

# Learn How to Detect a Phishing Email

## 1 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.

## 2 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.

## 3 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.

## 4 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.

## 5 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.

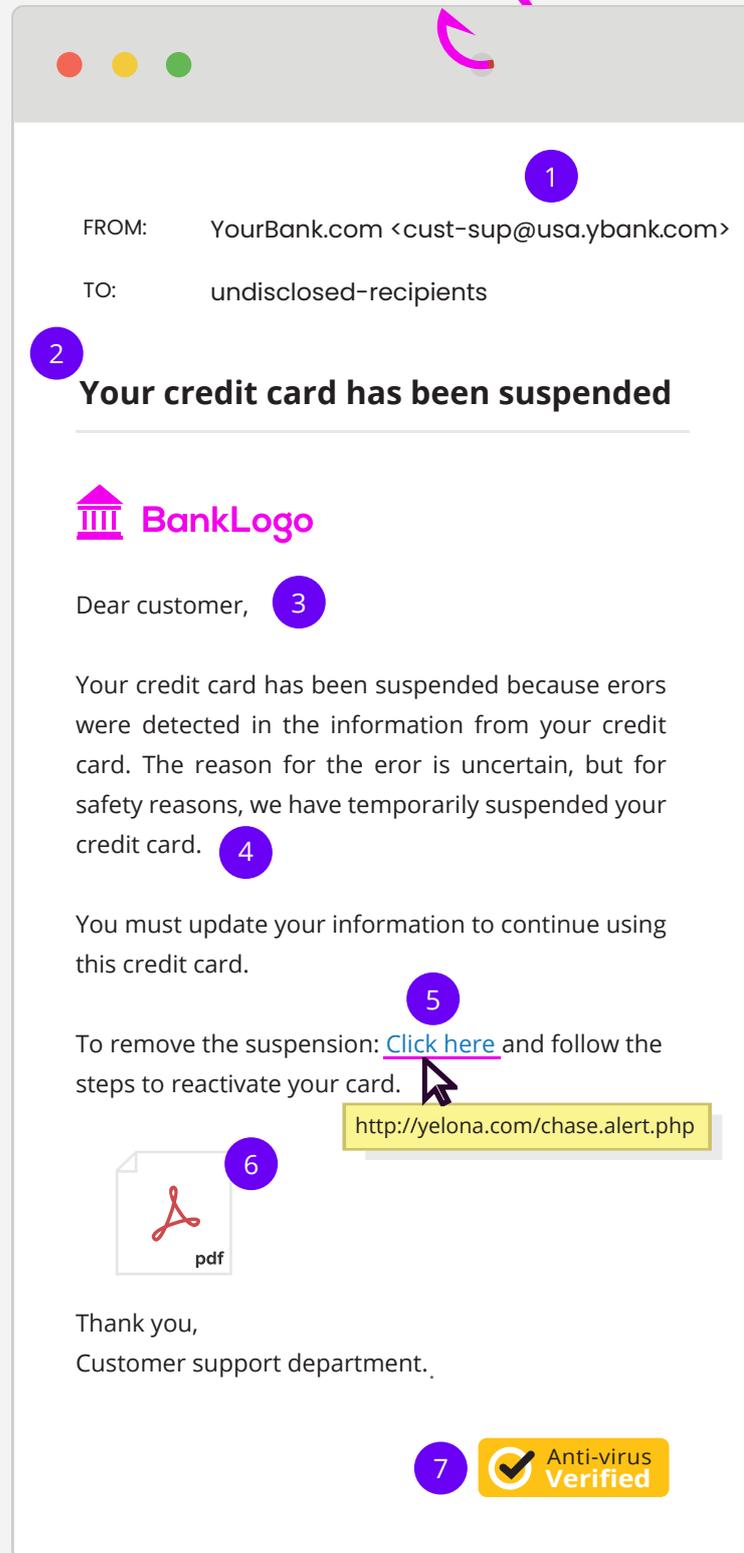
[http://ignorethis.IMPORTANT\\_URL.com/doesn'tmatter](http://ignorethis.IMPORTANT_URL.com/doesn'tmatter)

## 6 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.

## 7 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.



When in doubt, check it out.

[IsItPhishing.AI](#) is a free service that performs real-time analysis of the URL and web page to determine if it's phishing.