

PHISHING

don't get hooked

- Sandeep Kumar

Objectives

- Define phishing and identify various types of phishing scams
- Recognize common baiting tactics used in phishing scams
- Examine real phishing messages
- Understand how to protect yourself from being hooked by a phishing scam



Phishing: What is it?

- **Phishing** – Cybercriminal attempts to steal personal and financial information or infect computers and other devices with malware and viruses
 - Designed to trick you into clicking a link or providing personal or financial information
 - Often in the form of emails and websites
 - May appear to come from legitimate companies, organizations or known individuals
 - Take advantage of natural disasters, epidemics, health scares, political elections or timely events



Types of Phishing

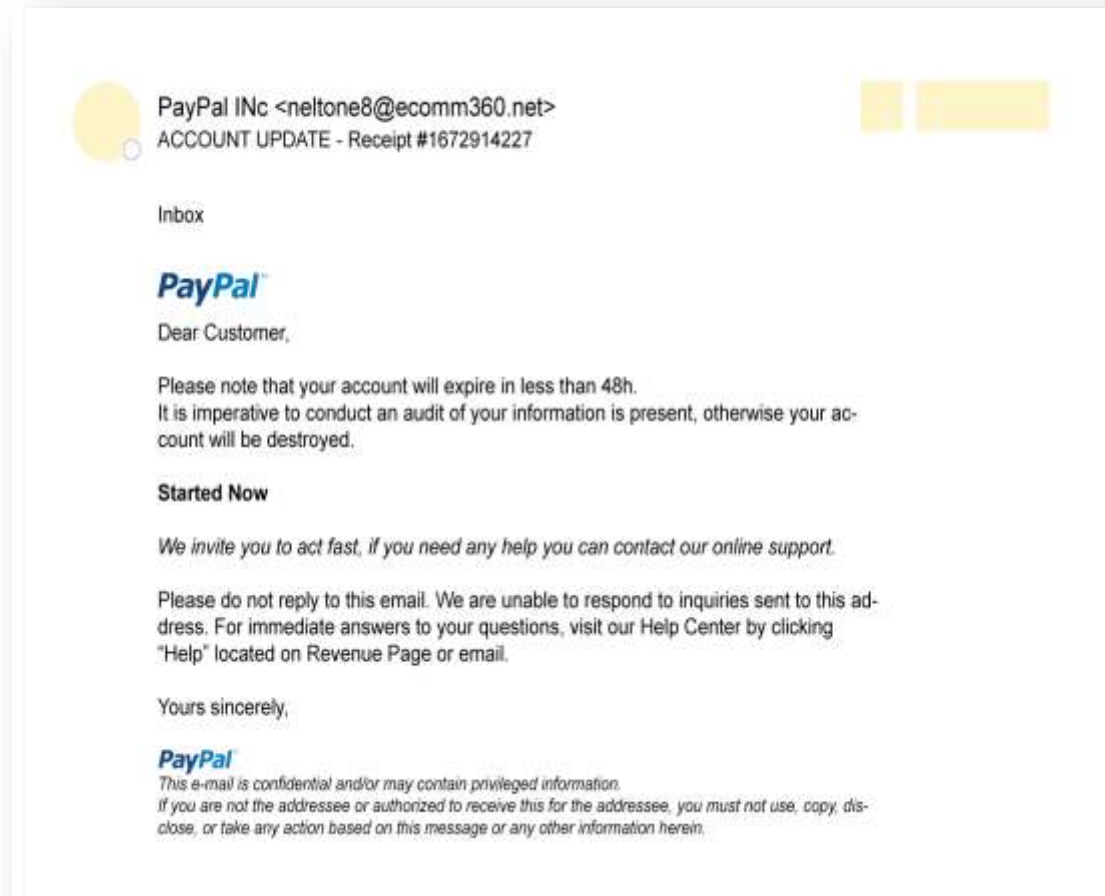
- **Mass Phishing** – Mass, large-volume attack intended to reach as many people as possible
- **Spear Phishing** – Targeted attack directed at specific individuals or companies using gathered information to personalize the message and make the scam more difficult to detect
- **Whaling** – Type of spear phishing attack that targets “big fish,” including high-profile individuals or those with a great deal of authority or access
- **Clone Phishing** – Spoofed copy of a legitimate and previously delivered email, with original attachments or hyperlinks replaced with malicious versions, which is sent from a forged email address so it appears to come from the original sender or another legitimate source
- **Advance-Fee Scam:** Requests the target to send money or bank account information to the cybercriminal

Common Baiting Tactics

- **Notification from a help desk or system administrator**
Asks you to take action to resolve an issue with your account (e.g., email account has reached its storage limit), which often includes clicking on a link and providing requested information.
- **Advertisement for immediate weight loss, hair growth or fitness prowess**
Serves as a ploy to get you to click on a link that will infect your computer or mobile device with malware or viruses.
- **Attachment labeled “invoice” or “shipping order”**
Contains malware that can infect your computer or mobile device if opened. May contain what is known as “ransomware,” a type of malware that will delete all files unless you pay a specified sum of money.
- **Notification from what appears to be a credit card company**
Indicates someone has made an unauthorized transaction on your account. If you click the link to log in to verify the transaction, your username and password are collected by the scammer.
- **Fake account on a social media site**
Mimics a legitimate person, business or organization. May also appear in the form of an online game, quiz or survey designed to collect information from your account.

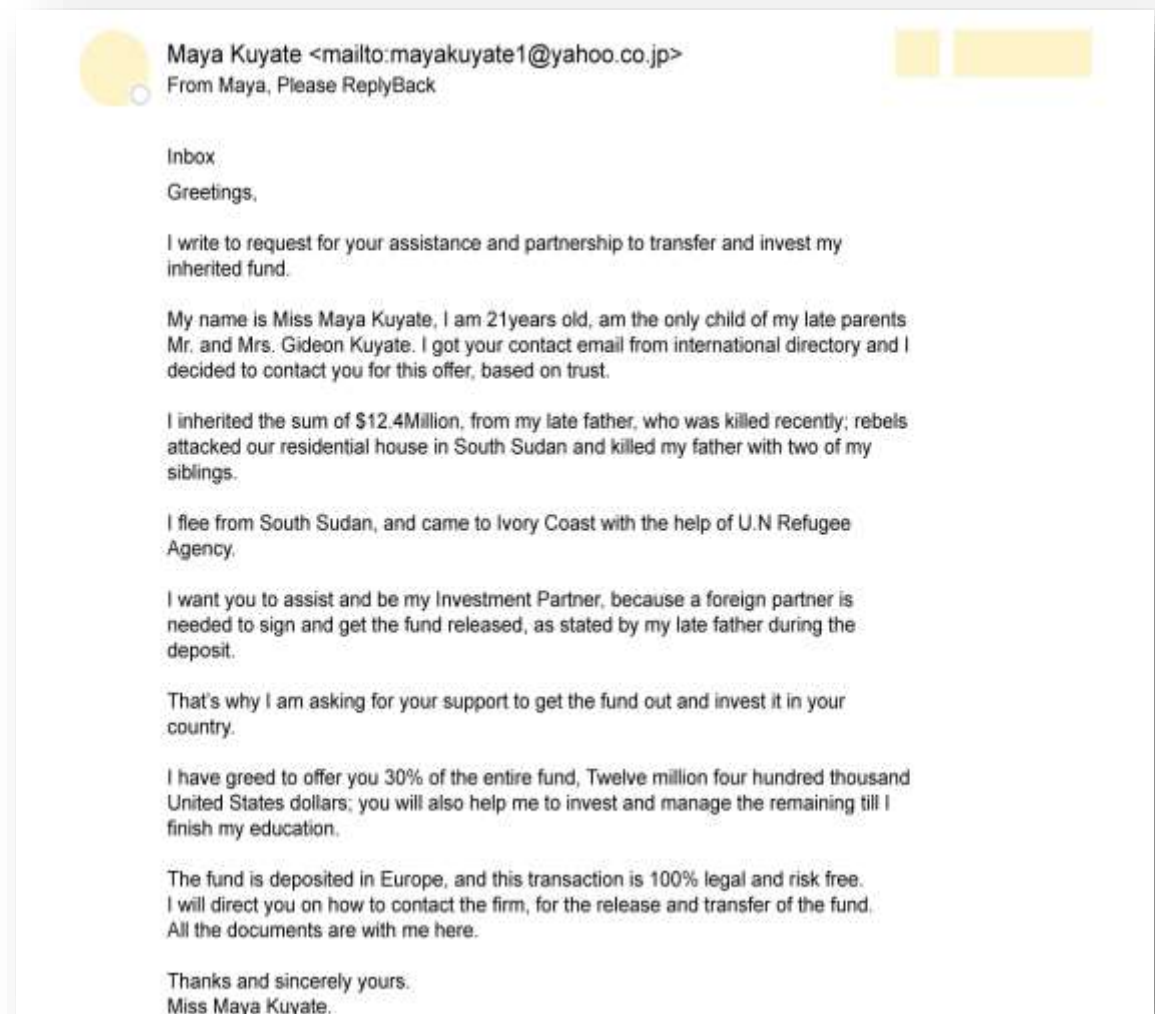
Phishing Lure

- Claims to come from PayPal
 - Includes PayPal logo, but from address is not legitimate (@ecomm360.net)
 - Calls for immediate action using threatening language
- Includes hyperlink that points to fraudulent site



Phishing Lure

- Likely an advanced-fee scam
 - Takes advantage of ongoing humanitarian crisis
 - If it sounds too good to be true, it likely is



Detect a Phishing Scam

- Spelling errors (e.g., “pessward”), lack of punctuation or poor grammar
- Hyperlinked URL differs from the one displayed, or it is hidden
- Threatening language that calls for immediate action
- Requests for personal information
- Announcement indicating you won a prize or lottery
- Requests for donations

Can you detect a phishing scam?



Tricia Jardon <jardonTricia607@hafenweb.com>



Inbox

Please see the attached invoice and remit payment according to terms listed at the bottom of the invoice.

If you have any questions please let us know.



copy_847637.zip
3 MB



↓ Do you know the sender?



Tricia Jardon <jardonTricia607@hafenweb.com>

Inbox

Please see the attached invoice and remit payment according to terms listed at the bottom of the invoice.

↑ There is no greeting

If you have any questions please let us know.

↑ There is no salutation or signature



copy_847637.zip
3 MB


↑ Are you expecting an attachment from this person or company?

Protect Yourself: Refuse the Bait

- STOP. THINK. CONNECT.
 - Before you click, look for common baiting tactics
 - If the message looks suspicious or too good to be true, treat it as such
- Install and maintain antivirus software on your electronic devices
- Use email filters to reduce spam and malicious traffic

Protect Yourself: Refuse the Bait

- Do not click on any hyperlinks in the email
 - User your computer mouse to hover over each link to verify its actual destination, even if the message appears to be from a trusted source
 - Pay attention to the URL and look for a variation in spelling or different domain (e.g., **HACKITTECH.COM** vs. **HACKITHECH.COM**) here one is Capital I and another is small L
 - Consider navigating to familiar sites on your own instead of using links within messages
- Examine websites closely
 - Malicious websites may look identical to legitimate sites
 - Look for "https://" or a lock icon in the address bar before entering any sensitive information on a website



THANK
YOU