Phishing Awareness

Don’t let curiosity sink your security!

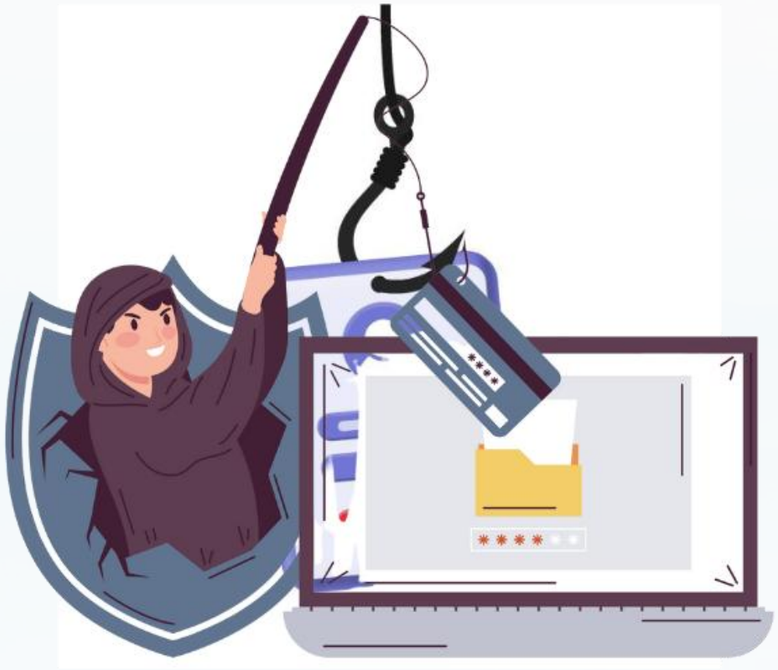
Detection & Awareness

Protection & Prevention

Education & Response

MD SHAMIUL ISLAM - Cyber Security Intern

What is Phishing?



Digital Scam

Cybercriminals try to steal sensitive information by impersonating trusted organizations or individuals.

Massive Scale

Over 300,000 phishing attacks happen daily worldwide.

Mimicked Trust

Attackers impersonate familiar brands to trick victims into sharing information.

Primary Targets

Passwords, financial details, and personal identity information are at risk.

The Real Cost of Phishing

$4.45M

Average Breach Cost

Per data breach in 2023

83%

Organizations Affected

Experienced phishing attacks in 2023

$8,000

Individual Loss

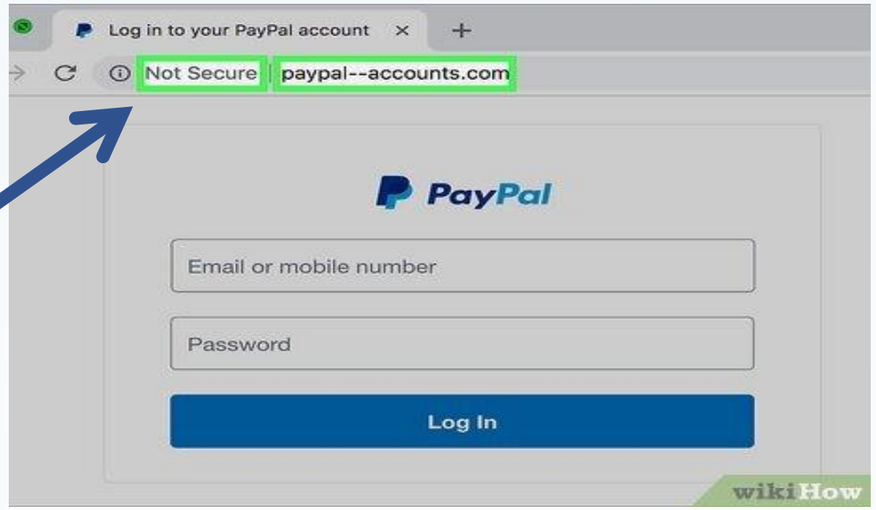
Average financial impact per victim

In addition to financial losses, organizations also experience severe damage to their reputation, which can take years to restore.

Common Types of Phishing

Email Phishing

Do Not Click!
That's Obviously a Malicious Email



Alert!
Unsecure page
Not the official PayPal website
Do not enter your credentials

Website Phishing

Common Types of Phishing

Smishing Phishing (SMS)

Spam Message!!
Do Not Click

Caller ID Spoofing
Do Not FALL

Vishing Phishing (Voice)

How Phishing Works

Deceptive Messages

Criminals craft emails that mimic legitimate organizations.

Urgency Tactics

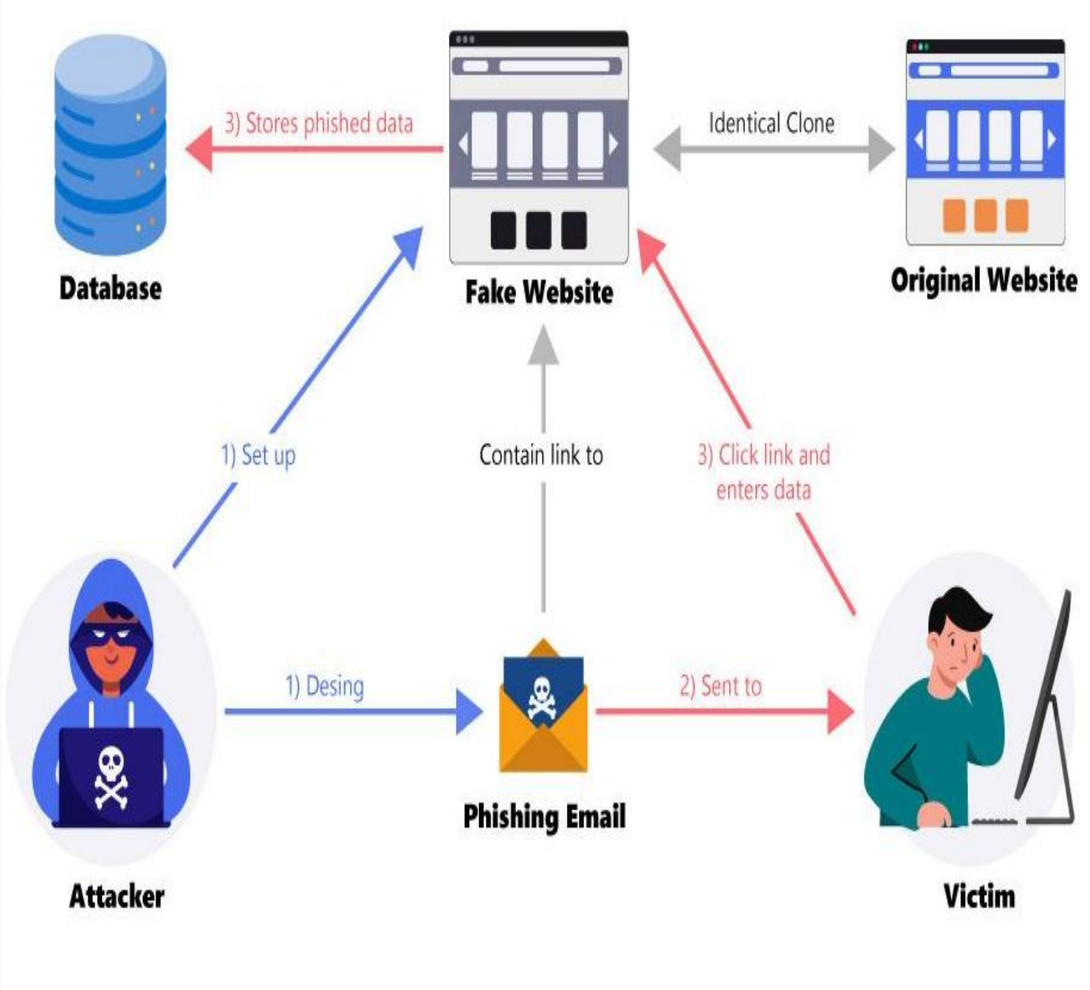
Messages create false emergencies requiring immediate action.

Malicious Attachments

Files contain hidden malware that installs when opened.

Disguised Links

URLs appear legitimate but direct to fraudulent websites.



Red Flags to Recognize

Suspicious Sender

Email addresses with slight misspellings or unusual domains.

Poor Grammar

Spelling errors and awkward phrasing indicate fraudulent messages.

Urgent Requests

Messages demanding immediate action to create panic.

Too Good To Be True

Unrealistic offers or unexpected winnings signal scams.

Verification Techniques

Inspect Links

Hover over links to see the actual URL before clicking. Ensure it matches the expected destination.

Examine Sender Details

Check the full email address, not just the display name. Look for subtle misspellings.

Verify Independently

Contact organizations through official phone numbers or websites you manually navigate to.

Enable Protection

Use multi-factor authentication on all accounts to add an extra security layer.

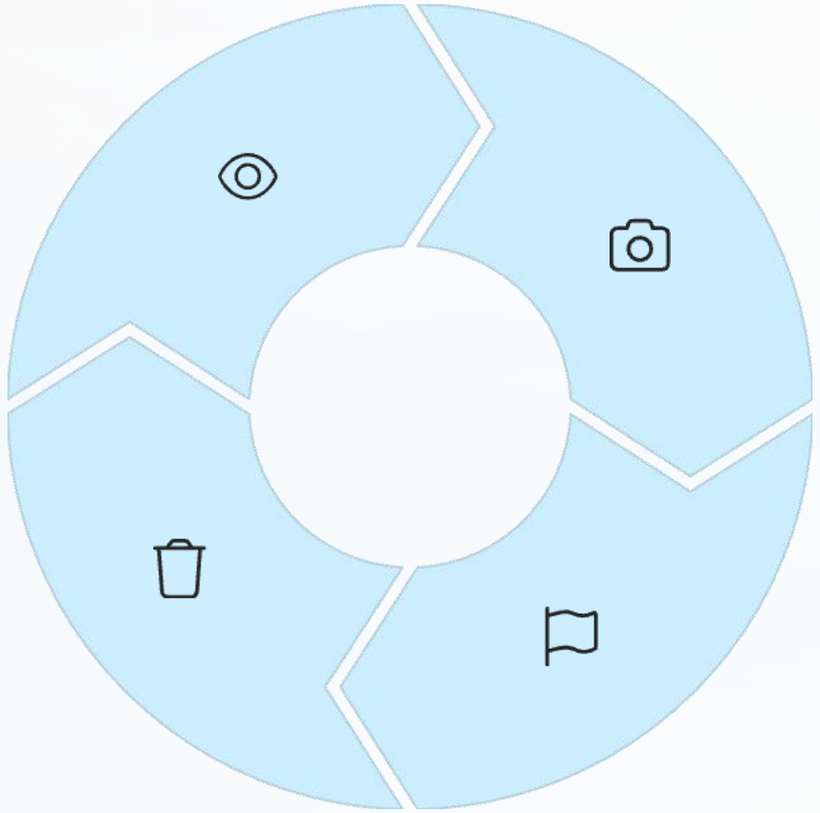
Reporting Suspicious Activity

Identify

Recognize potential phishing attempts using red flags.

Document

Take screenshots of suspicious messages for evidence.



Delete

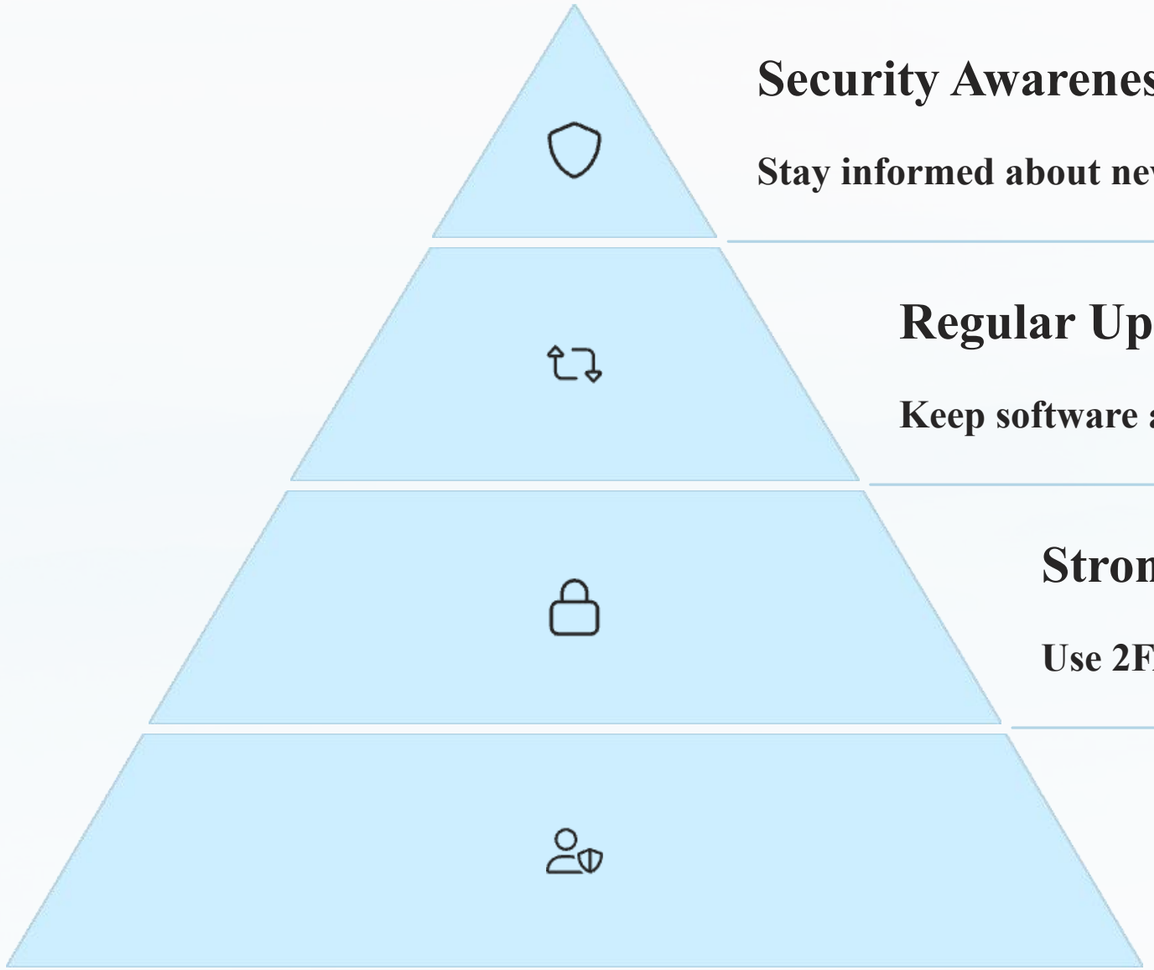
Remove the suspicious email from your inbox.

Report

Forward to IT security team.

Quick reporting can prevent attacks from spreading to colleagues. Your vigilance protects everyone.

Protecting Your Digital Self



Security Awareness

Stay informed about new threats

Regular Updates

Keep software and systems current

Strong Authentication

Use 2FA and password managers

Personal Vigilance

Think before clicking any links

Stay Vigilant, Stay Safe

Shared Responsibility

Every employee plays a critical role in organizational security.

One-Click Impact

A single click can compromise entire networks. Think before you act.

Trust Your Instincts

If something feels suspicious, it probably is. Follow your gut feeling.

Ask For Help

When uncertain, contact IT security for guidance before proceeding.

THANK YOU