Spotting 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!**

Consider this example!

URGENT MESSAGE: PAYMENT FAILED!
Now
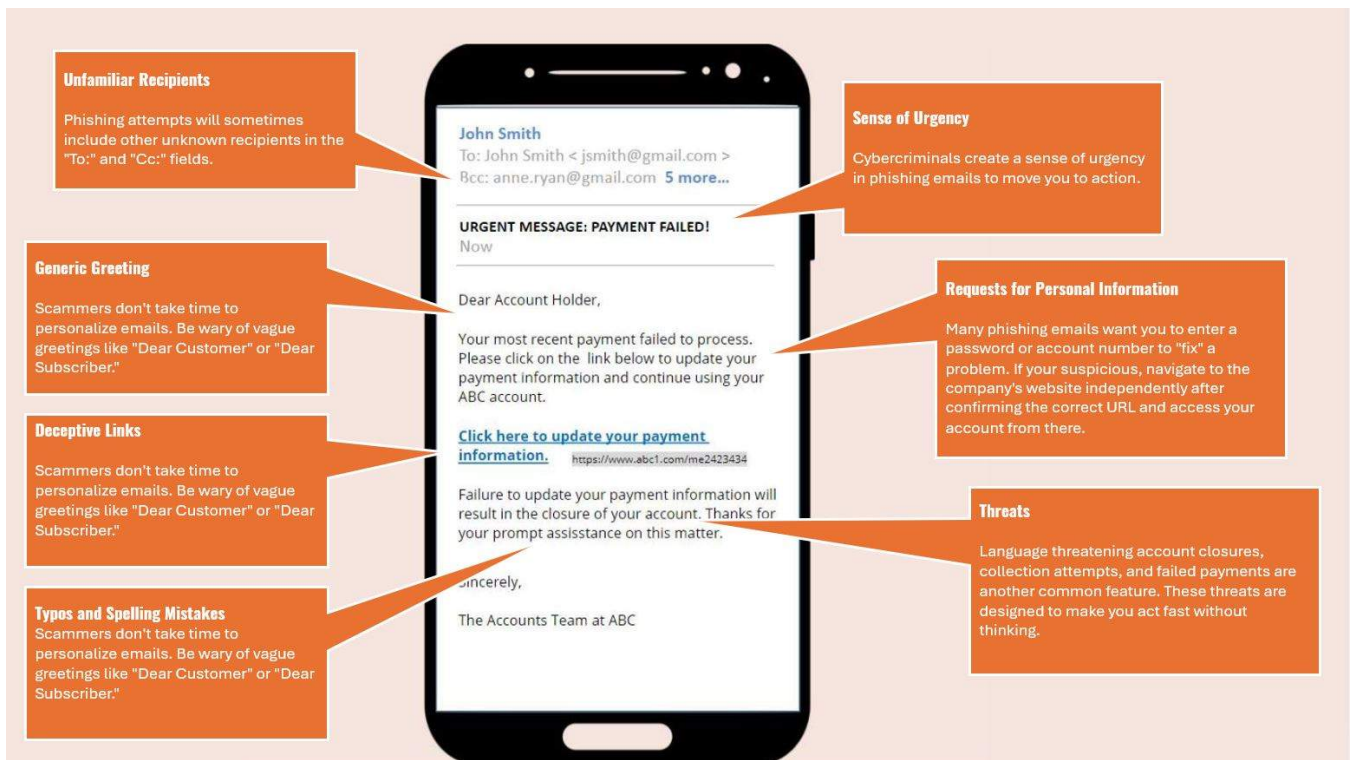
It looks like your payment to ABC Ltd. was declined... *or was it?* Let's examine the message more closely on the next screen.

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

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

Typos and Spelling Mistakes

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

Sense of Urgency

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

Requests for Personal Information

Many phishing emails want you to enter a password or account number to "fix" a problem. If your suspicious, 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.

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 assisstance on this matter.

Sincerely,

The Accounts Team at ABC

Next time you're faced with a phishing email, will you outwit the trickster or take the bait?

Summary

Phishing emails are a common online threat designed to steal personal or sensitive information. In this short lesson, you've learnt how to recognise the warning signs of phishing emails and the importance of always being vigilant. Here are some of the key points you can take away:

1. **Sense of urgency**. Phishing emails often create a sense of urgency to prompt immediate action.

2. **Look out for errors**. Misspellings, grammatical errors, and generic greetings can indicate a phishing attempt.

3. **Avoid clicking links**. Be cautious about clicking on links in emails and providing personal information.

4. **Regularly review red flags**. Consistently review phishing red flags to protect yourself and your data.

Stay vigilant and informed to safeguard your personal information from phishing attacks.

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!
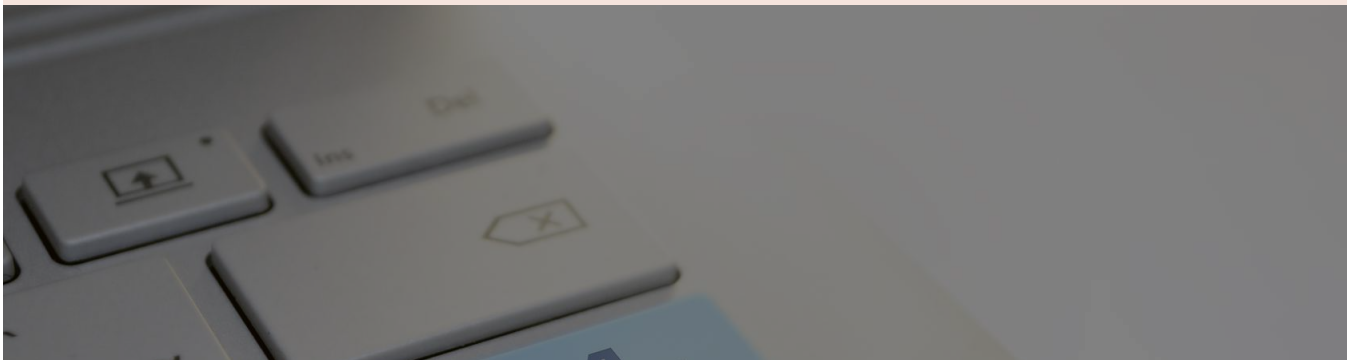
Thanks for completing this lesson!

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

Visit our website www.vigitrust.com

Email: info@vigitrust.com

VIGITRUST