Phishing Awareness Training

By:-

Shreya Kale

Introduction

Objective: To educate people on the dangers of phishing and how to recognize and avoid phishing attempts.

WHAT IS PHISHING?

Phishing is a cyberattack where attackers disguise themselves as legitimate entities to steal sensitive information.

Common Targets: Emails, websites, social media, phone calls.

Types of Phishing Attacks

1) Email Phishing

2) Spear Phishing

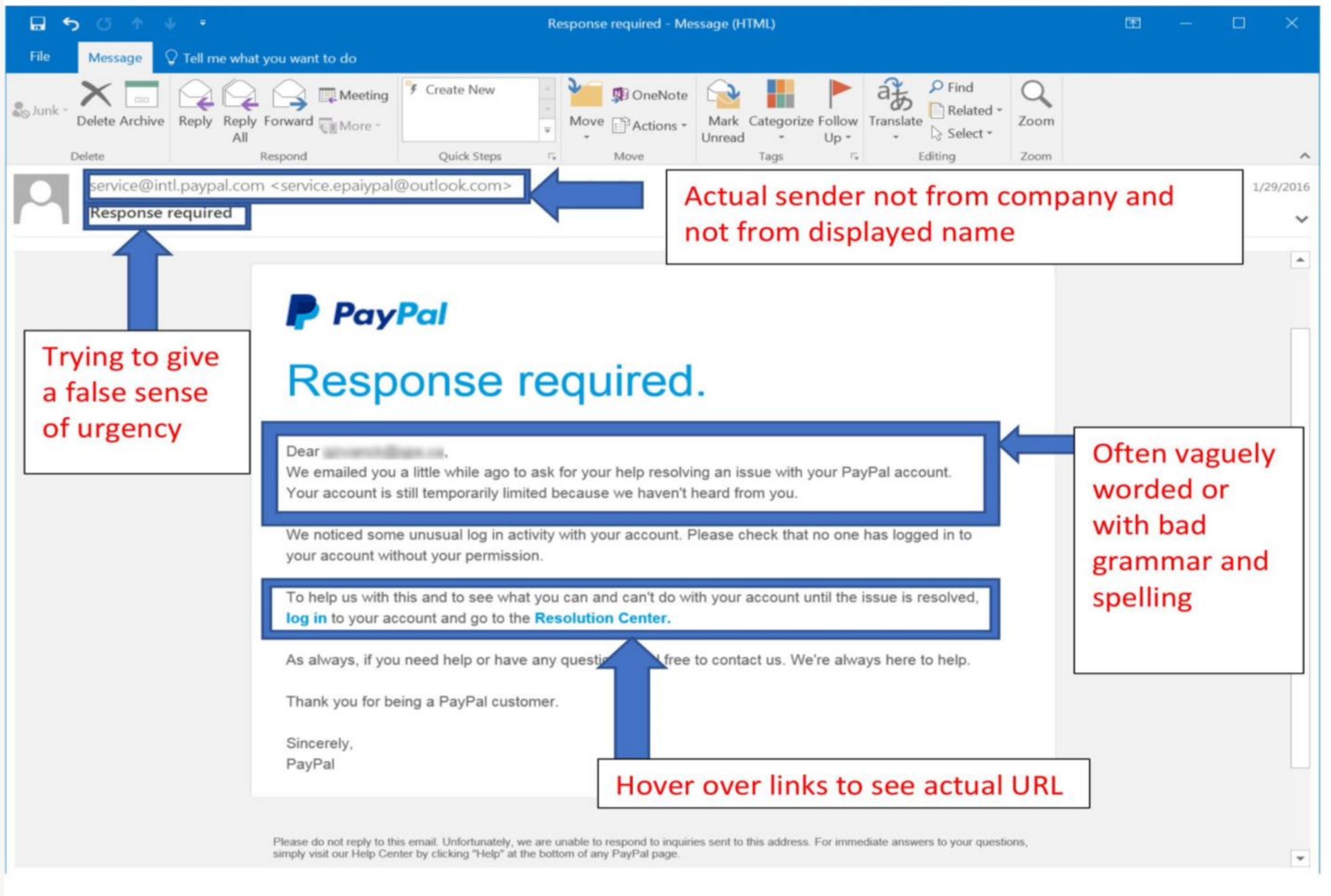
3) Whaling

4) Smishing

5) Vishing

Anatomy of a Phishing Email

- **Sender's Address:** Often looks legitimate but with slight variations.
- **Subject Line:** Urgent or alarming messages.
- **Content:** Requests for personal information, fake links, and attachments with malware.
- **Example:** Show a screenshot of a typical phishing email and highlight the red flags.



service@intl.paypal.com <service.epaiypal@outlook.com>

Response required

Actual sender not from company and not from displayed name

Trying to give a false sense of urgency

Response required.

Dear [redacted],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, **log in** to your account and go to the **Resolution Center.**

As always, if you need help or have any questi[illegible] free to contact us. We're always here to help.

Thank you for being a PayPal customer.

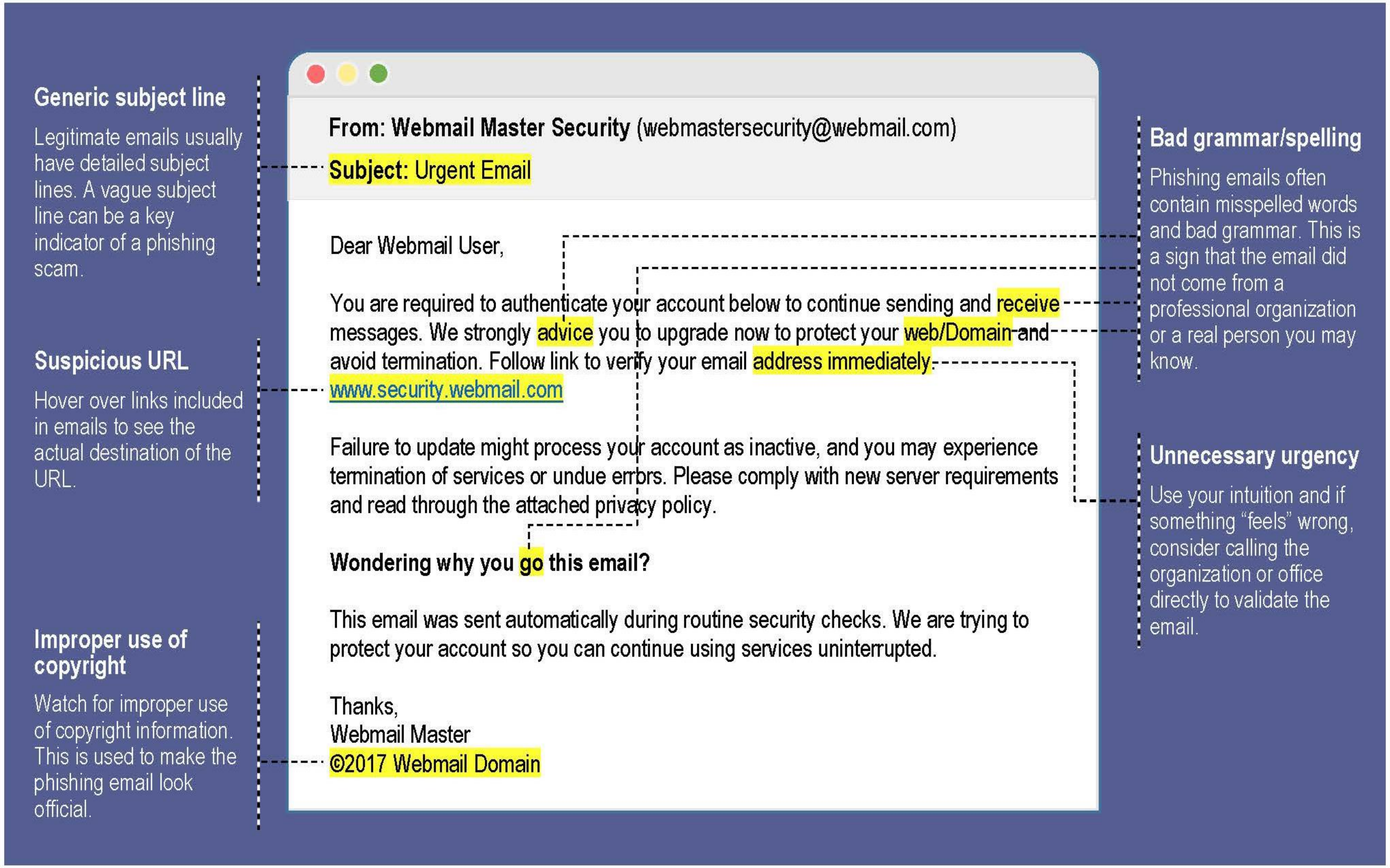
Sincerely,
PayPal

Often vaguely worded or with bad grammar and spelling

Hover over links to see actual URL

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

How to Spot a Phishing Email



Generic subject line

Legitimate emails usually have detailed subject lines. A vague subject line can be a key indicator of a phishing scam.

Suspicious URL

Hover over links included in emails to see the actual destination of the URL.

Improper use of copyright

Watch for improper use of copyright information. This is used to make the phishing email look official.

From: Webmail Master Security (webmastersecurity@webmail.com)

Subject: Urgent Email

Dear Webmail User,

You are required to authenticate your account below to continue sending and receive messages. We strongly advice you to upgrade now to protect your web/Domain and avoid termination. Follow link to verify your email address immediately.
www.security.webmail.com

Failure to update might process your account as inactive, and you may experience termination of services or undue errors. Please comply with new server requirements and read through the attached privacy policy.

Wondering why you go this email?

This email was sent automatically during routine security checks. We are trying to protect your account so you can continue using services uninterrupted.

Thanks,
Webmail Master
©2017 Webmail Domain

Bad grammar/spelling

Phishing emails often contain misspelled words and bad grammar. This is a sign that the email did not come from a professional organization or a real person you may know.

Unnecessary urgency

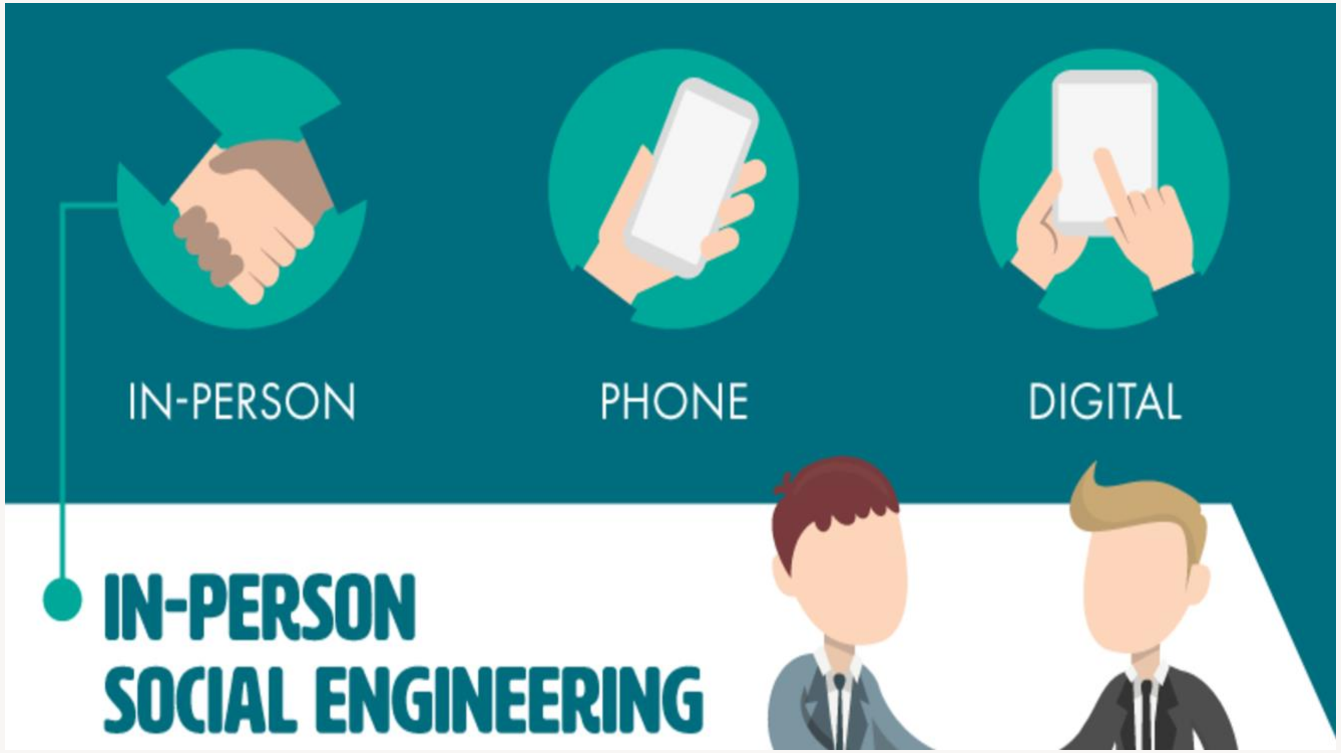
Use your intuition and if something "feels" wrong, consider calling the organization or office directly to validate the email.

Recognizing Phishing Websites

- **URL Check:** Look for slight misspellings or unusual domains.
- **HTTPS vs. HTTP:** Not all HTTPS sites are safe, but absence of HTTPS is a red flag.
- **Design Flaws:** Poor grammar, spelling mistakes, and low-quality logos.
- **Example:** Show screenshots comparing a legitimate website and a phishing website.

Social Engineering Tactics

- **Impersonation:** Attackers posing as trusted entities.
- **Pretexting:** Creating a fabricated scenario to steal information.
- **Baiting:** Offering something enticing to lure victims.
- **Tailgating:** Following someone into a restricted area.



Real - World Example

Recent phishing scan news:

- **Incident Date:** March 2020
- **What Happened:** A sophisticated phishing campaign targeted users by impersonating the World Health Organization (WHO) amid the COVID-19 pandemic.
- **Method:** Attackers sent emails that appeared to come from WHO, using fear and urgency related to COVID-19 to trick recipients into clicking on malicious links or downloading infected attachments.
- **Impact:** The campaign led to the compromise of personal information, credentials, and in some cases, financial losses for individuals and organizations.

How to Protect Yourself?

- **Verify Before Trusting:** Always verify the source before clicking on links or providing information.
- **Use Multi-Factor Authentication (MFA):** Adds an extra layer of security.
- **Keep Software Updated:** Regular updates protect against known vulnerabilities.
- **Educate Yourself and Others:** Stay informed about the latest phishing techniques.

Best Practices for Email Security:

- **Don't Click on Suspicious Links:** Hover over links to check the URL.
- **Check Email Headers:** Examine the sender’s email address.
- **Report Suspicious Emails:** Know your organization's protocol for reporting phishing attempts.
- **Use Spam Filters:** Ensure your email client has effective spam filtering enabled.

Conclusion

In conclusion, phishing is a common cyberattack where scammers try to steal your personal information by pretending to be trustworthy sources. To protect yourself, always verify the sender's identity, be cautious of suspicious links and attachments, use multi-factor authentication, keep your software updated, and report any suspicious activity to your IT or security team. Staying informed and vigilant are your best defenses against phishing attempts.

Thank you

Shreya Kale

shreyakale660@gmail.com