6 Signs
an Email is a Phish

1

Plays on Fear and Urgency
Legitimate sources will use a **calm, credible** voice. Watch for exclamation points and other tactics.

2

Asks for Credentials or Personal Information
Legitimate messages will **not** send you to a website requesting your credit card number, account details or other personal information.
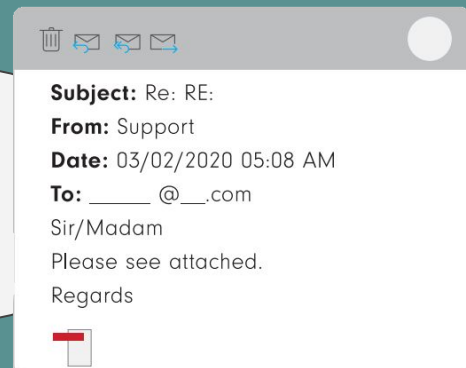
3

Uses an Unfamiliar Greeting
Legitimate sources will use a greeting you are **familiar** with. Watch for overly formal or otherwise strange greetings such as "Dear Sir/Madam".

4

Has a Strange from Name or Email Address
Be careful with messages from people you don't **usually** hear from especially from domains (the part after the @ symbol) you don't **usually** hear from.

Subject: Re: RE:
From: Support
Date: 03/02/2020 05:08 AM
To: _____ @__.com
Sir/Madam
Please see attached.
Regards

5

Spelling or Grammar Mistakes
Messages from legitimate sources are unlikely to have spelling and grammar mistakes.

6

Unexpected or Strange Links and Attachments
Inspect links carefully for links to websites that you don't recognize. Be careful of attached files with unusual names or file types.

click here.