. If you're concerned about your account, navigate to the company's website independently after confirming the correct URL and access your account from there.



Threats

Language threatening account closures, collection attempts, and failed payments are another common feature. These threats are designed to make you act fast without thinking.

Next time you're faced with a phishing email, will you outwit the trickster or take the bait? Let's find out! Continue to test your phishing IQ.

Complete the knowledge check below by dragging and dropping each statement into the correct category: **True** or **False.**

True

Never click on an email link without examining it.

Phishing emails usually have a sense of urgency.

Phishing emails often use generic greetings.

Phishing email recipients may be unfamiliar.

False

If you know the sender, you can click an email link.

Phishing emails never sound threatening.

Phishing scams mostly just waste people's time.

Phishing emails rarely have typos or strange phrasing.

Nice work! You're ready to face the phishers. Review phishing red flags periodically to protect yourself and your data, and remember that phishers are *very* good at what they do!

Thanks for completing this course!

Explore our comprehensive course catalog today and embark on a journey of lifelong learning!

Visit our website www.vigitrust.com

Email: info@vigitrust.com