Don't Get Hooked
6 Tips to Avoid Phishing Attacks

1 Watch out for Emails That Have Improper Grammar or Spelling

One of the most common signs that an email isn't legitimate is that it contains spelling and grammar mistakes. Check the email closely for misspellings and improper grammar.

2 Check That Hyperlinked URLs are the Same as the URL Shown

The hypertext link in a phishing email may include the name of a legitimate organization. However, when you move the mouse over the link (without clicking it), the actual URL is different than the one displayed.

3 Be Wary of Emails That Urge You to Take Immediate Action

Phishing emails often try to trick you into clicking a link by claiming that your account has been closed or put on hold. Don't click the link no matter how authentic it appears. Login to the account in question by directly visiting the appropriate website, then check your account status.

4 The Email Claims You've Won a Contest You Haven't Entered

If you receive an email notifying you that you won the lottery or another prize when you haven't entered a contest, the email is probably scam. Don't click the link or give any personal information.

5 The Email Asks You to Donate to a Worthy Cause After a Tragedy

Scammers often send phishing emails inviting people to donate to an organization after a natural disaster or other tragedy. The links send users to malicious sites that steal credit card and other personal information. If you'd like to make a donation to charity, visit the website directly.

6 Suspicious Attachments Sent via Email Should Never be Downloaded

Typically, you shouldn't receive an email with an attachment unless you've requested the document. If you receive an email that looks suspicious, don't click to download the attachment.