

Objectives:

This investigation is to demonstrate how to identify a phishing email and the tell-tell signs that can be used to protect organisations. To continuously enhance email security by leveraging available sandboxes and real-time monitoring

Introduction

What is Phishing?

Is a type of cyber-attack where attackers masquerade as a trusted entity to trick individuals into revealing sensitive information such as login credentials, financial details, or personal data. It is commonly carried out through emails, fake websites, text messages, or phone calls.

Common types of Phishing:

Email Phishing: Fake emails that appear to come from a legitimate source to steal credentials or deliver malicious software.

Spear Phishing: These are targeted attacks on specific individuals or organisations using personalized information:

Whaling: High-level phishing targeting executives or high-profile individuals.

Smishing: Fraudulent text messages with malicious links or requests for sensitive data.

Vishing: Phone scams where attackers pretend to be a trusted entity e.g. calls for banks, IT dept.

Phishing emails are highly successful and are among the most effective cyber-attack methods. Their success varies based on the target sophistication, attack method, and security awareness of the individual receiving the email.

Factors that increase phishing email success:

1. **Social Engineering:** Attackers use urgency, fear, or curiosity for example urgent password reset, fake invoices
2. **Personalisation:** Spear phishing emails normally include personal details making them highly successful.
3. **Poor Cybersecurity awareness:** Employees without are more susceptible to clicking on fake emails

How to identify a phishing email: There are initial indicators that can be used to determine/warn a phishing attempt. These include

- **Urgent or Threatening language:** Phishing emails use language that prompts immediate action for example account closures, or urgent changing of password/s.
- **Generic Salutation:** "Dear Customer" is a common salutation that is used in phishing emails. Legitimate organisations normally personalize emails.
- **Look-a-like Sender Information:** Phishing emails may come from an address that closely resembles a legitimate organisation but with subtle differences, for example, unusual domain names, and misspellings.
- **Suspicious Links and Attachments:** It is good practice to hover over any links without clicking them this will show the URL be sure it matches what you expect before clicking. As for attachments, it is advisable to get an expert opinion if unsure.

- **Poor Grammar/Spelling mistakes:** Multiple errors in the grammar and spelling mistakes can be a red flag. Legitimate professional organizations have a high standard of communication

Further analysis can be carried out on the suspected email to determine if it is a phishing attempt by looking at the Email header.

Email headers are pieces of metadata that provide detailed information about the email's origins, route taken, and handling before it reaches the final destination. Some of the details contained in the email headers are

- **Sender and Recipient information:** Email address of the sender and the receiver
- **Routing data:** A series of "Received" lines that trace the email's journey across different mail servers, indicating the path it took and the timestamps at each step
- **Authentication results:** Information from mechanisms like SPF, DKIM, and DMARC help verify the sender's identity and access the email's legitimacy.
- **Message Metadata:** This data contains the Subject, date, time the email was sent, and a unique message ID which can be used for tracking the email.

What is SPF, DKIM, and DMARC?

SPF, DKIM, and DMARC are three email authentication methods. Together these can be used to identify spammers, phishing emails, and other unauthorised parties that send emails.

How does SPF work?

Sender Policy Framework (SPF): Is a way for the domain to list all the servers they send emails from. SPF records list all the IP addresses of all the servers that are allowed to send emails from an organization's domain. Mail servers that receive emails check against the SPF record before passing it on to the recipient's inbox.

How does DKIM work?

Domain Keys Identified Mail (DKIM) enables domain users to automatically sign emails for their domain. The DKIM signature is a digital signature that uses public key cryptography to verify that the email came from the domain. The DKIM record stores the public key and the mail servers receiving emails from the domain can check this record to obtain the public key. The private key is kept secret by the sender who signs the email header with this key

How does DMARC work?

Domain-based Message Authentication and Conformance (DMARC) tells the receiver that receives emails what to do given the results after checking SPF and DKIM. The DMARC policy can be set in various ways one of which is to quarantine emails that fail SPF or DKIM or both.

Part 2

Demonstration of checking a suspicious phishing email.

Example 1

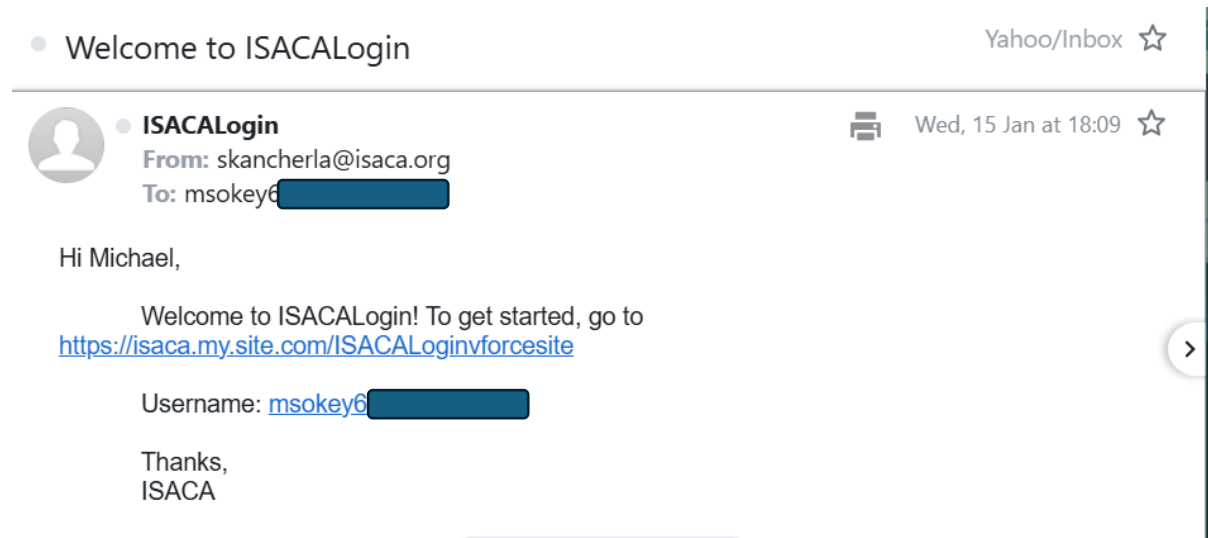


Figure 1

The above email was sent to all ISACA members. Most members thought it was a phishing email. To investigate this, click on the 3 dots next to Spam then click on View raw message

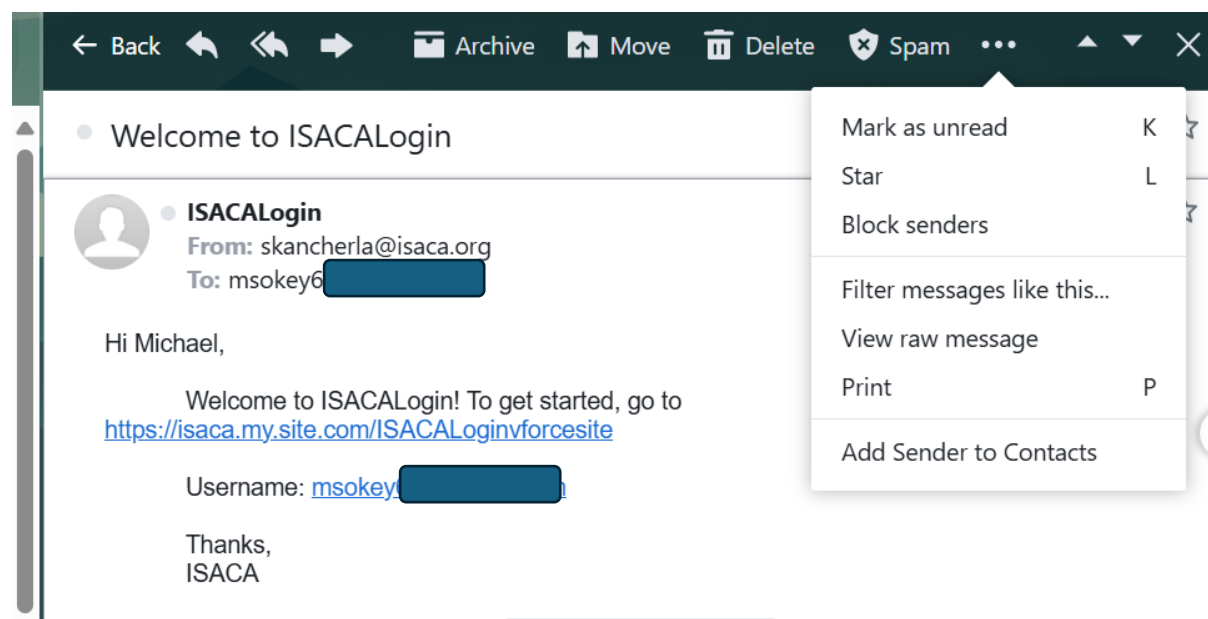


Figure 2

The raw format of the email will be displayed - Figure 3

```

Received: from 10.197.40.105
by atlas207.free.mail.bf1.yahoo.com pod-id NONE with HTTPS; Wed, 15 Jan 2025 18:09:06 +0000
Return-Path: <skancherla@isaca.org_4r3fhv7ntm1035f9@s174e836j1eb.a-ku9nmaw.usa692.bnc.salesforce.com>
X-Originating-IP: [54.149.23.30]
Received-SPF: pass (domain of s174e836j1eb.a-ku9nmaw.usa692.bnc.salesforce.com designates 54.149.23.30 as permitted sender)
Authentication-Results: atlas207.free.mail.bf1.yahoo.com;
dkim=pass header.i=@isaca.org header.s=selector5 arc_overridden_status=NOT_OVERRIDDEN;
spf=pass smtp.mailfrom=s174e836j1eb.a-ku9nmaw.usa692.bnc.salesforce.com arc_overridden_status=NOT_OVERRIDDEN;
dmarc=pass(p=QUARANTINE,sp=QUARANTINE) header.from=isaca.org arc_overridden_status=NOT_OVERRIDDEN;

```

Figure 3

Things to look out for spf, dkim,, dmarc return path. The spf = pass , dkim=pass and dmarc = pass, return path normally should be the same as the From address in the main email.

The link in the email can be copied and pasted into a tool like Virus Total. If a match is found in the database, it will be flagged in this case it was not.

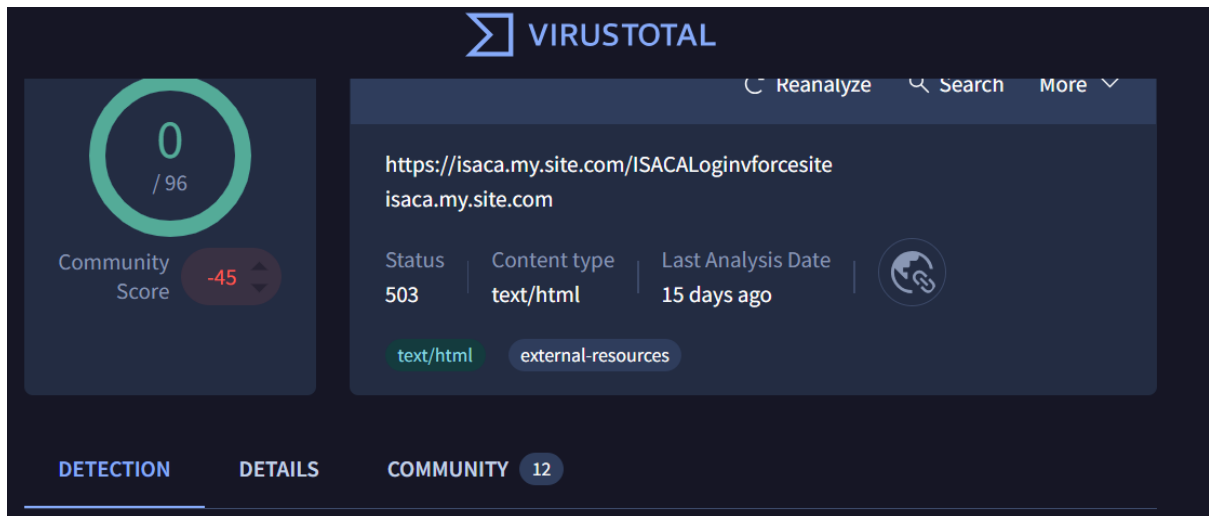


Figure 4

This email looks legit as ISACA confirmed a few hours later with a statement.

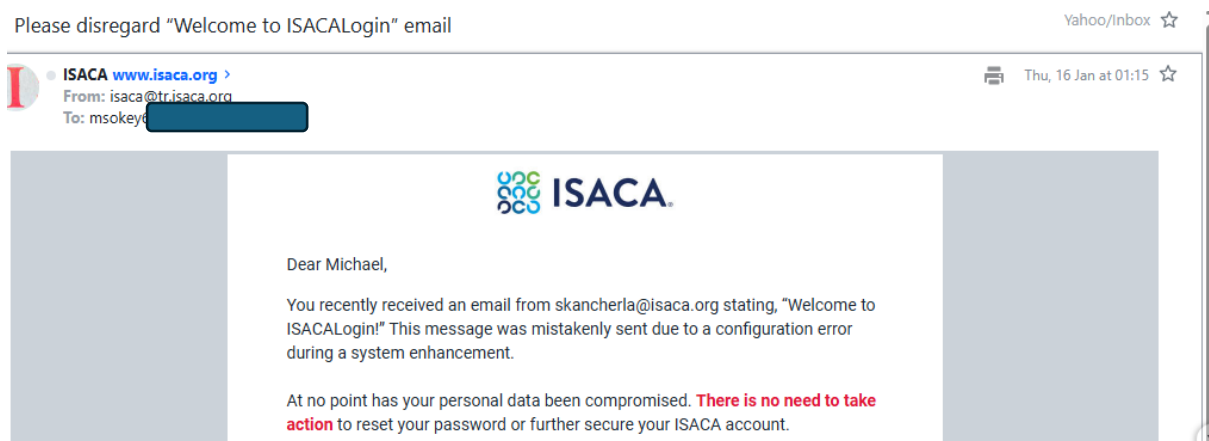
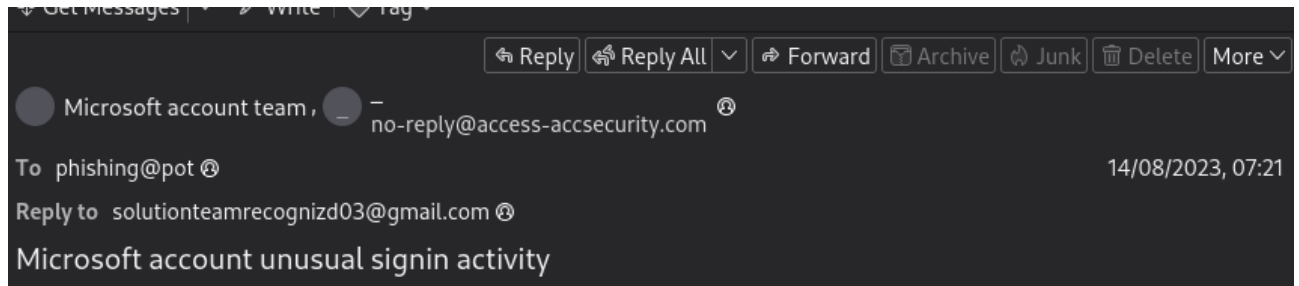


Figure 5

This link provides emails that can be used to practise phishing email investigations
[phishing_pot/email at main · rf-peixoto/phishing_pot · GitHub](#)

Download a few for analysis. NB Open the email samples in a virtual environment. To avoid clicking a link by accident. In this case, Kali Linux virtual machine was used

Example 2



Microsoft account

Unusual sign.in activity

We detected something unusual about a recent sign-in to the Microsoft account [phishing@pot](#).

Sign-in details

Country/region: **Russia/Moscow**

IP address: **103.225.77.255**

Date: **Mon, 14 Aug 2023 06:21:21 +0000**

Platform: **Windows 10**

Browser: **Firefox**

A user from **Russia/Moscow** just logged into your account from a new device. If this wasn't you, please report the user. If this was you, we'll trust similar activity in the future.

[Report The User](#)

To opt out or change where you receive security notifications, [click here](#).

Thanks,
The Microsoft account team

Figure 6

The looks like an email from the Microsoft Team reporting Unusual sign.in activity.

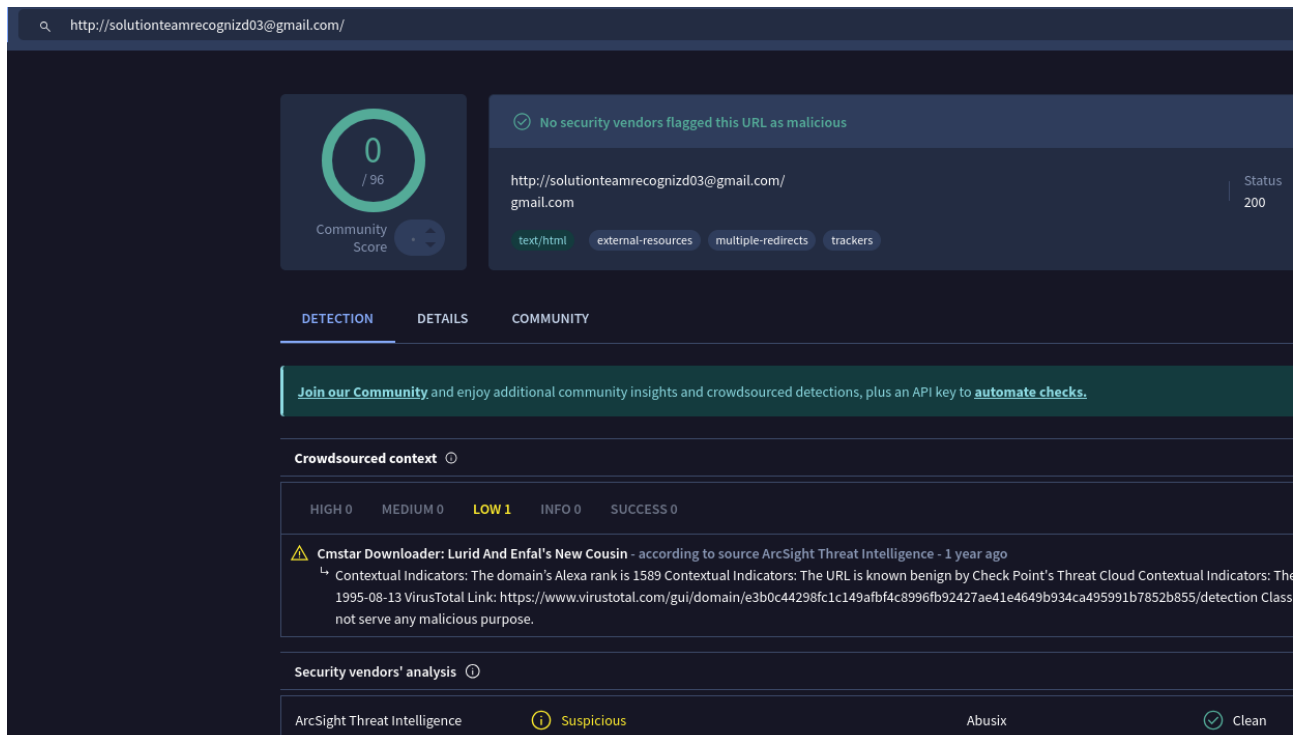
Take note of the links and any attachments ensuring not to open any Open the email in raw format

```
Received: from SA3PR19MB7419.namprd19.prod.outlook.com (::1) by
MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Mon, 14 Aug 2023 06:21:39
+0000
Received: from BN9P223CA0001.NAMP223.PROD.OUTLOOK.COM (2603:10b6:408:10b::6)
by SA3PR19MB7419.namprd19.prod.outlook.com (2603:10b6:806:31b::20) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6678.24; Mon, 14 Aug
2023 06:21:38 +0000
Received: from BN8NAM12FT105.eop-nam12.prod.protection.outlook.com
(2603:10b6:408:10b:cafe::b5) by BN9P223CA0001.outlook.office365.com
(2603:10b6:408:10b::6) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6652.33 via Frontend
Transport; Mon, 14 Aug 2023 06:21:37 +0000
Authentication-Results: spf=none (sender IP is 89.144.44.6)
smtp.mailfrom=inventorecfety.co.uk; dkim=none (message not signed)
header.d=none;dmarc=permerror action=none header.from=access-accsecurity.com;
Received-SPF: None (protection.outlook.com: inventorecfety.co.uk does not
designate permitted sender hosts)
Received: from inventorecfety.co.uk (89.144.44.6) by
BN8NAM12FT105.mail.protection.outlook.com (10.13.182.158) with Microsoft SMTP
Server id 15.20.6699.10 via Frontend Transport; Mon, 14 Aug 2023 06:21:37
+0000
X-IncomingTopHeaderMarker:
OriginalChecksum:06D5E44D57FDABA2A9FF26571D32632925A077655904CD0FE295CB7E1AEB69F9;UpperCaseD
From: Microsoft account team , <no-reply@access-accsecurity.com>
Subject: Microsoft account unusual signin activity
To: phishing@pot
Content-Length: 22448528
Content-Length: 49413
Date: Mon, 14 Aug 2023 06:21:37 +0000
Reply-To: solutionteamrecognizd03@gmail.com
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 8bit
X-IncomingHeaderCount: 12
Message-ID:
<a9613552-f1da-4356-8c9b-e7bf988f0121@BN8NAM12FT105.eop-nam12.prod.protection.outlook.com>
Return-Path: bounce@inventorecfety.co.uk
X-MS-Exchange-Organization-ExpirationStartTime: 14 Aug 2023 06:21:37.9190
(UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
```

Figure 7

The SPF, DKIM and DMARC show none, this is widely considered to be a “fail” and this would trigger further investigation. This email most likely should be deleted from the user's inbox

The links did not produce any results however the return email was flagged as suspicious.



The screenshot shows the VirusTotal interface for the URL `http://solutionteamrecognizd03@gmail.com/`. The top section displays a green circle with the number 0, indicating a Community Score of 0/96. To the right, a green checkmark icon and the text "No security vendors flagged this URL as malicious" are shown. Below this, the URL is repeated, and the status is listed as 200. A row of tags includes `text/html`, `external-resources`, `multiple-redirects`, and `trackers`. The interface has three tabs: DETECTION, DETAILS, and COMMUNITY. A green banner encourages joining the community. The "Crowdsourced context" section shows a "LOW 1" rating and a warning icon. The "Security vendors' analysis" section shows a "Suspicious" flag from ArcSight Threat Intelligence and a "Clean" flag from Abusix.

http://solutionteamrecognizd03@gmail.com/

0 / 96
Community Score

✓ No security vendors flagged this URL as malicious

http://solutionteamrecognizd03@gmail.com/
gmail.com

Status 200

text/html external-resources multiple-redirects trackers

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Crowdsourced context ⓘ

HIGH 0 MEDIUM 0 LOW 1 INFO 0 SUCCESS 0

⚠ Cmstar Downloader: Lurid And Enfal's New Cousin - according to source ArcSight Threat Intelligence - 1 year ago
↳ Contextual Indicators: The domain's Alexa rank is 1589 Contextual Indicators: The URL is known benign by Check Point's Threat Cloud Contextual Indicators: The 1995-08-13 VirusTotal Link: <https://www.virustotal.com/gui/domain/e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855/detection> Class not serve any malicious purpose.

Security vendors' analysis ⓘ

ArcSight Threat Intelligence ⓘ Suspicious Abusix ✓ Clean

Figure 8

This suspicious flag warrants further investigation.

Example 3

In this email, the SPF, DKIM, and DMARC all passed but on further investigation, the links were flagged as malicious.

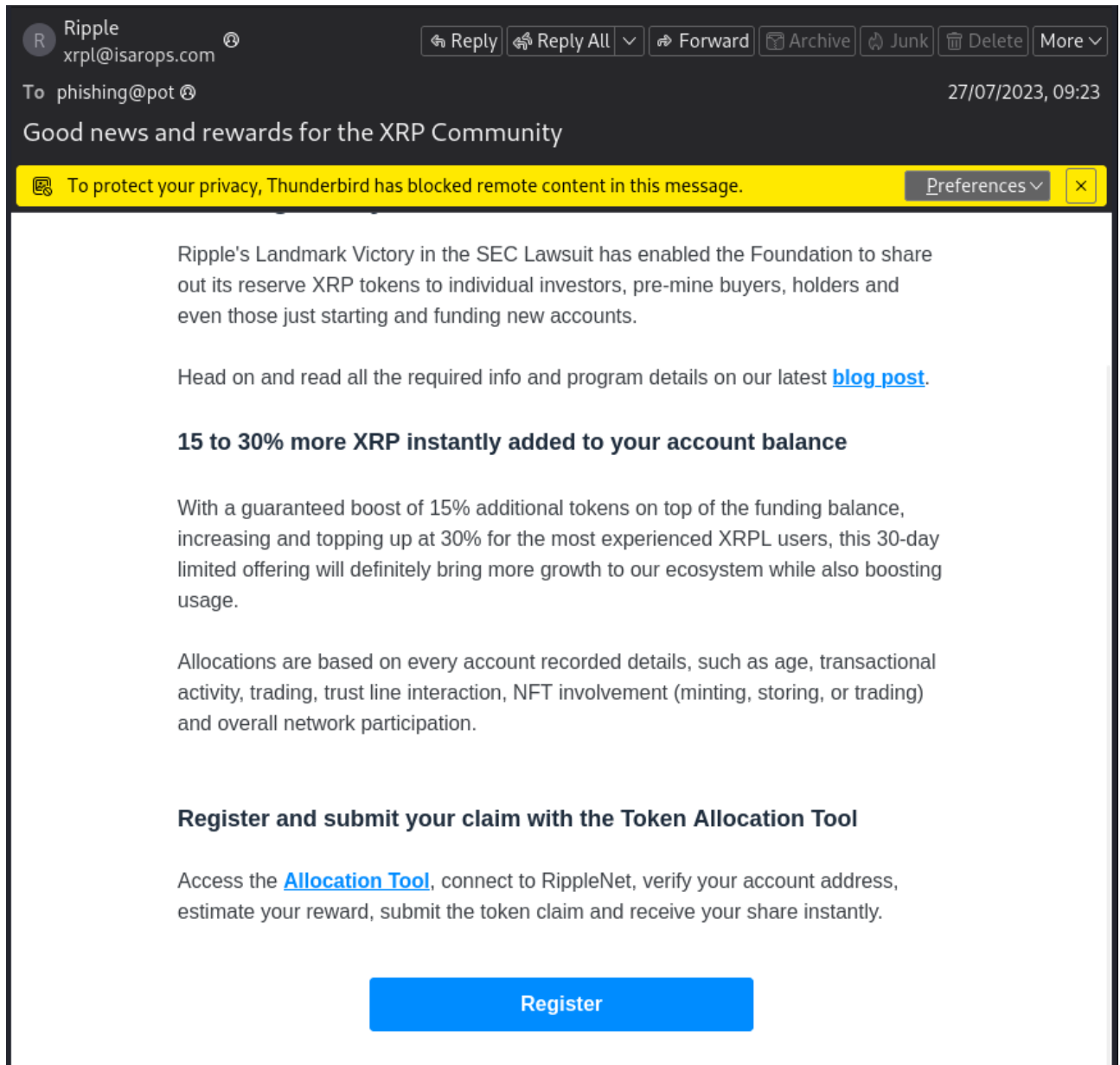


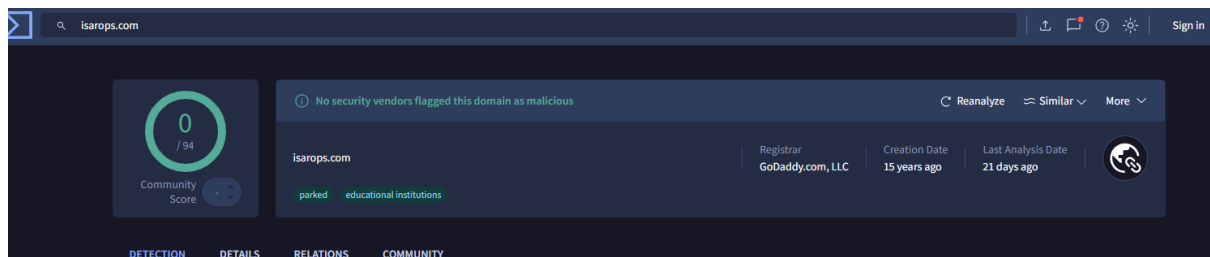
Figure 9

Viewed in raw format

```
Received: from LV3PR19MB8443.namprd19.prod.outlook.com (::1) by
MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Thu, 27 Jul 2023 08:23:12
+0000
Received: from BN9PR03CA0370.namprd03.prod.outlook.com (2603:10b6:408:f7::15)
by LV3PR19MB8443.namprd19.prod.outlook.com (2603:10b6:408:20c::11) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6631.29; Thu, 27 Jul
2023 08:23:11 +0000
Received: from BN1NAM02FT029.eop-nam02.prod.protection.outlook.com
(2603:10b6:408:f7:cafe::34) by BN9PR03CA0370.outlook.office365.com
(2603:10b6:408:f7::15) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6631.29 via Frontend
Transport; Thu, 27 Jul 2023 08:23:11 +0000
Authentication-Results: spf=pass (sender IP is 198.61.254.42)
smtp.mailfrom=isarops.com; dkim=pass (signature was verified)
header.d=isarops.com;dmarc=pass action=none
header.from=isarops.com;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of isarops.com designates
198.61.254.42 as permitted sender) receiver=protection.outlook.com;
client-ip=198.61.254.42; helo=so254-42.mailgun.net; pr=C
Received: from so254-42.mailgun.net (198.61.254.42) by
BN1NAM02FT029.mail.protection.outlook.com (10.13.2.143) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.6631.29 via Frontend Transport; Thu, 27 Jul 2023 08:23:11 +0000
X-IncomingTopHeaderMarker:
OriginalChecksum: B0A5FF703E2CEFE70F0C4F98812D23A05291EBB2F0D3BC3FE5F973A3863BEFA;Up
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=isarops.com;
q=dns/txt; s=k1; t=1690446191; x=1690453391; h=Content-Type:
Content-Transfer-Encoding: Message-Id: To: To: From: From: Subject: Subject:
Mime-Version: Date: Sender: Sender;
bh=ds41Q0ZYDEJ0DdvyBZr5L/5Cwnlp5PQm6BDV+pEg+Lk=;
b=CLy4q8zRh1urirFT9DafxY8T5BYtVyIU8i+sg/+vDFsZYXkoELz0ogukC8eLzMAGuZcnCbsjgg3txf/8Pi
X-Mailgun-Sending-IP: 198.61.254.42
X-Mailgun-Sid: WyJiZWU2MiIsInJvZHZpZ28tZi1wQGhvdG1haWwY29tIiw0TEYNDMyIl0=
Received: from <unknown> (<unknown> []) by 58e756f13322 with HTTP id
64c2296f8eae254b7e3ea0a4; Thu, 27 Jul 2023 08:23:11 GMT
Sender: xrpl@isarops.com
Date: Thu, 27 Jul 2023 08:23:11 +0000
Subject: Good news and rewards for the XRP Community
From: Ripple <xrpl@isarops.com>
To: phishing@pot
X-Mailgun-Track: false
Message-Id: <20230727082311.9d0b426cad4b843b@isarops.com>
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="utf-8"
X-IncomingHeaderCount: 14
Return-Path: bounce+5384b0.912432-phishing@pot=hotmail.com@isarops.com
X-MS-Exchange-Organization-ExpirationStartTime: 27 Jul 2023 08:23:11.7626
(UTC)
```

Figure 10

The domain was not flagged in Virus Total



However, the links were flagged as malicious on Virus Total

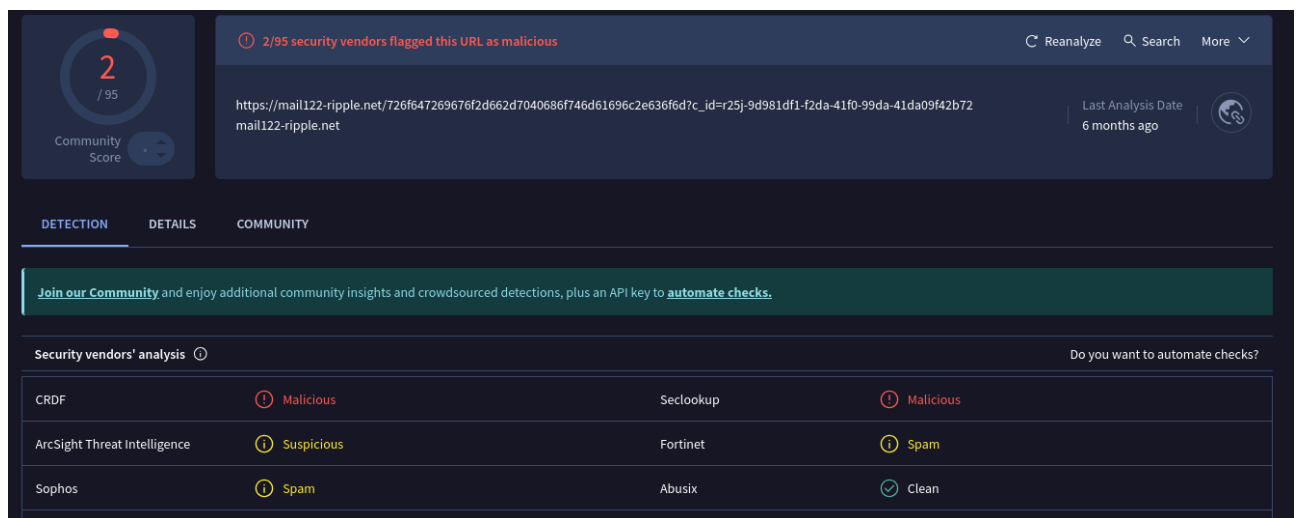


Figure 11

And Symantec

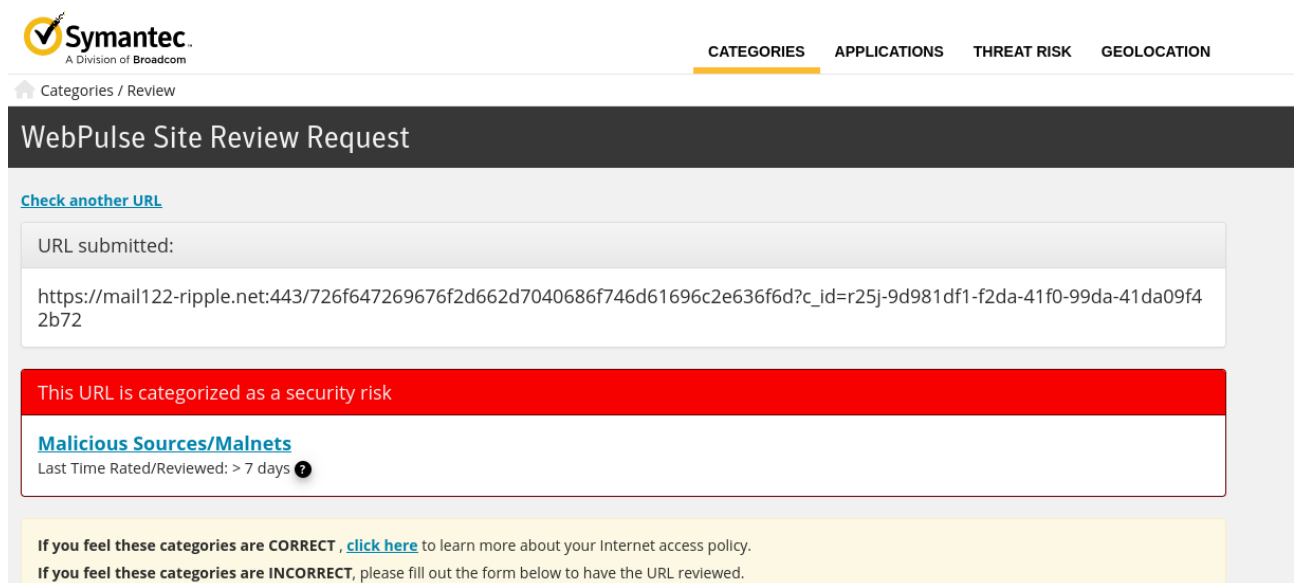


Figure 12

Some graphical user interfaces can be used to view email headers e.g. Google Admin Tool

Messageheader

Google Admin Toolbox Messageheader	
MessageId	c0930be9-cbff-41f7-a020-807ea72a19b6@atl1s11mta837.xt.local
Created at:	1/16/2025, 1:15:19 AM GMT (Delivered after 36 sec)
From:	"ISACA" <isaca@tr.isaca.org>
To:	<msokey6[REDACTED]>
Subject:	Please disregard "Welcome to ISACALogin" email
SPF:	pass with IP Unknown! Learn more
DKIM:	pass with domain tr.isaca.org pass with domain s11.y.mc.salesforce.com Learn more
DMARC:	pass Learn more

Figure 13

Figure 13 is obtained by copying the raw format of the email in Figure 5

Conclusion

For all the emails that were flagged, it is recommended that the user who received the email to change the password. Users normally say they did not click or open any links but just to be on the safe side have them change their passwords anyway.

Lessons Learned

1. Checking SPF, DKIM, and DMARC for authentication of a suspected email
2. Leveraging Virus Total, Symantec, and other sandboxes to check for matches of suspected links, websites, and IP addresses
3. Using the GUI email header analyser