Mail in the Middle

Like Man in the Middle, but for Mail

orange™ Cyberdefense

Become a real Hacker
acer

EHLO

> EHLO felipe.es szymon.pl

- **Felipe Molina de la Torre**
- Proud dad & Simpsons fan
- Security Analyst (~10 y)

- **Szymon Ziółkowski**
- Pentester
- Exposed Phishing Campaign

Agenda

The Problem with Phishing

A Manual Approach
- The Process
- Infrastructure
- Impact

Automated Approach
- Further Benefits
- How it Works?
- Demo

Landscape

Defenses

The Problem

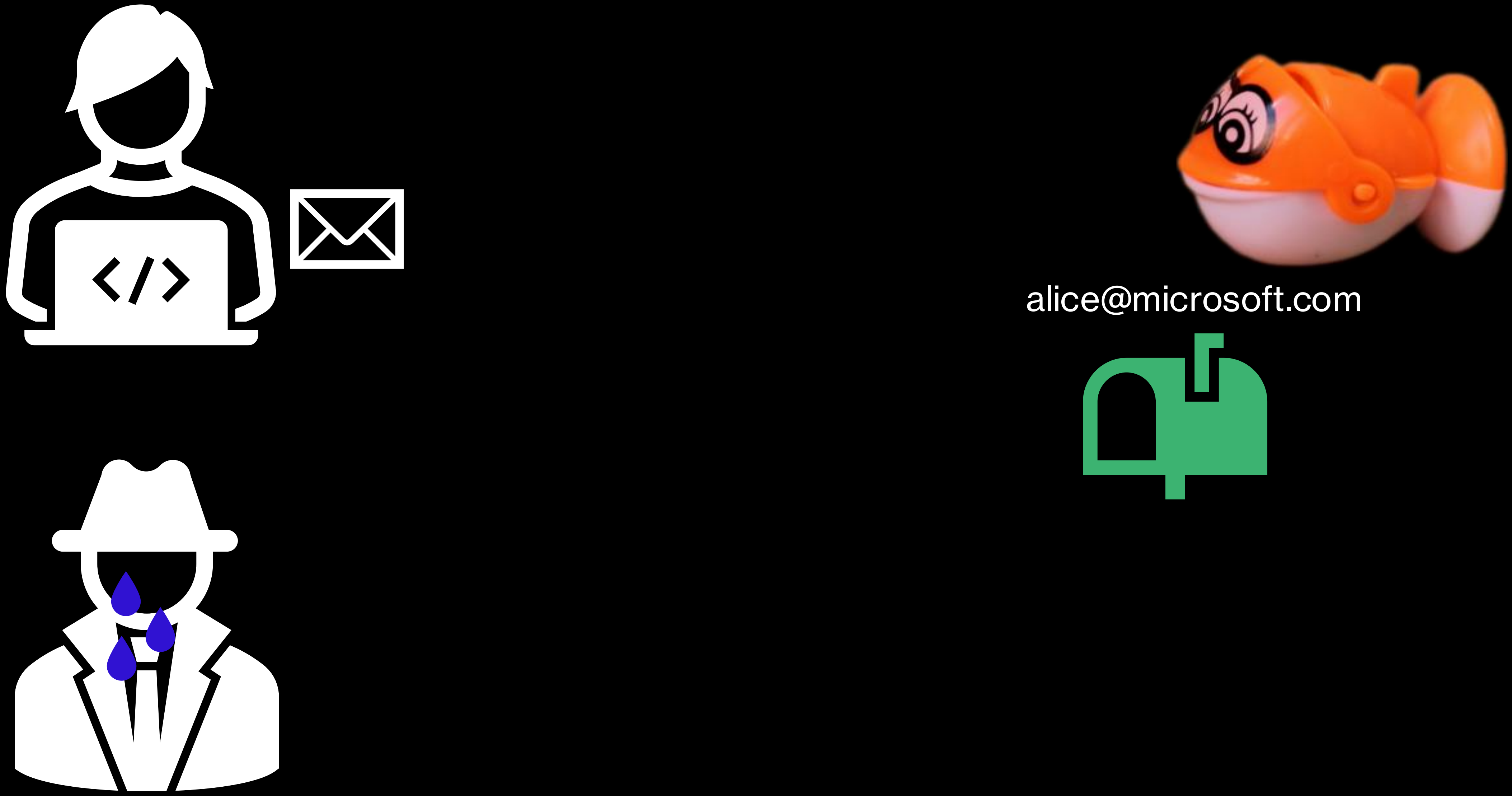
The Problem

proofpoint

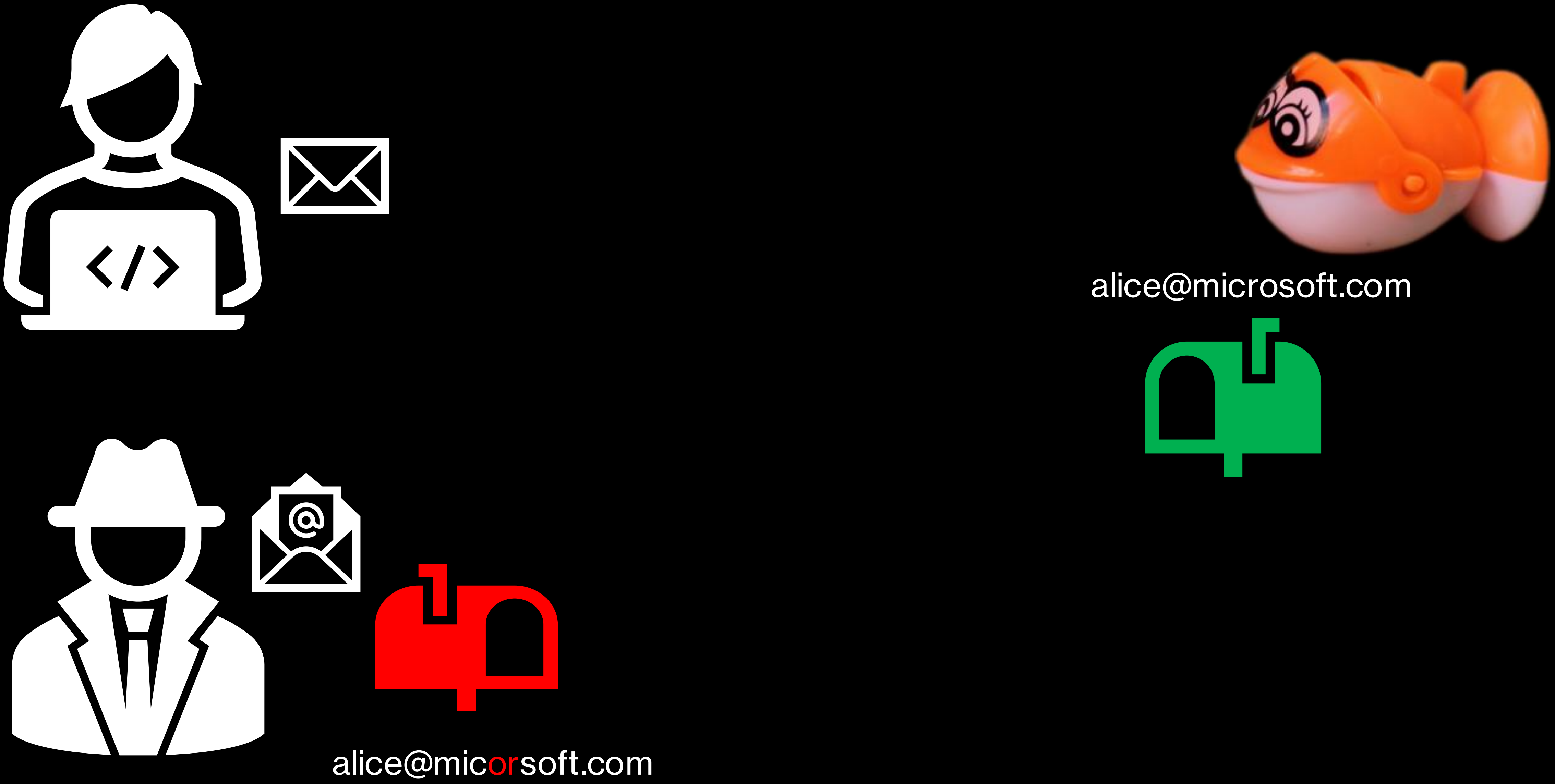
Technique

Typo
WIN $10K
WIN $10K
How To Enter
$24.99
$14.99
WIN
JOIN THE TEAM
$19.99
po

! 🎣

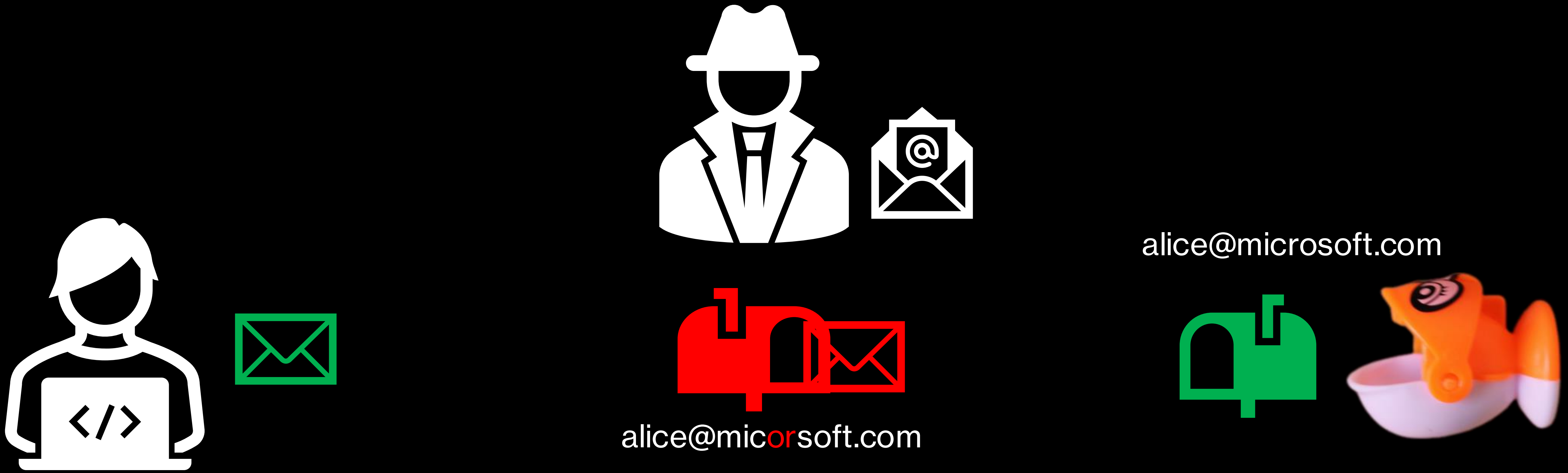


alice@microsoft.com



alice@microsoft.com

alice@micorsoft.com



alice@microsoft.com

alice@micorsoft.com

✋ A Manual Approach

✋ A Manual Approach

Why?

Why?

Information Leakage

Accounts Takeover

Time Sensitive Operations

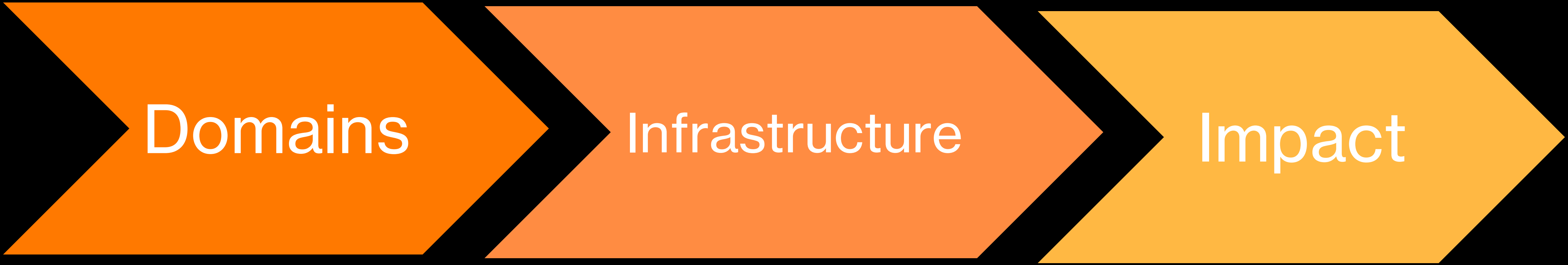
OTP Interception

Plausible email

© 1715 Fleet – Queens Jewels, LLC

The Process

The Process



Domains

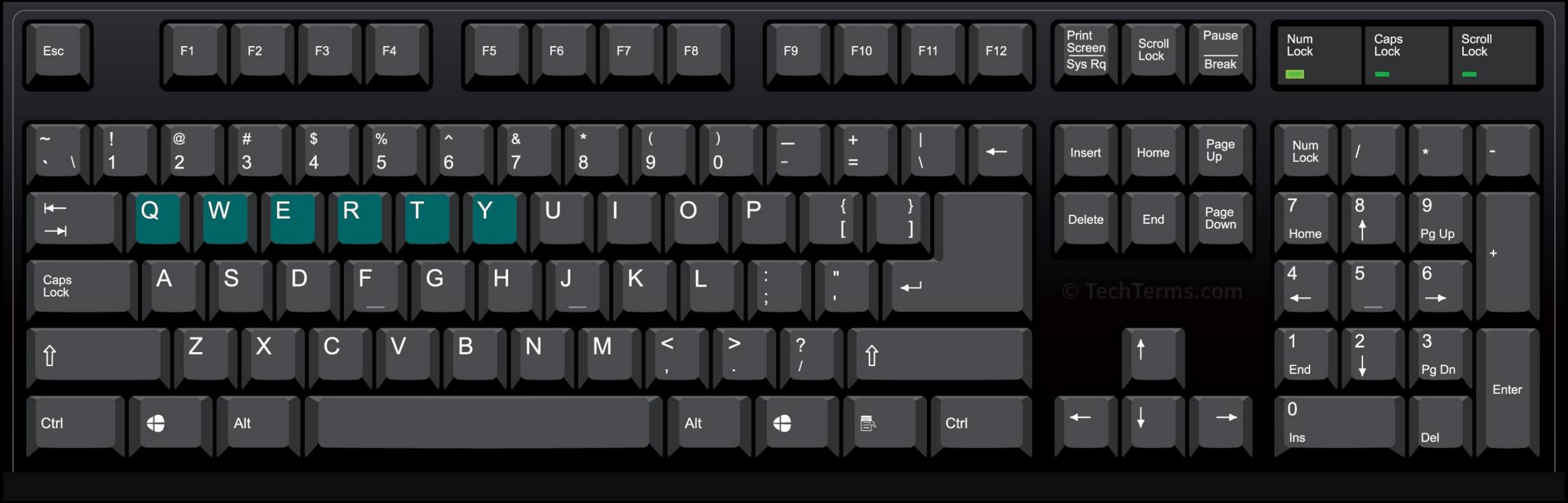
Infrastructure

Impact

Domains

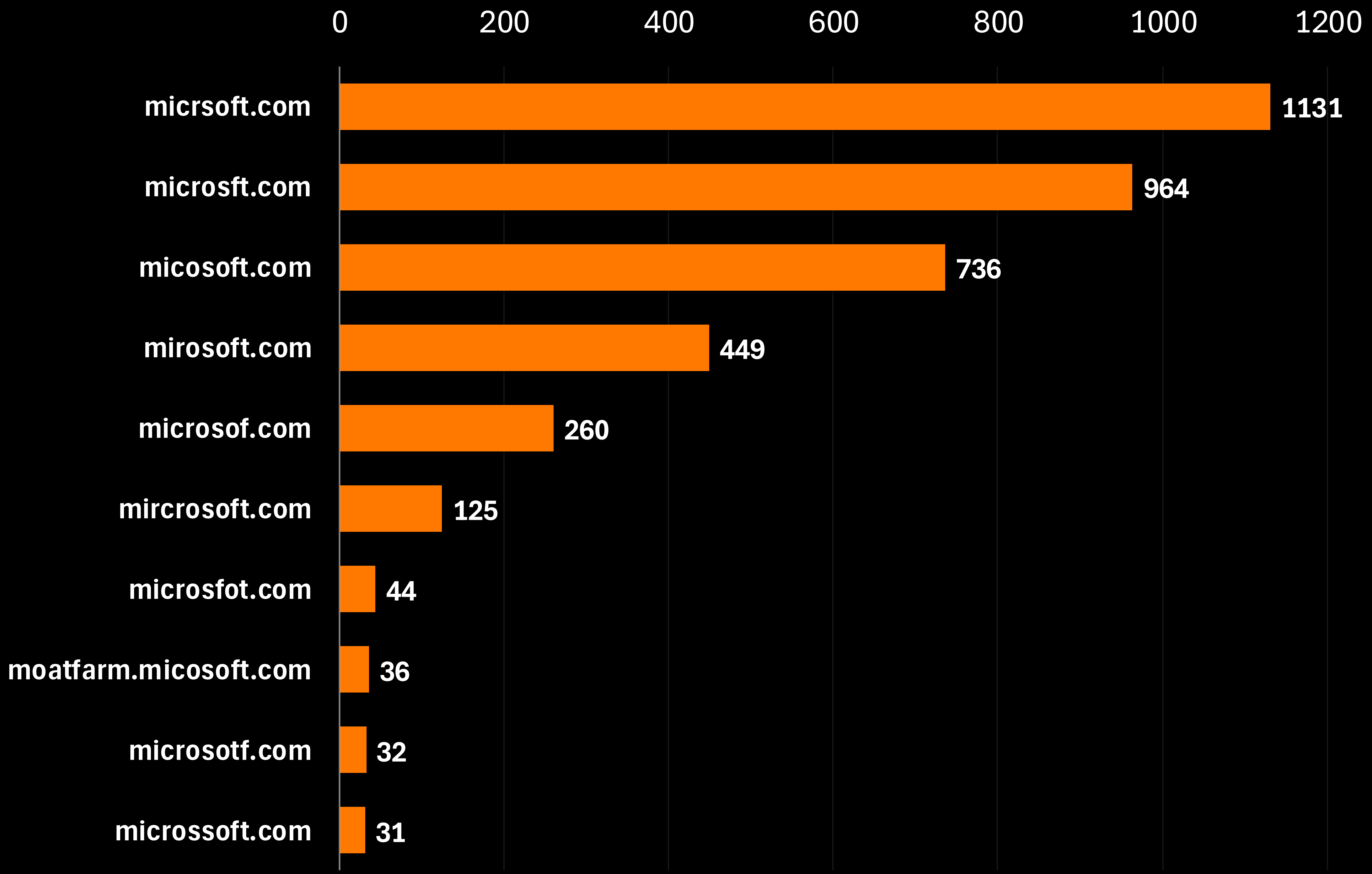
Domains

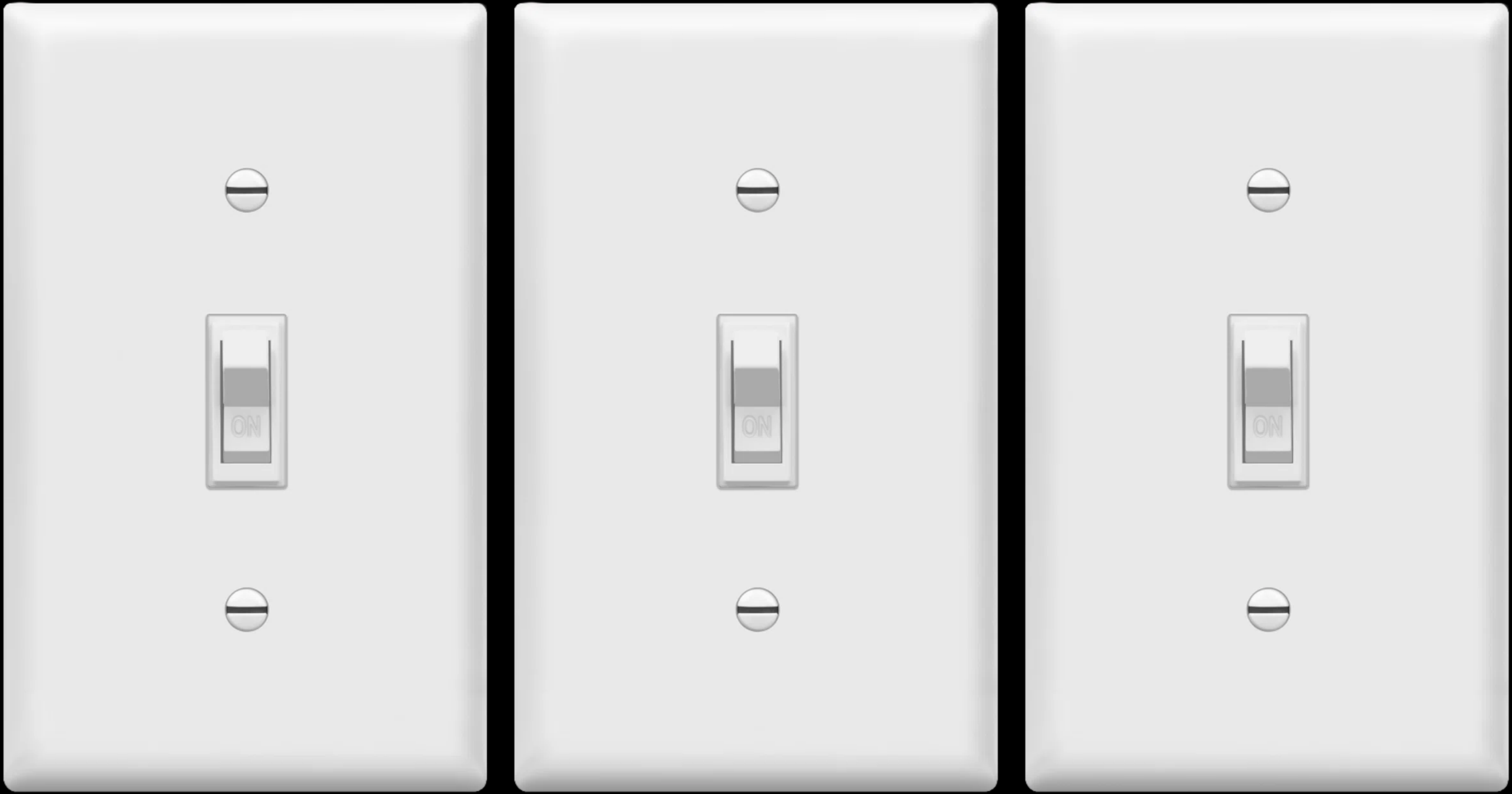
Theory Says


Esc
F1
F2
F3
F4
F5
F6
F7
F8
F9
F10
F11
F12
Print Screen Sys Rq
Scroll Lock
Pause Break
Num Lock
Caps Lock
Scroll Lock
~ ` \
! 1
@ 2
# 3
$ 4
% 5
^ 6
& 7
* 8
(9
) 0
— -
+ =
| \
←
Insert
Home
Page Up
Num Lock
/
*
-
Q
W
E
R
T
Y
U
I
O
P
{ [
}]
Delete
End
Page Down
7 Home
8 ↑
9 Pg Up
+
Caps Lock
A
S
D
F
G
H
J
K
L
: ;
" '
4 ←
5
6 →
⇧
Z
X
C
V
B
N
M
< ,
> .
? /
⇧
↑
1 End
2 ↓
3 Pg Dn
Enter
Ctrl
Alt
Alt
Ctrl
←
↓
→
0 Ins
Del

m	i	c	r	o	s	o	f	t	.	c	o	m
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
3	4	4	4	4	6	4	6	4	1	4	4	3

Practically We Do


0
200
400
600
800
1000
1200
micrsoft.com
1131
microsft.com
964
micosoft.com
736
mirosoft.com
449
microsof.com
260
mircrosoft.com
125
microsfot.com
44
moatfarm.micosoft.com
36
microsotf.com
32
microssoft.com
31



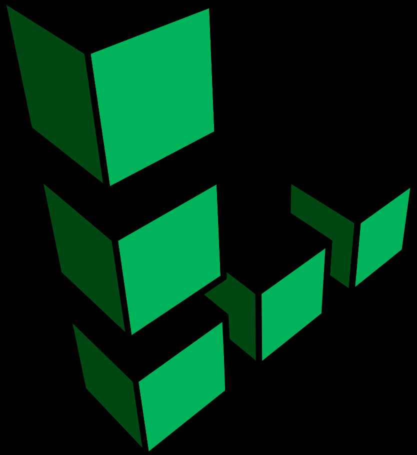
https://www.youtube.com/watch?v=R_roEB2sz9M

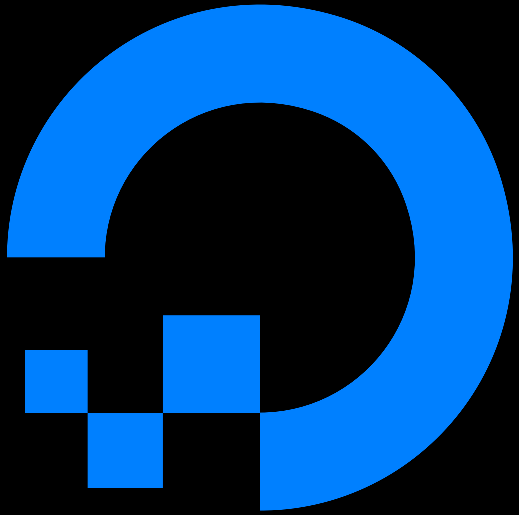
https://github.com/happycakefriends/certainly

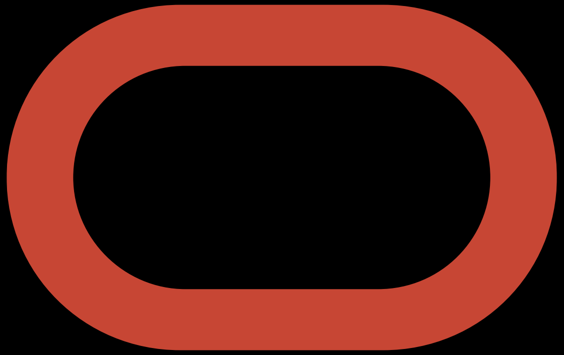
https://www.blackhat.com/us-24/briefings.html#flipping-bits-your-credentials-are-certainly-mine

Infrastructure

Infrastructure

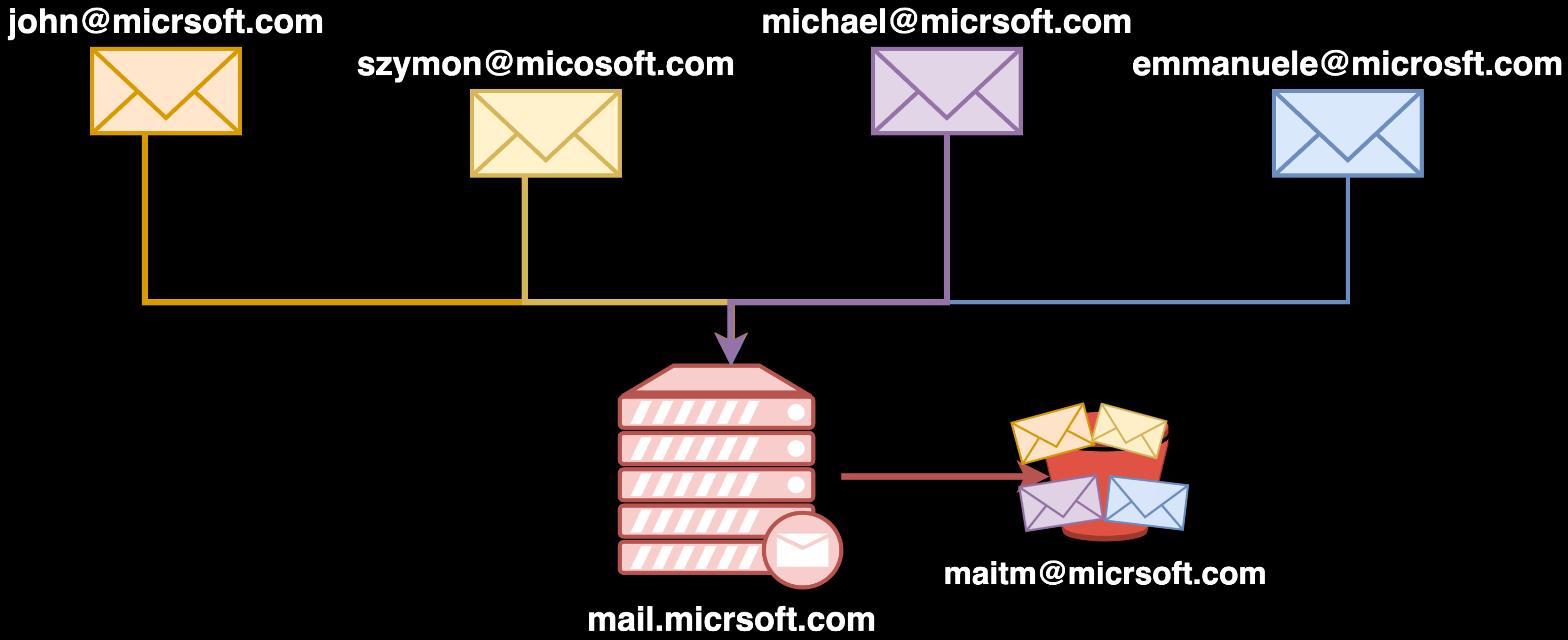






Root domain	MX Entry
micrsoft.com	mail.micrsoft.com
microsft.com	mail.micrsoft.com
micosoft.com	mail.micrsoft.com
...	mail.micrsoft.com

LEATHERMAN® Charge®
AAA
Roadside & Battery Service
1.800.222.4357
AAA.com
CE0123①
Saddleback Leather Co.



john@micrsoft.com

szymon@micosoft.com

michael@micrsoft.com

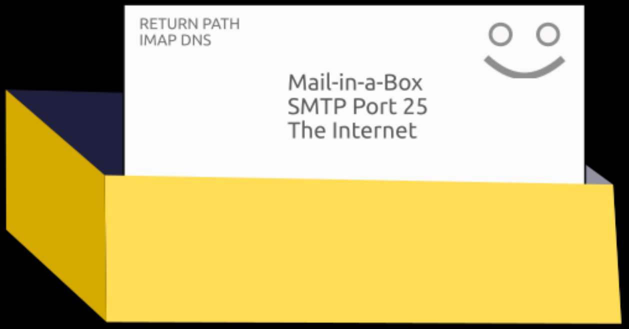
emmanuele@microsft.com

mail.micrsoft.com

maitm@micrsoft.com

MAIL

E


RETURN PATH
IMAP DNS
Mail-in-a-Box
SMTP Port 25
The Internet

Impact

Impact

Links

UNC Paths

Attachments

Headers

🤖 Automated Approach

🤖 Automated Approach

Why Automate?

HTTPS://XKCD.COM/303/

POP·SECRET
PREMIUM
IMPORTANT:
HANDLE CAREFULLY: VERY HOT OIL & BAG
PICK UP HERE
PRENDRE LE SACHET
SUPERIOR
Poop Later

Knife goes in,guts come out

Mail in the Middle

Date
Read status
Subject

Source Domain
Destination Domain

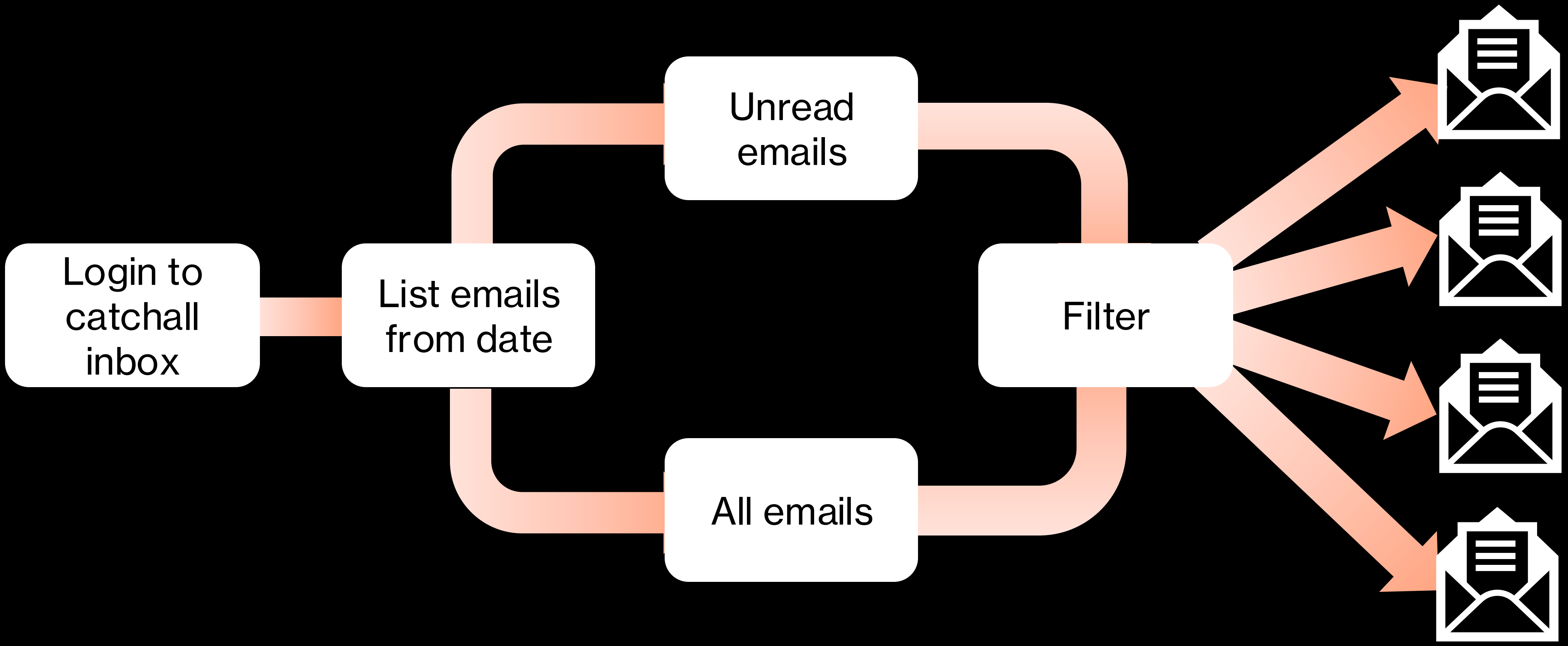
Links
UNC Paths

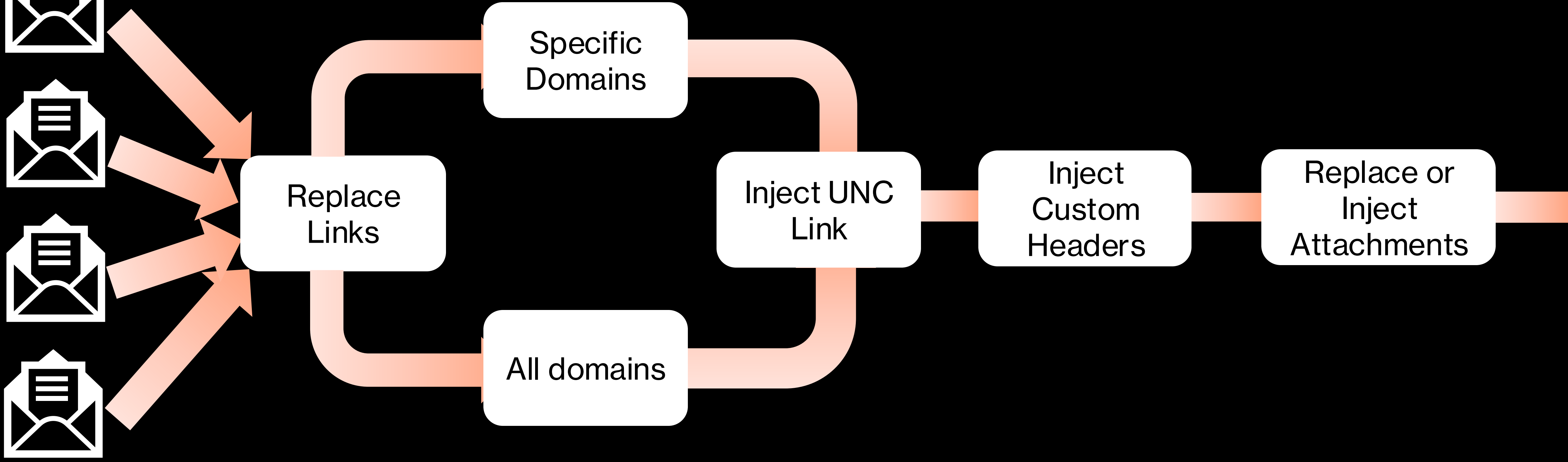
Attachments
Headers

Delivery
Notify Webhooks

How it works?

How it works?


Login to catchall inbox
List emails from date
Unread emails
All emails
Filter


Replace Links

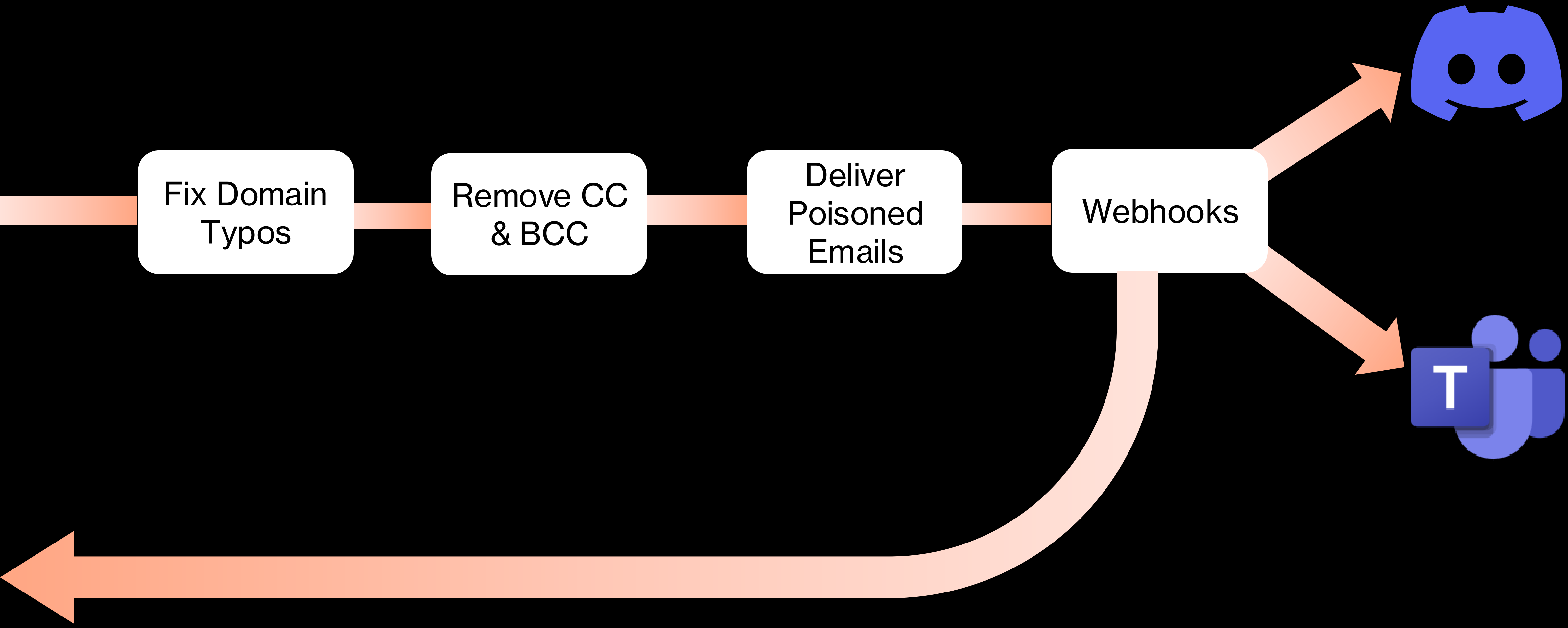
Specific Domains

All domains

Inject UNC Link

Inject Custom Headers

Replace or Inject Attachments



Fix Domain Typos

Remove CC & BCC

Deliver Poisoned Emails

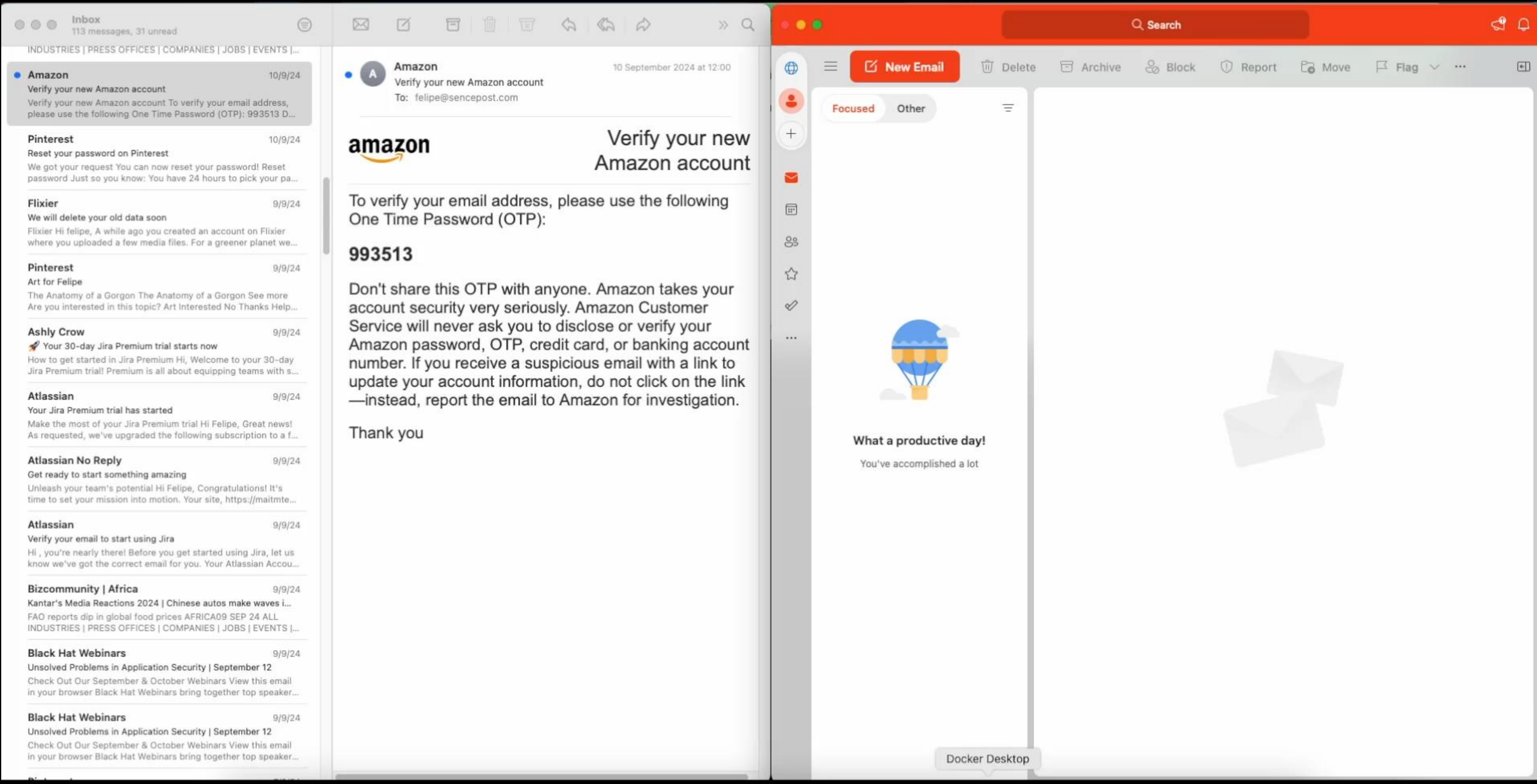
Webhooks

Demo

Demo

OTP Email

Link and Attachment injection



INDUSTRIES | PRESS OFFICES | COMPANIES | JOBS | EVENTS |...

Amazon 10/9/24
Verify your new Amazon account
Verify your new Amazon account To verify your email address, please use the following One Time Password (OTP): 993513 D...

Pinterest 10/9/24
Reset your password on Pinterest
We got your request You can now reset your password! Reset password Just so you know: You have 24 hours to pick your pa...

Flixier 9/9/24
We will delete your old data soon
Flixier Hi felipe, A while ago you created an account on Flixier where you uploaded a few media files. For a greener planet we...

Pinterest 9/9/24
Art for Felipe
The Anatomy of a Gorgon The Anatomy of a Gorgon See more Are you interested in this topic? Art Interested No Thanks Help...

Ashly Crow 9/9/24
🚀 Your 30-day Jira Premium trial starts now
How to get started in Jira Premium Hi, Welcome to your 30-day Jira Premium trial! Premium is all about equipping teams with s...

Atlassian 9/9/24
Your Jira Premium trial has started
Make the most of your Jira Premium trial Hi Felipe, Great news! As requested, we've upgraded the following subscription to a f...

Atlassian No Reply 9/9/24
Get ready to start something amazing
Unleash your team's potential Hi Felipe, Congratulations! It's time to set your mission into motion. Your site, https://maitmte...

Atlassian 9/9/24
Verify your email to start using Jira
Hi , you're nearly there! Before you get started using Jira, let us know we've got the correct email for you. Your Atlassian Accou...

Bizcommunity | Africa 9/9/24
Kantar's Media Reactions 2024 | Chinese autos make waves i...
FAO reports dip in global food prices AFRICA09 SEP 24 ALL INDUSTRIES | PRESS OFFICES | COMPANIES | JOBS | EVENTS |...

Black Hat Webinars 9/9/24
Unsolved Problems in Application Security | September 12
Check Out Our September & October Webinars View this email in your browser Black Hat Webinars bring together top speaker...

Black Hat Webinars 9/9/24
Unsolved Problems in Application Security | September 12
Check Out Our September & October Webinars View this email in your browser Black Hat Webinars bring together top speaker...

Amazon 10 September 2024 at 12:00
Verify your new Amazon account
To: felipe@sencepost.com

amazon

Verify your new Amazon account

To verify your email address, please use the following One Time Password (OTP):

993513

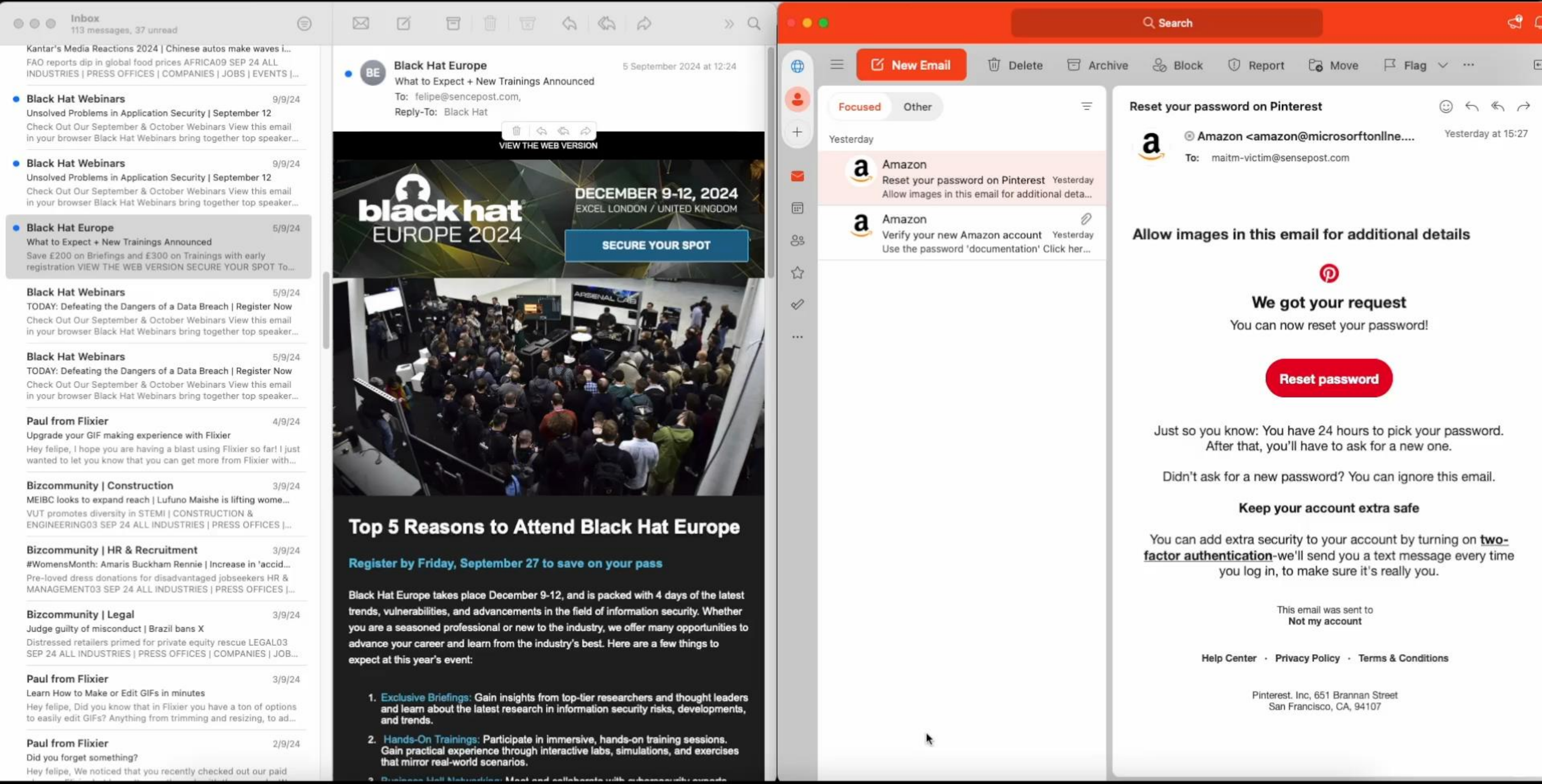
Don't share this OTP with anyone. Amazon takes your account security very seriously. Amazon Customer Service will never ask you to disclose or verify your Amazon password, OTP, credit card, or banking account number. If you receive a suspicious email with a link to update your account information, do not click on the link—instead, report the email to Amazon for investigation.

Thank you

What a productive day!
You've accomplished a lot

Newsletter

TUI usage
Link, tracking & UNC injection



Kantar's Media Reactions 2024 | Chinese autos make waves i...
FAO reports dip in global food prices AFRICA09 SEP 24 ALL INDUSTRIES | PRESS OFFICES | COMPANIES | JOBS | EVENTS |...

Black Hat Webinars — 9/9/24
Unsolved Problems in Application Security | September 12
Check Out Our September & October Webinars View this email in your browser Black Hat Webinars bring together top speaker...

Black Hat Webinars — 9/9/24
Unsolved Problems in Application Security | September 12
Check Out Our September & October Webinars View this email in your browser Black Hat Webinars bring together top speaker...

Black Hat Europe — 5/9/24
What to Expect + New Trainings Announced
Save £200 on Briefings and £300 on Trainings with early registration VIEW THE WEB VERSION SECURE YOUR SPOT To...

Black Hat Webinars — 5/9/24
TODAY: Defeating the Dangers of a Data Breach | Register Now
Check Out Our September & October Webinars View this email in your browser Black Hat Webinars bring together top speaker...

Black Hat Webinars — 5/9/24
TODAY: Defeating the Dangers of a Data Breach | Register Now
Check Out Our September & October Webinars View this email in your browser Black Hat Webinars bring together top speaker...

Paul from Flixier — 4/9/24
Upgrade your GIF making experience with Flixier
Hey felipe, I hope you are having a blast using Flixier so far! I just wanted to let you know that you can get more from Flixier with...

Bizcommunity | Construction — 3/9/24
MEIBC looks to expand reach | Lufuno Maishe is lifting wome...
VUT promotes diversity in STEMI | CONSTRUCTION & ENGINEERING03 SEP 24 ALL INDUSTRIES | PRESS OFFICES |...

Bizcommunity | HR & Recruitment — 3/9/24
#WomensMonth: Amaris Buckham Rennie | Increase in 'accid...
Pre-loved dress donations for disadvantaged jobseekers HR & MANAGEMENT03 SEP 24 ALL INDUSTRIES | PRESS OFFICES |...

Bizcommunity | Legal — 3/9/24
Judge guilty of misconduct | Brazil bans X
Distressed retailers primed for private equity rescue LEGAL03 SEP 24 ALL INDUSTRIES | PRESS OFFICES | COMPANIES | JOB...

Paul from Flixier — 3/9/24
Learn How to Make or Edit GIFs in minutes
Hey felipe, Did you know that in Flixier you have a ton of options to easily edit GIFs? Anything from trimming and resizing, to ad...

Paul from Flixier — 2/9/24
Did you forget something?
Hey felipe, We noticed that you recently checked out our paid

Black Hat Europe — 5 September 2024 at 12:24
What to Expect + New Trainings Announced
To: felipe@sencepost.com,
Reply-To: Black Hat

Top 5 Reasons to Attend Black Hat Europe

Register by Friday, September 27 to save on your pass

Black Hat Europe takes place December 9-12, and is packed with 4 days of the latest trends, vulnerabilities, and advancements in the field of information security. Whether you are a seasoned professional or new to the industry, we offer many opportunities to advance your career and learn from the industry's best. Here are a few things to expect at this year's event:

1. Exclusive Briefings: Gain insights from top-tier researchers and thought leaders and learn about the latest research in information security risks, developments, and trends.
2. Hands-On Trainings: Participate in immersive, hands-on training sessions. Gain practical experience through interactive labs, simulations, and exercises that mirror real-world scenarios.
3. Business Hall Networking: Meet and collaborate with cybersecurity experts

Yesterday

Amazon
Reset your password on Pinterest — Yesterday
Allow images in this email for additional deta...

Amazon
Verify your new Amazon account — Yesterday
Use the password 'documentation' Click her...

Reset your password on Pinterest

Amazon <amazon@microsorftonllne.... — Yesterday at 15:27
To: maitm-victim@sensepost.com

Allow images in this email for additional details

We got your request

You can now reset your password!

Reset password

Just so you know: You have 24 hours to pick your password. After that, you'll have to ask for a new one.

Didn't ask for a new password? You can ignore this email.

Keep your account extra safe

You can add extra security to your account by turning on **two-factor authentication**-we'll send you a text message every time you log in, to make sure it's really you.

This email was sent to
Not my account

Help Center · Privacy Policy · Terms & Conditions

Pinterest. Inc, 651 Brannan Street
San Francisco, CA, 94107

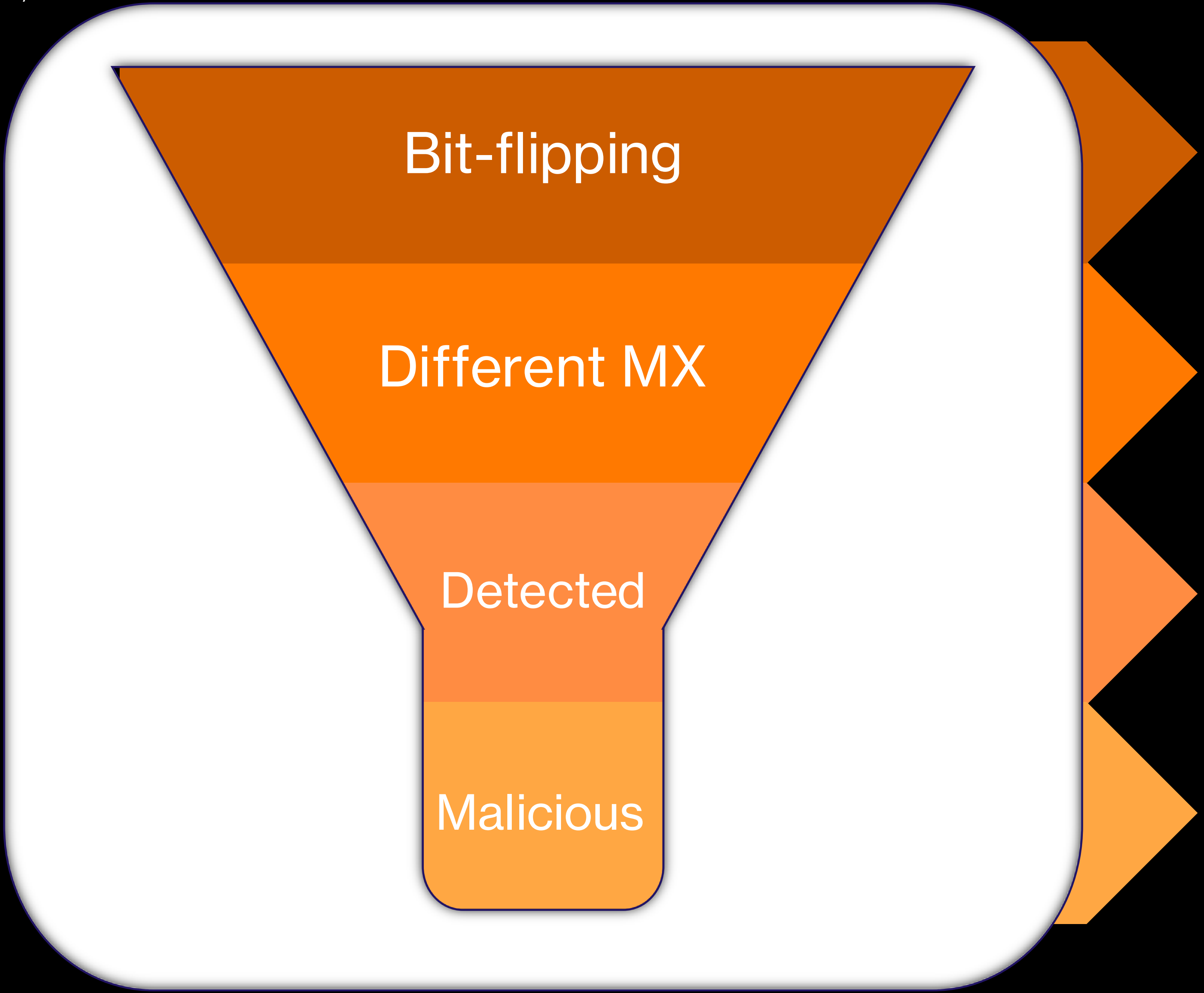
The Landscape

Bit-flipping 100K popular domains

Retrieve MX entries and find differences

Query
DNS Block Lists
and other sources*

Spot Malicious MX and bitflipped-domains



~4.3M flipped domains

~65K domains

117 MX servers

?

117 MX servers

117 Potential MX servers

[UNLIKELY]

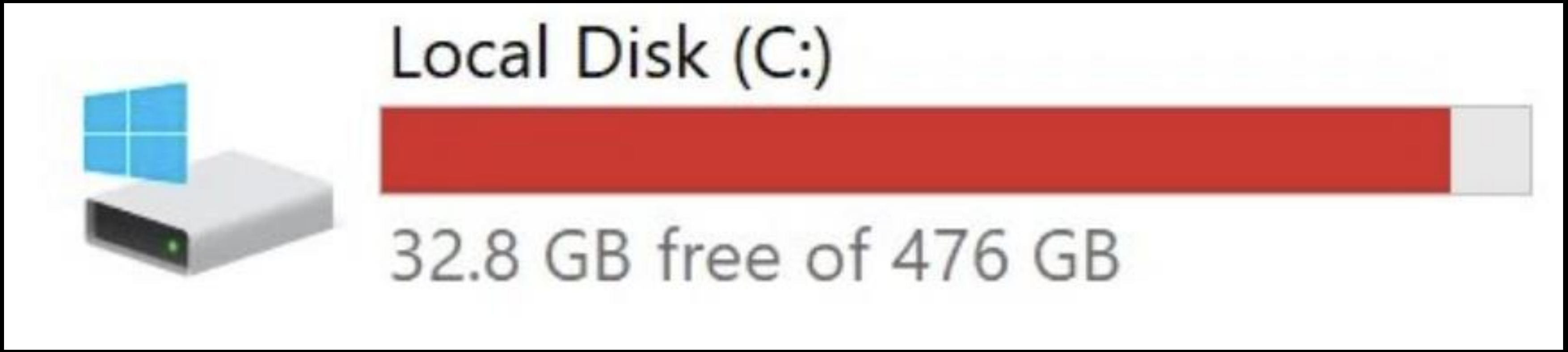
The Defenses

The Defenses

Electronic Cash Registers
Electronic Cash Register
Total
Cash

42
43
44
45
46
47
48
49
50
51
52
53
54

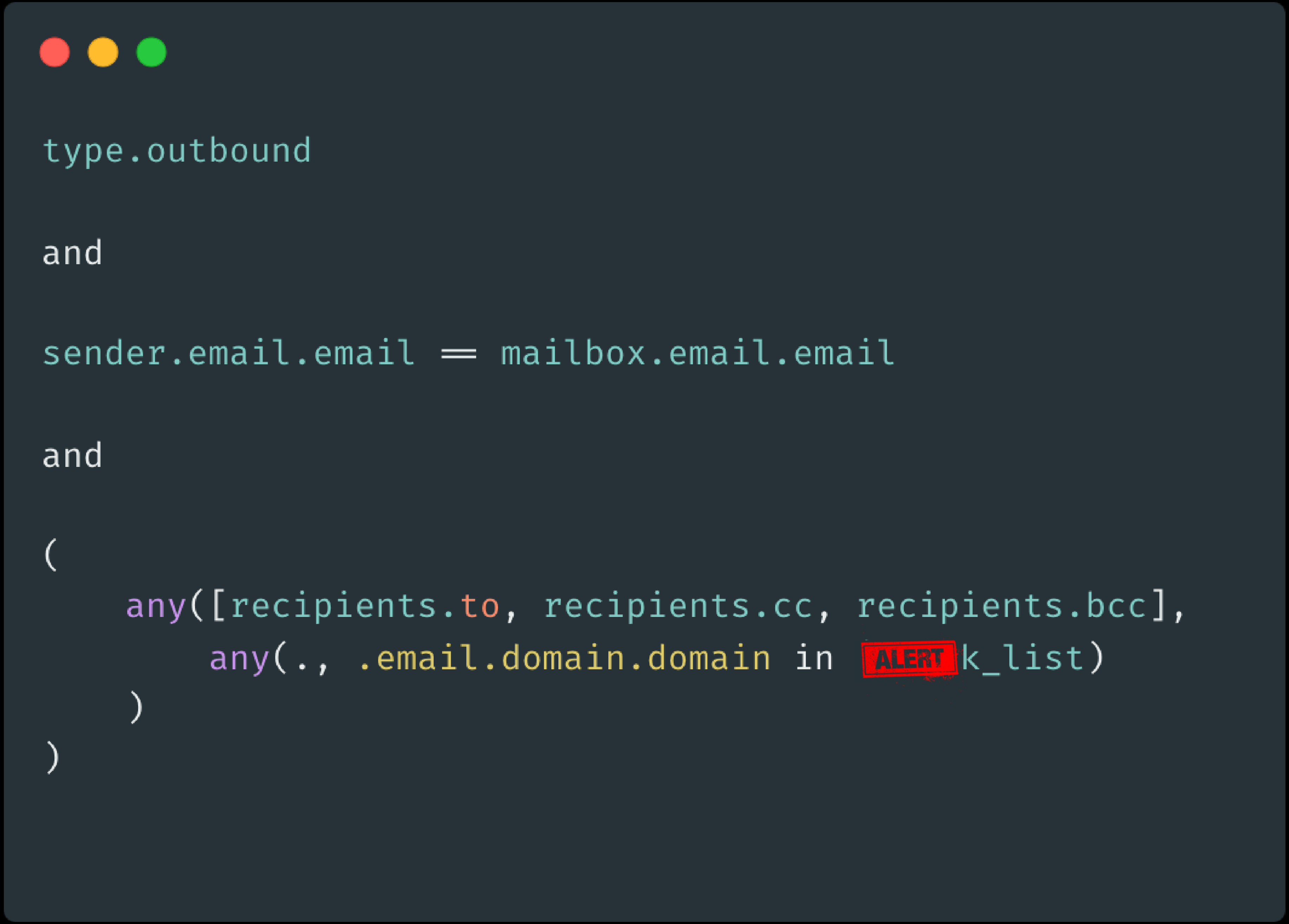
PHILIPS



Local Disk (C:)

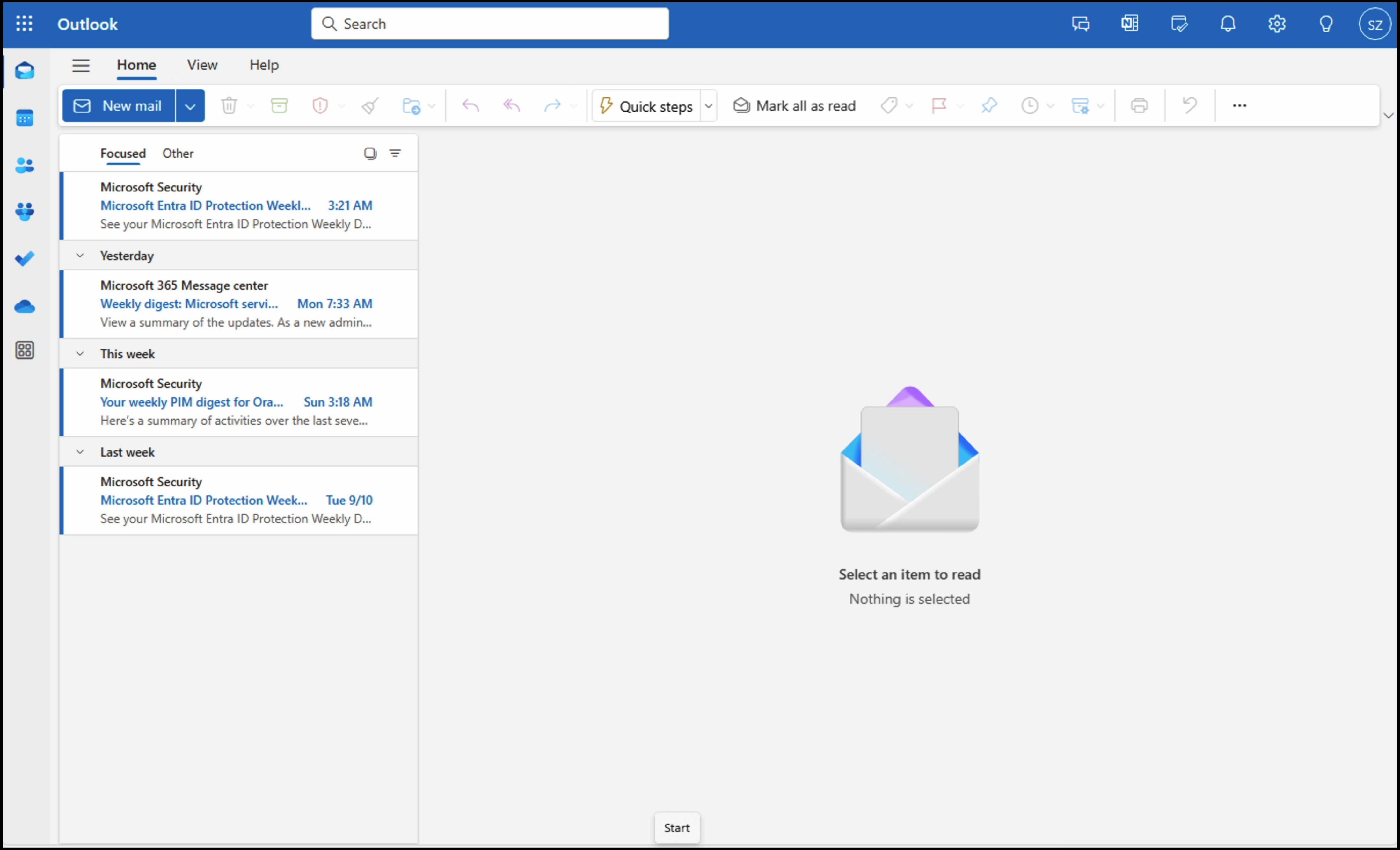
32.8 GB free of 476 GB

* not affiliated – but a cool tool



```
type.outbound

and

sender.email.email == mailbox.email.email

and

(
    any([recipients.to, recipients.cc, recipients.bcc],
        any(., .email.domain.domain in ALERTk_list)
    )
)
```

O



Microsoft Security
Microsoft Entra ID Protection Weekl... 3:21 AM
See your Microsoft Entra ID Protection Weekly D...

Yesterday

Microsoft 365 Message center
Weekly digest: Microsoft servi... Mon 7:33 AM
View a summary of the updates. As a new admin...

This week

Microsoft Security
Your weekly PIM digest for Ora... Sun 3:18 AM
Here's a summary of activities over the last seve...

Last week

Microsoft Security
Microsoft Entra ID Protection Week... Tue 9/10
See your Microsoft Entra ID Protection Weekly D...

Select an item to read
Nothing is selected

xerox
1
2
3
4
5

E

MAIL

SOFTWARE
CLOUD SERVICES
SOFTWREVEI

Success!

Success?

Recap

The Problem with Phishing

The effort

A Manual Approach

Nice but tedious

Automated Approach

Much better than manual!

Defenses

Say bye to typos in mails!

Takeaways

Leaks to typo-squatted domains pose a real threat

Anybody (including you) can take advantage of it

Automating the process relieves some of the pains

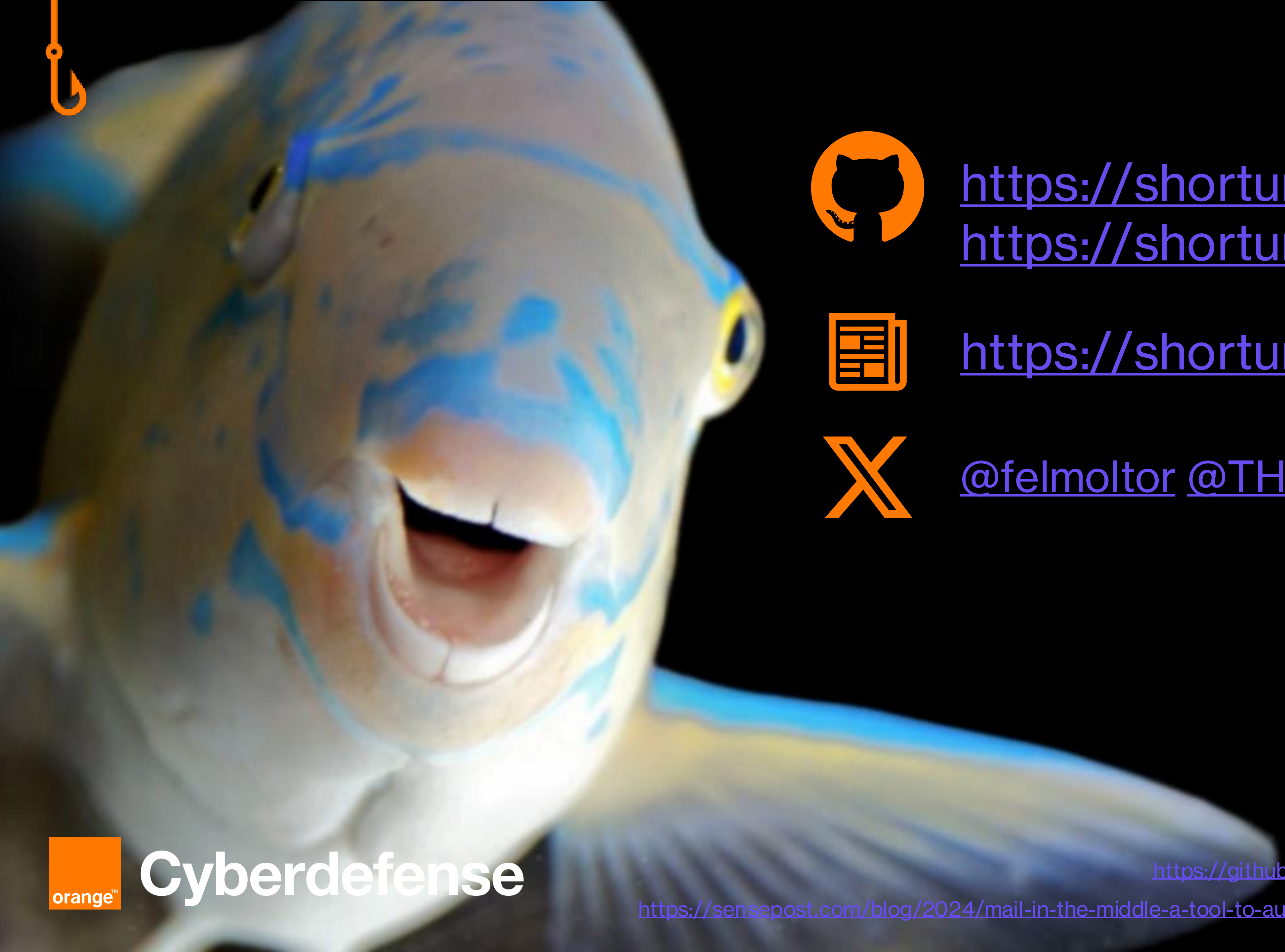
Takeaways

Implement detection and prevention mechanisms
(for typos and mistyped domains)

Define incident response policies

Questions?

Thank you!



https://shorturl.at/h7AIj
https://shorturl.at/hHkmF

https://shorturl.at/4XI0K

@felmoltor @TH3_GOAT_FARM3R

https://github.com/sensepost/mail-in-the-middle

https://sensepost.com/blog/2024/mail-in-the-middle-a-tool-to-automate-spear-phishing-campaigns/