



CYBER SECURITY



Phishing attacks are more rampant than ever before, rising by [more than 162 percent](#) in the recent years. They cost organizations around the globe [\\$4.5 billion every year](#) and over half of internet users get at least one phishing email per day.

The best defence companies have against phishing attacks is to block malicious emails before they reach the users. Unfortunately, no matter what companies do, some phishing emails will always make it to the inbox. And those messages are extremely effective—97% of people around the globe cannot identify a sophisticated phishing email. That's where customer education comes in.

Here are 10 tips on how to identify a phishing or spoofing email.

Tip 1: Don't trust the display name

A favourite phishing tactic among cybercriminals is to spoof the display name of an email. [Return Path analysed more than 760,000 email threats](#) targeting 40 of the world's largest brands and found that nearly half of all email threats spoofed the brand in the display name.

Here's how it works: If a fraudster wanted to spoof the hypothetical brand "My Bank," the email may look something like:

```
To: You <you@yourdomain.com>
From: My Bank <accounts@secure.com> ←
Subject: Unauthorized login attempt
```

Since My Bank doesn't own the domain "secure.com,". This fraudulent email, once delivered, appears legitimate because most user inboxes only present the display name.

Safety//FIRST

A GRINDROD SHIPPING promise



CYBER SECURITY

Don't trust the display name. Check the email address in the header from—if looks suspicious, don't open the email.

Tip 2: Look but don't click

Hover your mouse over any links embedded in the body of the email. If the link address looks weird, don't click on it. If you want to test the link, open a new window and type in website address directly rather than clicking on the link from unsolicited emails.

Tip 3: Check for spelling mistakes

Brands are pretty serious about email. Legitimate messages usually do not have major spelling mistakes or poor grammar. Read your emails carefully and report anything that seems suspicious.

Tip 4: Analyse the salutation

Is the email addressed to a vague "Valued Customer?" If so, watch out—legitimate businesses will often use a personal salutation with your first and last name.

Tip 5: Don't give up personal information

Legitimate banks and most other companies will never ask for personal credentials via email. Don't give them up.

Tip 6: Beware of urgent or threatening language in the subject line

Invoking a sense of urgency or fear is a common phishing tactic. Beware of subject lines that claim your "account has been suspended" or your account had an "unauthorized login attempt."

Tip 7: Review the signature

Lack of details about the signer or how you can contact a company strongly suggests a phish. Legitimate businesses always provide contact details.

Tip 8: Don't click on attachments

Including malicious attachments that contain viruses and malware is a common phishing tactic. Malware can damage files on your computer, steal your passwords or spy on you without your knowledge. Don't open any email attachments you weren't expecting.

Tip 9: Don't trust the header from email address

Fraudsters not only spoof brands in the display name, but also spoof brands in the header from email address. Return Path found that nearly 30% of more than 760,000 email threats spoofed brands somewhere in the header from email address with more than two thirds spoofing the brand in the email domain alone.

Tip 10: Don't believe everything you see

Phishers are extremely good at what they do. Just because an email has convincing brand logos, language, and a seemingly valid email address, does not mean that it's legitimate. Be sceptical when it comes to your email messages—if it looks even remotely suspicious, don't open it.