



# 10 COMMON TRAITS OF PHISHING EMAILS

Phishing is one of the most common attack methods used by cybercriminals and the one we're all probably most familiar with. Fortunately, there are signs that can help you identify whether or not that email in your inbox is a scam.

## Asking for Personal Information.

Most reputable organizations will never email you asking for your address, phone number, national ID number, or other personal data.

## Inconsistencies in Links.

Always hover over links with your mouse pointer to display the full URL. If it leads somewhere that doesn't logically belong within the context of the email, or generally looks nonsensical, don't click!

## Unrealistic Threats.

Phishing emails often feature threatening language, such as "Payment overdue!" or "Your account has been compromised!", in order to generate a response from their targets.

## Generic Greetings.

Unlike legitimate entities that will address you by your full name or username, phishing emails usually opt for generic greetings, such as Dear Customer or Dear Sir/Madam.

## A Sense of Urgency.

Similar to unrealistic threats, emails that urge you to click on a link or download an attachment or update your account immediately are likely scams.

## You're Asked to Send Money.

Whether it be overdue taxes or an upfront payment to cover expenses, any email that asks for money should immediately raise your suspicions.

## Too Good to Be True.

The old saying remains true to this day: if it's too good to be true, it's likely untrue. Keep that in mind any time you get an email claiming you won the lottery or are due a large family inheritance.

## Poor Spelling & Grammar.

Most generic phishing attempts contain spelling and grammar errors or feature awkward wording phrasing.

## Suspicious Attachments.

Attachments aren't always malicious, but use extreme caution whenever you receive them unexpectedly.

## From a Government Agency.

In South Africa, government agencies rarely use email for important communication. For example, the South African Revenue Service (SARS) will never email you about tax returns, refunds, or payments. Official government communication is usually done through secure portals, registered mail, or in-person visits. Always verify messages directly with the relevant department to avoid falling victim to phishing scams.

