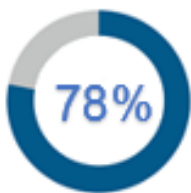


# Social Engineering Phishing

## What is Phishing?

A phishing attack uses a fake email designed by hackers. Hackers will try to make it look as if the email comes from a trusted brand (often used: DHL, FedEx, Amazon, Microsoft, Google, banks, Facebook, IRS, etc.) or institution – which might also include your employer. The goal is to make you click on a link and/or open an attachment.



According to Verizon's Data Breach Investigation Report, 78% of all cyber-attack attempts in 2017 relied on some form of email link or attachment sent to employees.

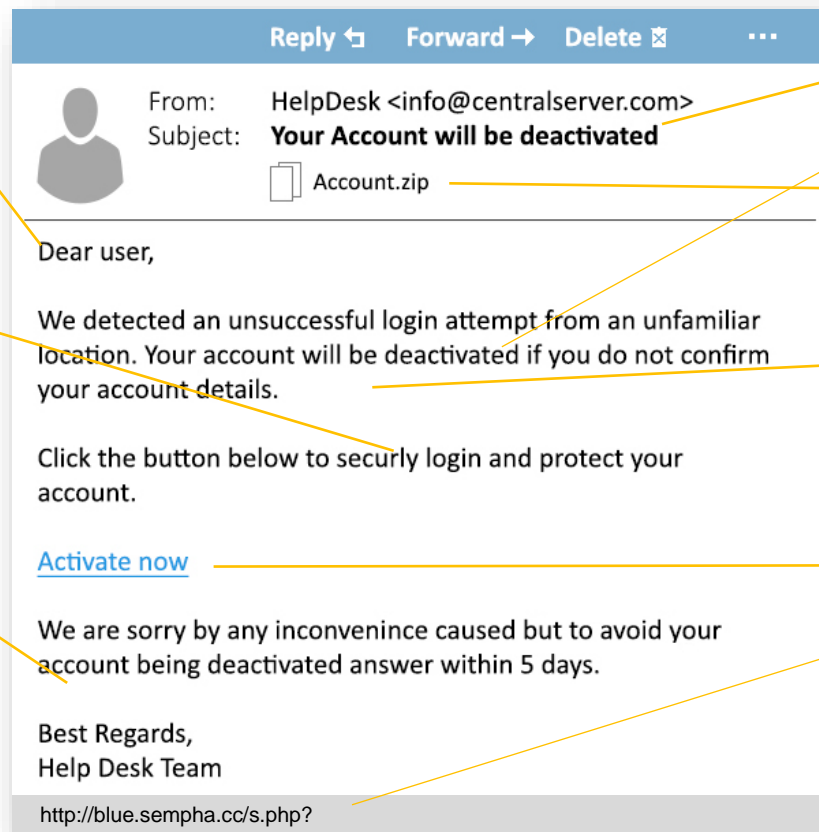
Nearly every day, most people will get at least one phishing email. Around 8% of all targeted persons click on the link or open the attachment.

## How to spot a phishing attack

Legitimate emails normally\* start with greeting you by your name.

Typos, misspellings and improper grammar.\*

Generic signature.\*



Urgent or threatening tone.

Beware of suspicious unwanted attachments.

Helpdesk will never ask for your account information in a mail.

Fake or hidden web address. Hovering over the link reveals the true website destination.

\*Note: A more targeted spear phishing attack can greet you with your name and may have no misspellings.