# PHISHING ATTACK

Your Guidance to this trap

# Whoami ?

- ➔ Junior Penetration Tester
- ➔ CTF Player
- ➔ Cyber Security Enthusiast

# Agenda

- ➔ Introduction to Phishing
- ➔Common Phishing Techniques
- ➔Indicators of Phishing
- ➔ Protective Measures
- ➔ Security Software and Updates
- ➔ Training and Simulation
- ➔ Consequences of Falling Victim
- ➔ Conclusion and Resources

# What is Phishing Attack ?

It is a cyber attack or deceitful attempt to trick individuals into revealing sensitive information, such as usernames, passwords, or financial details , by posing as a trustworthy entity in electronic communication, typically through emails, messages, or fake websites.

# Phishing attack Techniques

Email Phishing

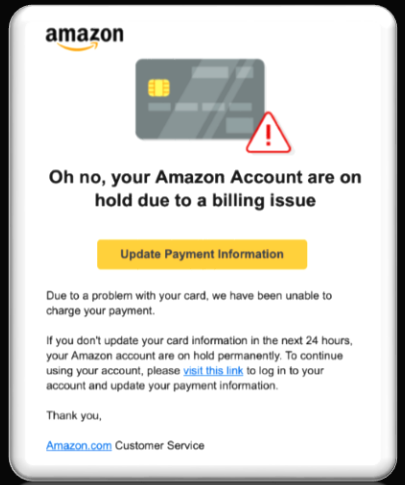

SMS Phishing ( Smishing )

Voice Phishing ( Vishing )

# Indicators Of Phishing

## Email Spoofing :

The attacker can forge the sender's Email Address to appear legitimate .



# Suspicious URLs

the attacker can manipulate In the attached Links through

➔ misspelled domain names

https://Amazon.com , https://AmazOn.com

➔ Extra Characters

https://Facebook.com , https://Faceboook.com

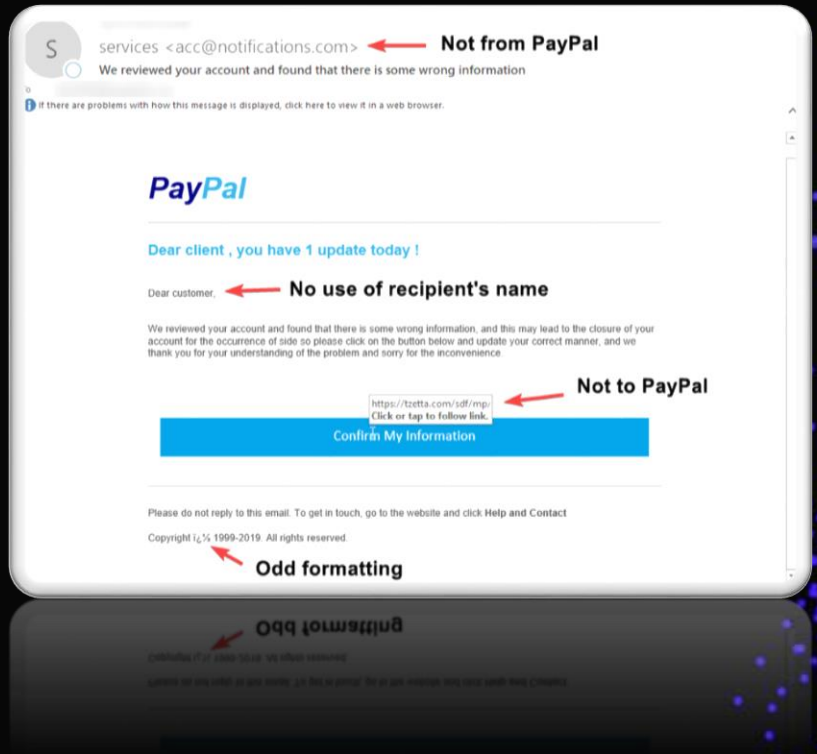
# Urgency and fear tactics

**The attacker can use urgent language like**

**➔ An Account Compromise**

**➔ A security breach**

**➔ Your Password Is Weak**



# Protective Measures

1- Verify Sender Information  ( Sender Email Address )

2- Hover Before you Click  ( to verify the destination before clicking )

3- Use MFA ( Multi Factor Authentication )

# Security Software and Updates

**Updated Software :**

You must update the software , Browsers and security applications ( Up-To-Date )

**Anti-Phishing Tools :**

You must install anti-phishing tools , It helps in detecting and Preventing Phishing Attacks .

# Training and Simulation

## Phishing Simulation :

- You should Simulate the Phishing exercises to provide hands-on experience through Phishing Campaigns .

## Continuous Training :

This simulation should be on-going process and it should be through regular Training sessions

# Consequences Of Failing Victims

## Data Breach

Successful phishing attack can steal

sensitive data like ( Emails , Passwords ,

Cookies , Visa card passwords )

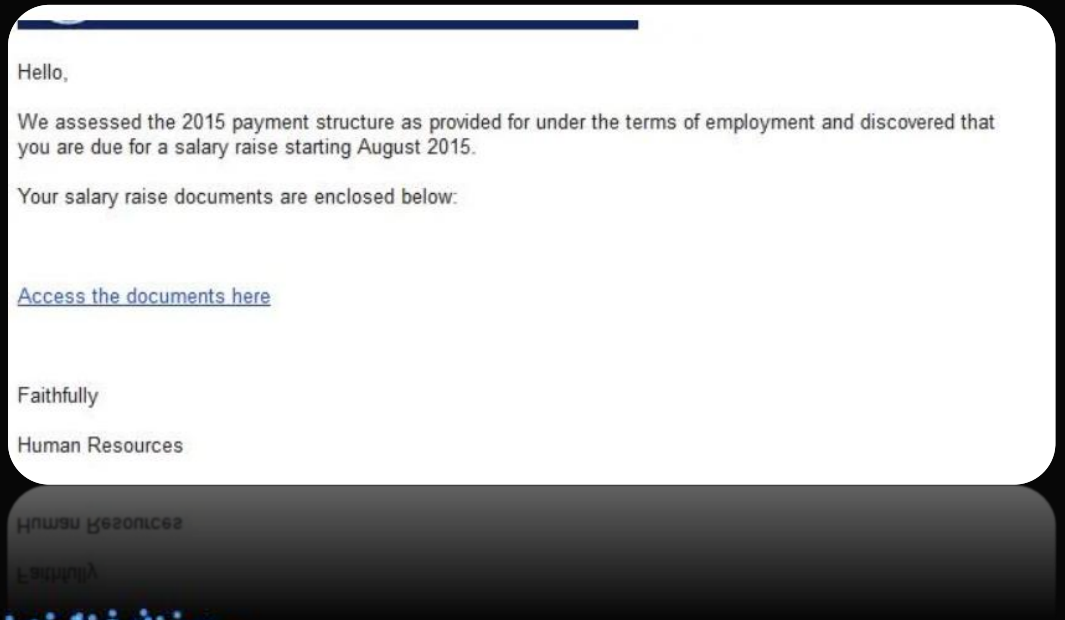
# Financial Loss

You May loss a lot of money Due fraudulent

activities resulting from phishing attacks

# Examples of Phishing Scenarios

1) **Message from HR scam**



Hello,

We assessed the 2015 payment structure as provided for under the terms of employment and discovered that you are due for a salary raise starting August 2015.

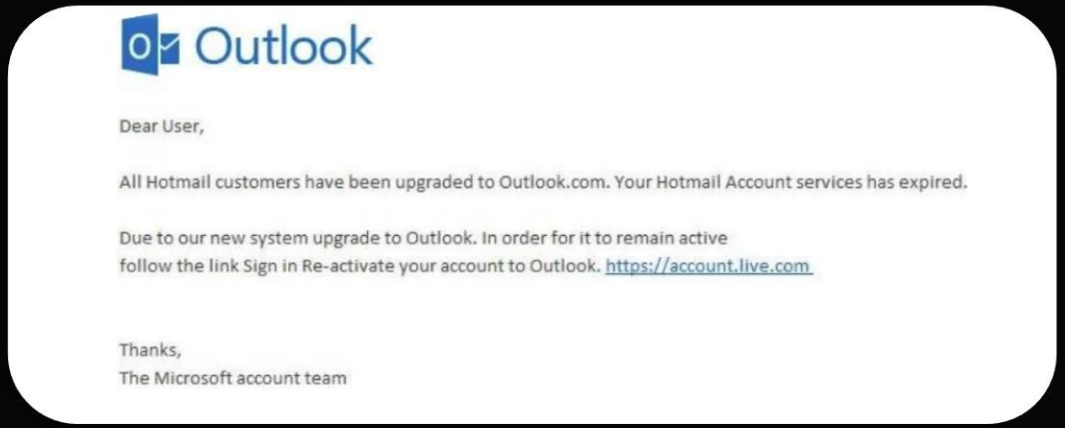
Your salary raise documents are enclosed below:

Access the documents here

Faithfully

Human Resources

# 2) Email account upgrade scam



Outlook

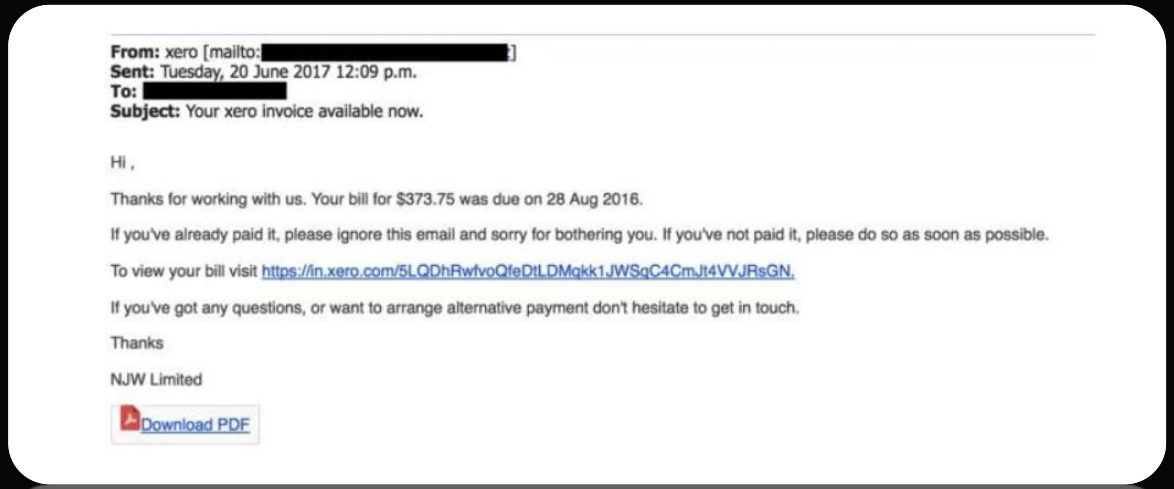
Dear User,

All Hotmail customers have been upgraded to Outlook.com. Your Hotmail Account services has expired.

Due to our new system upgrade to Outlook. In order for it to remain active
follow the link Sign in Re-activate your account to Outlook. https://account.live.com

Thanks,
The Microsoft account team

# 3) Fake invoice scam



**From:** xero [mailto:[redacted]]
**Sent:** Tuesday, 20 June 2017 12:09 p.m.
**To:** [redacted]
**Subject:** Your xero invoice available now.

Hi ,

Thanks for working with us. Your bill for $373.75 was due on 28 Aug 2016.

If you've already paid it, please ignore this email and sorry for bothering you. If you've not paid it, please do so as soon as possible.

To view your bill visit https://in.xero.com/5LQDhRwfvoQfeDtLDMqkk1JWSqC4CmJt4VVJRsGN.

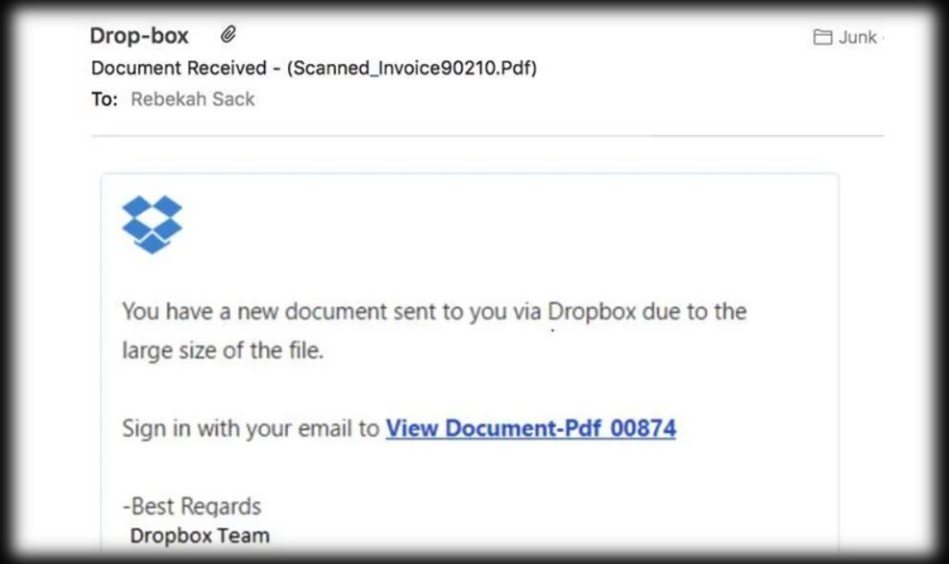
If you've got any questions, or want to arrange alternative payment don't hesitate to get in touch.

Thanks

NJW Limited

Download PDF

# 4) Dropbox scam



# Thanks !