Home About Contact

PHISHING ATTAKS

CYBER THREATS ARE REAL. BE PREPARED.

Prepared by: Aitsy Imane

INTRODUCTION

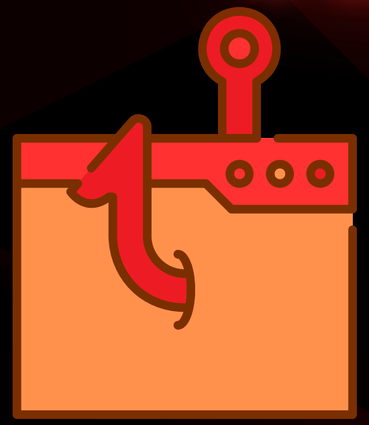
WHAT IS PHISHING?

-Phishing- refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information. By masquerading as a reputable source with an enticing request, an attacker lures in the victim in order to trick them, similarly to how a fisherman uses bait to catch a fish.

How is phishing carried out?

The most common examples of phishing are used to support other malicious actions, such as on-path attack and cross-site scripting attacks. These attacks typically occur via email or instant message, and can be broken down into a few general categories. It's useful to become familiar with a few of these different vectors of phishing attacks in order to spot them in the wild.

COMMON TYPES OF PHISHING



Bulk Phishing

a mass email scam where attackers send the same generic message to many people, hoping some will fall for it.

Spear Phishing

Highly targeted phishing attack aimed at a specific person or organization.

Whaling

A form of spear phishing targeting high-profile individuals like CEOs, executives, or managers, also known as "the big fish."

Smishing (SMS+pishing)

Phishing attempt sent via SMS .

Vishing (Voice + Phishing)

Phishing done via phone calls, often using caller ID spoofing.

HOW TO RECOGNIZE A PHISHING EMAIL?

🔴 Urgent Language

“Act now” or “Urgent!” messages try to scare you. Pause and verify before reacting.

👤 Unknown Sender

Marked [External]? Unknown name? Treat with caution.

📎 Suspicious Links

Hover over the link. Don’t click if the address looks off or unfamiliar.

✉️ Generic Greeting

"Dear user" or "Sir/Madam" is not personal. Be suspicious.

📝 Bad Grammar

Misspelled words, weird phrasing = poor-quality scam.

📧 Fake Email Address

Watch for domains like micros0ft.com or rnicrosoft.com

FAKE WEBSITES

1. Check the URL: Watch for misspellings or strange domain endings (amaz0n.com, amazon-shop.net).

2. Look for a Site Seal: Trusted sites often show a clickable security seal (DigiCert). If it doesn't work, it might be fake.

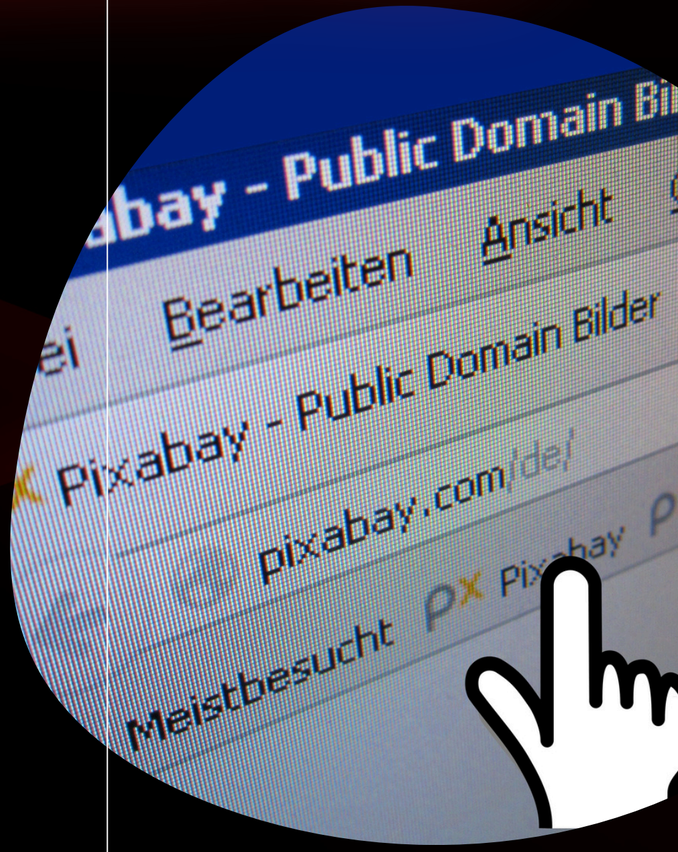
3. Verify Security: Click the padlock icon in the address bar to view certificate info. Avoid sites marked “Not Secure” or showing warnings.

4. Use a Website Checker: Tools like Google Safe Browsing help verify if a site is safe. Just paste the URL.

5. Look for Trust Signals: Legit sites usually include:

- Privacy & return policies
- Contact info
- Correct grammar
- Realistic offers

If it seems too good to be true, it probably is.



SOCIAL ENGINEERING TACTICS USED BY ATTACKERS

What is Social Engineering?

Social engineering tricks people into revealing sensitive information or taking harmful actions by manipulating their emotions, rather than hacking systems.

Common Psychological Tactics:

- Authority

Pretending to be someone important, such as your manager, IT support, or your bank, to pressure you into obeying quickly.

- Fear

Creating panic with threats like “Your account will be locked” or “You’re under investigation.”

- Curiosity or Reward

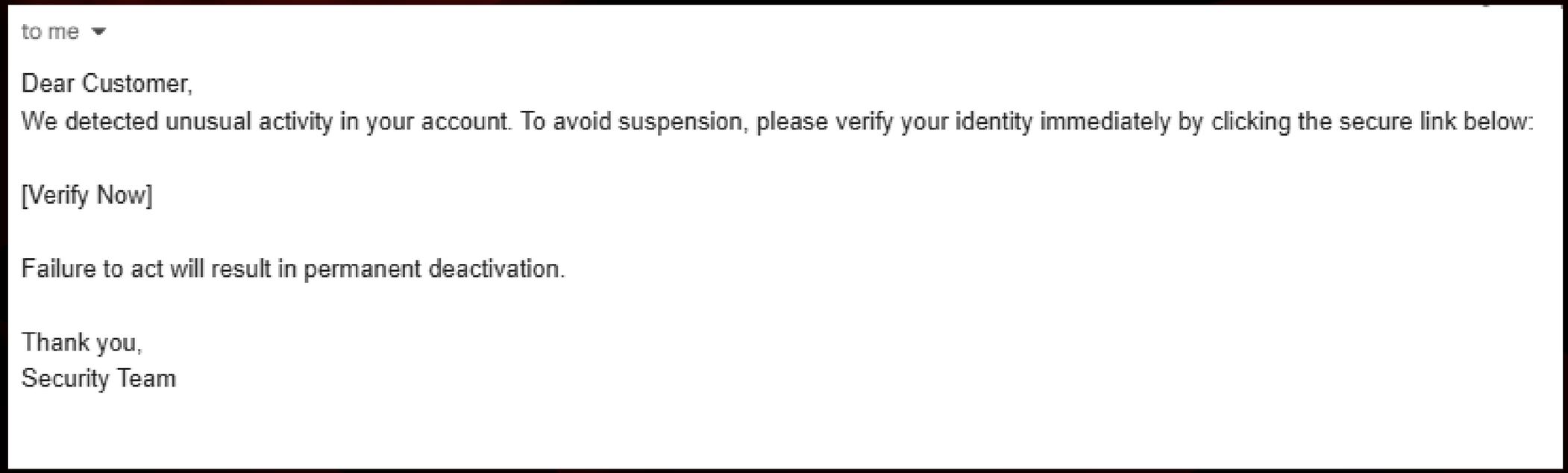
Tempting you with fake prizes, urgent invoices, or exciting news to get you to click or respond.

HOW TO PROTECT YOURSELF

BEST PRACTISES!

- ✔ Never click links in suspicious emails
- ✔ Always check the sender’s address
- ✔ Hover over links before clicking
- ✔ Use multi-factor authentication (MFA)
- ✔ Keep software up to date
- ✔ Report suspicious messages to IT

QUIZ TIME!
SPOT THE PHISH



to me

Dear Customer,
We detected unusual activity in your account. To avoid suspension, please verify your identity immediately by clicking the secure link below:

[Verify Now]

Failure to act will result in permanent deactivation.

Thank you,
Security Team

What are the red flags in this email?

A. Vague sender identity
B. Sense of urgency/threat
C. Poor grammar and generic greeting
D. Secure-looking link
E. It asks you to click a link

Correct Answers:
A, B, C, E

REAL-WORLD EXAMPLE

The Sony Pictures Leak

2014 saw a huge data leak from Sony. Over 100 Terabytes containing confidential company activities were breached, resulting in well over $100 million lost. The phishers pretended to be colleagues of the top-level employees who opened the malicious attachments in the phishing emails.
Specifically, a fake Apple ID verification email was used in the attack. Through a combination of LinkedIn data and Apple ID logins, the phishers managed to find passwords that matched the ones used for the Sony network - a great example of why using different passwords for different online accounts is so important.

2018 World Cup

The Federal Trade Commission released this statement regarding phishing attempts during the 2018 World Cup in Russia. The scam claimed the victim won tickets to the World Cup through a lottery and prompted them to enter their personal information to claim the prize.
At the same time, a handful of rental scams were reported as well. Cybercriminals stole the email addresses of genuine landlords in Russia and offered ridiculously low prices for their properties during the sporting event. Once a "lucky buyer" accepted the offer, his or her credit card information was stolen.