



**Familiarize yourself with phishing attacks**  
**<HR and Marketing>**



## What is phishing?

- Phishing is when hackers trick you into giving away sensitive information by pretending to be someone you trust.
- It can take many forms such as a fake email from "a job applicant" with a malware-infected resume or email pretending to be from a client or vendor requesting a password reset.



## Why is phishing dangerous?

- **Data Breaches & Identity Theft**

Attackers steal employee credentials, gaining access to HR records, payroll systems, or marketing accounts. Stolen identities can be used for fraud or unauthorized financial transactions

- **Reputation Damage**

A breach of employee or customer data can result in loss of trust and negative media attention. If a marketing email list gets compromised, customers may receive phishing emails from the company, damaging credibility.



# Learn to spot phishing emails

Here's an example of a phishing email, let's spot the red flags

Dear HR Team,

We have detected an issue with your employee payroll details in our new **secure** payment system. In order to **avoid delay in salary disbursement**, all HR personnel must verify and update their credentials **IMMEDIATELY**.

Click below to confirm your details:

 <http://company-payroll-update.secure-hrportal.com>


Failure to do so **before 6:00 PM TODAY** will result in a hold on employee salary processing.

Thank you for your prompt action.

Best Regards,

**Payroll Administrator**

Company HR Team

 Contact: +1 (555) 123-4567



# Learn to spot phishing emails

From the email example, we can list the red flags

Fake Email Address: "@company-secure.com" (not a real company domain).

Urgency & Fear Tactics: "Avoid delay," "IMMEDIATELY," and "before 6:00 PM TODAY."

Suspicious Link: Looks legit but actually leads to a fake site.

Spelling & Grammar Errors: "Best Regard" instead of "Best Regards."

Unusual Contact Information: Random phone number not associated with the company.



# Learn to spot phishing emails

From the email example, we can list the red flags

Fake Email Address: "@googie-ads.com" instead of "@google.com."

Urgency & Fear Tactics: "Prevent suspension," "within 24 hours."

Suspicious Link: The URL looks like Google Ads but is actually fake.

Unrealistic Request: Google wouldn't ask for login details via email.

Poor Grammar & Formatting: "Googie" typo, and spacing is off.



# Lets learn to stop getting phished

- Verify Before Clicking: Always check email sender addresses.
- Careful not to Download Suspicious Attachments: Use a sandbox for unknown files.
- Report Phishing Emails: Forward them to IT/security team.
- Enable Multi-Factor Authentication (MFA): Even if credentials are stolen, MFA helps prevent access.