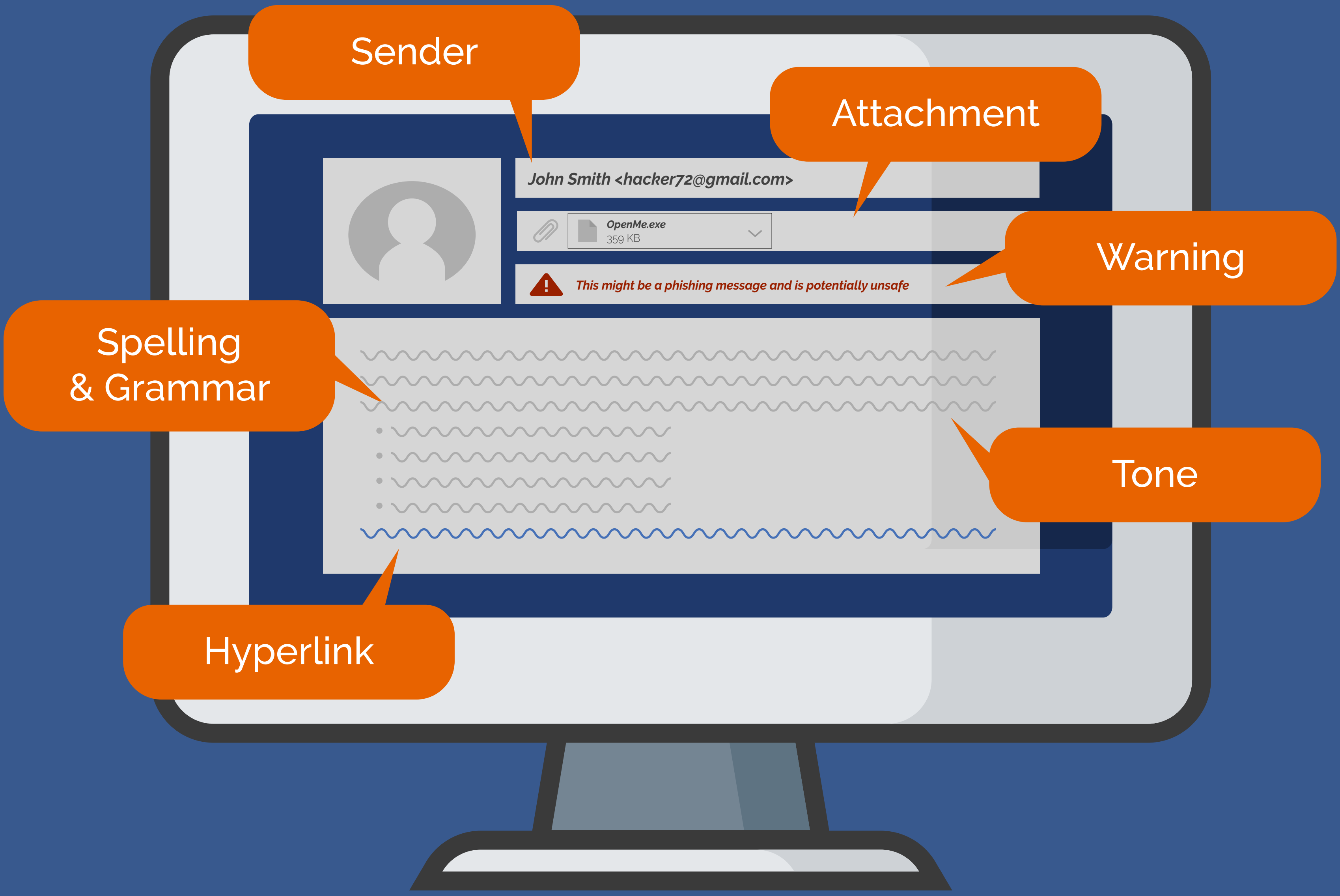
How to Spot a Phishing Email


Sender
Attachment
Warning
Spelling & Grammar
Tone
Hyperlink
John Smith <hacker72@gmail.com>
OpenMe.exe
359 KB
This might be a phishing message and is potentially unsafe

1 Sender

Always check who the sender is when you receive an email. You should be on alert if you don't recognize the sender, the display name doesn't match the email address, or if the email address is from a suspicious domain.

2 Attachment

Do not click on an attachment if you don't recognize the sender or if the attachment is nonsensical or unexpected. File types can be masked so do not assume any file type is completely safe. When in doubt, report it to your IT department.

3 Warning

If you have phishing warning enabled on your email platform, any email that is a potential threat will be flagged. It is possible that some phishing emails won't get flagged by the auto-detection so exercise caution while dealing with every email.

4 Tone

Phishing emails often give off a tone or urgency or danger. An urgent tone will cause some users to take action immediately without thinking it through. An example of using an urgent tone would be an email telling you an account of yours has been compromised and you need to click this link to recover your account.

5 Hyperlink

Always inspect links thoroughly before clicking on them. Check to see if the link is a misspelling of a common website. Links can be spoofed so use your mouse to hover over a link and make sure the pop-up link is consistent with the link in the email.

6 Spelling & Grammar

Spelling and grammatical errors are common in phishing emails. If an email is riddled with spelling and grammatical errors then that should tip you off that the email may not be legitimate.

ALDRIDGE
Your Technology Solutions Partner

**For more educational content visit us at:
aldridge.com**