

# Learn How to Detect a Phishing Email.

# **Suspicious Sender**

Cybercriminals use various spoofing techniques to trick users into believing an email is legitimate. Check the domain closely for close 'cousin' domains. Be cautious when reading email on your mobile device, as only the display name may be visible even if the email is bogus.

## Subject Line & Tone

Enticing, urgent, or threatening language is commonly used to encourage the recipient to take immediate action. Evoking a sense of curiosity, greed, or fear is a common tactic among phishing schemes.

## Greeting

Phishers often send out mass emails to gather information, so they use generic greetings. But, sophisticated phishers personalize their emails with information such as names, email addresses, and even breached passwords.

#### Errors

Read the email carefully. Grammatical errors are an obvious red flag, but sophisticated hackers do not make glaring errors. Instead, there may be more subtle mistakes, such as minor spacing issues or use of symbols instead of words. In some cases, there will be no errors.

### Links

Before clicking, hover over the link to see the URL of where the link actually leads, and beware of link shorteners, such as Bitly or TinyURL. Keep in mind that phishing emails can include clean URLs in addition to the phishing URL to trick users and email filters.

http://ignorethis.IMPORTANT\_URL.com/doesn'tmatter

### **Attachments**

Be wary of emails that include attachments. Phishing emails may include a link in an attachment, rather than the body of the email, to avoid detection by an email filter.

## **Images**

Cybercriminals can easily replicate brand logos, images, and badges in emails and webpages that are indistinguishable from the real thing. Consider all the above factors as you decide whether to click.





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

TO: undisclosed-recipients

Your credit card has been suspended



Dear customer,



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.

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

To remove the suspension: <u>Click here</u> and follow the steps to reactivate your card.

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



Thank you,

Customer support department.





## When in doubt, check it out.

<u>ISITPHISHING.Al</u> is a free service that performs real-time analysis of the URL and web page to determine if it's phishing.