Vade Secure
Advanced Email Protection

Learn How to **Detect a Phishing Email.**

1 Suspicious Sender

Just because the email appears to be from a valid organization does not mean that it is. Cybercriminals can disguise emails to look like they are coming from a specific person or organization when they are actually coming from a different source.

2 Subject Line

Threatening or enticing language is commonly used to encourage the recipient to take immediate action.Evoking a sense of urgency, fear, curiosity, or greed is a common tactic amongst phishing schemes.

3 Generic Greeting

Emails with generic, impersonal greetings or without any indication that the email is for the specific recipient, should be considered suspicious. Phishers often send out mass emails to try to gather as much personal information as possible.

4 Errors

Read the email carefully. Drastic stylistic problems or spelling and grammar problems should raise a red flag, especially if it is purportedly from a reputable company. Many phishing attacks come from other countries, so emails are often written by non-native English speakers. In contrast, most companies will carefully proofread their work.

5 Links

Before clicking on any link, make sure to hover over it. A bubble will show the URL of where the link actually leads. If the destination is not the website you were expecting, it is probably a phishing attack. Be especially careful that the core URL is what you think it should be.

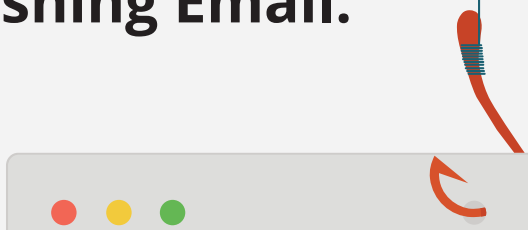
http://ignorethis.IMPORTANT_URL.com/doesn'tmatter

6 Tone

Be wary of emails that provide a specified amount of time to take immediate action. This technique is often used to coerce people into giving their personal information for fear of the threatened repercussions.

7 Images

Remember, just because the logos and trademarks of a brand look real does not mean they are legitimate. Cybercriminals can easily replicate these images in order to convince phishing victims that the email is real.



1

FROM: YourBank.com <cust-sup@usa.ybank.com>

TO: undisclosed-recipients

2

Your credit card has been suspended

BankLogo

Dear customer, 3

Your credit card has been suspended because erors were detected in the information from your credit card. The reason for the eror is uncertain, but for safety reasons, we have temporarily suspended your credit card. 4

You must update your information to continue using this credit card.

5

To remove the suspension: Click here and follow the steps to reactivate your card.

http://yelona.com/chase.alert.php

NOTE: If you do not resolve the problem within 72 hours, we will be forced to permanently suspend your credit card.

6

Thank you,
Customer support department.

7 Anti-virus Verified

How do I report a phishing?

So, you have spotted a phishing email, well done! But what can you do about it?
Always contact your internal IT department immediately, as they will know how to securely handle the attack.

Doubting the link? ISITPHISHING.ORG provides a safe webpage search engine to determine if the link provided is a legitimate website or a phishing attack.

© Vade Secure