



## AVOID FALLING VICTIM TO PHISHING EMAILS

### What is Phishing?

Phishing is an email scam where the sender spoofs their identity and tries to obtain sensitive information, such as usernames, passwords, and credit card details. Phishing can be either a social engineering attack or an information technology (IT) compromise.

These attacks are carried out by sending emails with URLs that look like they come from legitimate sites, but they lead to fake versions of those sites instead. Phishers aim to trick recipients into providing personal information or clicking on links that will infect their computers with malware.



Payments or prizes  
promised



Requesting for  
sensitive information



A mail with unexpected  
attachments



Prompts and scare  
tactics to get a quick  
response



Links posing as safe  
but are dangerous



Fake URL acting as the  
legitimate page

**A suspicious email? Don't click! Let your IT department review it.**  
**Or take the help of [Protected Harbor](#)**  
**Also, [read Top Phishing Email Attacks to Watch For](#)**