Cybercrime Prevention Flyer

CPF 0013-2020-CID361-9H 05 August 2020

Phishing Scams and Email Spoofing

The Internet Crime Complaint Center identified phishing and spoofing in the top five methods cybercriminals used during 2019 to cause more than $350 million in victim losses. With a little knowledge, the losses could likely have been reduced.

What is a phishing email?

A phishing email is an email designed to convince the recipient to divulge personal information, banking or credit card information, or passwords.

What is email spoofing?

Email spoofing is the forgery of the “From” address to make the email appear as if it was sent from a different, or more reputable, sender. Email spoofing is display-name deception and a tactic often used by cybercriminals to lure unsuspecting victims to the legitimacy of phishing scam emails.

How are phishing and email spoofing used together?

Combining the two, cybercriminals use deception to convince, scam, recipients into believing an email was sent from a legitimate and reputable organization or company and that a specific action is required. The sender’s email address looks authentic, the subject line appears valid, and the email body contains a simple and somewhat convincing message usually accompanied by a website link. However, not everything is as it appears. See if you can recognize some indicators in the following email phishing scam.

From: PayPal<directiq.com@Hayato--Lapu-Lapu.pj0l3pirubtramsd.masukgan.nuliskun.com>
Date: June 20, 2020 at 2:24:55 PM EDT
To: [redacted]@yahoo.com
Subject: Your account has been limited until we hear from you Case-ID: 117461 date: 6/20/2020 6:24:52 PM

PayPal

Dear, [redacted]@yahoo.com,

Suspicious Activity on Your Account

Your Account information has been changed. [Billing or Shipping Address] As our security precautions, we need more informations from you. Your account Has been limited until you provide some additional information.
Please login into your Account and review your activity by clicking link below:

https://paypal.com/login?

Your action is required to help us to protect you PayPal account securely.

PayPal.com

Report a crime to U.S. Army Criminal Investigation Command

Major Cybercrime Unit

27130 Telegraph Road
Quantico, Virginia 22134

Email

MCU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

“DO WHAT HAS TO BE DONE”

The email appears to come from PayPal. After closer examination, the actual sender of the email is identified as directiq.com[@]Hayato--Lapu-Lapu.pj0l3pirubtramsd.masukgan.nuliskun.com.

From: PayPal <directiq.com@Hayato--Lapu-Lapu.pj0l3pirubtramsd.masukgan.nuliskun.com>

The email was sent at 2:24:55 PM on June 20, 2020, but the subject of the email has a time of four hours in the future.

Date: June 20, 2020 at 2:24:55 PM EDT
To: [redacted]@yahoo.com
Subject: Your account has been limited until we hear from you Case-ID: 117461 date: 6/20/2020 6:24:52 PM

The last sentence in the email contains a grammatical error.

Your action is required to help us to protect you PayPal account securely.

Hovering over the hypertext, you would see the link is actually directed to the URL https[:]//rebrand.ly9s79hts, registered to an entity residing in Italy.

https://paypal.com/login?

https://rebrand.ly/9s79ht5

The scammer who created this email used PayPal's reputation to convince the recipient of the email's legitimacy. PayPal is not the only company scammers will use, but one of many.

Furthermore, the recipient has a Yahoo email address. Yahoo is not the only email service provider receiving spoofed emails. Scam emails, with spoofed email addresses, are also sent through other email service providers, including the government and military.

Detect, Protect, and Report

Email service providers, as hard as they may try, cannot detect all phishing and spoofed emails and cannot protect you should you click on links in phishing emails. You, the email recipient, are the last and most pivotal line of defense from becoming a cybercrime victim. Here are some steps you can take to detect, protect, and report phishing and spoofed emails.

Detect

- Keep an eye out for incorrect spelling and poor grammar in emails.
- Pay close attention to the sender email address; click on the display name if the email address is not visible.
- Be extra cautious if an email asks for personally identifiable information, financial account information, or passwords.
- Be suspicious of emails asking you to click a link to change a password, especially if you did not make the password change request.

Protect

- If the email seems suspicious, but you recognize the display name, contact the sender offline, via call or text, to verify they sent the email. Do not use any phone numbers provided in the email.
- Never click an unfamiliar link or download an attachment if you suspect the email is spoofed.
- Type in URLs or use a search engine to locate websites, if you have to log into an account.
- Turn on spam filtering to stop the majority of phishing and spoofed emails. Keep in mind, legitimate emails are sometimes flagged as spam emails.
- Scan your computer for malware regularly.
- Check account settings. If any accounts offer multifactor authentication, enable it for an additional layer of security.

Report

- Report phishing and spoofed emails to your email service provider for personal email accounts. For official government and military email accounts, report them to your system administrator or security representative.
- If you become a fraud, identity theft, or deceptive business practice victim, file a report with the Federal Trade Commission and the Internet Crime Complaint Center.

Think you can spot email phishing?

Test your skills with this Phishing Quiz.

References

How to Recognize and Avoid Phishing Scams - FTC

How to Recognize and Avoid a Phishing Scam - UIOWA

Phishing email examples to help you identify phishing scams - Norton

Email Spoofing 101: How to Avoid Becoming a Victim - Security Boulevard

To receive future MCU Cybercrime Prevention Flyers, send an email to:
usarmy.belvoir.usacidc.mbx.mcu-cyber-crime-intelligence@mail.mil
with "SUBSCRIBE: CPF" in the subject line.