

## Features of a Phishing Email

A phishing email is basically a fake message designed to trick you.

It tries to look real, but it always has some signs that something is off.

Easiest ways to spot one:

1. The email tries to make you panic or rush

Phishing emails love drama.

They say things like:

“Your account will be suspended in 1 hour.”

“Someone tried to hack your account.”

“Click here immediately.”

They want you to react fast without thinking, so you click the link.

2. The sender’s address looks strange

It may look similar to a real company, but something will be slightly wrong.

Example:

support@paypal-verification.com

info@amaz0n-support.net

If the domain looks weird or overly complicated, it’s not legit.

3. The message doesn’t feel personal

Instead of using your real name, phishing emails say things like:

“Dear User”

“Dear Customer”

“Hello Member”

Real companies usually know your name.

#### 4. The link is fake or suspicious

The link text may say one thing, but the real URL is something else.

Example: Looks like: [www.bank.com/reset](http://www.bank.com/reset)

Actually, goes to: [malicious.site.ru/login](http://malicious.site.ru/login)

If you hover your mouse and the link doesn't match what it claims, it's a red flag.

#### 5. Poor grammar, spelling mistakes, weird sentence

Many phishing emails have:

Awkward English

Strange formatting

Words that don't fit the tone of a real company

Real companies check their emails carefully.

#### 6. Unexpected attachments

Phishing emails sometimes attach dangerous files like:

.zip

.exe

.pdf with hidden malware

Fake invoices or receipts

If you weren't expecting a file, don't open it.

#### 7. No official branding or poorly copied branding

Some phishing emails have:

Blurry logos

Wrong colors

Outdated designs

It looks like someone tried to copy the real company but didn't do it well.

8. The email asks for things no real company would

Real companies never ask for:

Passwords

OTP or verification codes

Bank details

Personal info through email

If an email wants sensitive information, it's almost always a scam.

In short:

A phishing email feels like a message that is pretending to be someone it's not.

Something about it always feels "off," and it usually tries to scare you, rush you, or steal your information.