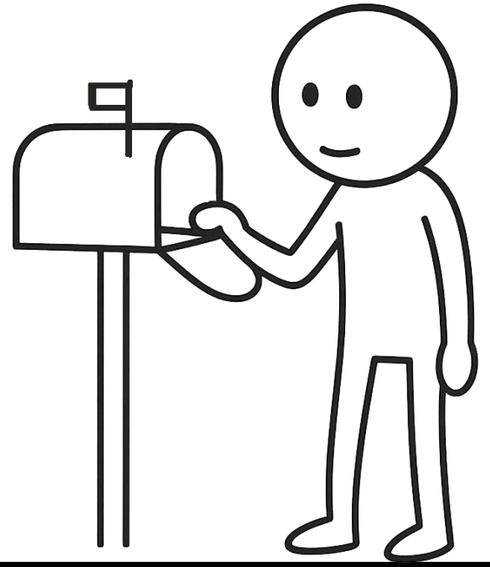
Spoofed & Trusted: Next-Generation Email Attacks Targeting Email Design and Implementation Flaws



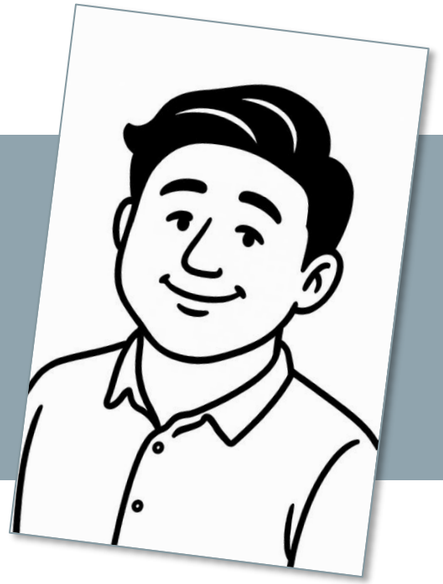
Caleb Sargent & Hao Wang

TROOPERS

ABOUT US

Caleb Sargent

(@squared_)



Hao Wang

(@MrRed_Panda)

CVE-2024-7208 A vulnerability in multi-tenant hosting allows an authenticated sender to spoof the identity of a shared, hosted domain, thus bypass security measures provided by DMARC (or SPF or DKIM) policies.

CVE-2024-7209 A vulnerability exists in the use of shared SPF records in multi-tenant hosting providers, allowing attackers to use network authorization to be abused to spoof the email identify of the sender.

darkreading.com/threat-intelligence/20-million-trusted-domains-vulnera...

DARKREADING

NEWSLETTER SIGN

THREAT INTELLIGENCE | ENDPOINT SECURITY | VULNERABILITIES & THREATS | APPLICATION

20 Million Trusted Domains Vulnerable to Email Ho Exploits

Three newly discovered SMTP smuggling attack techniques can exploit misconfigurations and desig decisions made by at least 50 email-hosting providers.

Elizabeth Montalbano, Contributing Writer
July 18, 2024

4 Min Rea

kb.cert.org/vuls/id/244112

CERT Coordination Center

Home | Notes | Search | Report a Vulnerability | Disclosure

Home › Notes › VU#244112

Multiple SMTP services are susceptible to spoofing attacks due to insufficient enforcement

Vulnerability Note VU#244112

Original Release Date: 2024-07-30 | Last Revised: 2024-08-06

Overview

Multiple hosted, outbound SMTP servers are vulnerable to email impersonation. This allows authenticated users and certain trusted networks to send emails containing spoofed sender information. Two vulnerabilities were identified that reduce the authentication and verification of the sender, provided by the combination of Sender Policy Framework (SPF) and Domain Key Identified Mail (DKIM). Domain-based (DMARC) builds on SPF and DKIM, adding linkage to or recipient handling of authentication failures, and onitor protection of the domain from fraudulent an spoof the identity of a sender when sending

sans.org/newsletters/newsbites/xxvi-59/

Top of the News | The Rest of the Week's News

Share:

2024-08-02

SMTP Spoofing Vulnerabilities

The CERT Coordination Center (CERT/CC) at Carnegie Mellon University has published a vulnerability note describing a pair of vulnerabilities that could be exploited to spoof email addresses. The issue affects multiple Simple Mail Transfer Protocol (SMTP) servers. CERT/CC writes, "An authenticated attacker using network or SMTP authentication can spoof the identity of a shared hosting facility, circumventing any DMARC policy and sender verification provided by a domain name owner."

Editor's Note

There are two flaws here: CVE-2024-7208, sender email not verified against authorized domains and CVE-2024-7209, shared SPF record spoofing. The vulnerabilities don't have CVSS scores, nor have many vendors stepped up to say they are vulnerable, or have addressed the flaw. The researchers from PayPal, Caleb Sargent and Hao Wang, who discovered the attack, are presenting their findings in a talk titled "Into the Inbox: Novel Email Spoofing Attack Patterns," on Wednesday at Black Hat. Aside from making sure your SPF, DKIM and DMARC records are as specific as possible, you can consider the use of S/MIME or PGP for messages requiring high assurance of the sender identity.

Lee Neely

DISCLAIMER

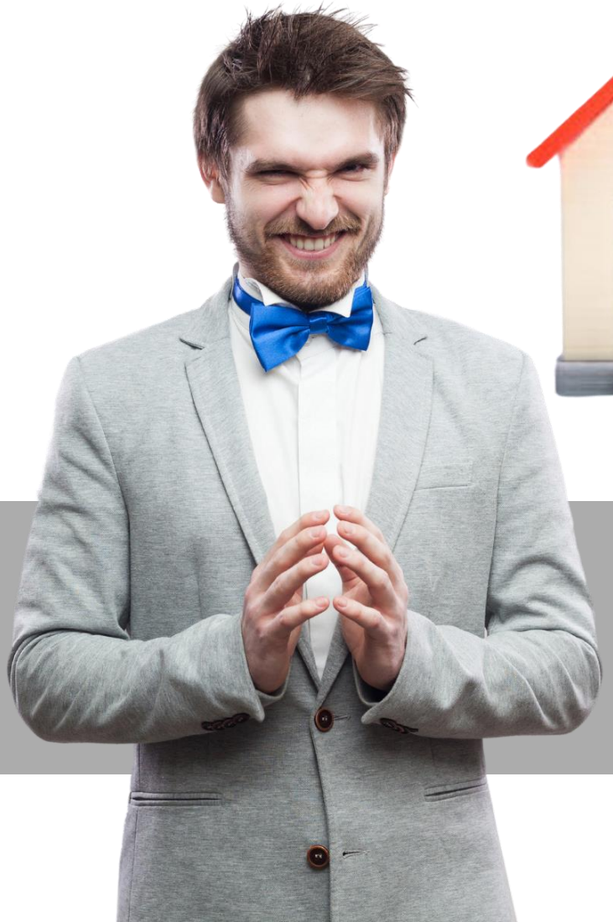
The views, opinions, and content presented in this talk are solely my own and do not reflect those of my employer, past or present. This presentation is intended for educational and awareness purposes only. Any techniques or findings discussed should not be used for unauthorized activities or misinterpreted as guidance to conduct malicious behavior.

AGENDA

1. Story Time
2. Email Security Basics
3. Attack Patterns
4. Recommendations
5. Key Takeaways

EVER BEEN PRANKED

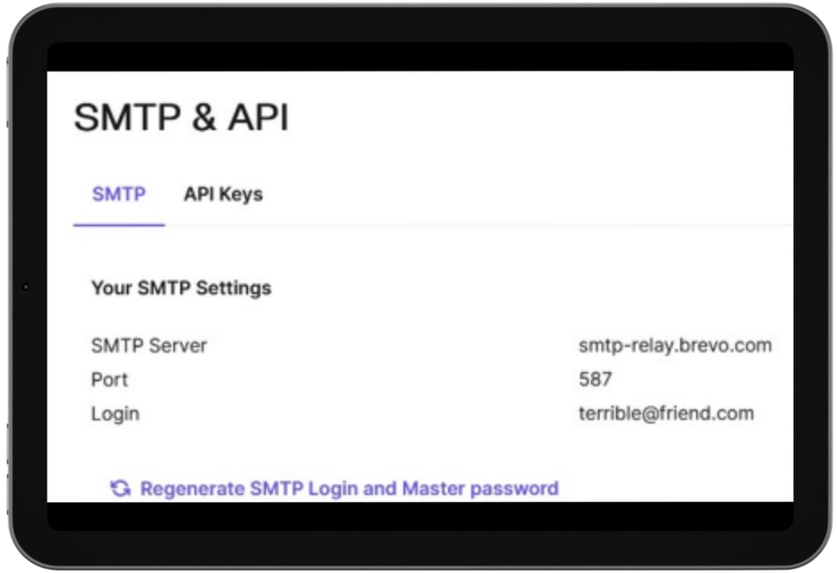
CRAFTING THE ULTIMATE PRANK.

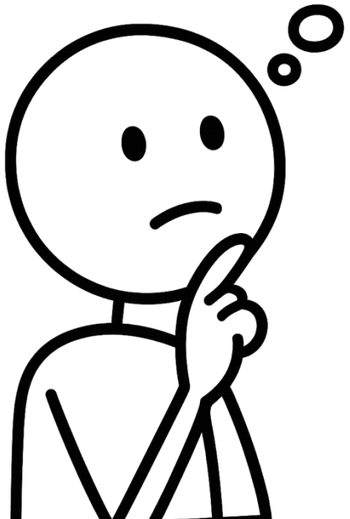


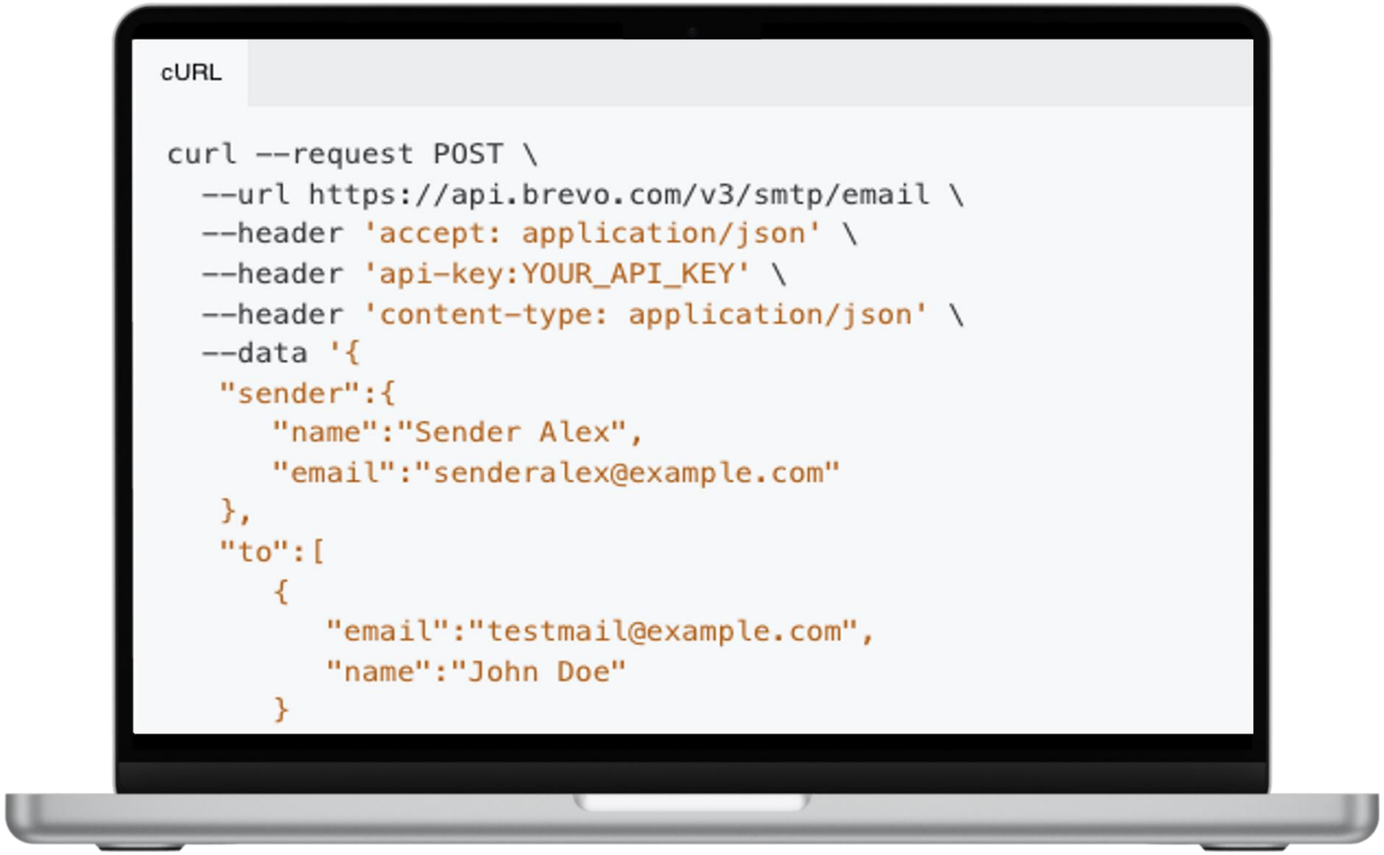
WEG?

VS

HOW TO SPOOF AN EMAIL?







cURL

```
curl --request POST \
  --url https://api.brevo.com/v3/smtp/email \
  --header 'accept: application/json' \
  --header 'api-key:YOUR_API_KEY' \
  --header 'content-type: application/json' \
  --data '{
   "sender":{
      "name":"Sender Alex",
      "email":"senderalex@example.com"
   },
   "to":[
      {
         "email":"testmail@example.com",
         "name":"John Doe"
      }
```

TESTING IF THIS WORKS

SECURITY CHECKS PASS?

Original message

Message ID	<4deb8dc3-63ab-4880-a5ba-7077a05c9047@smtp-relay.sendinblue.com>
Created on:	1 April 2024 at 17:15 (Delivered after 1 second)
From:	"darryla@[redacted]com" <darryla@223030174.t-sender-sib.com> Using sendEmail-1.56
To:	[redacted]gmail.com
Subject:	Subject: Urgent Action Required: HOA Notice - House Repainting Required
SPF:	PASS with IP 185.41.28.5 Learn more
DKIM:	'PASS' with domain t-sender-sib.com Learn more
DMARC:	'PASS' Learn more

GO TIME

darryla <darryla@223030174.t-sender-sib.com>
to me

Dear

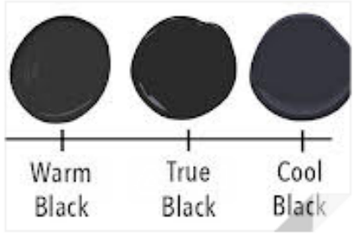
We hope this email finds you well. It has come to our attention that the exterior paint color of your house located at [insert address] does not comply with the approved colors outlined in the HOA guidelines.

The shade of black used on your house is not correct and will need to be repainted to match the approved color. This is the only aspect of your house that requires repainting.

Please ensure that the shade of black is corrected within 30 days from the date of this notice. Example approved shades can be found attached.

•••

2 attachments • Scanned by Gmail



THE AFTERMATH...

Me 04/01/2024 5:48 PM

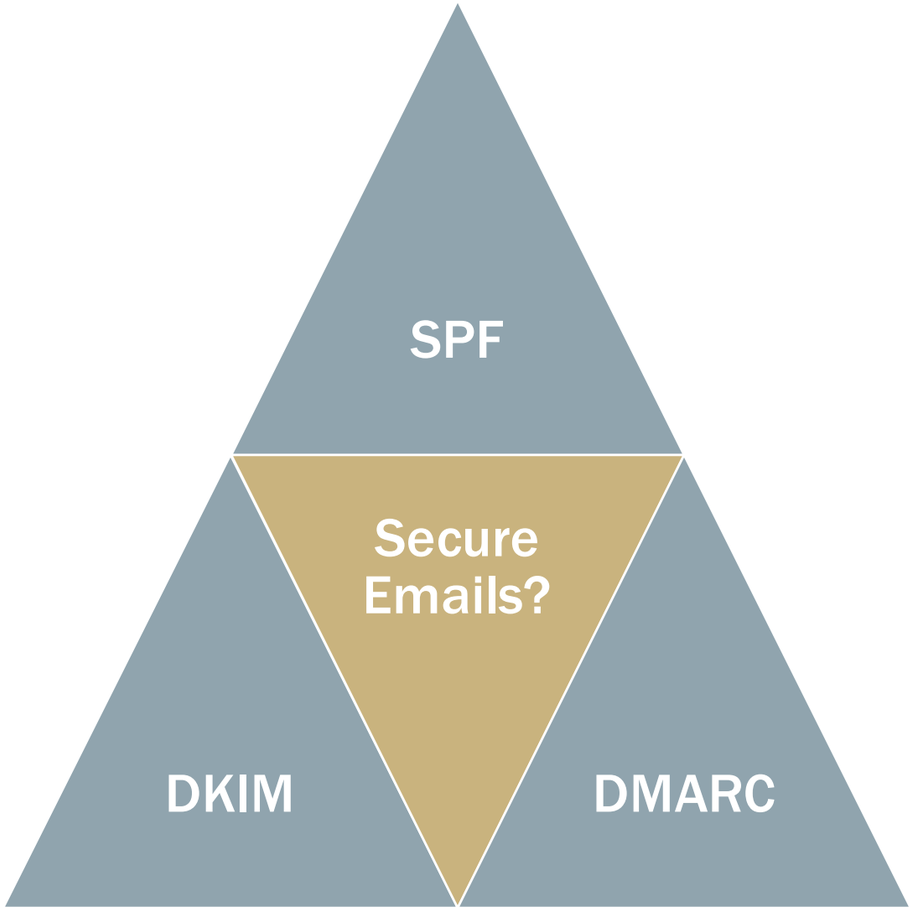
What else you got going on tonight?

Friend 04/01/2024 5:50 PM

Just got a letter from the HOA saying our house color is not approved

So drinking

EMAIL SECURITY TRINITY



SPF – ARE YOU ON THE LIST?

❖ SPF

❑ Verify Sender IP based on TXT record of domain via **MAIL FROM / HELO**

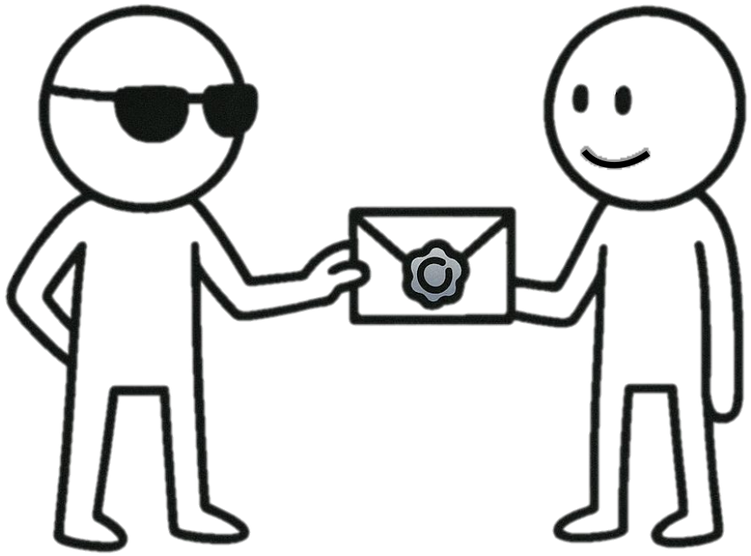
```
v=spf1 include:example.com ip4:198.51.100.25 -all
```

DKIM – SIGNED & SEALED

❖ DKIM

- ❑ Verify email based on the added DKIM signature

```
selector1._domainkey.example.com IN TXT "v=DKIM1; k=rsa; p=MIIBIjANBqh...QAB"
```

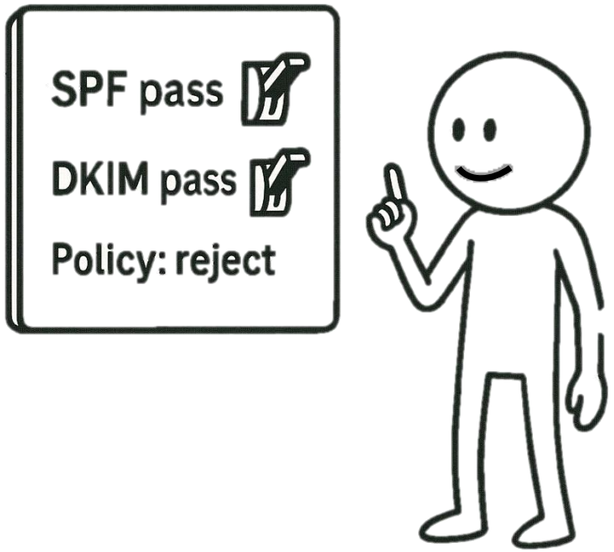


DMARC – CAN I SPEAK TO YOUR MANAGER

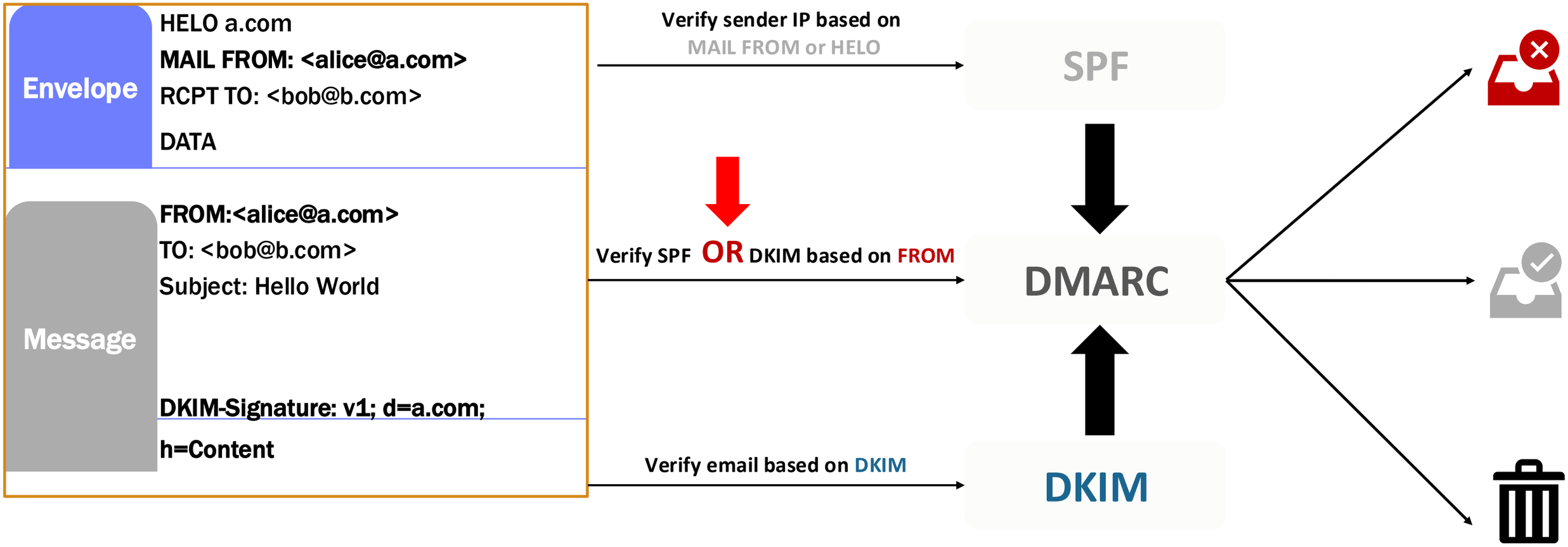
❖ DMARC

- ❑ Tell email receivers on how to handle unauthenticated emails
- ❑ Verify SPF or DKIM based on the domain passed via **FROM**

```
_dmarc.example.com IN TXT "v=DMARC1; p=reject;"
```



SAMPLE SMTP FLOW



Reference: https://www.usenix.org/conference/usenixsecurity21/presentation/shen-kaiwen

ALL THE MISCONFIGURATIONS

✓
```
v=spf1 include:spf.mailanyone.net -all
```

✗
```
v=spf1 include:spf.mailanyone.net ~all
```

✓
```
_dmarc.example.com. IN TXT "v=DMARC1; p=reject;"
```

✓
```
domainkey.example.com. IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GC"
```

✗
```
_dmarc.example.com. IN TXT "v=DMARC1" no policy
```

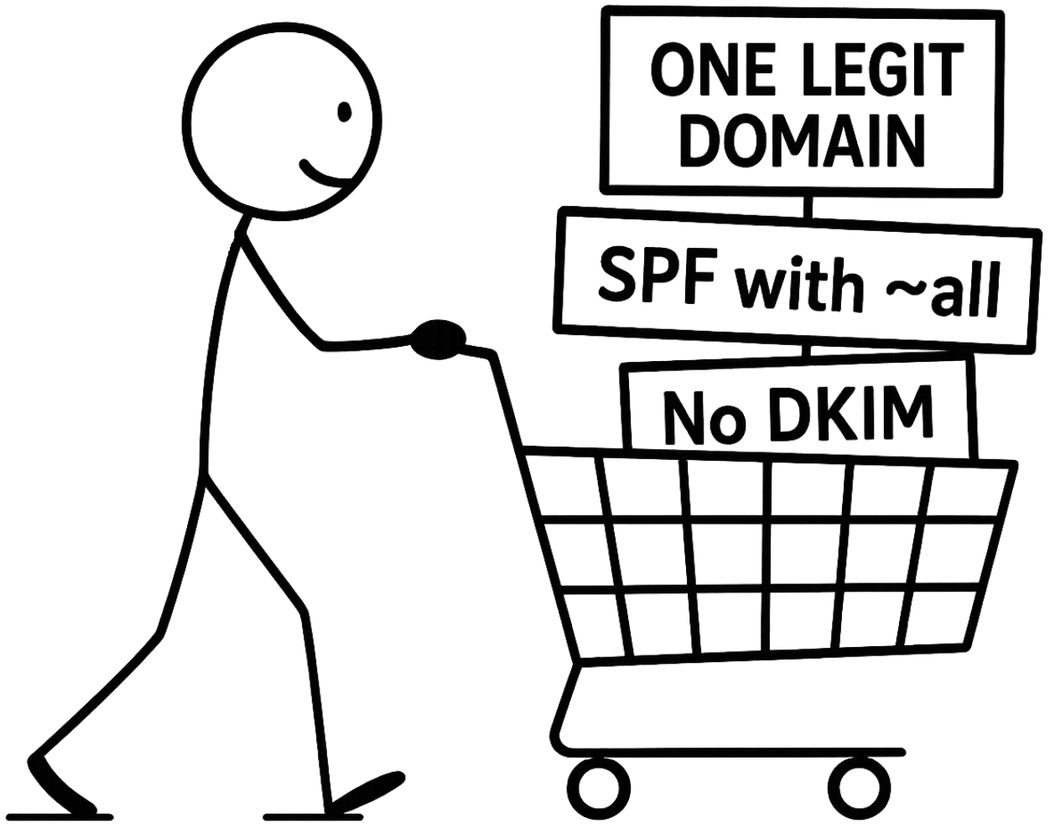
✗
```
_domainkey.example.com. IN TXT "v=DKIM1; k=rsa; p=" no pub key
```

ARC, OUR HERO

Authenticated Received Chain

ARC **preserves the results of email authentication checks** as a message passes through multiple hops, which is particularly valuable for emails that are forwarded or relayed through intermediate servers.

SO IS EMAIL EASY TO SPOOF?



COMPANIES WITH ISSUES

Brevo

Go Daddy®

Google

Microsoft

Fastmail

Attack Pattern #1

SPF Abuse

Example: spoof email from networksolutions.com

```
; <<>> DiG 9.18.18-0ubuntu2.1-Ubuntu <<>> networksolutions.com txt
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39459
; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
; QUESTION SECTION:
;networksolutions.com.          IN      TXT

; ANSWER SECTION:
networksolutions.com.   266     IN      TXT     "google-site-verification=4eIncVtJhJSW6qpb
networksolutions.com.   266     IN      TXT     "MS=ms37265135"
networksolutions.com.   266     IN      TXT     "MS=ms78547785"
networksolutions.com.   266     IN      TXT     "v=spf1 ip4:91.199.212.0/24 include:spf1.w
sforce.com include:spf.websitewelcome.com include:eig.spf.a.cloudfilter.net -all"
networksolutions.com.   266     IN      TXT     "facebook-domain-verification=m4lpzwyjv2uy
networksolutions.com.   266     IN      TXT     "google-site-verification=5hT-6CoNzJ0wCHwJ
```

What is spf.websitewelcome.com?

Hostgator, probably like most shared hosting services, has a master SPF record that is designed to cover all of its email servers. This allows the company to reorganize their servers without all of their customers having to edit their SPF records. To include Hostgator's record in my own, I needed to set my SPF record to the following:

```
v=spf1 +a +mx +ip4:50.87.144.137 +include:websitewelcome.com ~all
```

Reference: https://serverfault.com/questions/723911/setting-up-an-spf-record-for-a-shared-hosting-service-with-lots-of-email-gateway

Allowed SPF IP ranges by HostGator

```
; <<>> DiG 9.18.18-0ubuntu2.1-Ubuntu <<>> spf.websitewelcome.com txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60077
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;spf.websitewelcome.com.                IN      TXT

;; ANSWER SECTION:
spf.websitewelcome.com. 263     IN      TXT     "v=spf1 ip4:192.185.0.0/16 ip4:50.116.64.0/
18 ip4:50.87.152.0/21 ip4:108.167.128.0/18 ip4:216.172.160.0/19 ip4:108.179.192.0/18 ip4:16
2.144.0.0/16 -all"

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Jul 20 16:19:02 UTC 2024
;; MSG SIZE  rcvd: 214
```

```
"websitewelcome" => [
  "50.87.152.0/21",
  "50.116.64.0/18",
  "108.167.128.0/18",
  "108.179.192.0/18",
  "162.144.0.0/16",
  "192.185.0.0/16",
  "216.172.160.0/19"
]
```

Enable HostGator SMTP credentials

Mail Client Manual Settings

If you do not see an auto-configuration script for your client in th

Secure SSL/TLS Settings (Recommended)	
Username:	[illegible]
Password:	*Use the email account's password.*
Incoming Server:	gator4208.hostgator.com IMAP Port: 993 POP3 Port: 995
Outgoing Server:	gator4208.hostgator.com SMTP Port: 465

IMAP, POP3, and SMTP require authentication.

HostGator SMTP server is included in the master SPF

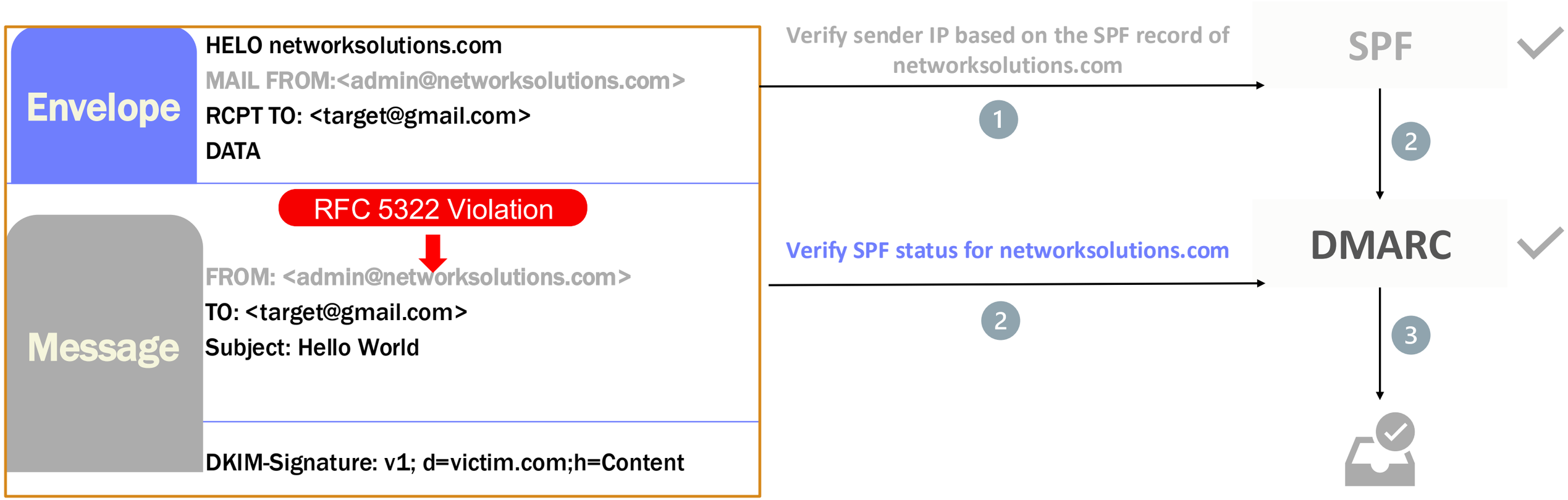
```
; <<>> DiG 9.18.18-0ubuntu2.1-Ubuntu <<>> gator4208.hostgator.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56938
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;gator4208.hostgator.com.       IN      A

;; ANSWER SECTION:
gator4208.hostgator.com. 7170   IN      A       108.167.189.34
```

```
"websitewelcome" => [
  "50.87.152.0/21",
  "50.116.64.0/18",
  "108.167.128.0/18",
  "108.179.192.0/18",
  "162.144.0.0/16",
  "192.185.0.0/16",
  "216.172.160.0/19"
]
```

ATTACK FLOW


Envelope
HELO networksolutions.com
MAIL FROM:<admin@networksolutions.com>
RCPT TO: <target@gmail.com>
DATA
RFC 5322 Violation
Message
FROM: <admin@networksolutions.com>
TO: <target@gmail.com>
Subject: Hello World
DKIM-Signature: v1; d=victim.com;h=Content
Verify sender IP based on the SPF record of networksolutions.com
1
SPF
2
Verify SPF status for networksolutions.com
2
DMARC
3

Send the email via utility

```
sendEmail -f admin@networksolutions.com
          -xu $username
          -xp $password
          -t target@gmail.com
          -u “Subject"
          -m "Something believable"
          -s gator4208.hostgator.com:587
```

Reference: https://github.com/zehm/sendEmail

Enable HostGator SMTP credentials

Hello World Inbox ×

admin@networksolutions.com <admin@networksolutions.com>
to me

This is a test email sent from the command line using sendEmail and HostGator.

Original Message

Message ID	<735738.005812408-sendEmail@ubuntu-s-1vcpu-1gb-sfo3-01>
Created at:	Fri, Jun 21, 2024 at 3:05 PM (Delivered after 3 seconds)
From:	"admin@networksolutions.com" <admin@networksolutions.com> Using sendEmail-1.56
To:	"smtpcloudops@gmail.com" <smtpcloudops@gmail.com>
Subject:	Hello World
SPF:	PASS with IP 35.89.44.37 Learn more
DMARC:	'PASS' Learn more

SPOOF ROOT DOMAINS ALSO

Subject:	HostGator Support Follow-Up Minutes
SPF:	PASS with IP 44.202.169.33 Learn more
DMARC:	'PASS' Learn more

HostGator Support Follow-Up Minutes

HA

Hostgator Accounting <no-reply@hostgator.com> <admin@hostgator.com>

To: Caleb Sargent

Retention: DPT default 3 year delete Expires: 05/06/2028.

This message is from an external sender.

Hi Caleb,

We just wanted to check in regarding your account. Let us know if you need anything else.

Thanks,
HostGator Support

SAMPLED RESULTS – SPF ABUSE

6M
Domain Data Set

4.1M
Vulnerable Domains

Vulnerable Domains

~60%

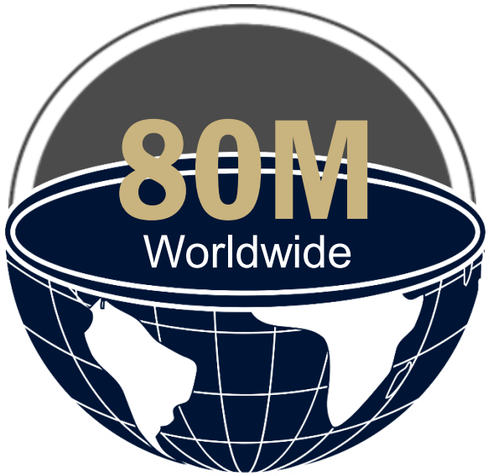
The majority did not have DMARC configured

SAMPLED RESULTS – SPF ABUSE

Go Daddy®

~30%

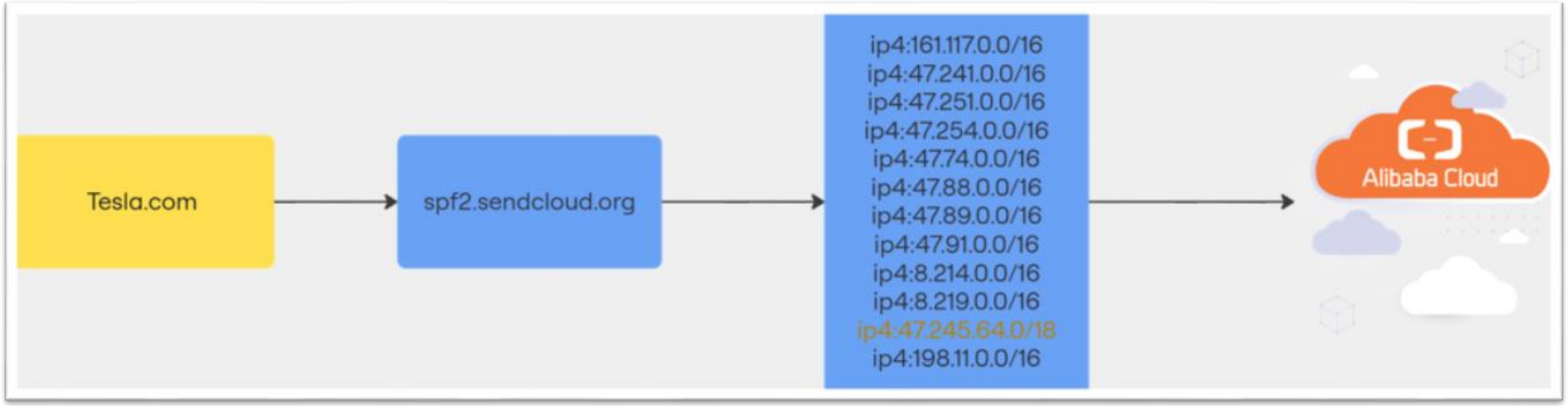
Domain Vulnerability



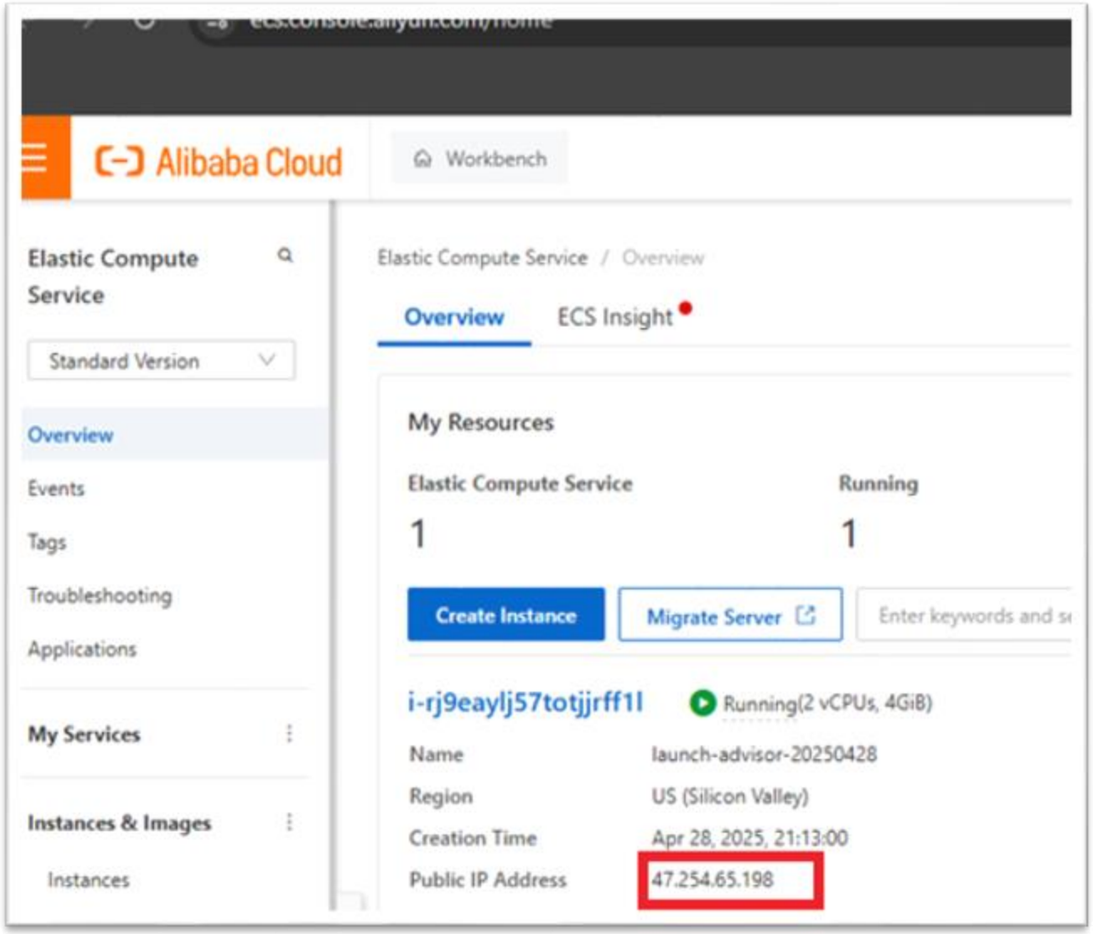
?%

Domain Vulnerability

CLOUD COMPUTE TRUST



COMPUTE INSTANCE WITHIN IP RANGE



EXAMPLE IN THE WILD

```
root@Email:~# sudo dmidecode -s system-manufacturer
DigitalOcean
root@Email:~# curl ipconfig.io/ip
142.93.198.253
root@Email:~#
```

spf:morling.edu.au Solve Email Delivery Problems

```
v=spf1 include:_s00155613.autospf.email ~all
```

Prefix	Type	Value
	v	spf1
+	include	_s00155613.autospf.email
~	all	

SuperTool Beta9

_s00155613.autospf.email SPF Record Lookup

spf:_s00155613.autospf.email Find Problems Solve Email Delivery Problems spf

```
v=spf1 ip4:40.92.0.0/15 ip4:66.102.0.0/20 ip4:74.125.0.0/16 ip4:35.191.0.0/16 ip4:54.240.0.0/18 ip4:128.17.0.0/20 ip4:13.111.0.0/16 ip4:
149.72.58.233 ip4:167.89.0.0/17 ip4:50.31.32.0/19 ip4:198.21.0.0/21 ip4:149.72.0.0/16 ip4:138.68.0.0/16 ip4:159.89.0.0/16 ip4:159.6
5.0.0/16 ip4:167.99.0.0/16 ip4:142.93.0.0/16 ip4:68.183.0.0/16 ip4:167.71.0.0/16 ip4:64.225.0.0/16 ip4:40.107.0.0/16 ip4:52.100.0.0/15 i
nclude:_s001556130.autospf.email ~all
```

EXAMPLE IN THE WILD

Original message

Message ID	<20250526230107.B23F040A43@morling.edu.au>
Created on:	26 May 2025 at 19:01 (Delivered after 0 seconds)
From:	root <no-reply@morling.edu.au>
To:	[redacted]@gmail.com
Subject:	Test from DigitalOcean
SPF:	PASS with IP 142.93.198.253 Learn more
DMARC:	'PASS' Learn more

Test from DigitalOcean

R

root <no-reply@morling.edu.au>

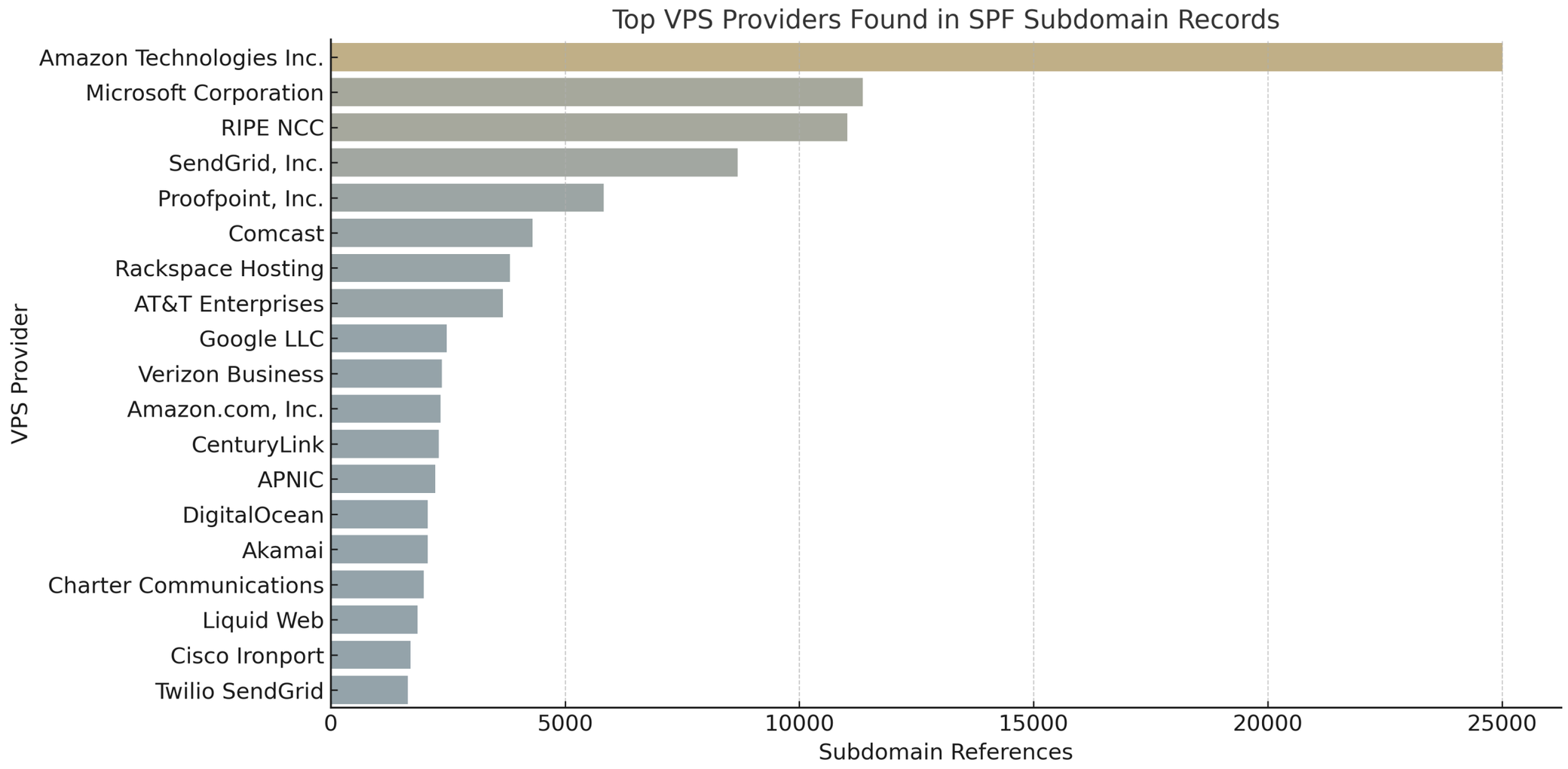
To: Caleb Sargent

Retention: DPT default 3 year delete Expires: 05/26/2028.

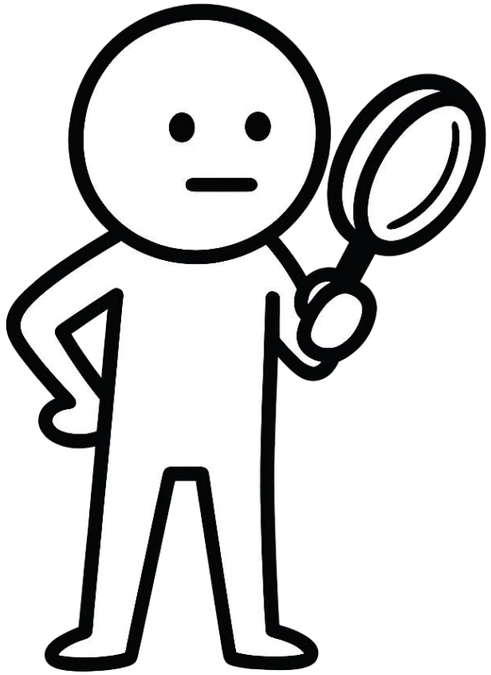
This message is from an external sender.

This is a test

CLOUD TRUST RESULTS



How did we get this data?



Sample Trust Chain

```
example.com
└── includes → mailhosted.net
    └── WHOIS → MegaMail LLC
        └── IP block: 198.51.100.0/227
```

- This means example.com implicitly trusts MegaMail's infra
- Attackers can spoof example.com if they control a sending IP inside that range

GIVE ME THE DATA

RE: 25302-Requesting access to Open Data datasets

Hao Wang
To

Reply | Reply All | Forward

Thu 4/11/2024

Retention Policy DPT default 3 year delete (3 years) Expires 4/12/2027

This message is from an external sender.

Hi Hao,

lead the global strategic alliances team at Rapid7.

What you have outlined below definitely falls under our commercial use case. There is a $35,000 USD annual fee associated with access to the data.

This includes

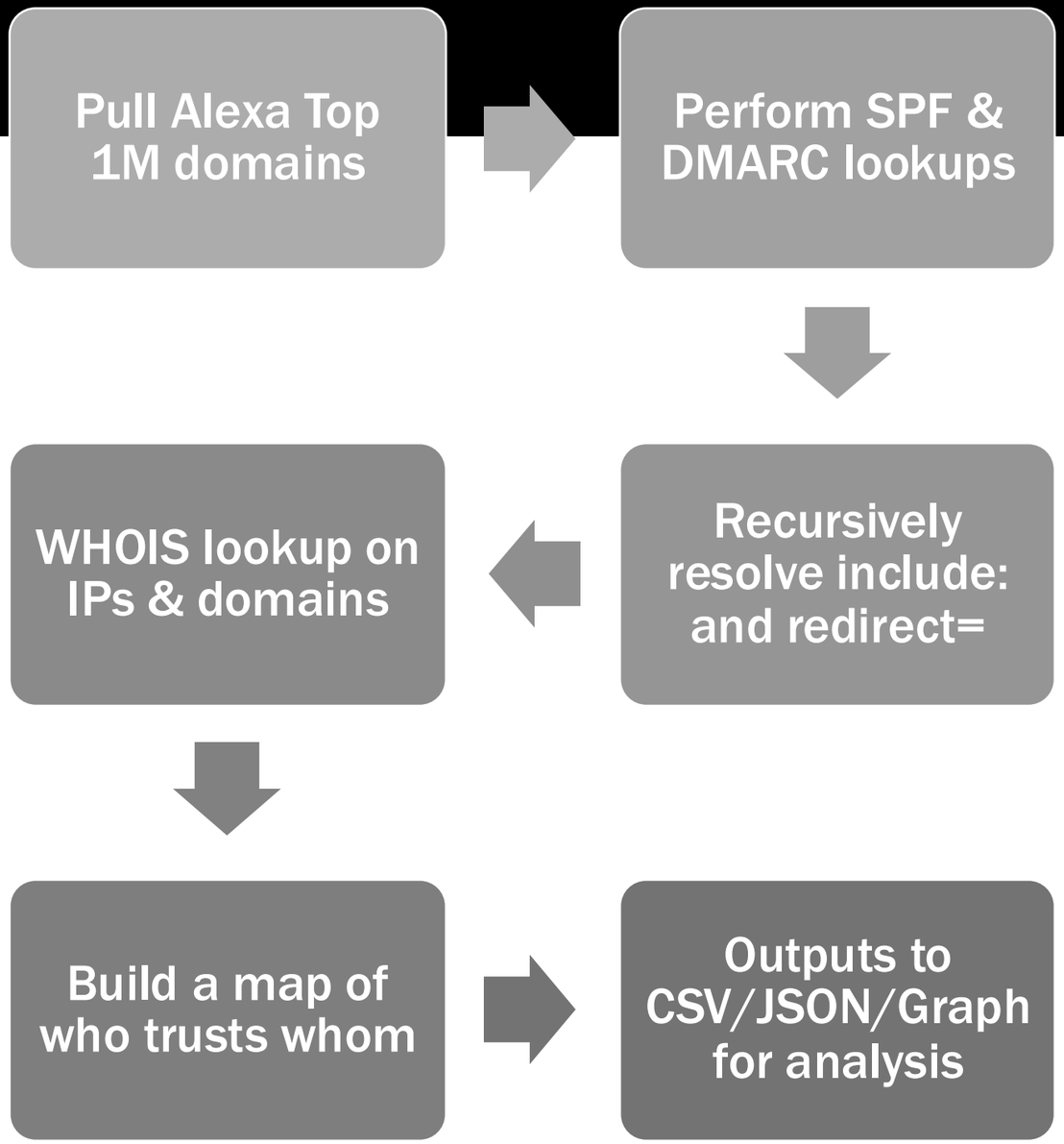
- The data is a package so you get all sources listed here vs an a la carte approach
- We provide 37 months of historical
- All data can be pulled directly from the site or programmatically site or via API

When you're ready, I'm happy to draw up an official quote & send over the Terms of Service.

mx 2023-10-18 Dataset

Item & Description	Amount
mx 2023-10-18 Full dataset from Email Hosting Providers - Category Datasets 191,768,664 Unique Web Domains covering 7,829,179,421 technology records over 74,386,167 website and subdomains.	$112,124

DISCOVERING DOMAIN TRUSTS



MAIL FROM + FROM + SPF ABUSE

Who is vulnerable?

Large **domain** registrar & email **service** & **hosting** providers

- **CVE-2024-7208**
- **CVE-2024-7209**

What is the impact?

Spoof emails from **6M+** domains

Only **15% of the domains** owned by two email and hosting providers were scanned.

Potentially affect **any type** of mailbox

Attack pattern prerequisites?

- ❑ Email address is not verified from **MAIL FROM** field
- ❑ Email address is not verified from **FROM** field
- ❑ Victim domains include the overly permissive / master SPF records

Attack Pattern: #2

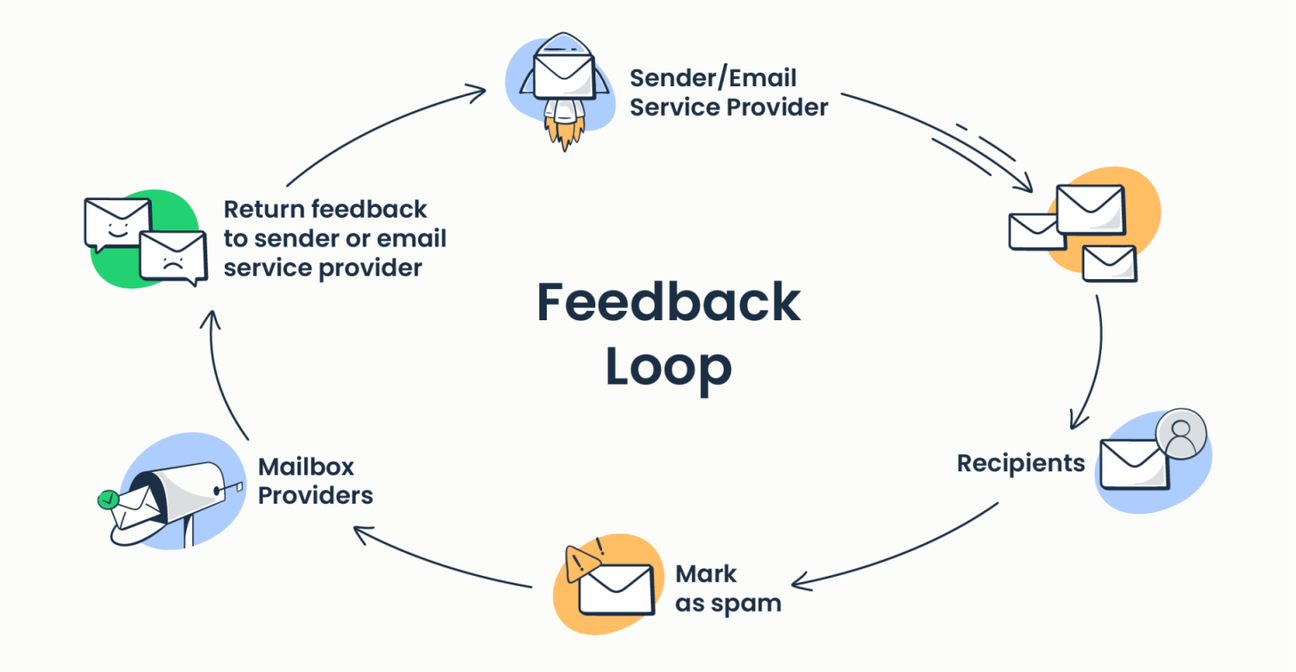
Domain verification + DKIM signature

DKIM replay

Dual DKIM ?

```
Authentication-Results: mx.google.com;
       dkim=pass header.i=@purplecloudops.com header.s=k1 header.b=tKXbD8q6;
       dkim=pass header.i=@mailgun.org header.s=mg header.b=n8GM3R1B;
       spf=pass (google.com: domain of bounce+f9deec.4b1f2a-smtpcloudops=gmail.com@purp
smtpcloudops=gmail.com@purplecloudops.com";
       dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=mailgun.org
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=purplecloudops.com; q=dns/txt;
From: Message-ID: Sender: Sender: X-Feedback-Id; bh=QK/yDOHl7MptNkDjFgt5TvbLuMrPXB12Lab
b=tKXbD8q69JsyW4jWJ5HIoBo7VsIEk60fdIgrwQpz3vRO8OzarimMp/gj2lwu2PMTsG3x1VLlrTONP1b9af+GH
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=mailgun.org; q=dns/txt; s=mg; t
Message-ID: Sender: Sender: X-Feedback-Id; bh=QK/yDOHl7MptNkDjFgt5TvbLuMrPXB12LabiZX9Xr
b=n8GM3R1BVmifkBs+YUkU23iFk04azOpPamaBBVamAinFHcvR2Sbkg43F+vcp4G9WSKYRlUO9AsUjaO0rZk8pF
X-Feedback-Id: admin@mailgun.org::65fdb68787282b7c4c4411b1:mailgun
```

What is the Feedback Loop?



Reference: https://mailtrap.io/blog/email-feedback-loop/

Gmail Feedback Loop requirement

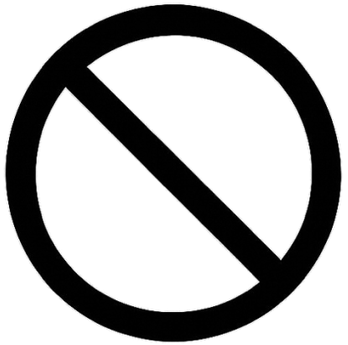
About the data

The aggregate data will be generated for the first 4 fields (as separated by ':') of the `Feedback-ID:`, starting from the right side. If the `SenderId` is empty, no data will be generated. If another field is empty, data will be generated for the rest of the fields.

n order to prevent spoofing of the `Feedback-ID`, the traffic being sent to Gmail needs to be DKIM signed by a domain owned (or controlled) by the sender, after the addition of this header. This domain should be added and verified to the Gmail Postmaster Tools, so the sender can access the FBL data.

Reference: https://support.google.com/a/answer/6254652

FROM + DKIM ABUSE

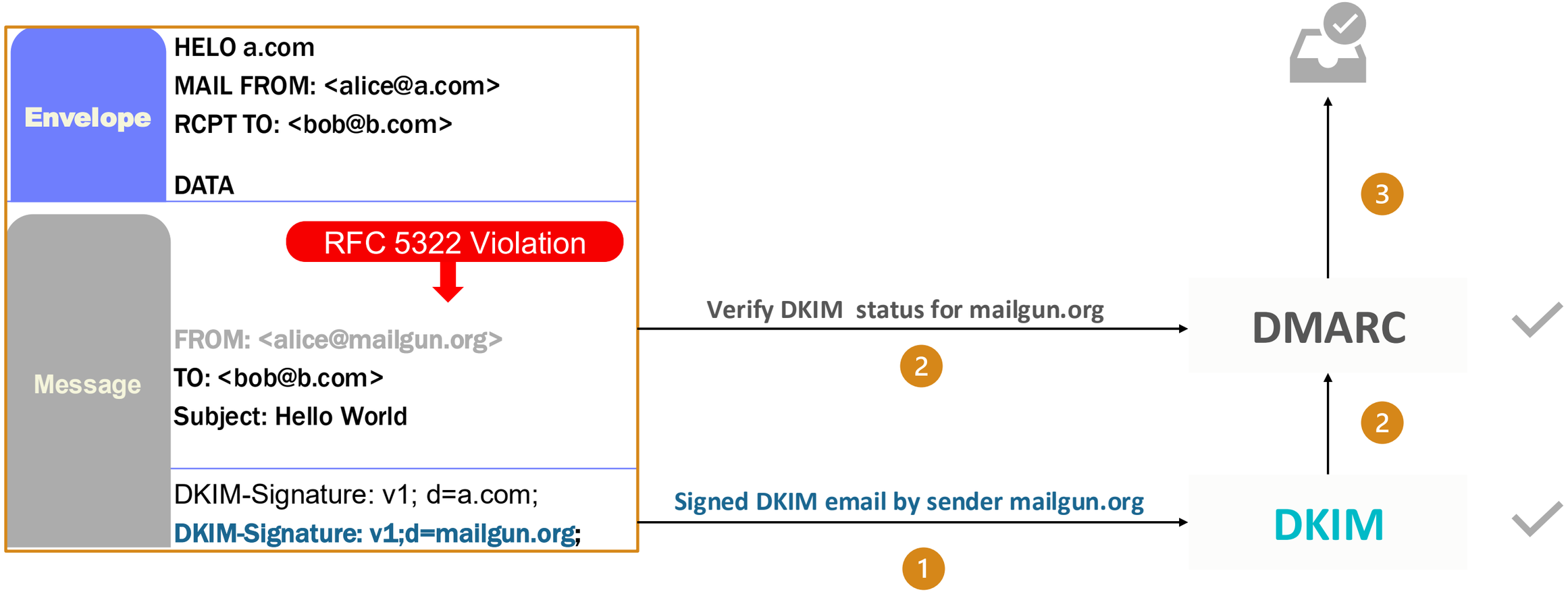


DOMAIN VERIFICATION

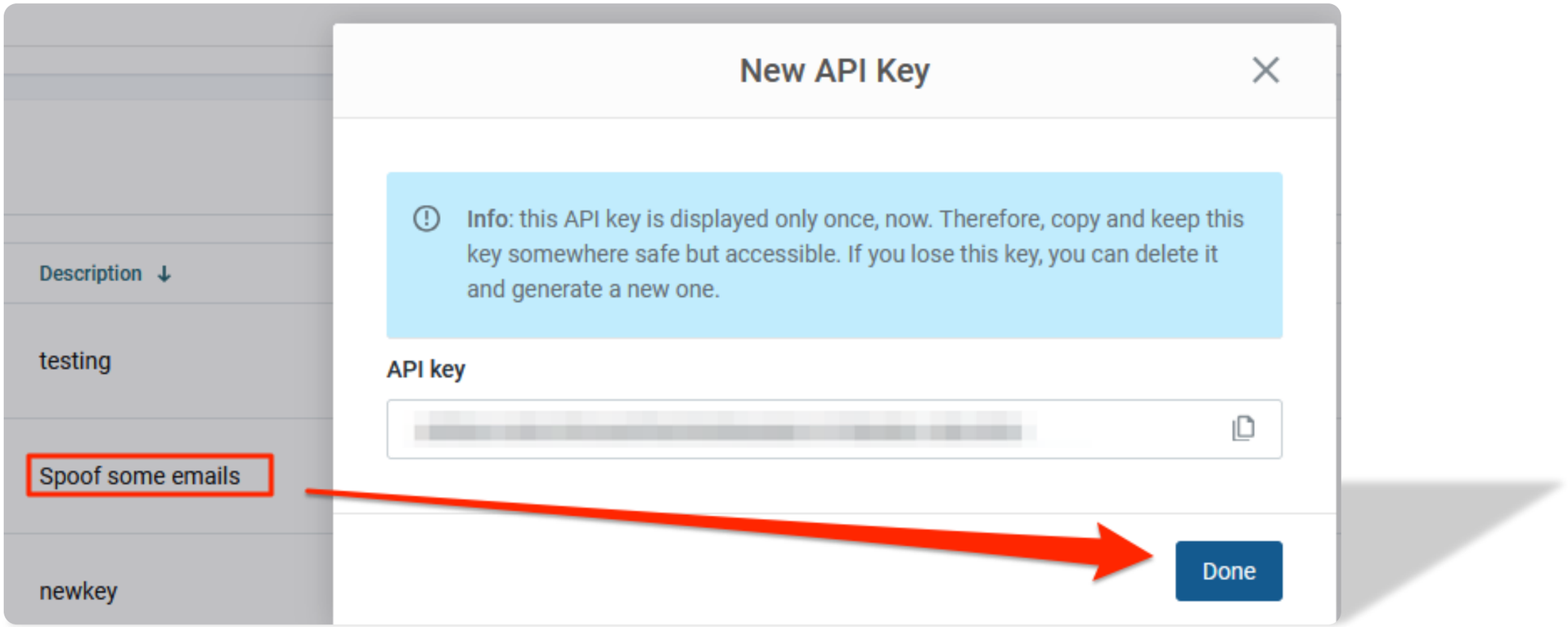
+

DKIM

ATTACK FLOW: SPOOF MAILGUN.ORG INTO GMAIL MAILBOX



Generate some API keys

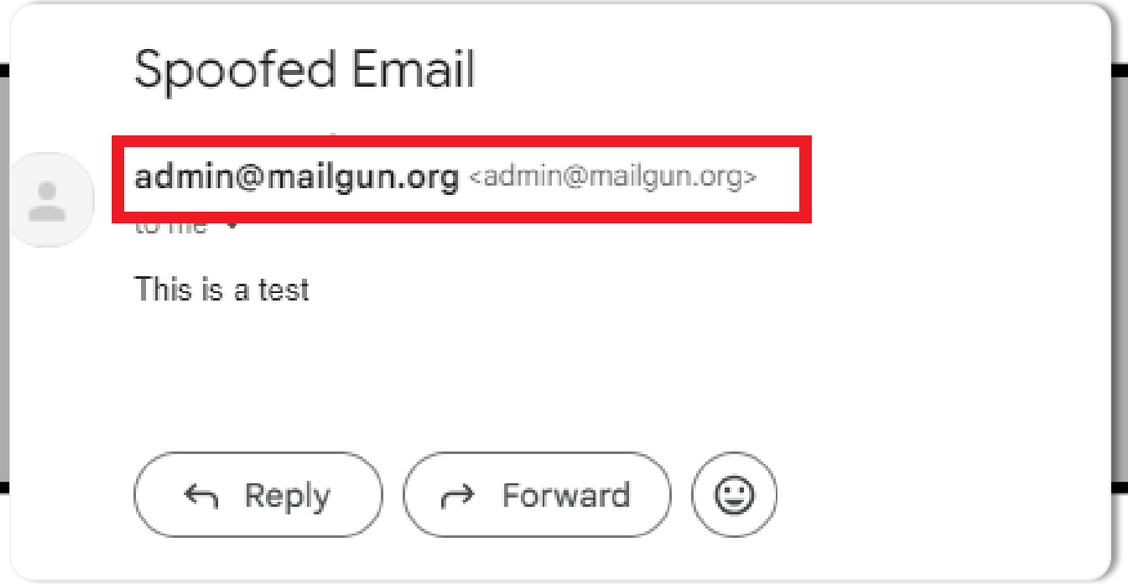


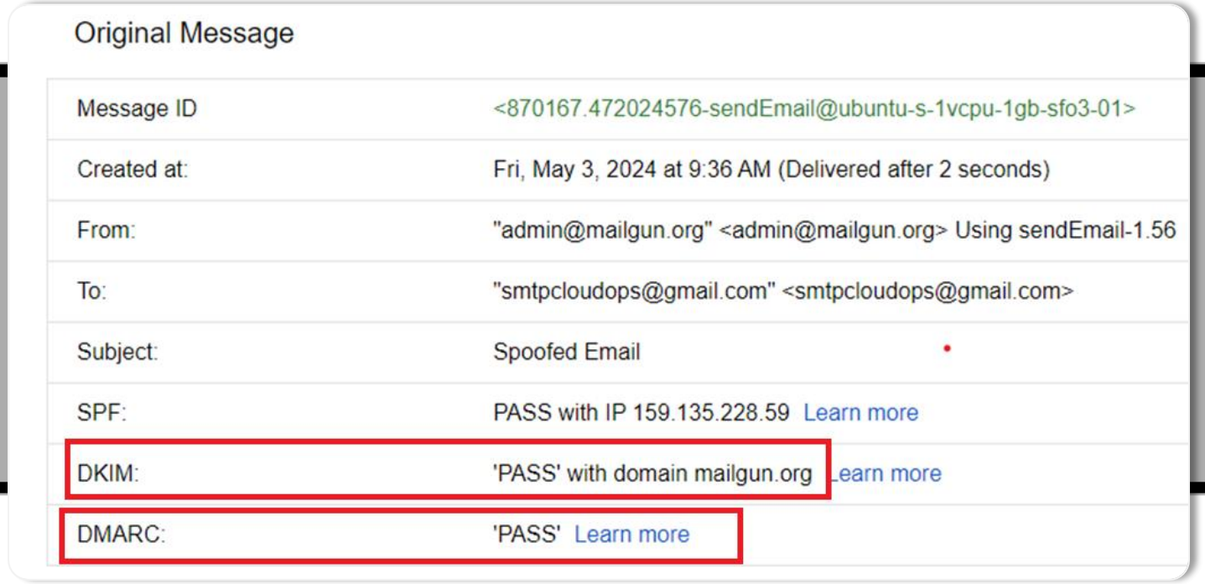
Send the email via utility

```
sendEmail -f admin@mailgun.org
          -xu $username
          -xp $password
          -t target@gmail.com
          -u "Spoofed Email"
          -m "This is a test"
          -s smtp.mailgun.com:587
```

Reference: https://github.com/zehm/sendEmail

Example: Spoof mailgun.org for Gmail mailbox





Original Message

Message ID	<870167.472024576-sendEmail@ubuntu-s-1vcpu-1gb-sfo3-01>
Created at:	Fri, May 3, 2024 at 9:36 AM (Delivered after 2 seconds)
From:	"admin@mailgun.org" <admin@mailgun.org> Using sendEmail-1.56
To:	"smtpcloudops@gmail.com" <smtpcloudops@gmail.com>
Subject:	Spoofed Email
SPF:	PASS with IP 159.135.228.59 Learn more
DKIM:	'PASS' with domain mailgun.org Learn more
DMARC:	'PASS' Learn more

SPOOFING ROOT DOMAINS

Brevo

sendinblue.com

brevosend.com

Mailgun.org

*Dependent on how the FROM field is displayed in the inbox

Examples: Spoofing from Brevo

Outlook

Unverified We didn't start the fire

test@outlook.com <test@outlook.com>

To:

Retention: DPT default 3 year delete Expires: 07/23/2027.

Authentication-Results: spf=pass (sender IP is 185.41.28.5)
smtp.mailfrom=ae.d.mailin.fr; dkim=pass (signature was verified)
header.d=sendinblue.com;dmarc=fail action=none
header.from=outlook.com;compauth=fail reason=001
Received-SPF: Pass (protection.outlook.com: domain of ae.d.mailin.fr
designates 185.41.28.5 as permitted sender) receiver=protection.outlook.com;
client-ip=185.41.28.5; helo=ae.d.mailin.fr; pr=C

sendinblue.com

Private Email

It was always burning

test@outlook.com
To admin@purplecloudops.com

Reply Reply all Forward Delete

Received: from asp-relay-pe.jellyfish.systems (unknown [198.54.122.240])
by mxs-10.mxs.mxs.svc.cluster.lan (Postfix) with ESMTP id F366A761CA
for <admin@purplecloudops.com>; Mon, 22 Jul 2024 14:55:03 +0000 (UTC)
Authentication-Results: asp-relay-pe.jellyfish.systems;
dkim=pass header.d=sendinblue.com header.s=mail header.b=GXziGEK+;
spf=pass (asp-relay-pe.jellyfish.systems: domain of "bounces-223030174-
test=outlook.com@ae.d.mailin.fr" designates 185.41.28.5 as permitted sender)

sendinblue.com

Gmail

Since the world's been turning Inbox ×

test@outlook.com <test@223030174.t-sender-sib.com>
to me

Says Billy

SPF PASS with IP 185.41.28.5 Learn more

DKIM 'PASS' with domain t-sender-sib.com Learn more

DMARC 'PASS' Learn more

t-sender-sib.com

FROM + DKIM ABUSE

Who is vulnerable?

Large email service providers, such as **Brevo and Mailgun**, who leverage **Feedback Loop (FBL)** feature of popular mailbox providers such as **GMAIL, Outlook, and Yahoo Mail** to collect users' complaints

- **CVE-2024-7208**

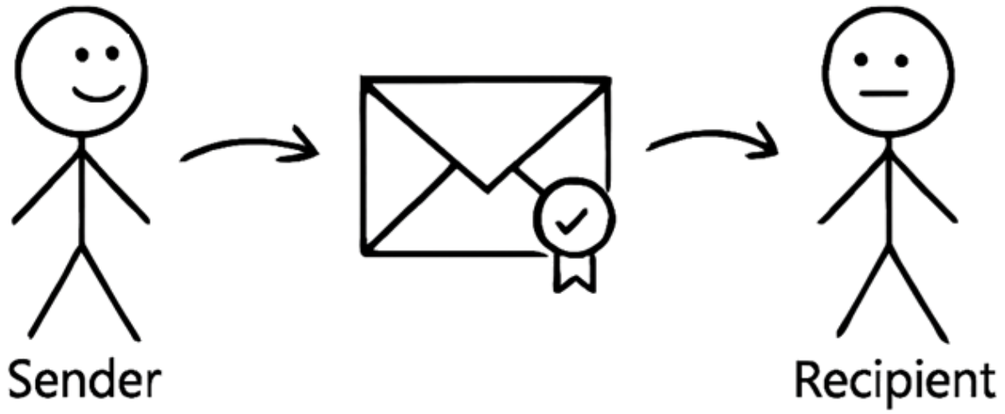
What is the impact?

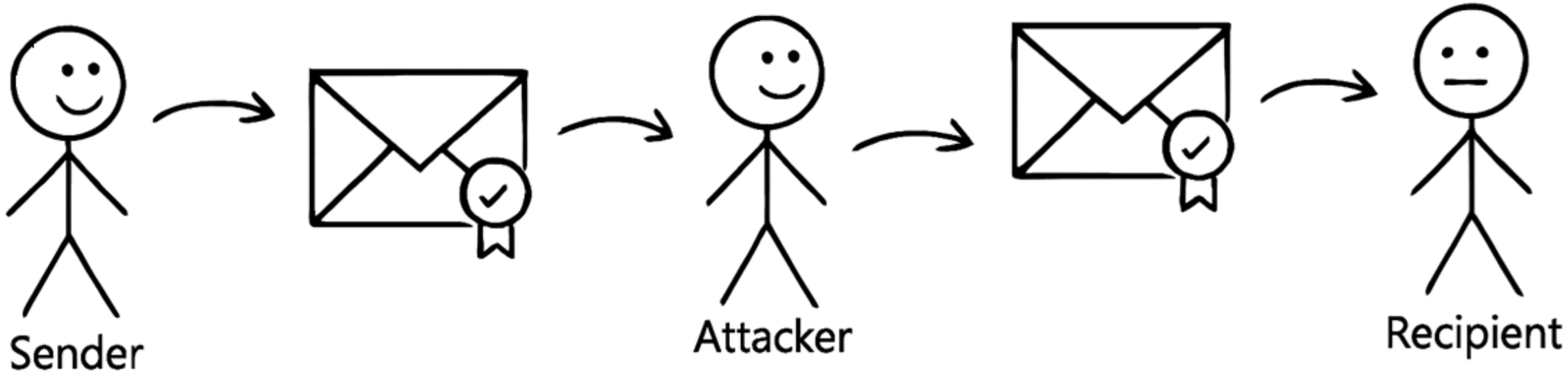
Spoof emails from the sender DKIM domain used for FBL

Attack pattern prerequisites?

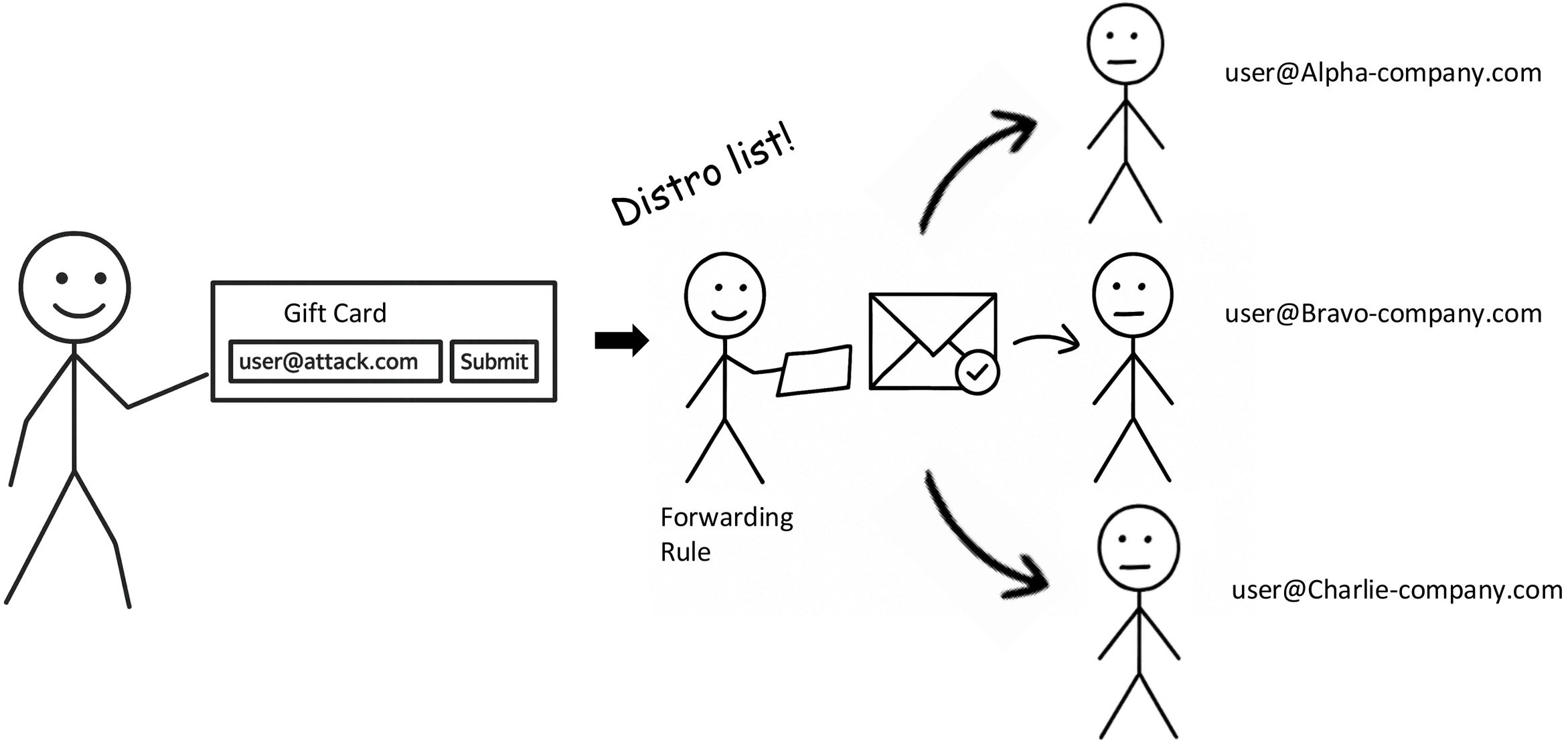
- ❑ Email address is not verified from **FROM** field
- ❑ A **DKIM** signature is required by FBL for email sender

DKIM REPLAY?

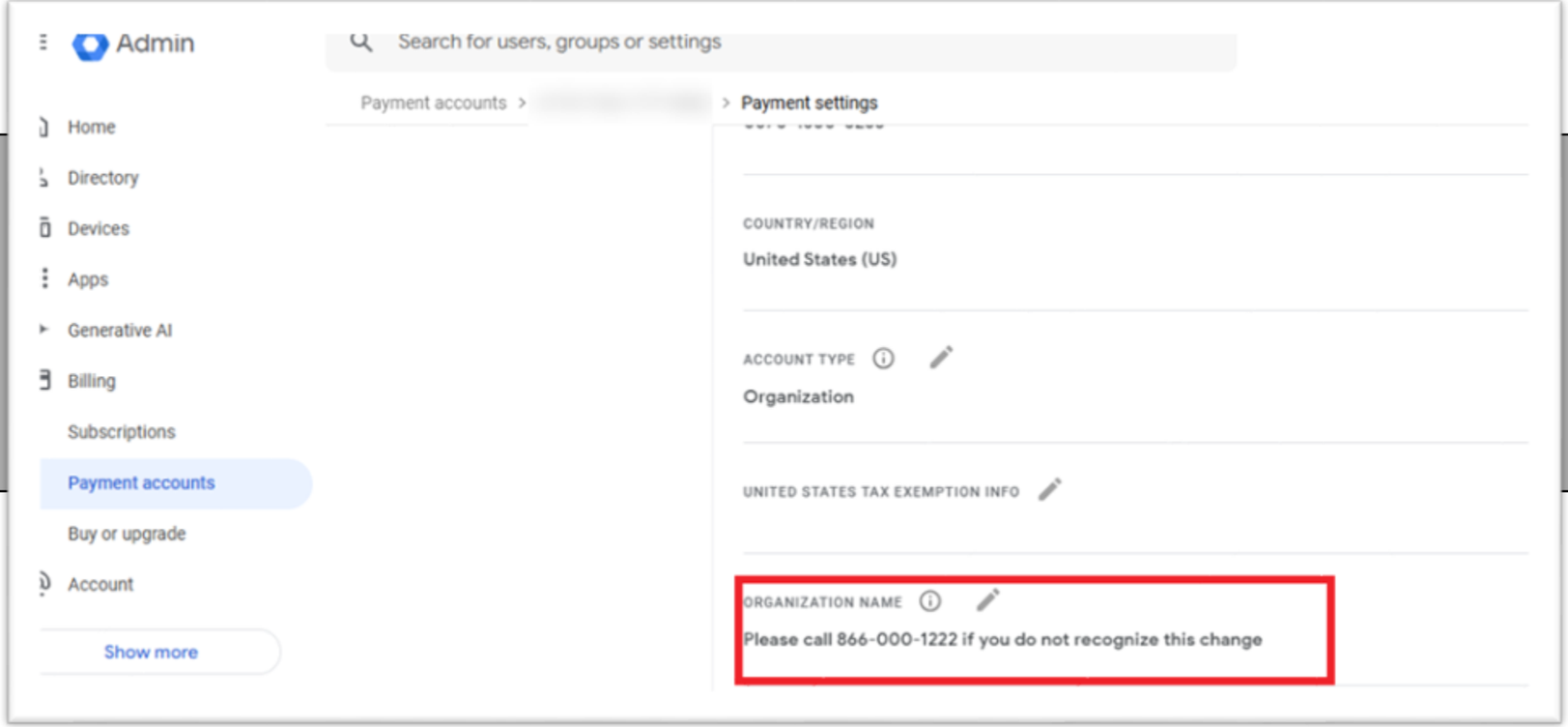




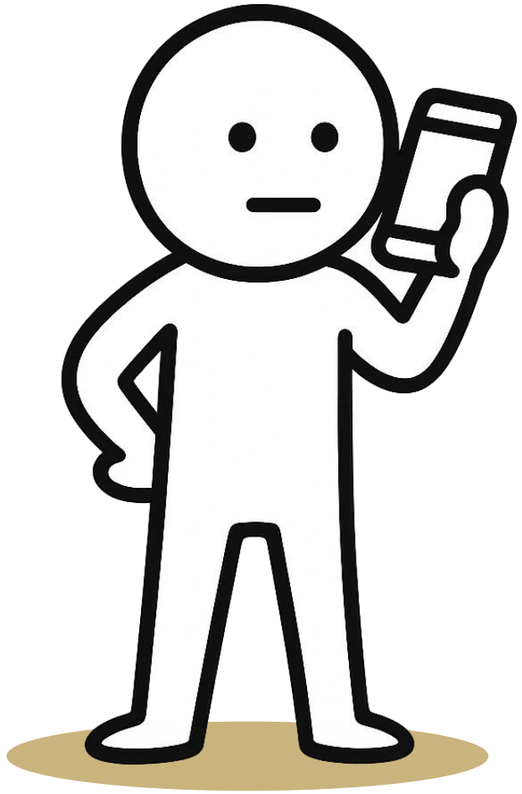
DKIM REPLAY DETAILS

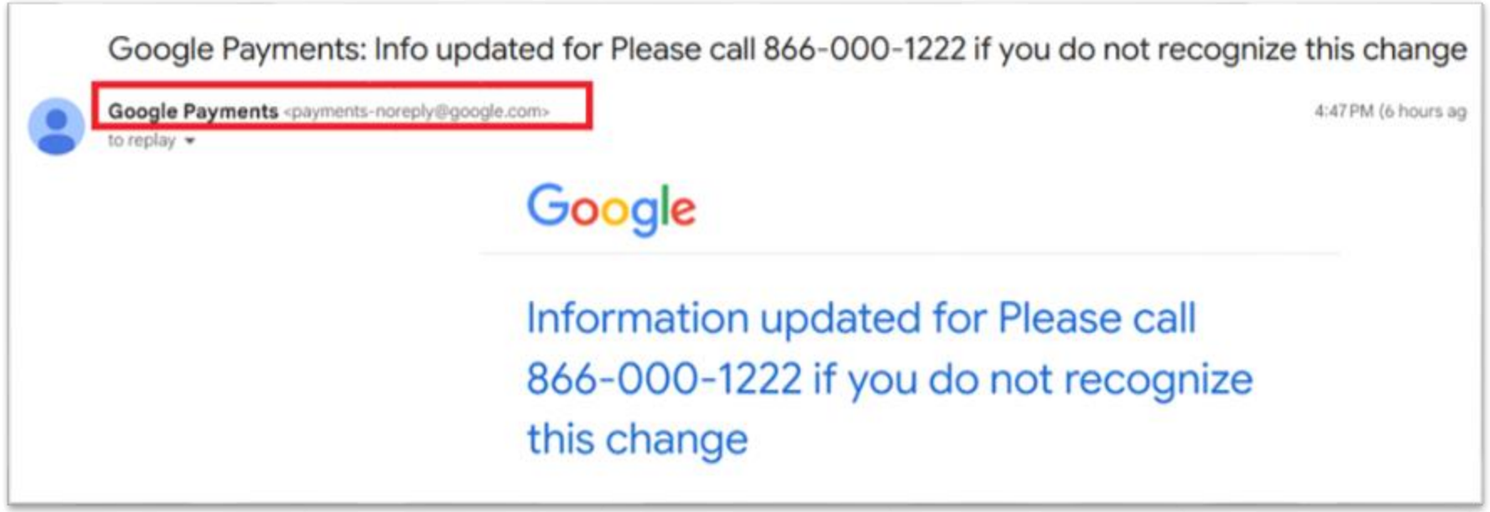


Inject Phishing Content into Org Name



Trigger Email Security Notification

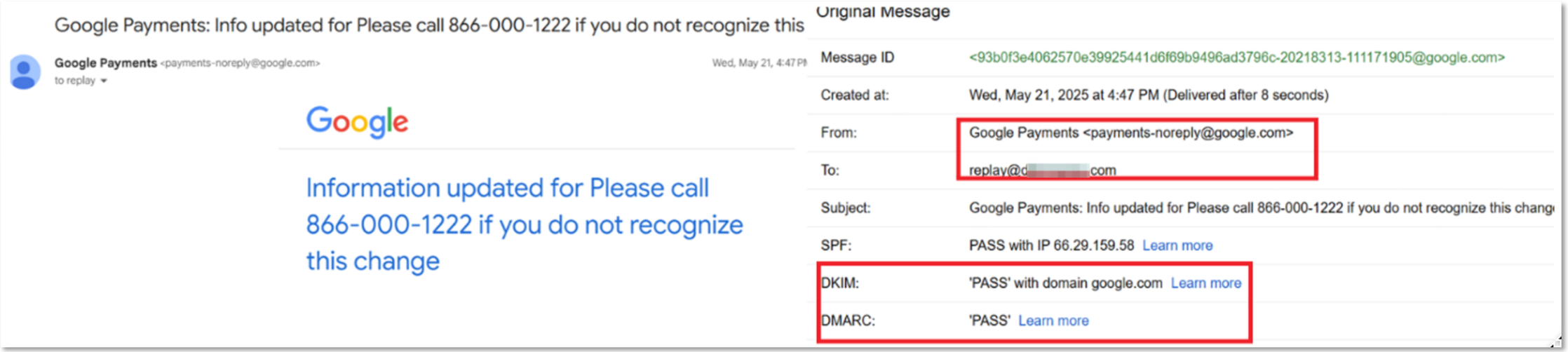




ATTACK FLOW

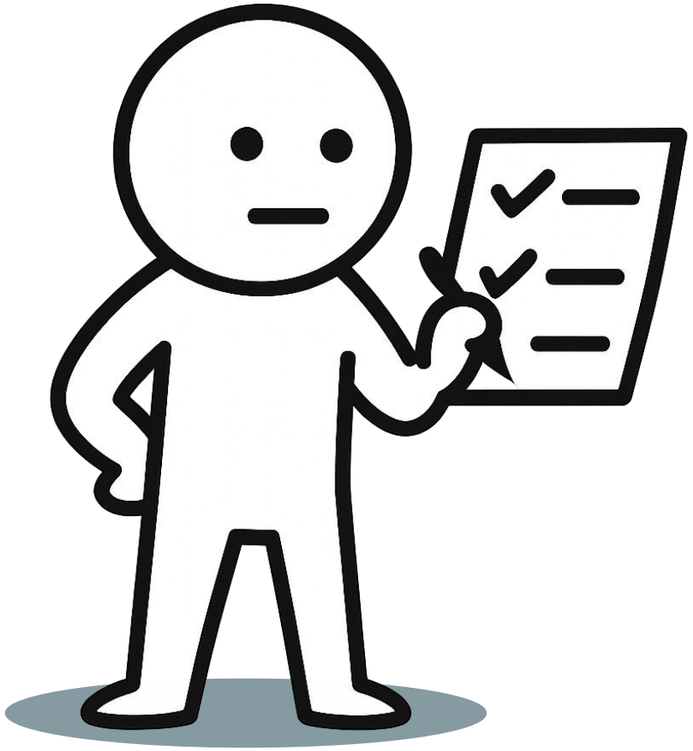
payments-noreply@google.com → replay@replaydomain.com → victiminbox@gmail.com

Valid Platform Address | **Distro List** | **Victim**



PENDING DISCLOSURE

“WORKING AS INTENDED”



ca...@google.com <ca...@google.com> #5 Jun 4

Status: Won't Fix (Intended Behavior)

Hi!

We've reviewed your submission and decided not to track it as a security bug, as we are already aware of this issue.

For the same reason, your report will also not be accepted to our VRP. Only first reports of technical security vulnerabilities are in scope for VRP :(Sorry about that.

Nevertheless, we're looking forward to your next report! To maximize the chances of it being accepted, check out the Bug Hunter University and learn some Secrets of Google VRP.

Thanks again for your report and time,
Google Trust & Safety Team

Other Examples

Coinbase <no-reply@info.coinbase.com>
to dl

coinbase

You just received 0.00001194 BTC ($1.00)

ust sent you 0.00001194 BTC. Sign up and verify your ID to claim your transferred currency. You can view transaction details in your Coinbase account.

Message from sender: Please call me if you have questions

Sign up to claim this amount

Microsoft <microsoft-noreply@microsoft.com>
to

Expires 2/26/2028

are problems with how this message is displayed, click here to view it in a web browser.
re to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Microsoft

Your Power BI Premium Per User subscription is ready to use

Your organization now has a subscription to Power BI Premium Per User. Sign in to the Microsoft 365 admin center to set up your new service, assign licenses to users, and manage your subscription.

Additional resources

- Learn how to assign licenses.
- Learn how to add users.

Account information

Organization name: Your (Microsoft Corporation) .Your subscription has been successfully purchased for 689.89 USD using your checking account. If you did not authorize this transaction, please call 1(234) 456-0000 to request a refund account verification code

Cash App <cash@square.com>
to

J

Payment from $

$1.00

for please call f you have questions

DKIM REPLAY

Who is vulnerable?

ANYONE?

What is the impact?

Spoof emails from the sender's DKIM domain

Attack pattern prerequisites?

- A web form that allows a user supplied email address + some form of user supplied information – Name, address, comment, etc.

Attack Pattern #3

SMTP Parsing Problems

Does email providers parse FROM field consistently?

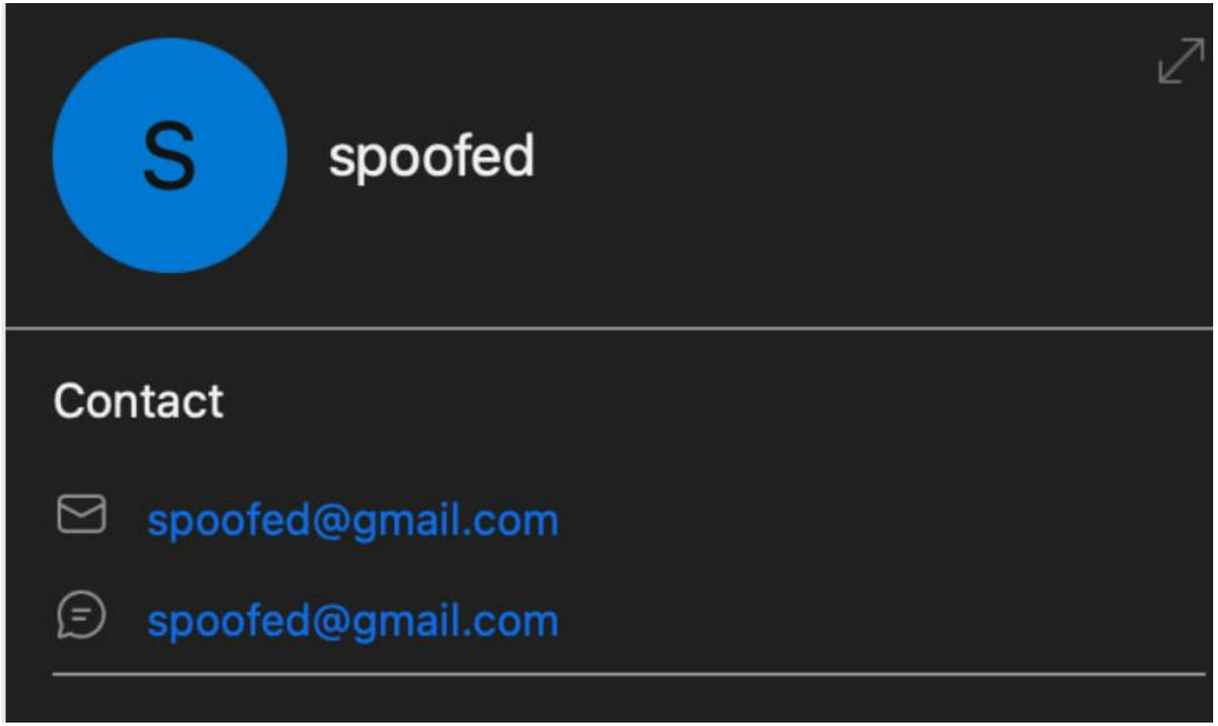
Governed by RFC 5322: defines syntax (groups, display names, angle brackets, etc.)

However, provider implementations might vary.

- Differ in strictness, error tolerance, and interpretation
- Some accept malformed headers
- Others rewrite/sanitize headers due to DMARC/SPF policies

Spoofing emails via manipulating email headers

Encouraged by Slonser's blog



Reference: https://blog.slonser.info/posts/email-attacks

Header injection via group names

Standard structure – FROM: Group Name: <user1@example.com>

↓

No-standard structure – FROM: <spoof@example.com>: <user1@example.com>

Spoofing emails via manipulating email headers

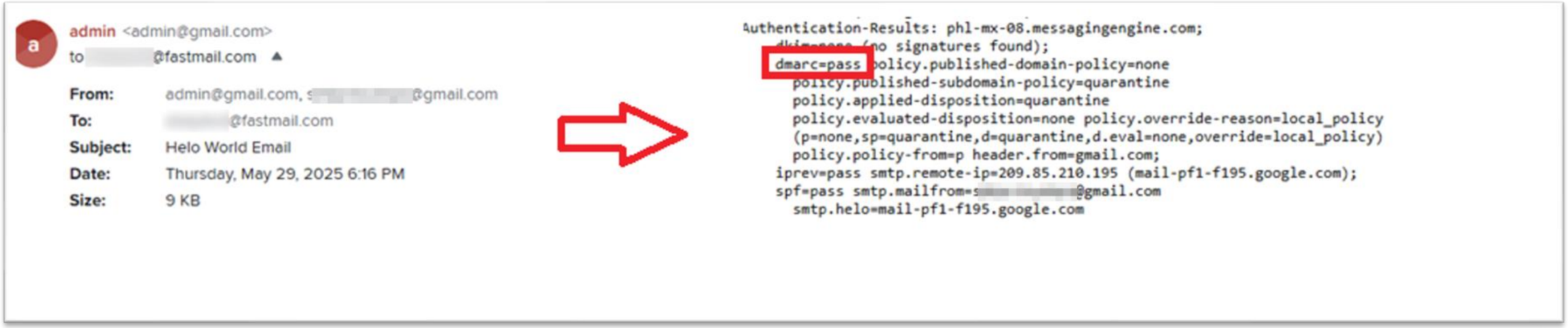
Gmail to Fastmail: Header injection via group names

Payload: Use angle brackets (<>) to inject spoofed email address within the group name field

From: **<admin@gmail.com>:** <example@gmail.com>

Spoofed email

Attacker-controlled email



Spoofing emails via manipulating email headers

Outlook to a Proton Mail Inbox: Header injection via group names

Payload: Use angle brackets (<>) to inject spoofed email address within the group name field

From: “Hello World"<example@outlook.com>:<admin@github.com> → From: “Hello World":<admin@github.com>

Attacker-controlled email

Spoofed email

Vendor Fix

From "hello" : <admin@github.com>

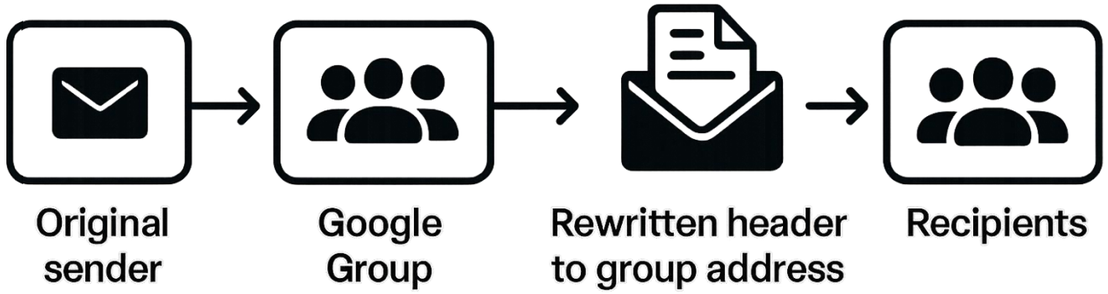
To [redacted]l@proton.me

Our system flagged this as suspicious. If it is not a phishing or scam email, mark as legitimate. Learn more

Header rewrite by email service provider

Some email providers auto-modify email headers to maintain DMARC compliance

- Example: Google Groups rewrite the FROM field if sender's domain has specific DMARC records



Enabling unauthorized messages to appear as if sent from trusted sources

Google Group: Header rewrite

Google Groups rewrites the "From" field for emails from domains with DMARC set to p=reject or p=quarantine.

Original sender’s address is replaced by the Google Group’s email address.

Message ID	<BY5PR14MB39214402F4C3712DFFAE049CDC98A@BY5PR14MB3921.namprd14.prod.outlook.com>
Created at:	Fri, May 23, 2025 at 4:29 PM (Delivered after 6 seconds)
From:	'John Cloud' via DL <DL@smtpgroup.org>
To:	"dl@smtpgroup.org" <dl@smtpgroup.org>
Subject:	hello
SPF:	PASS with IP 209.85.220.69 Learn more
DKIM:	'PASS' with domain smtpgroup-org.20230601.gappssmtp.com Learn more
DMARC:	'PASS' Learn more

Enabling unauthorized messages to appear as if sent from trusted sources

Some email providers allow creation of deceptive subdomains

GOAL: SPOOF Disney

no-reply@534535.brevosend.com

tickets@disney.brevosend.com

Example Deception

Brevo: deceptive subdomain “creation”

- Brevo allows fake subdomains like disney.brevosend.com
- DMARC policy doesn’t matter on target spoof domain
- DKIM & SPF pass as brevosend.com, so spoofed mail looks valid
- Result: You can send email as any brand

Example Deception

Subject:	URGENT: Your Bahamas Cruise Has Been Cancelled
SPF:	PASS with IP 77.32.148.112 Learn more
DKIM:	'PASS' with domain 6468295.brevosend.com Learn more
DMARC:	'PASS' Learn more

URGENT: Your Bahamas Cruise Has Been Cancelled Inbox ×

cruise-support@disney.go.com <no-reply@disney.brevosend.com> Unsubscribe

to me

from:	**cruise-support@disney.go.com** <no-reply@disney.brevosend.com>
reply-to:	"cruise-support@disney.go.com" <no-reply@disney.brevosend.com>
to:	[redacted]@gmail.com
date:	28 May 2025, 11:15
subject:	URGENT: Your Bahamas Cruise Has Been Cancelled
mailed-by:	kh.d.sender-sib.com
Signed by:	6468295.brevosend.com
security:	Standard encryption (TLS) Learn more
:	Important according to Google magic.

Images i

Show i

Dear

We re cancelled due to unforeseen operational issues.

A full ing issue, we require verification of your account to complete the refund.

To proceed, please call our Refund Support Hotline at +1[redacted] within the next 48 hours.

Failure to respond within this timeframe may result in delays processing your refund.

We apologize for the inconvenience and appreciate your understanding.

Sincerely,
Disney Cruise Refund Services
http://disn3y-support.net

One last trick...

If at first you don't succeed, Google it Inbox ×

larry.page@gmail.com via

to me

The most searched phrase on Bing? 'Google'.

Reply Forward

Unverified **Re: Don't listen to the other guy**

Bill Gates <bill.gates@microsoft.com>

To: Caleb Sargent

Retention: DPT default 3 year delete Expires: 06/25/2027.

We just made Windows updates easier than finding a relevant Google+ post

SMTP PARSING PROBLEMS

Who is vulnerable?

All large email inbox providers could be vulnerable to this

What is the impact?

Spoof emails from high reputational domains and target affected email providers' inboxes

Attack pattern prerequisites?

- ❑ Identify the right pair of outbound and inbound SMTP servers
- ❑ Outbound SMTP allows non-RFC complaint mail headers
- ❑ Inbound SMTP fails parse the malformed headers correctly

Disclosure

DOES ABUSE@COMPANY.COM WORK?

Email Spoofing Vulnerability Responsible Disclosure - DCU-826755 Inbox ×

Digital Crimes Unit <care@services.godaddy.com> Wed, 24 Apr, 14:09
to me

GoDaddy

Everything you need to know about your Abuse Report:

This email inbox isn't monitored. To finish your report, please go to the Abuse Reporting Form.

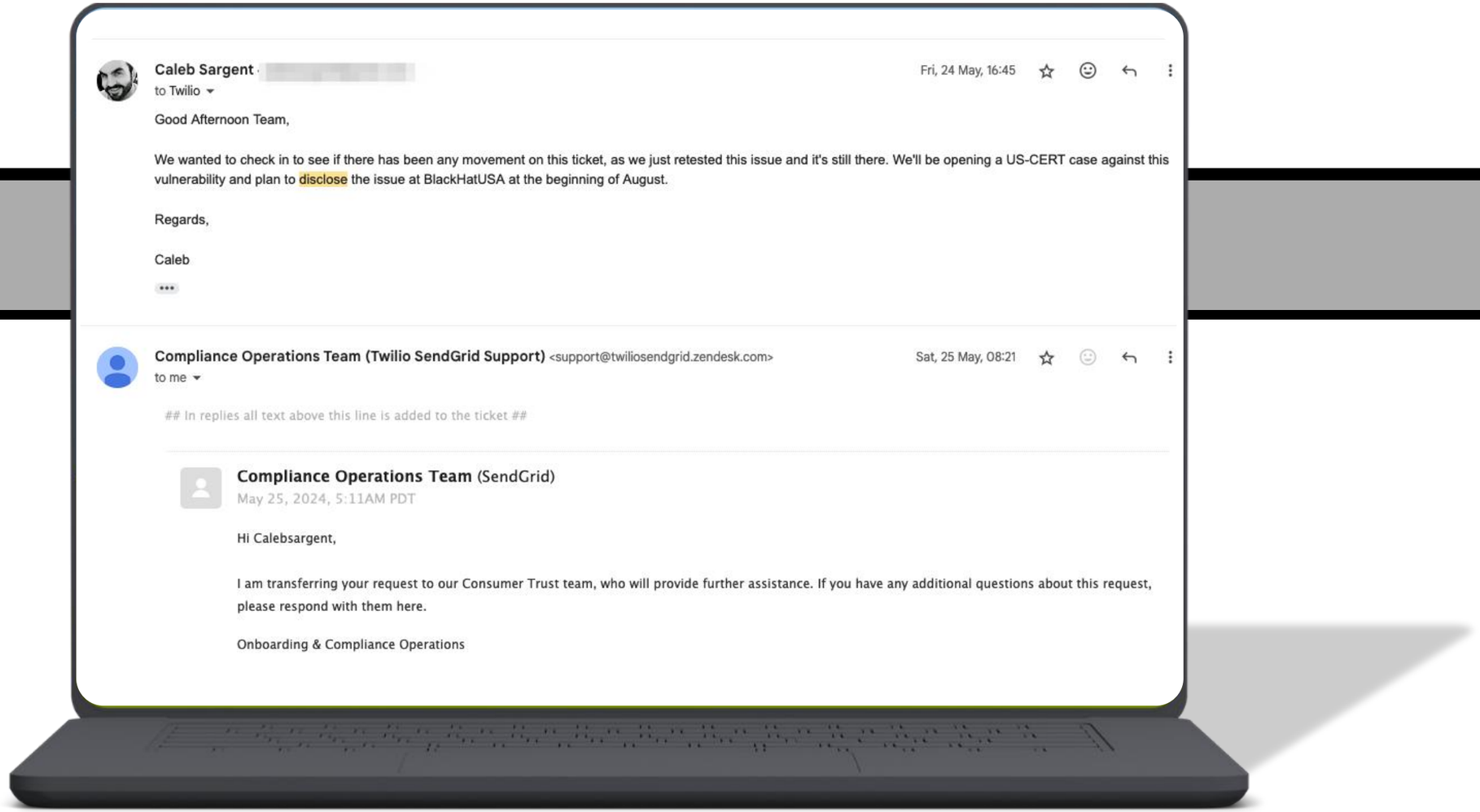
We'll review your complaint and process in accordance with our policies, and will contact you only if necessary and at our discretion.

If you submit (or have already submitted) your report using the Abuse Reporting Form, additional submissions from the same email within 24 hours may not receive another notice of receipt.

To send reports in bulk, you can use our API for brand protection and industry partners.

View Abuse Reporting Form →

BUT SOMETIMES THINGS TAKE A WHILE



Caleb Sargent · [redacted]
to Twilio
Fri, 24 May, 16:45

Good Afternoon Team,

We wanted to check in to see if there has been any movement on this ticket, as we just retested this issue and it's still there. We'll be opening a US-CERT case against this vulnerability and plan to disclose the issue at BlackHatUSA at the beginning of August.

Regards,

Caleb

•••

Compliance Operations Team (Twilio SendGrid Support) <support@twiliosendgrid.zendesk.com>
to me
Sat, 25 May, 08:21

In replies all text above this line is added to the ticket

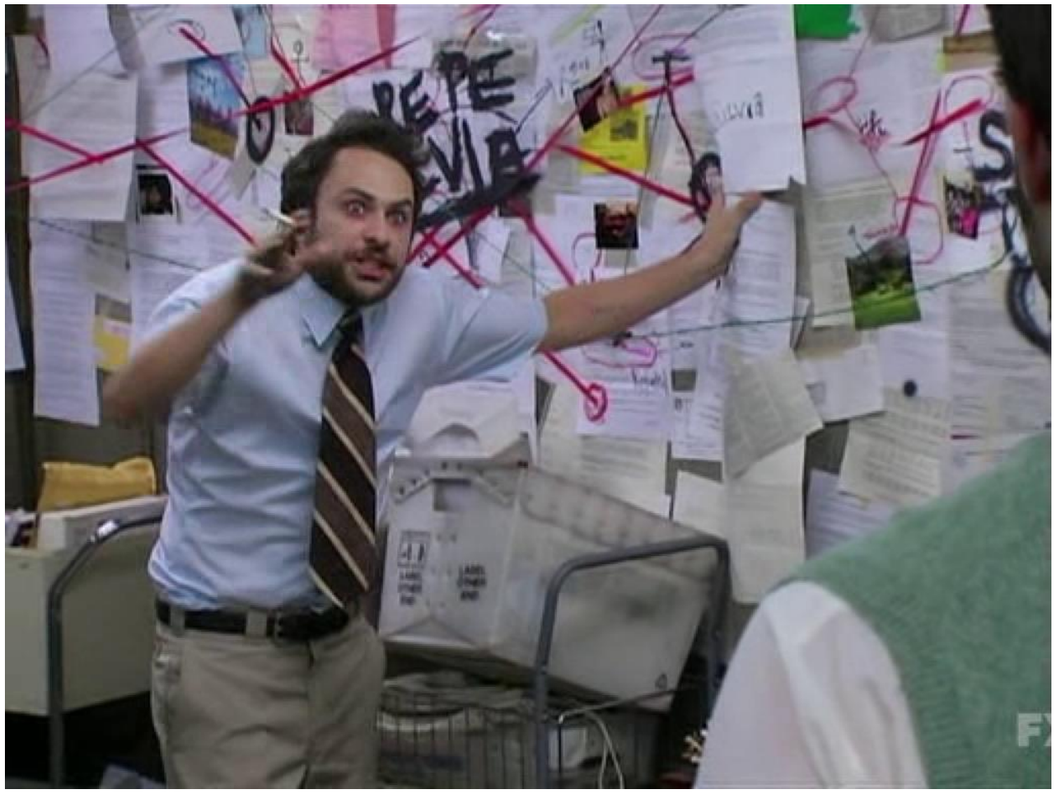
Compliance Operations Team (SendGrid)
May 25, 2024, 5:11AM PDT

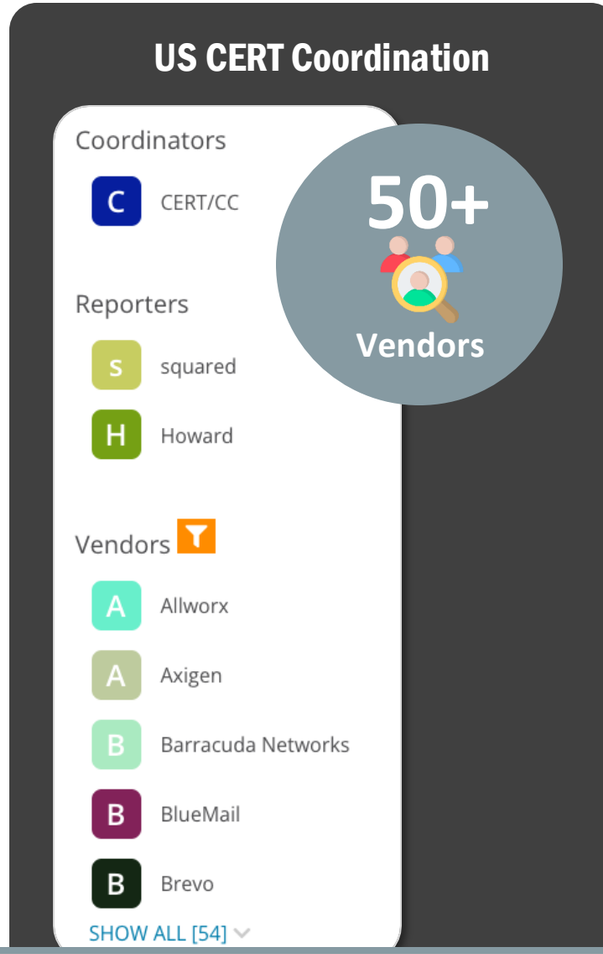
Hi Calebsargent,

I am transferring your request to our Consumer Trust team, who will provide further assistance. If you have any additional questions about this request, please respond with them here.

Onboarding & Compliance Operations

DISCLOSURE





Reference: https://kb.cert.org/vuls/id/244112

Recommendations

MISCONFIGURATIONS ABOUND

MISCONFIGURATION	RECOMMENDED FIX
❌ No SPF record	v=spf1 ip4:192.0.2.10 -all (Defines authorized sender IPs)
❌ SPF ends in ~all	v=spf1 include:_spf.google.com -all (Use -all for hard fail)
❌ No DKIM record	default._domainkey.example.com → v=DKIM1; k=rsa; p=MIIB...
❌ No DMARC record	_dmarc.example.com → v=DMARC1; p=reject; rua=...
❌ DMARC set to p=none	v=DMARC1; p=quarantine → Later: p=reject
❌ Overly permissive SPF	v=spf1 ip4:203.0.113.5 include:mydomain.com -all
❌ Alignment mismatch	Ensure SPF, DKIM, and DMARC use same base domain

DKIM

Problem with DKIM

- **DKIM-signed emails can be replayed by attackers** from unauthorized servers.
- **Signatures remain valid** even when messages are resent out of context.
- **No binding to sender IP or timestamp**, making spoofed delivery hard to detect.

DKIM2
YOU'RE OUR ONLY HOPE

Closing the gap

- DKIM2 **enhances DKIM** by adding protections against replay attacks.
- Introduces **time-bound signatures**, **sender IP binding**, and **unique message metadata – headers.**
- Helps receivers detect when a **signed email is resent** from an unauthorized source.
- **Backwards compatible** and designed for phased adoption alongside existing DKIM setups.
- Strengthens email trust by **adding context** to message authenticity.

FOLLOW THE RFC

SPF / DKIM / DMARC

RFC 5322 Section 3.6.2

In all cases, the "From:" field **SHOULD NOT** contain any mailbox that does not belong to the author(s) of the message

Defines the syntax for Internet email headers, **group syntax** is a formal structure allowing the grouping of multiple email addresses under a named label.

RFC 7489 Section 4.2

DMARC's filtering function is based on whether the RFC5322.From field domain is aligned with (matches) an **authenticated domain** name from SPF or DKIM.

It is important to note that the authentication mechanisms employed by DMARC authenticate only a DNS domain and do not authenticate the local-part of any email address identifier found in a message…

RFC 7208 Section 11.4

It is up to mail services and their MTAs to directly prevent cross-user forgery: based on SMTP AUTH ([RFC4954]), **users MUST** be restricted to using only those email addresses that are under their control...

RFC 6409 Section 6.1

The MSA **MAY** issue an error response to a RCPT command if inconsistent with the permissions given to the user (if the session has been authenticated)

TAKEAWAYS

Offensive security – easier than ever to spoof your targets

Organizations – Make sure those DKIM/SPF records are valid and reevaluate who you are trusting to send email on your behalf

Industry – It's 2025, and email trust does not enforce encryption. We can do better by adopting DKIMv2

Questions?

THANKS!

Caleb Sargent

(@squared_)

Hao Wang

(@MrRed_Panda)

REFERENCES

Dark Reading blog about our research

- https://www.darkreading.com/threat-intelligence/20-million-trusted-domains-vulnerable-to-email-hosting-exploits

CERT Blog about our research

- https://kb.cert.org/vuls/id/244112

Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks

- https://www.darkreading.com/threat-intelligence/20-million-trusted-domains-vulnerable-to-email-hosting-exploits

REFERENCES

RFC - Internet Message Format

- https://datatracker.ietf.org/doc/html/rfc2822
- https://datatracker.ietf.org/doc/html/rfc5322
- https://datatracker.ietf.org/doc/html/rfc5321
- https://datatracker.ietf.org/doc/html/rfc7489
- https://datatracker.ietf.org/doc/html/rfc7208
- https://datatracker.ietf.org/doc/html/rfc6409

REFERENCES

- https://serverfault.com/questions/723911/setting-up-an-spf-record-for-a-shared-hosting-service-with-lots-of-email-gateway
- https://github.com/zehm/sendEmail
- https://mailtrap.io/blog/email-feedback-loop/
- https://www.twilio.com/docs/sendgrid/ui/account-and-settings/spf-records
- https://support.google.com/a/answer/6254652