



# 10 Ways to Spot a Phishing Email


**Did you know?** In 2019, ransomware from phishing emails increased 109% over 2017,<sup>1</sup> and the average cost of a ransomware attack on businesses was \$133,000.<sup>2</sup>


With ransomware infections from phishing attacks climbing at an unprecedented rate, educating your staff is paramount in protecting your organization. There is no time to wait.


Here are the top ten ways to detect a phishing email:


**1 Sender impersonations**  
 Don't simply trust the display name on an email. Cyber criminals often attempt to impersonate someone you may know or trust. Be sure to check the email address to confirm the true sender.


**2 Sender uses a public email domain**  
 Legitimate organizations typically will not contact you from an email address that ends in a public email domain such as @gmail.com.


**3 Generic salutations**  
 Typically, a reputable company will use your name or an appropriate title to address you. Be cautious of emails beginning with "To whom it may concern" or "Dear sir or madam".


**4 Requests for personal information**  
 Legitimate organizations do not typically ask for this type of information over email (e.g. ssn verification, login info, etc). Usually when companies need this information, it's because they are verifying your identity for contacting them.


**5 Spelling errors**  
 Attackers tend to be grammatically incorrect and make typing mistakes in their message. This is also a clever tactic used in sender impersonations, so verify the spelling on the sender's email address for validation.

**6 Suspicious links**  
 Hover over a link without clicking to reveal the destination URL. If the URL doesn't match the linked content, do not click and report the email to your IT manager.

**7 Malicious attachments**  
 Never open a questionable attachment (e.g. exe or encrypted zip file, macro-enabled documents). If you suspect malicious content, it's always best to contact the sender separately for confirmation of file validity.

**8 Urgent requests**  
 Phishing scammers often do their homework before they target you for an urgent request (e.g. the CEO needs an immediate wire transfer or gift card purchase). Always verify legitimacy before making hasty purchases from an email request.

**9 Unbelievable offers**  
 If the deal seems too good to be true, it probably is. Beware of emails offering big rewards for little effort (e.g. cash prizes, dream vacations, etc.).

**10 Suspicious messaging**  
 Last but not least. If an email feels off or makes you question its legitimacy **AT ALL**, it's better to play it safe and ignore or delete it.

<sup>1</sup> PhishMe Q3 Malware Review  
<sup>2</sup> Sophos Independent Study: The State of Endpoint Security Today