

# 5 WAYS TO AVOID PHISHING ATTACK

A Phishing attack is a fraudulent message usually in the form of an email, which lures users into clicking a link. That link in turn either leads the victim to a malicious websites or initiates a malicious download.



The way to avoid these attacks is to **Identify them before you can become a victim.**

Here are 5 ways to identify and avoid a phishing attack



01

## Be cautious of emails from unknown senders

These emails come in many different forms, but the rule of thumb is: If you don't know the source, don't click. In addition, emails that aren't personalized are another red flag.



02

## Do not click on links within an email

Although the link may say that it connects to your bank, it could just be a hyperlink that leads you to a site that only looks like your bank's website. Don't trust email links. Type in or copy and paste any listed URLs into your browser.



03

## Don't download attachments or open email files you aren't expecting

Phishing scams can come from the infected account of your spouse or best friend. Be wary of opening files you aren't expecting to receive. It's best not to open attachments from unknown email addresses.



04

## Don't include personal or financial information in an email

Even if you trust the person you are sending this to, you never know who might gain access to your account or their account.



05

## Use anti-spam/anti-spyware firewalls

And update! This brings your computer up-to-speed on the latest threats. It's good for your systems to be in the know.

