

# Email phishing

▲ The actual senders are made to look legitimate from the Australian tax office

From: "...mygov messages..." From: ".myGov\_ ATO notice"

From: "Online. myGov. ato."

▲ The return path

send@a1.net and the mail server is smtpout06.a1.net with IP 80.75.33.6 originates from Austria

and is reported for email spam, source AbuseIP

send@a1.net and the mail server is smtpout05.a1.net with IP 80.75.33.5 which is used for spam and it's origin is Austria from virustotal

noreply@a1.net and the mail server is smtpout02.a1.net with IP 80.75.33.2 originates from Austria and is flagged as clean by virustotal

phish@cyberlynk.io and the mail server is sonic321-21.consmr.mail.gq1.yahoo.com with IP 98.137.66.84 originates from America and is flagged as spam and spoofing by AbuseIP

▲ By passing the SPF check, this means the emails were sent from a legitimate server which is authorized. SPF check → This is an email authentication whereby the receiving server ensures the sending server was authorized. This ensures that an email was sent from the said domain.

Checking SPF for a1.net domain

---

## Success!

Everything appears fine with your SPF record. [2 DNS queries](#)

Found SPF record in DNS:

```
v=spf1 include:aspf.a1.net include:cspf.a1.net -all
```

SPF record resolution:

```
🌐 a1.net -  
  include:aspf.a1.net -  
    ip4:80.75.33.0/27  
    ip4:194.48.128.0/27  
  -all  
  include:cspf.a1.net -  
    ip4:194.48.128.108
```

Checking SPF for cyberlynk.io

## Success!

Everything appears fine with your SPF record. [2 DNS queries](#)

Found SPF record in DNS:

```
v=spf1 include:_spf.mail.hostinger.com ~all
```

SPF record resolution:

```
🌐 cyberlynk.io -  
  include:_spf.mail.hostinger.com -  
    include:relay.mailchannels.net -  
      ip4:23.83.208.0/20  
      ip4:35.85.190.185/32  
      ~all
```

▲ DKIM stands for domain key identified mail which ensures email has not been tampered with in transit. It uses a digital signature to ensure integrity.

a1.net

resmail1

**Congratulations! Your DKIM record is valid.**

Query: resmail1.\_domainkey.a1.net

### Your DKIM Record

```
v=DKIM1; k=rsa;  
n=MTTCTiANRnkhkiG9w0BA0FFAA0CA8AMTTC0KCA0FA5kr2mr6r010dwo+KTNo11tR7Tv0A8Hi zd2r
```

## Checking DKIM more domain yahoo.com selector s2048

**Congratulations! Your DKIM record is valid.**

Query: s2048.\_domainkey.yahoo.com

Your DKIM Record

```
k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEAuoWufgbWw58McZUGbMv176RaxdZG0MkQmn800J/HGoQ6daLSMwiLaj8IMcHC1cubJx2gziAPQHVPtFYayyLA4ayJUSNk10/uqfByiU8qiPCE4JSFrpXflhMIKV4bt+gluHw7wLzguCf4YAoR6XxUKRsAoHuoF7M+v6bMZ/
```

▲ DMARC stands for domain-based message authentication, reporting and conformance. It builds upon DKIM and SPF, if both are pass, it allows the email.

## Checking mimecast for a1.net domain

v	DMARC1	DMARC protocol version.
p	reject	Apply this policy to email that fails the DMARC check. This policy b e set to 'none', 'quarantine', or 'reject'. 'none' is used to collect the DMARC report and gain insight into the current emailflows and th eir status.
rua	mailto:dmARC-reports@ai.net	A list of URIs for ISPs to send XML feedback to. NOTE: this is not a list of email addresses. DMARC requires a list of URIs of the form 'mailto:test@example.com'.

The policy has been set to reject meaning any unauthenticated email are rejected therefore never making it to the recipient's mailbox. The domain is legit, a telecom company but suspicious sub-domains.

## Checking mimecast for cyberlynk.io domain


## Declared tags

Tag	Value	Description
v	DMARC1	DMARC protocol version.
p	none	Apply this policy to email that fails the DMARC check. This policy be set to 'none', 'quarantine', or 'reject'. 'none' is used to collect the DMARC report and gain insight into the current emailflows and their status.










This is a monitoring way of any emails that simply not being actioned such as quarantine or reject

Let's check the domains

Upon further analysis using <https://toolbox.googleapps.com/apps/checkmx/> for the domain a1.net, below is the output. This is a good example of spoofing email headers done well.

 **a1.net**

There were some critical problems detected with this domain. Mail-flow is probably affected. Please refer to the corresponding help articles to fix these.



[SPF must allow Google servers to send mail on behalf of your domain.](#)

[Domain must have at least one mail server.](#)

DKIM is not set up.

DMARC is not set up.






[MTA-STS DNS Record.](#)

[No Google mail exchangers found. Relayhost configuration?](#)

[Effective SPF Address Ranges.](#)

Domain should have at least 2 NS servers.

Naked domain must be an A record (not CNAME).



[Help center article](#)

[Help center article](#)

[Help center article](#)

[Help center article](#)

[Help center article](#)

Next domain [cyberlynk.io](#)

	Test	Result
✖	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
✔	DNS Record Published	DNS Record found
✔	DMARC Record Published	DMARC Record found

## ▲ Using Virus total for the IP 80.75.33.5

```

— AUTHENTICATION HEADERS —
SPF Check: pass (google.com: domain of send@a1.net designates 80.75.33.5 as permitted sender) client-ip=80.75.33.5;
DKIM-Signature: Present
Partial DKIM: v=1; a=rsa-sha256; c=relaxed/relaxed; d=a1.net; s=resmail1; t=1732352213; h=from:from:reply-to:subje...
Authentication-Results: mx.google.com; dkim=pass header.i=@a1.net header.s=resmail1 header.b=qSciVIPN; spf=pass (
net; dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=a1.net
Return-Path: <send@a1.net>

```

### ! smtpout05.a1.net

There were some critical problems detected with this domain. Mail-flow is probably affected. Please refer to the corresponding help articles to fix these.

- ! [Domain must have at least one mail server.](#) ? [Help center article](#)
- ▲ DKIM is not set up. ? [Help center article](#)
- ▲ DMARC is not set up. ? [Help center article](#)
- ▲ [MTA-STS DNS Record.](#)
- ▲ [There should be a valid SPF record.](#) ? [Help center article](#)
- ▲ [No Google mail exchangers found. Relayhost configuration?](#) ? [Help center article](#)
- ✔ Domain should have at least 2 NS servers.

The above red error “Domain must have at least one mail server ” means the mail server cannot receive messages, only send them thereby good for spammers.

Using Virus total, the IP has been used to send spam and the tactic is passive DNS replication.

Passive DNS Replication (1)			
Date resolved	Detections	Resolver	Domain
2021-12-06	0 / 94	VirusTotal	smtpout05.a1.net
Files Referring (49)			
Scanned	Detections	Type	Name
2024-11-11	1 / 63	Email	____SPAM____ Ihre aktuelle A1 Online-Rechnung 11_2024 - Vertragsnummer 322313229_1.eml

▲ smtpout06.a1.net with the IP 80.75.33.6 which is not blacklisted

```

--- AUTHENTICATION HEADERS ---
SPF Check: pass (google.com: domain of send@a1.net designates 80.75.33.6 as permitted sender) client-ip=80.75.33.6;
DKIM-Signature: Present
Partial DKIM: v=1; a=rsa-sha256; c=relaxed/relaxed; d=a1.net; s=resmail1; t=1735395361; h=from:from:reply-to:subje...
Authentication-Results: mx.google.com; dkim=pass header.i=@a1.net header.s=resmail1 header.b=cujhYTRc; spf=pass (
net; dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=a1.net
Return-Path: <send@a1.net>

```

Upon further investigation, there are missing records as shown below

**smtpout06.a1.net**

There were some critical problems detected with this domain. Mail-flow is probably affected. Please refer to the corresponding help articles to f these.



- [Domain must have at least one mail server.](#) [Help center article](#)
- DKIM is not set up. [Help center article](#)
- DMARC is not set up. [Help center article](#)
- [MTA-STS DNS Record.](#)
- [There should be a valid SPF record.](#) [Help center article](#)
- [No Google mail exchangers found. Relayhost configuration?](#) [Help center article](#)
- Domain should have at least 2 NS servers.

There are no Google mail servers, the mail probably came from a third party.

ABuseIPDB highlights this mail server has been used for email spam

This IP address has been reported a total of 3 times from 2 distinct sources. 80.75.33.6 was first reported on September 27th 2022, and the most r report was 1 year ago.

Old Reports: The most recent abuse report for this IP address is from 1 year ago. It is possible that this IP is no longer involved in abusive activiti

Reporter	IoA Timestamp in UTC	Comment	Categories
	2024-03-01 15:49:32 (1 year ago)	Mail/25/465/587-993/995 Probe, Reject, BadAuth, Hack, SPAM -	Email Spam Hacking Brute-Force
	2023-11-07 13:09:31 (1 year ago)	Mail/25/465/587-993/995 Probe, Reject, BadAuth, Hack, SPAM -	Email Spam Hacking Brute-Force

It has been flagged as clean

Passive DNS Replication (1)			
Date resolved	Detections	Resolver	Domain
2022-03-04	0 / 94	VirusTotal	smtpout06.a1.net
Files Referring (49)			
Scanned	Detections	Type	Name
2025-07-03	0 / 63	Outlook	Mahnung.msg
2025-05-27	0 / 63	Email	Spam Report.eml

▲ Check DKIM by domain a1.net selector resmail1 for IP 80.75.33.2

```
— AUTHENTICATION HEADERS —
SPF Check: pass (google.com: domain of noreply@a1.net designates 80.75.33.2 as permitted sender) client-ip=80.75.33.2;
DKIM-Signature: Present
Partial DKIM: v=1; a=rsa-sha256; c=relaxed/relaxed; d=a1.net; s=resmail1; t=1735849398; h=from:from:reply-to:subje...
Authentication-Results: mx.google.com; dkim=pass header.i=@a1.net header.s=resmail1 header.b=k21L98nM; spf=pass (g
ly@a1.net; dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=a1.net
Return-Path: <noreply@a1.net>
```



## ! smtpout02.a1.net

There were some critical problems detected with this domain. Mail-flow is probably affected. Please refer to the corresponding help articles to fix these.

!	<a href="#">Domain must have at least one mail server.</a>	?	<a href="#">Help center article</a>
▲	DKIM is not set up.	?	<a href="#">Help center article</a>
▲	DMARC is not set up.	?	<a href="#">Help center article</a>
▲	<a href="#">MTA-STS DNS Record.</a>		
▲	<a href="#">There should be a valid SPF record.</a>	?	<a href="#">Help center article</a>
▲	<a href="#">No Google mail exchangers found. Relayhost configuration?</a>	?	<a href="#">Help center article</a>
✓	Domain should have at least 2 NS servers.		

Referencing virustotal, the possible attack is DNS replication attack which is where an attacker can copy previous domains visited by the user and redirect the user to sites they control such as command and control server.

Passive DNS Replication (1) ○			
Date resolved	Detections	Resolver	Domain
2022-03-01	0 / 94	VirusTotal	smtpout02.a1.net
Files Referring (47) ○			
Scanned	Detections	Type	Name
2025-06-05	0 / 62	Outlook	44aaef00fa68a243b4c19f8f9d7ec2c54e74b41ad0a1cb269fa9615b89bdfc34
2025-06-05	0 / 62	Outlook	e4ac84422df6af3bc59be44165d9703f1a3c02a0f7d7d4a396d79a2e899d189b
2025-05-02	0 / 61	Outlook	Anfrage 2505Ino1 ALFA.msg
2025-02-06	0 / 59	Outlook	TAGESAKTION!.msg

▲ [cyberlynk.io](#) domain DMARC from mimecast

Tag	Value	Description
v	DMARC1	DMARC protocol version.
p	none	Apply this policy to email that fails the DMARC check. This policy be set to 'none', 'quarantine', or 'reject'. 'none' is used to collect the DMARC report and gain insight into the current emailflows and their status.

When the value is p, it means that there are no actions taken such as quarantine and it's monitoring then sending reports.

	test	result
✖	SPF Authentication	SPF Failed for IP - 98.137.66.84
✖	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
✔	SPF Record Published	SPF Record found

## DKIM and DMARC pass

```

— AUTHENTICATION HEADERS —
SPF Check: pass (google.com: domain of phish@cyberlynk.io designates 98.137.66.84 as permitted sender) client-ip=98.137.66.84
DKIM-Signature: Present
Partial DKIM: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1735995382; bh=HlkcAm90sd6n3eUw55UtazT...
Authentication-Results: mx.google.com; dkim=pass header.i=@yahoo.com header.s=s2048 header.b=doo0e6Qu; spf=pass
Return-Path: <phish@cyberlynk.io>

```

Passive DNS replication is where a domain name resolves to an IP

No security vendor flagged this IP address as malicious

Passive DNS Replication (1) ⓘ			
Date resolved	Detections	Resolver	Domain
2020-09-25	0 / 94	VirusTotal	sonic321-21.consmr.mail.gq1.yahoo.com
Files Referring (32) ⓘ			
Scanned	Detections	Type	Name
2025-02-27	0 / 60	Email	467377_4e6dfd1b-2bb9-4f54-82fc-54952710ee50@467377
2025-02-27	0 / 61	XML	sharedStrings.xml
2025-02-08	0 / 60	XML	sharedStrings.xml



<https://shorturl.at/3UQvV> is flagged as clean by some vendors and belongs to cloudflarenets

💀 This is base64 encoding in an email. This email also has an attachment which is tied to trick the user to download and open the attachment.

---

```
aGVsbG8gaW5mby5jaWFjdHJsQGdtYWlsLmNvbSwgPGJyPiA8YnI+DQpZb3UgaGF2ZSBuZXcgQXNz
ZXNzbWVudCBzdGF0ZW1lbmVudG9yIFNjcmVlbmluZy4=
```

---

REC 130 3

### Output

---

```
hello info.ciactrl@gmail.com, <br> <br>
You have new Assessment statement Ready for Screening.
```

I used a python script to download the attachment, please refer to github for scripts.

The attachment on virus total and was undetected as malicious by some security vendors

DrWeb	✓ Undetected
eScan	✓ Undetected
Fortinet	✓ Undetected
Google	✓ Undetected
Huorong	✓ Undetected
Jiangmin	✓ Undetected

MITRE ATT&CK Tactics and Techniques		
— Initial Access TA0001		
📁 Phishing T1566		
📁 Spearphishing Link T1566.002		
Severity	Description	Match
INFO	Clickable URLs found in PDF	https://shorturl.at/4rcpy https://shorturl.at/4RCpY
— Execution TA0002		
📁 Exploitation for Client Execution T1203		
Severity	Description	Match
INFO	A possible heap spray exploit has been detected	pid: 5132

The malicious PDF is therefore used as part of initial access and compromise to gain credentials.

🦴 Wireshark Traffic analysis ⚠️

No.	Time	Source	Destination	Protocol	Length	Info
7	0.275517071	10.0.0.138	10.0.2.15	DNS	78	Standard query response 0xbd60 No such name A holyflamesnik.site
8	0.275517344	10.0.0.138	10.0.2.15	DNS	78	Standard query response 0xbe61 No such name AAAA holyflamesnik.site
9	0.275601547	10.0.2.15	10.0.0.138	DNS	86	Standard query 0x8a6d A holyflamesnik.site.gateway
10	0.275609396	10.0.2.15	10.0.0.138	DNS	86	Standard query 0x5b6f AAAA holyflamesnik.site.gateway
11	0.277082529	10.0.0.138	10.0.2.15	DNS	86	Standard query response 0x8a6d No such name A holyflamesnik.site.gateway
12	0.277082672	10.0.0.138	10.0.2.15	DNS	86	Standard query response 0x5b6f No such name AAAA holyflamesnik.site.gateway
13	0.278965518	10.0.2.15	10.0.0.138	DNS	78	Standard query 0xcbde A holyflamesnik.site
14	0.278982585	10.0.2.15	10.0.0.138	DNS	78	Standard query 0xa4d1 AAAA holyflamesnik.site
15	0.280412586	10.0.0.138	10.0.2.15	DNS	78	Standard query response 0xcbde No such name A holyflamesnik.site
16	0.280456204	10.0.0.138	10.0.2.15	DNS	78	Standard query response 0xa4d1 No such name AAAA holyflamesnik.site
17	0.280484266	10.0.2.15	10.0.0.138	DNS	86	Standard query 0xdd7e A holyflamesnik.site.gateway
18	0.280491318	10.0.2.15	10.0.0.138	DNS	86	Standard query 0xae7f AAAA holyflamesnik.site.gateway
19	0.281755957	10.0.0.138	10.0.2.15	DNS	86	Standard query response 0xdd7e No such name A holyflamesnik.site.gateway
20	0.281905825	10.0.0.138	10.0.2.15	DNS	86	Standard query response 0xae7f No such name AAAA holyflamesnik.site.gateway
21	0.411857018	10.0.2.15	10.0.0.138	DNS	82	Standard query 0x5fc3 A www.holyflamesnik.site
22	0.411941661	10.0.2.15	10.0.0.138	DNS	82	Standard query 0xf8c1 AAAA www.holyflamesnik.site

When the pdf attachment is opened and network traffic capture, there is routing to the suspicious site. The PDF has a link to a domain controlled by the attacker <https://holyflamesnik.site/viewmyprofile/> ABUSEIPDB reference for 10.0.2.15 used for the DNS protocol compromise.

Reporter	IoA Timestamp in UTC	Comment	Categories
 <a href="#">Macon Ritto</a>	2024-07-07 08:52:01 (1 year ago)	h	<div>DNS Compromise</div> <div>DNS Poisoning</div> <div>Fraud Orders</div> <div>DDoS Attack</div> <div>FTP Brute-Force</div> <div>Ping of Death</div> <div>Phishing</div> <div>Fraud VoIP</div> <div>Open Proxy</div> <div>Web Spam</div> <div>Email Spam</div> <div>Blog Spam</div> <div>VPN IP</div> <div>Port Scan</div>

 Shortened url 

```
JVBERi0xLjQKJdPr6eEKMSAwIG9iago8PC9DcmVhdG9yICkDaHJvbWl1bSkKL1Byb2R1Y2VyICht
a2lhL1BERiBtMTEwKQovQ3JlYXRpb25EYXRlICkE0jIwMjQxMTIzMDgzMjAwKzAwJzAwJyKkKL01v
ZERhdGUgKEQ6MjAyNDExMjMwODMyMDArMDAnMDAnKT4+CmVuZG9iagozIDAgb2JqCjw8L2NhIDEK
L0JNIC90b3JtYWw+PgplbmRvYmoKNiAwIG9iago8PC9UeXBlic9Bbm5vdAovU3VidHlwZSAvTGlu
awovRiA0Ci9Cb3JkZXIgwZAgMCAwXQovUmVjdCBbmjI2LjMwNjM0IDcwMCA4YmJA10CAzNjguNjKz
NiA3NDAuMTE2NTJdCi9BIDw8L1R5cGUgL0FjdGlvbG9vUyAvVVJJCi9VUkkGKGh0dHBzOi8vc2hv
cnR1cmwuYXQvNFJDcFkpPj4KL1N0cnVjdFBhcmVudCAxMDAwMDA+PgplbmRvYmoKNyAwIG9iago8
PC9GaWx0ZXIgL0ZsYXRlRGVjb2RlCi9MZW5ndGggMTA0Nz4+IHN0cmVhbQp4nH1W24okNwx9r6/w
c2A91s0XGAamq7eXPCwkoWE/YJJswHYC2fw/RJJd7apA9/RUly3L0pF0LHdEav4Xkn4+xN20MsQG
rdXw9r78s9g6cmkRcpZAKmpMDSn8+GP58LP4WzUw1pxTrey2jjM18fSJwtd/l9N1efolPD8/fv5/
PuvKy8vpvC5PF1br4frnAh0JqAu0jYoEQAzX9+U5JeSXcP22gESRVCqQal5/D7pCpa9wRMySueYK
Jv3Sf9H9Vd/UZTYfuz5+XpeP1yVyIBXVobolCr99Cv+T/Pi6ELaACcK7j0AofNdRjZazon0MRLnl
oKsRMFdsGcTcGjC6kGqS6sJUFSiFN7MUMzGa0EUUvGLXbu1EjXiZ91hVSLqemcWFNUjiB1RsgLnF
1XeZKrgpdmap1Rvi04WxehQxPejQ3Spoc6KlchD8f066++3RcjVNGwdxZwpubEgakMzW+reiAkb
W0o0/kRtC8oRmxDHLI1bMwiTifIgH+NVUuyJ8ZAbE5JmdJ9Ek2VohMeEm7gWAtgXRyJv6tdnXTl7
```

62829 819

## Output

<https://shorturl.at/4RCpY>)

<https://shorturl.at/4RCpY> resolves to <https://holyflamesnik.site/viewmyprofile/>  
on virustotal, confirmed this is a phishing attack

The screenshot shows the VirusTotal interface for the URL <https://holyflamesnik.site/viewmyprofile/>. The community score is 2/97. A warning states that 2/97 security vendors flagged this URL as malicious. Below this, a table lists the security vendors' analysis results.

Security vendors' analysis	
Bfore.Ai PreCrime	Malicious
Abusix	Clean
ADMINUSLabs	Clean
Fortinet	Phishing
Acronis	Clean
AILabs (MONITORAPP)	Clean

#curl -i <https://shorturl.at/4RCpY> shows redirection to the attack owned domain.





```
f-cache-status: DYNAMIC
report-to: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=1%2FVuCmRyYQUU%2FbWx0AJaIXS4TdbAdd4f0Qv..."}, {"url":"https://a.nel.cloudflare.com/report/v4?s=1%2FVuCmRyYQUU%2FbWx0AJaIXS4TdbAdd4f0Qv..."}], "group":"cf-nel", "max_age":604800}
nel: {"success_fraction":0,"report_to":"cf-nel", "max_age":604800}
server: cloudflare
server-timing: cfL4;desc="?proto=TCP&rtt=8671&min_rtt=3782&rtt_var=10562&sent=88&recv=96&lost=0&retrans=0&sent_bytes=36000&..."; curl -I https://shorturl.at/3LW30
```

🦴 Netflix subscription payment update for subscription legitimacy, email forwarding and use of urgent language.

```
<div>----- Forwarded message -----</div>
<div><b>From:</b> Netflix.com &lt;pharmacy@notificationmai=
.com></div><div><b>To:</b> "phish@cyberlynk.io" &lt;phish@cyberlynk=
.com></div><div><b>Sent:</b> Monday 17 June 2024 at 01:31:52 pm AEST</di=
<div><b>Subject:</b> Please update your payment details</div><div><br></d=
>
=20
=20
<div><div id=3D"ydp346daa9ayiv0030771440">=20
```

💀 A white background color making it obfuscated and %20 is encoding for space

[illegible]

The text is also white which adds to more obfuscation, therefore white fonts on white background.

```
<td align=3D"center" style=3D=
font-family:NetflixSans-Bold, Helvetica, Roboto, Segoe UI, sans-serif;font=
weight:700;font-size:14px;line-height:17px;letter-spacing:-0.2px;padding:1=
px 20px;color:#ffffff;"><a href=3D"https://qrco.de/bf9xmf?click?s=3DVwtvB1=
&li=3D{LIST_ID}&e=3DH&unsubscribe=3Dphish@cyberlynk.io&p=
3DankthyH9&id=3DY4SR8KTMSIMMBVEV3K047HUSH0LB2FVXACJGAT45CA0AI576U0?dg7=
fgbpi6oruegsx0mpaudiwpmxhrtkec4jgbulbeehfwlg38yzjtk9aqn1qpneu6uxiuhpgh5vy=
3kme97iykuvhu2jv86pq1&stpe=3Ddefault" style=3D"font-family:NetflixSans=
Bold, Helvetica, Roboto, Segoe UI, sans-serif;font-weight:700;font-size:14=
x;line-height:17px;letter-spacing:-0.2px;text-align:center;text-decoration=
none;display:block;color:#ffffff;" target=3D"_blank" rel=3D"noreferrer noo=
ener">Update information</a></td>
```

💀 Using cyberchef, the word is access using the recipe from quoted printable. This is an obfuscation tactic whereby the attacker used letters and numbers that look real.

```
=20
| To ensure uninterrupted =D0=B0cc=D0=B5ss| to your favorite movies and show=
s, we kindly ask you to update billing information. |
```

💀 Included valid URLs to make it look legitimate.

```
https://ci3.googl
https://beaconimages.netflix
https://www.netflix.com/browse?g=
https://ci3.go
https://qrco.de/bf9xmf?click?s=3DVwtvB1=
https://help.netflix.com/help?g=3D58ffd66c-8e71-4ed2-af78-6c86=
https://help.netflix.com/contactus?g=3D58ffd66c-8e71-4ed2-af78-6c86a529=
https://ci3.googleusercontent.com/meip=
https://assets.nflxext.com/us/email=
https://www.netflix.co
https://www.netflix.com/TermsOfUse?g=3D58ffd66c-8e71-4ed2-af78-6c86a529dbf7=
https://www.netflix.com/PrivacyPolicy?g=
https://help.netflix.com/help?g=3D58ffd66c-8e71-4ed2-af78-6c86a529dbf7&=
https://www.netflix.com/browse?g=3D58ffd66c-8e71-4ed2-af78-6c86a529dbf7=
```

## Conclusion

This phishing campaign used:

- High-quality header spoofing and SPF passing
- Base64 + quoted-printable encoding
- Redirection via short URLs and PDFs
- Abuse of clean infrastructure like cloudflare links

## Recommendations

- Block malicious domains and IPs in gateway firewall
- Submit all IOCs to SIEM/Threat Intel feed
- Educate users about obfuscated email tactics
- Strengthen email filtering and sandboxing policies

▲ Tools and resources

spf checker <https://mxtoolbox.com/spf.aspx>

Cyberchef <https://gchq.github.io/CyberChef/>

Sandbox <https://app.any.run/#register>

<https://mxtoolbox.com/EmailHeaders.aspx>

<https://toolbox.googleapps.com/apps/main/>

<https://dmarcian.com/dkim-inspector/>