Hacking the Human Firewall: Insights from Social Engineering Corporations

Ahmed Shah

Senior Security Analyst,

Malleum

Contents

1. Cases in the News
2. OSINT
3. NIST Phish Scale
4. Email Phishing
5. Phone Social Engineering
6. Physical Security

- Overall security is as strong as the weakest link

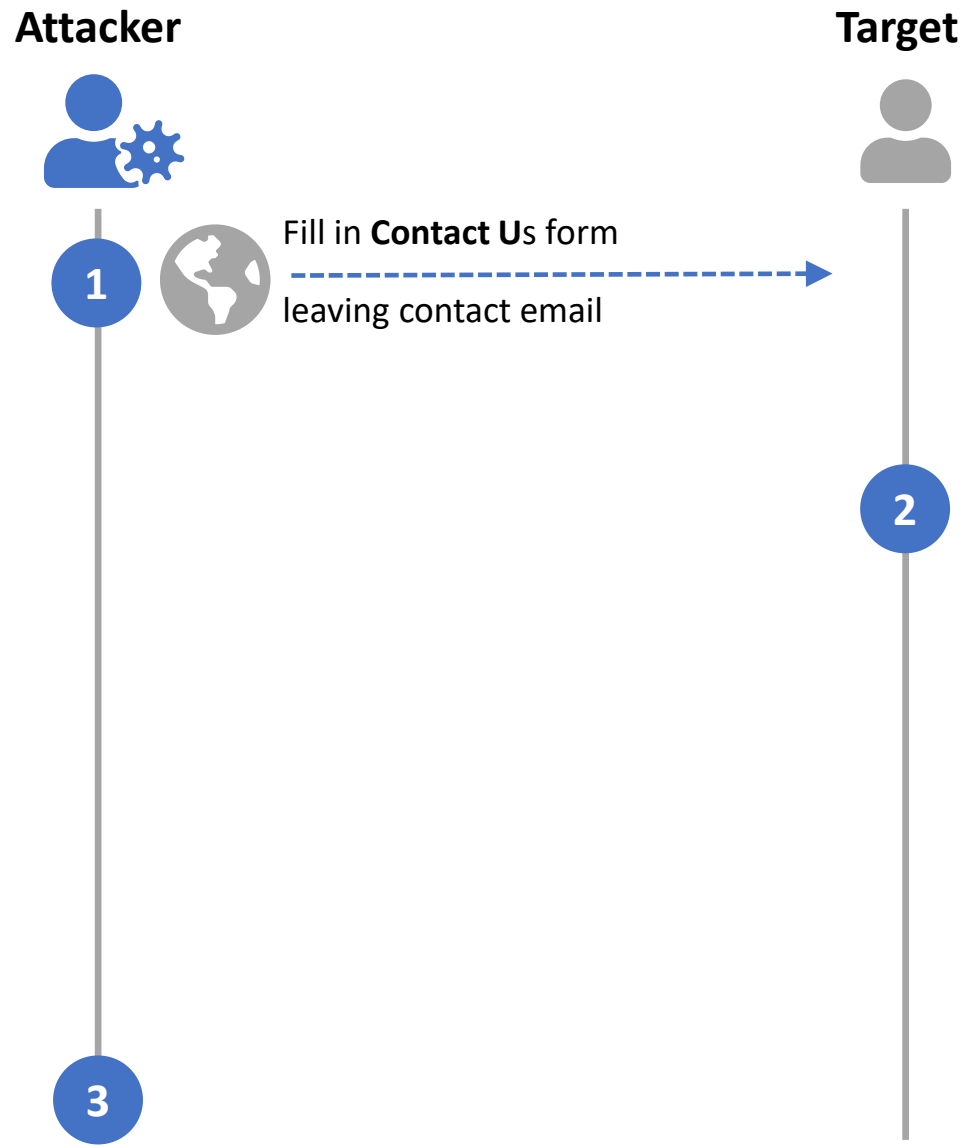
- Companies spend tons of $ on the latest and greatest, but not enough in training and processes

Cases in the News

ZipLine– 2025

- Targets “Contact Us” forms

> Hi, I am Thomas from Lamy Consulting, a sourcing company
>
> ….we're evaluating partners…

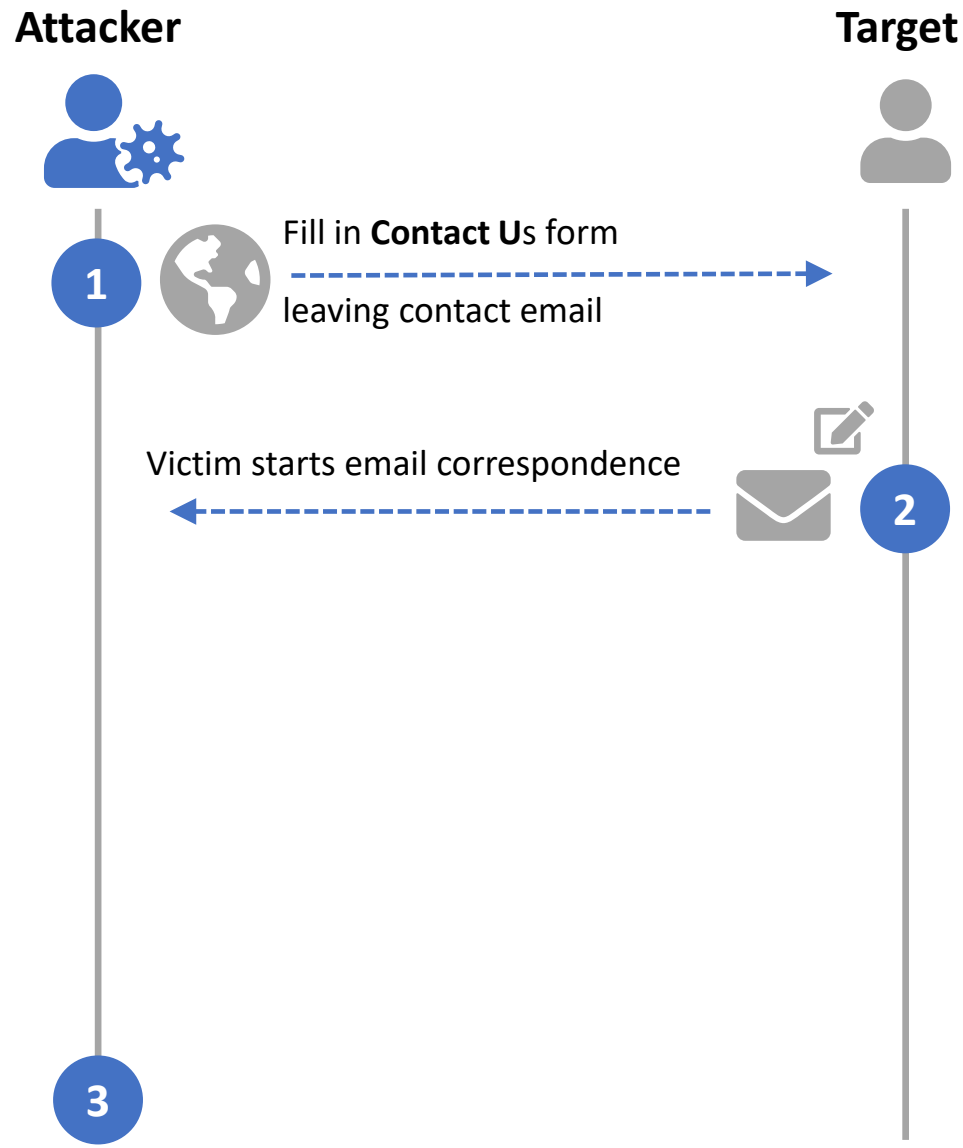


Cases in the News

ZipLine– 2025

- Targets “Contact Us” forms

> Hi, I am Thomas from Lamy Consulting, a sourcing company
>
> ….we're evaluating partners…

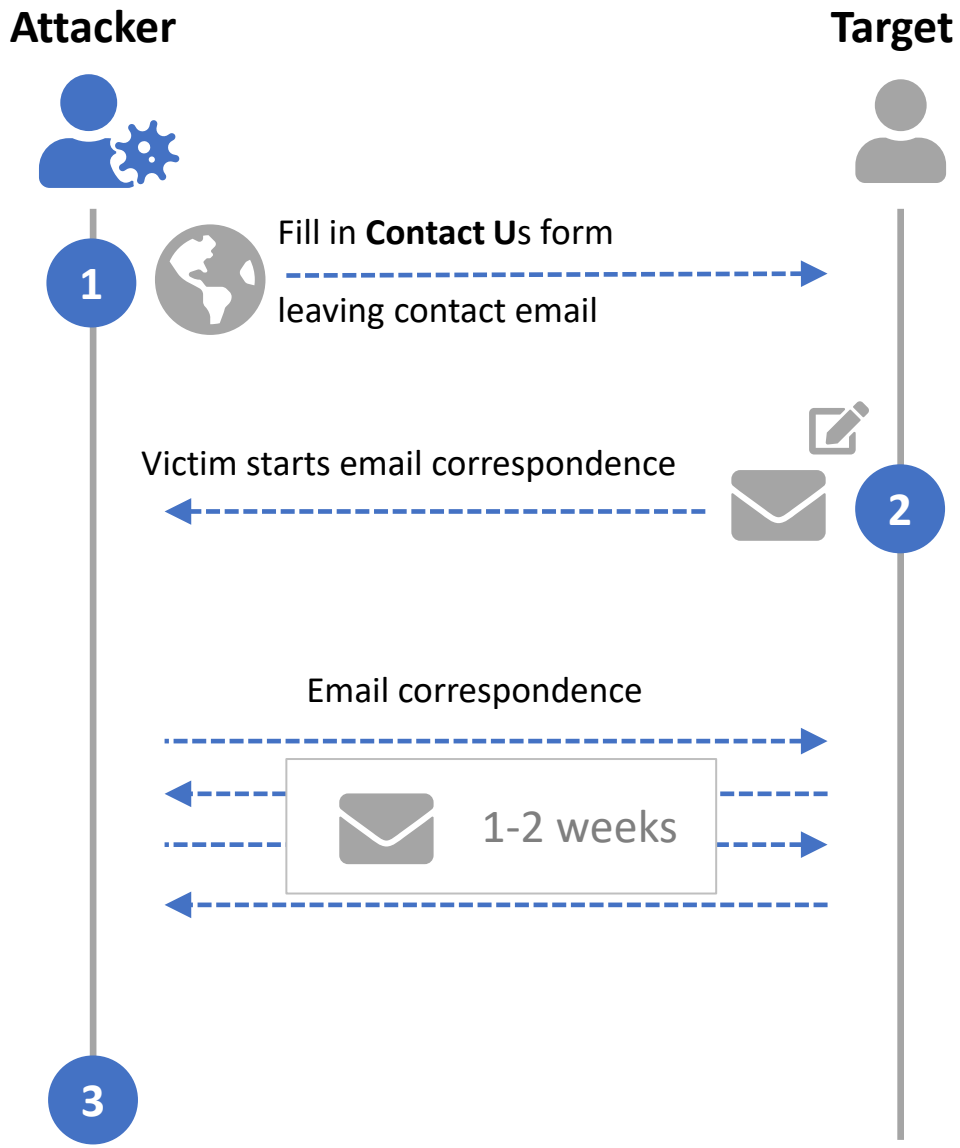


Cases in the News

ZipLine– 2025

- Targets “Contact Us” forms

> Hi, I am Thomas from Lamy Consulting, a sourcing company
>
> ….we're evaluating partners…

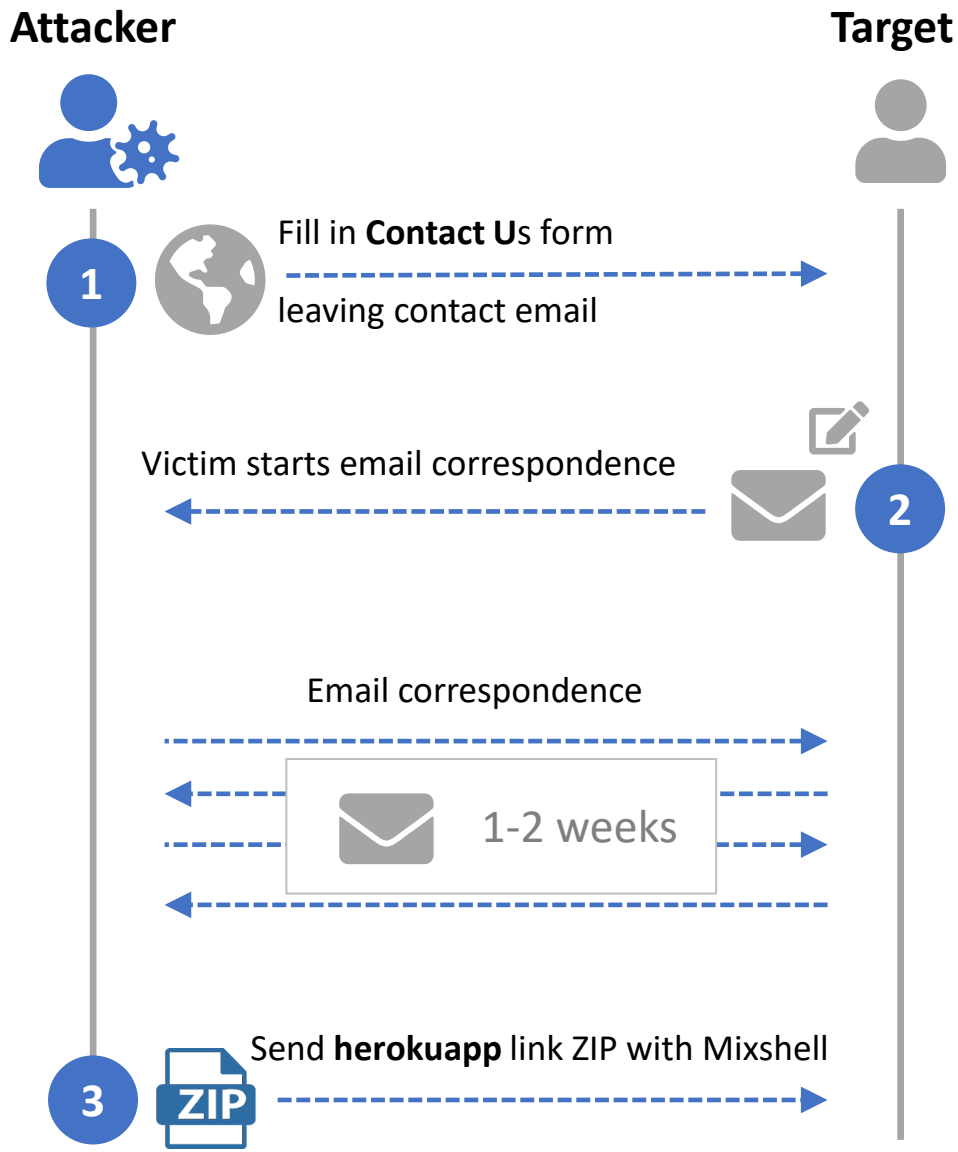


Cases in the News

ZipLine– 2025

- Targets “Contact Us” forms

> Hi, I am Thomas from Lamy Consulting, a sourcing company
>
> ….we're evaluating partners…



Cases in the News

MGM Resorts Attack - 2023

- Attackers found employee information on LinkedIn
- Pretended to be staff when calling help desk
- 10-minute conversation
- Timed the attack on the weekend

Image Credit: news3lv.com

Cases in the News

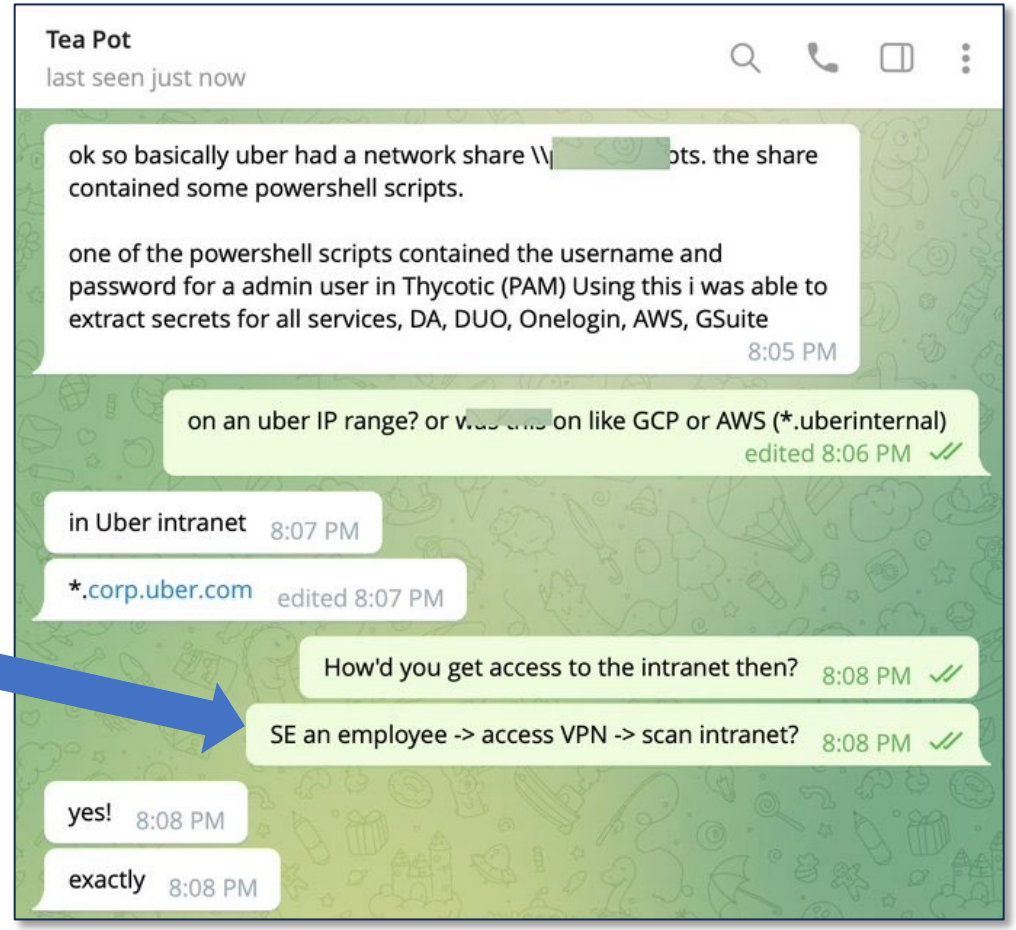
Uber MFA Fatigue – 2022

- Attacker purchased stolen credentials on dark web
- However, access required MFA
- Attacker (pretended to be from Uber security team) contacted target to accept MFA request
- Attacker sent a flood of MFA requests to pressure them.

Cases in the News

Uber MFA Fatigue – 2022

- Attacker purchased stolen credentials on dark web
- However, access required MFA
- Attacker (pretended to be from Uber security team) contacted target to accept MFA request
- Attacker sent a flood of MFA requests to pressure them.



Conversation between the Uber hacker and cybersecurity researcher Corben Leo
https://x.com/hacker_/status/1570582547415068672

OSINT

"INFORMATION IN THE OPEN IS A PUZZLE—OSINT IS THE ART OF FITTING THE PIECES TOGETHER BEFORE ANYONE ELSE REALIZES THEY'RE MISSING."

OSINT

Definition: Open-Source Intelligence

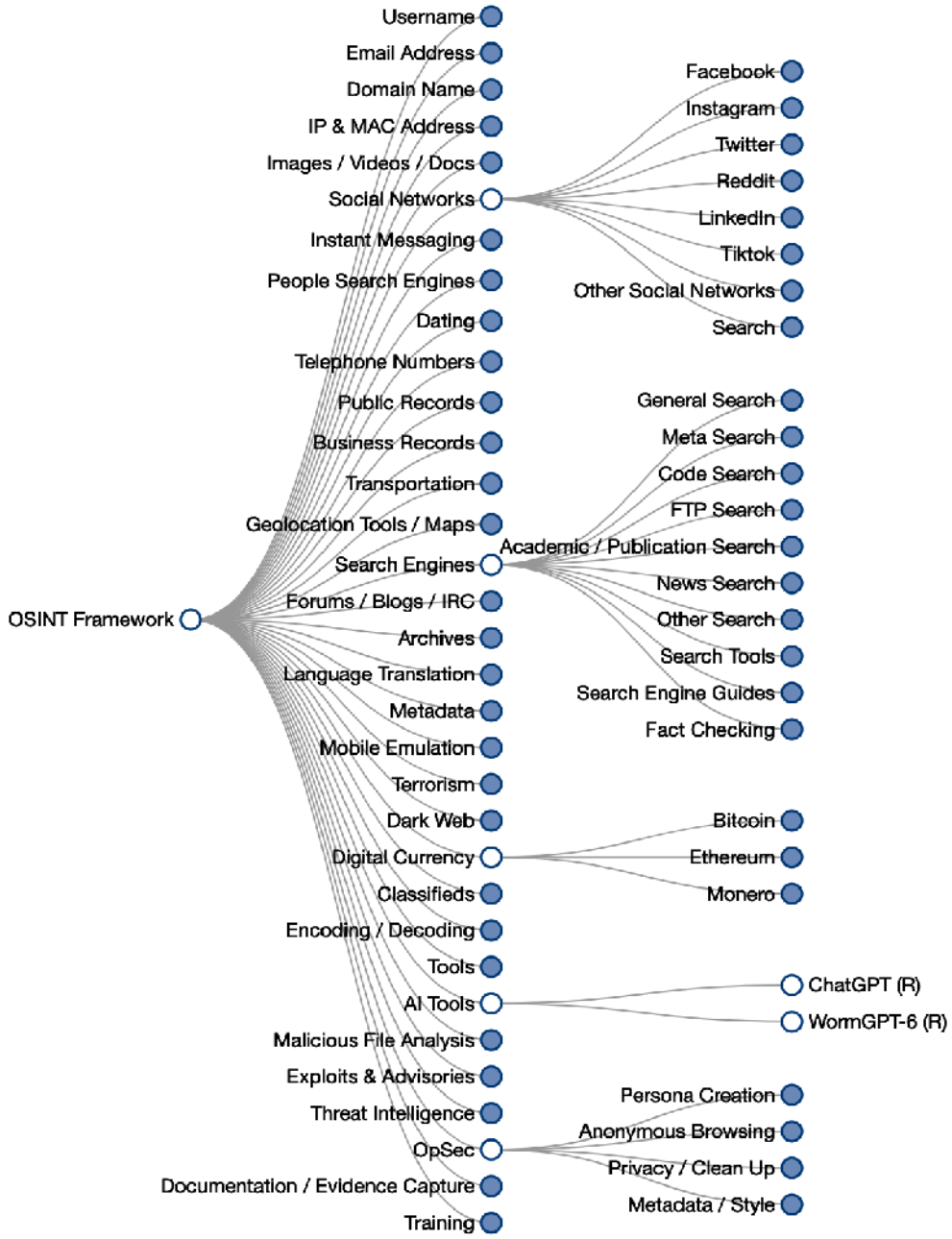
Goal: Obtain insights and information about the target organization and/or its personnel

Finding:

- Phone numbers
- Passwords
- Email addresses
- Building layouts
- Work relationships, etc....
- IT assets

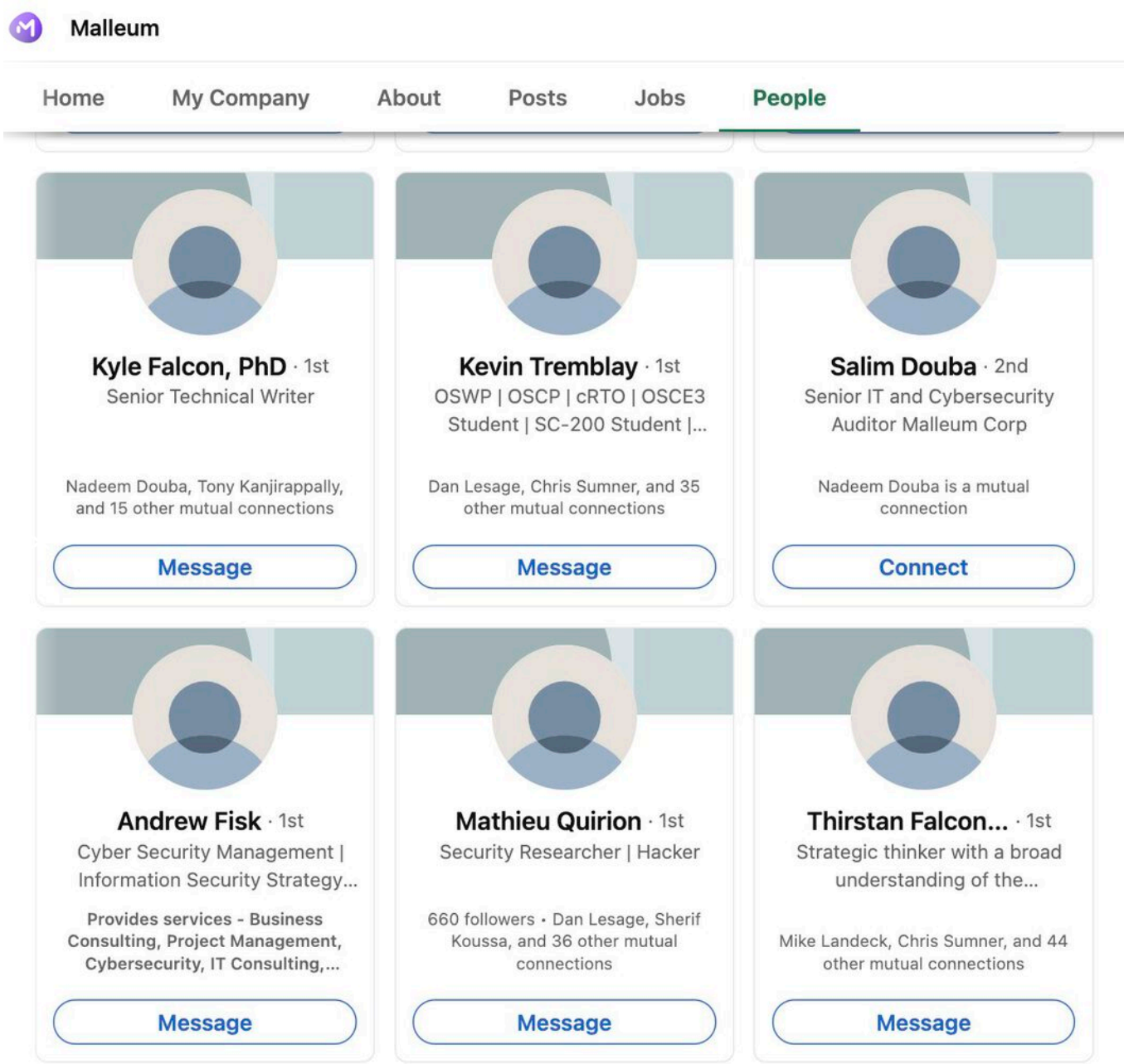
OSINT

- Websites:
  - Namechk
  - IntelTechniques
  - OSINTFramework
  - Spokeo
- Tools:
  - Maltego
  - Google Dorking
  - Recon-NG
  - Spiderfoot
  - AMASS



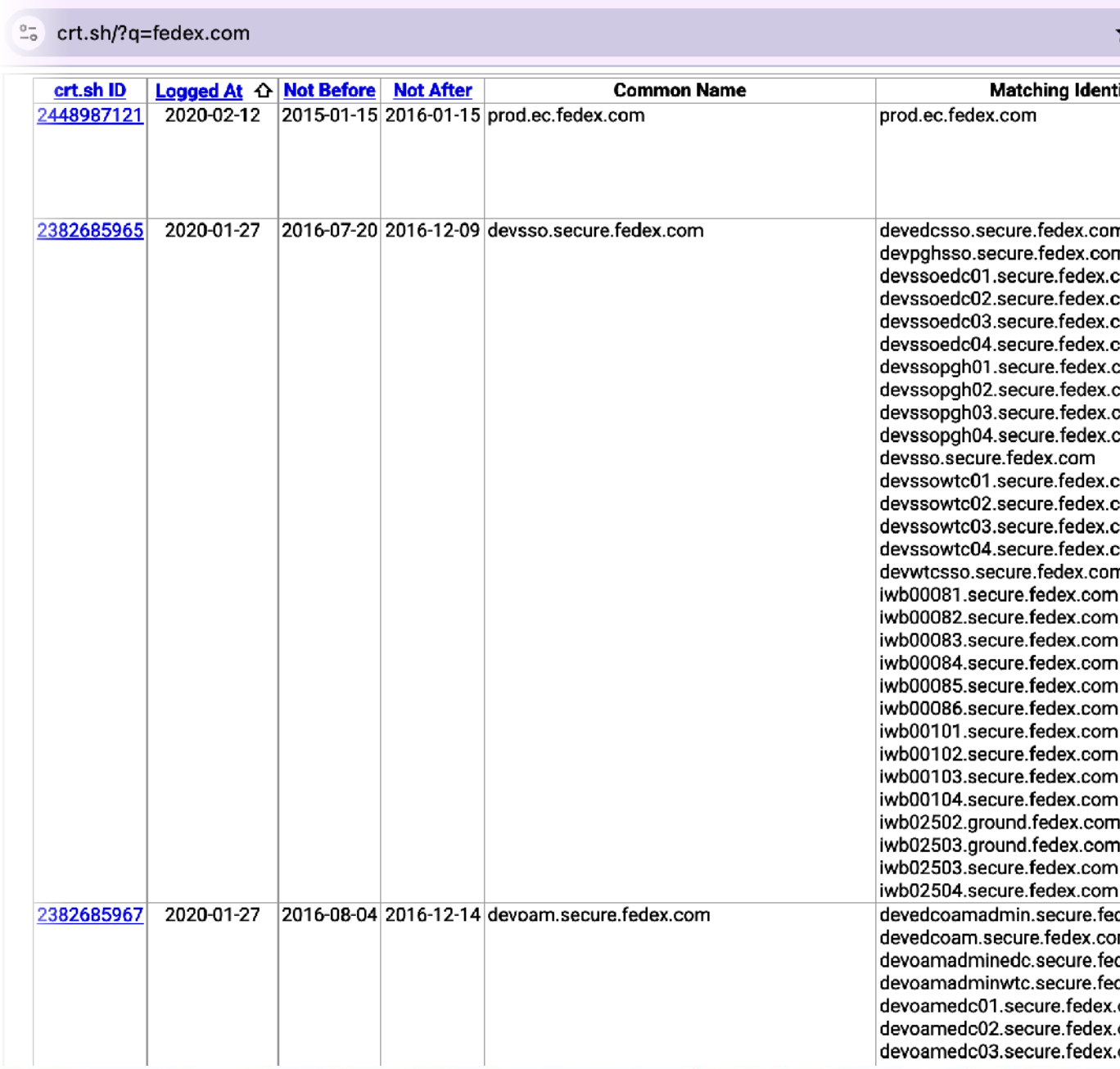
OSINT

- Social Medias & Personal Information:
  - LinkedIn-Scrapper (pypi project)
    - Searching for Employees
    - Scrappers need to change frequently
  - Twitter Scrapper
    - What's the target's hobbies
    - Anything we can help build a pretext



OSINT

- Domain and IP Enumeration:
  - AMASS
  - Sublist3r
  - Crt.sh
  - Finding IP Blocks
  - Shodan
  - fofa.io
  - RiskIQ-Microsoft TI Defender



Phishing Examples

"A WELL-CRAFTED RUBRIC IS MORE THAN A SCORING TOOL; IT'S A MIRROR THAT REFLECTS BOTH THE LEARNER'S PROGRESS AND THE CLARITY OF OUR EXPECTATIONS."

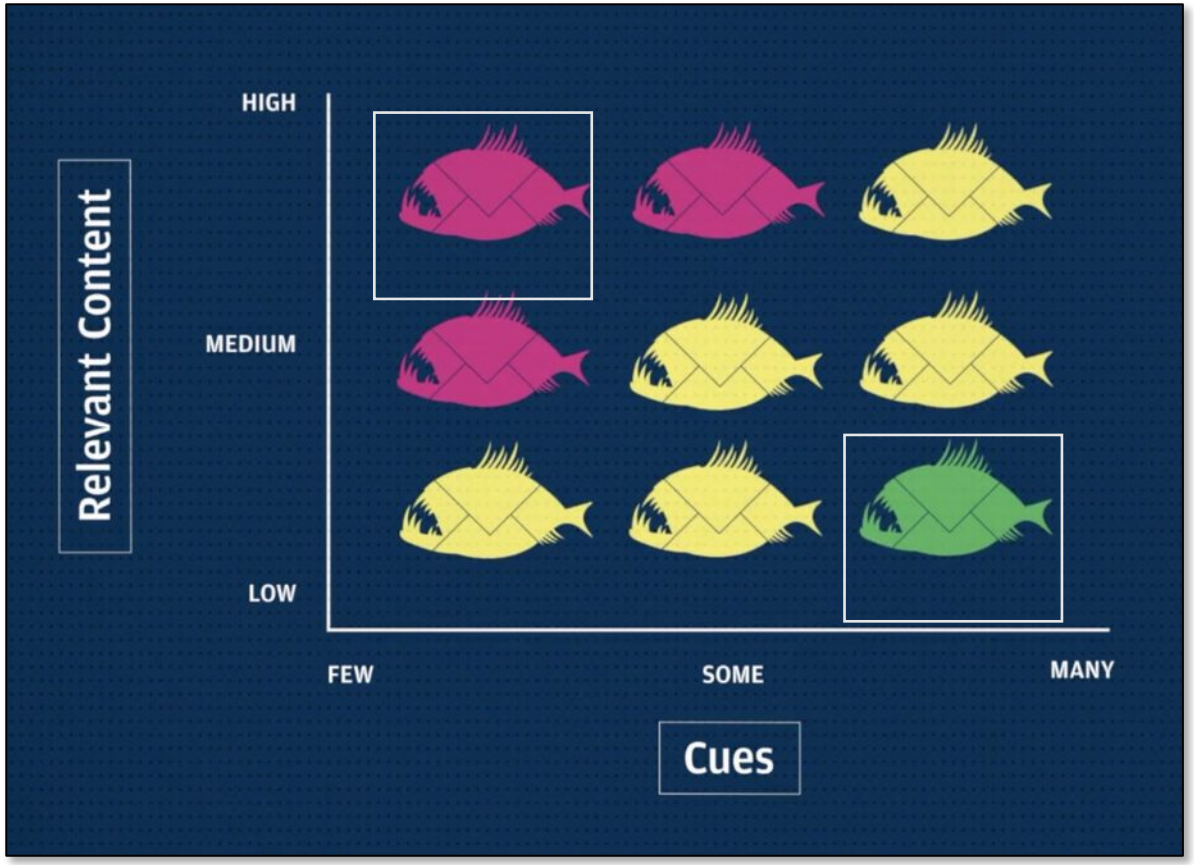
NIST Phish Scale

A scale that can be used to craft phishing campaigns that are designed to test varying degrees of awareness within organizations, from very easy to very difficult.

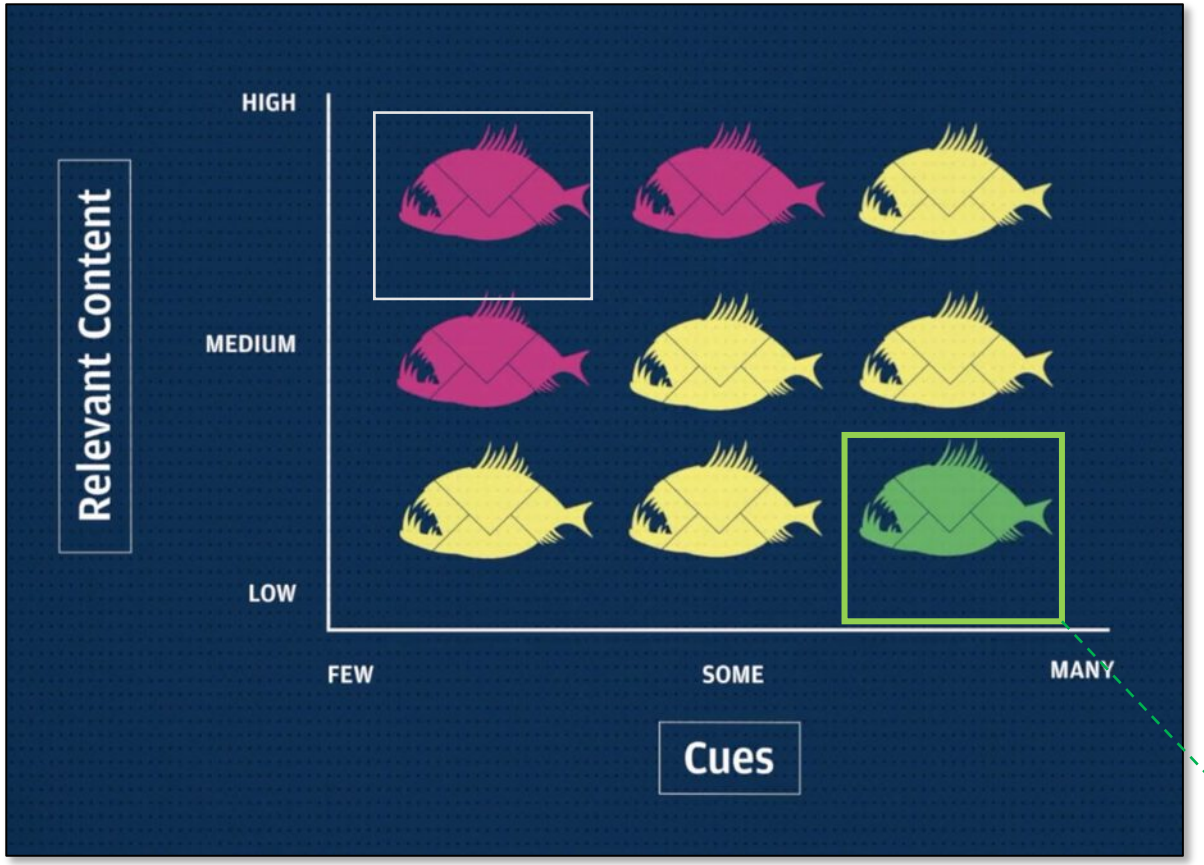
Uses two components:

1. **Cues:**
   - The observable characteristics of the phishing email.
   - How many suspicious cues are there?
2. **Premise Alignment:**
   - Alignment of the email's context to the user's work experience.
   - Is this an email they would realistically expect at work?

NIST Phish Scale



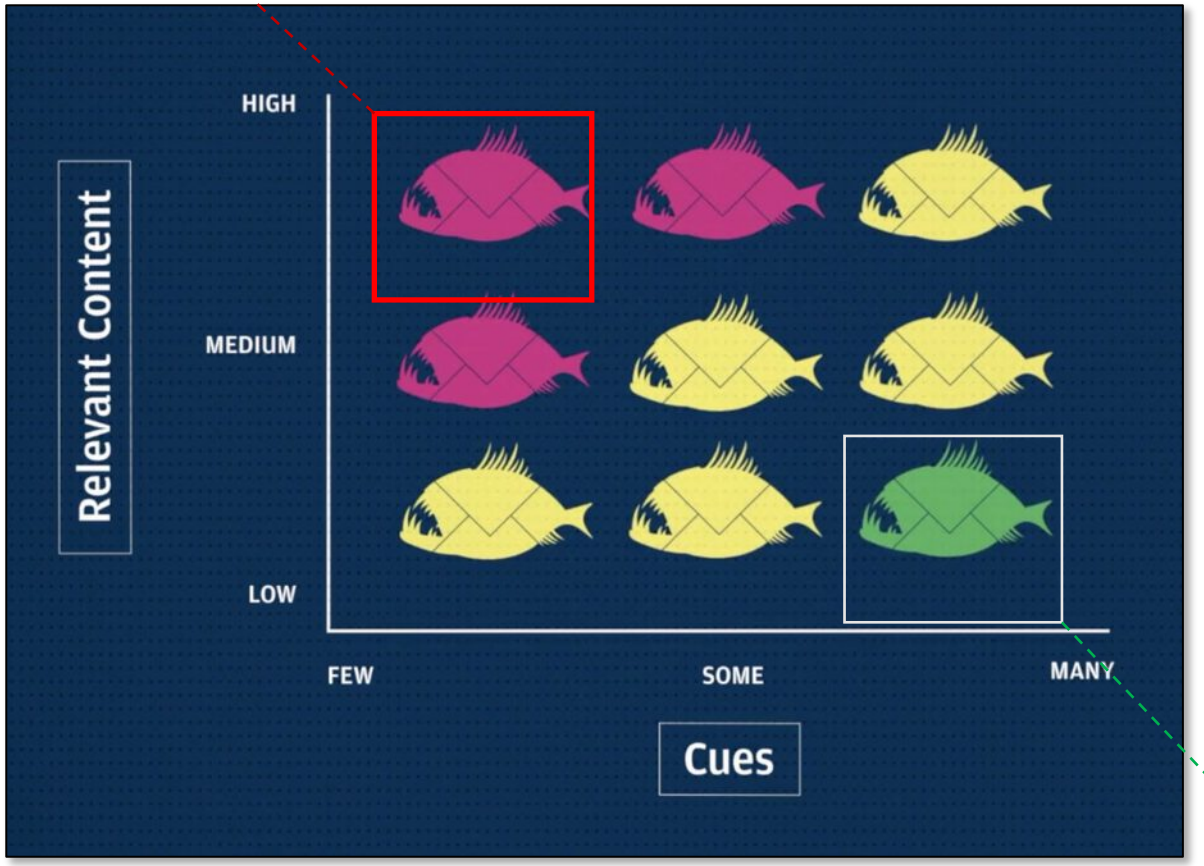
NIST Phish Scale



LOW relevance + HIGH cues = **VERY EASY** to identify

NIST Phish Scale

HIGH relevance + FEW cues = **VERY DIFFICULT** to identify



LOW relevance + HIGH cues = **VERY EASY** to identify

Changing Banking Details

From: Yellen Moore, Psy.D., <y3933@gmail.com>
Sent: Tuesday, August 5, 2025 10:20 AM
To: [redacted]>
Subject:

Good morning,

Prior to the next pay date, I want my banking details to be changed to a new one. What specific details are you going to need?

Best Regards,

Ye[redacted], Psy.D.
Licensed Clinical Psychologist
[redacted]

Sent from Outlook for iOS

Changing Banking Details

Gmail used for work

From: Yellen Moore, Psy.D., <y3933@gmail.com>
Sent: Tuesday, August 5, 2025 10:20 AM
To: [redacted]>
Subject:

Good morning,

Prior to the next pay date, I want my banking details to be changed to a new one. What specific details are you going to need?

Best Regards,

Ye[redacted], Psy.D.
Licensed Clinical Psychologist
[redacted]

Sent from Outlook for iOS

Changing Banking Details

Gmail used for work

From: Yellen Moore, Psy.D., <y3933@gmail.com>
Sent: Tuesday, August 5, 2025 10:20 AM
To: [redacted]>
Subject:

Good morning,

Prior to the next pay date, I want my banking details to be changed to a new one. What specific details are you going to need?

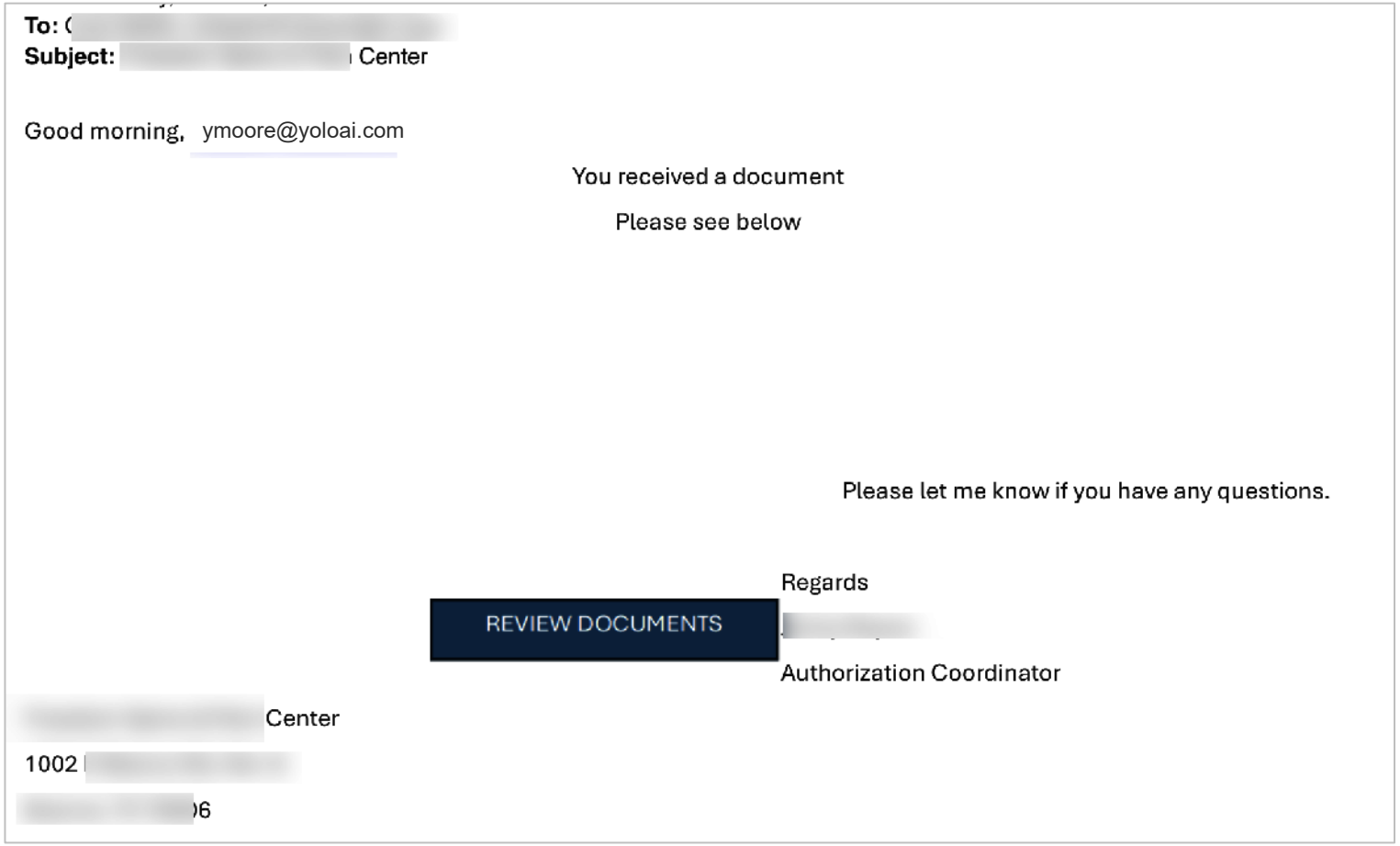
Best Regards,

Ye[redacted], Psy.D.
Licensed Clinical Psychologist
[redacted]

Sent from Outlook for iOS

What can you do?
Use alternative channels of communication
(e.g. verify the request by phone)

Credential Harvesting



To: [redacted]
Subject: [redacted] Center

Good morning, ymoore@yoloai.com

You received a document

Please see below

Please let me know if you have any questions.

Regards

REVIEW DOCUMENTS

[redacted]

Authorization Coordinator

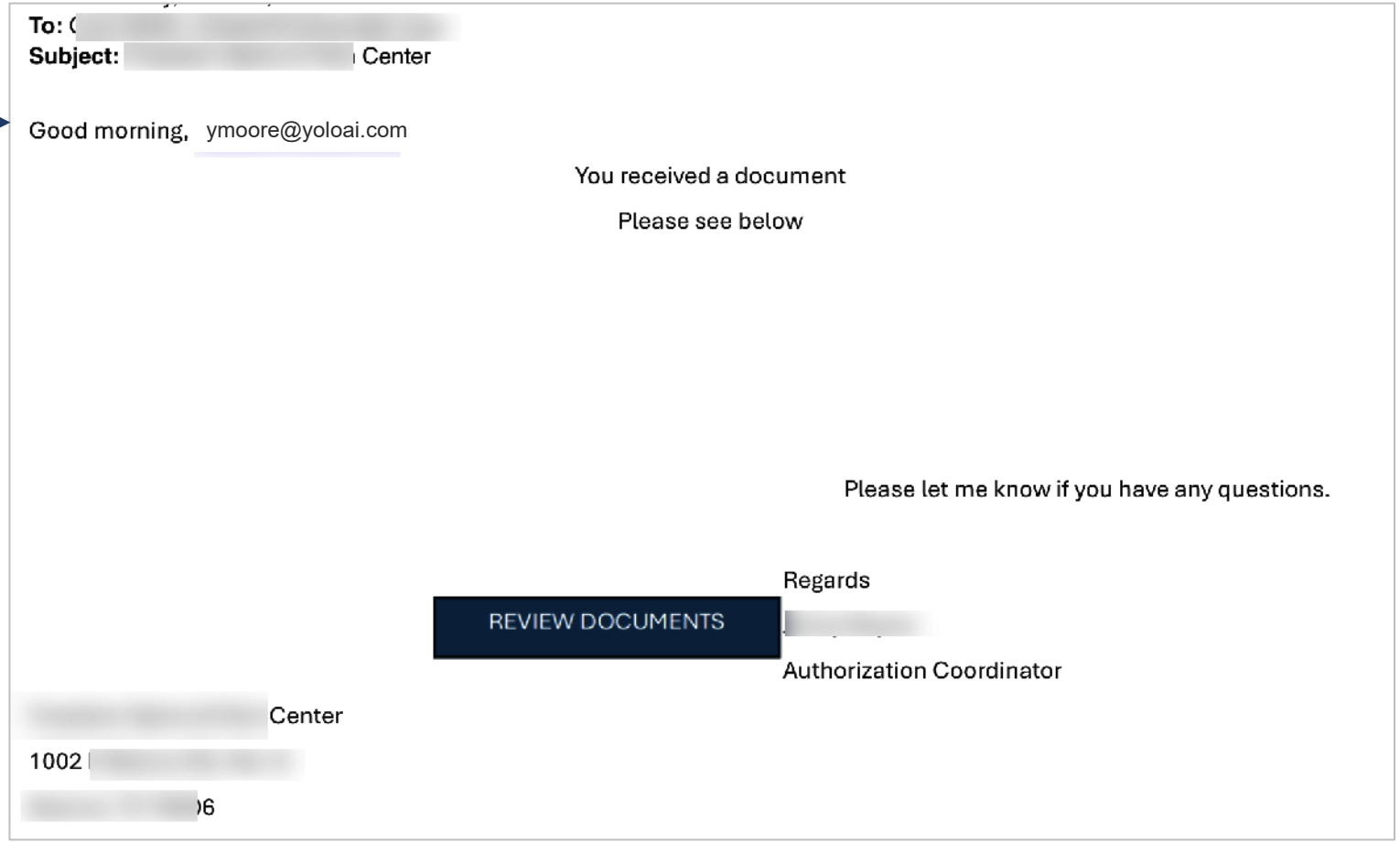
[redacted] Center

1002 [redacted]

[redacted]06

Credential Harvesting

Greeting not addressing a person



To: [redacted]
Subject: [redacted] Center

Good morning, ymoore@yoloai.com

You received a document

Please see below

Please let me know if you have any questions.

Regards

REVIEW DOCUMENTS

[redacted]

Authorization Coordinator

[redacted] Center

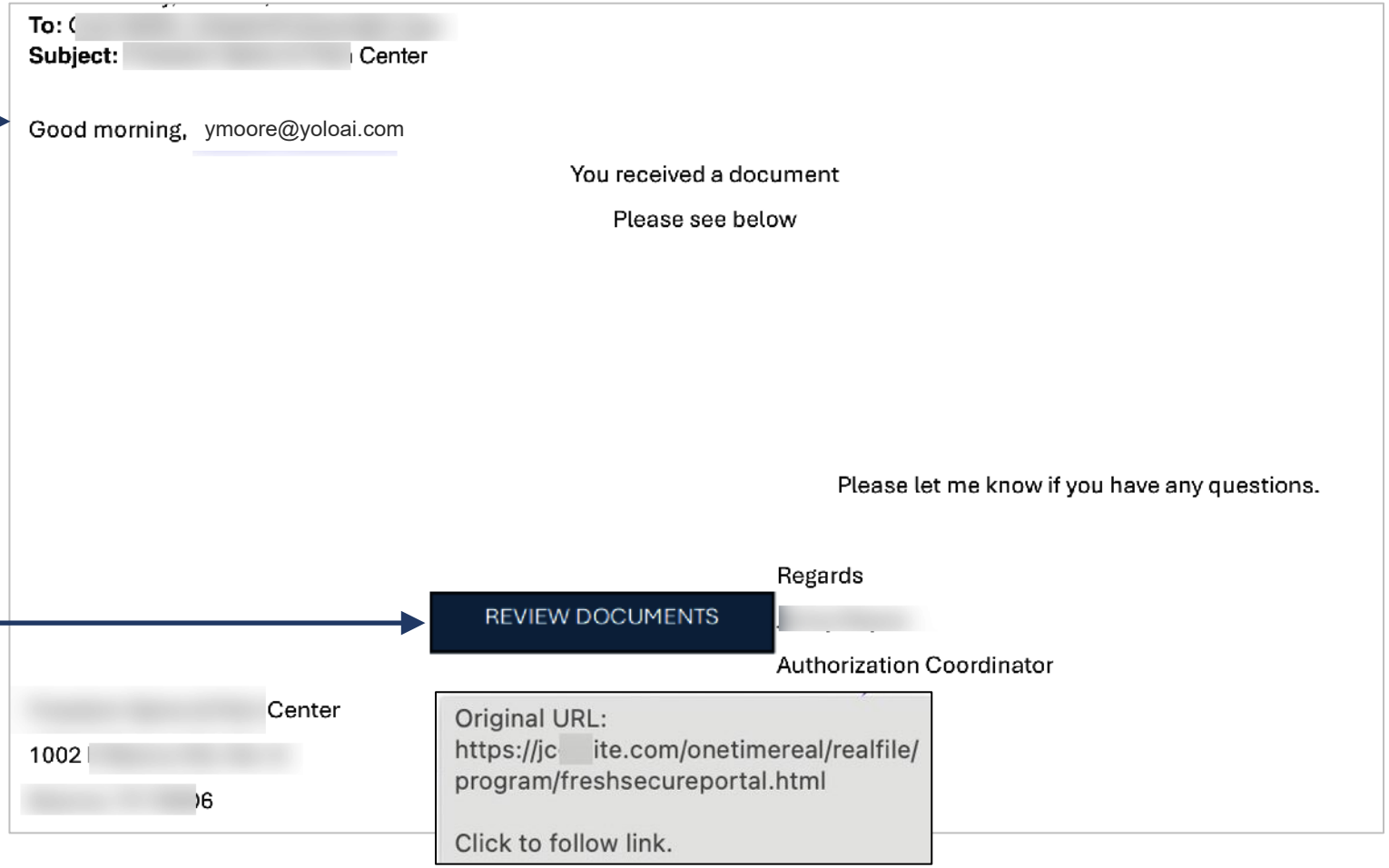
1002 [redacted]

[redacted]06

Credential Harvesting

Greeting not addressing a person

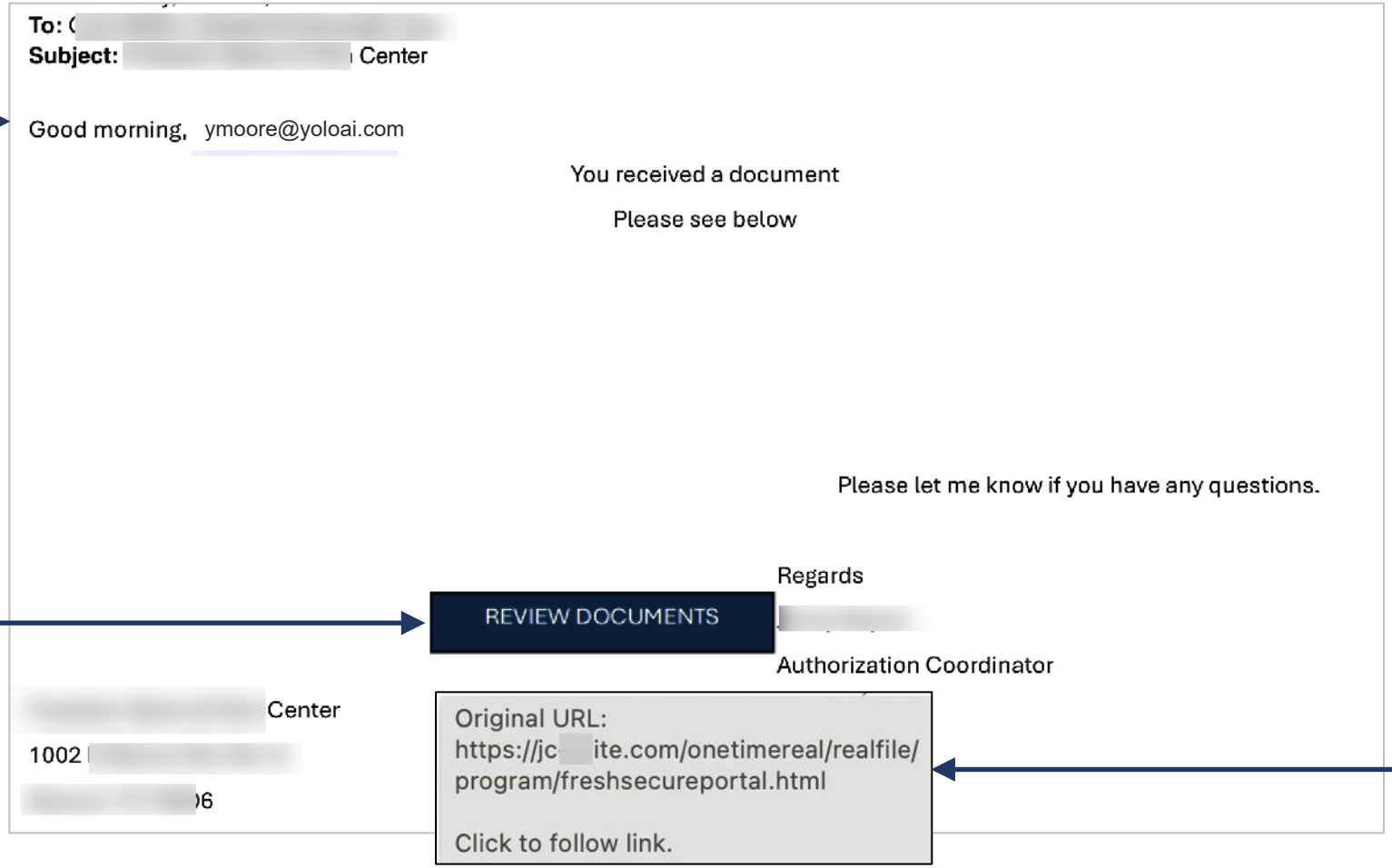
Hover over icon (don't click)



Credential Harvesting

Greeting not addressing a person

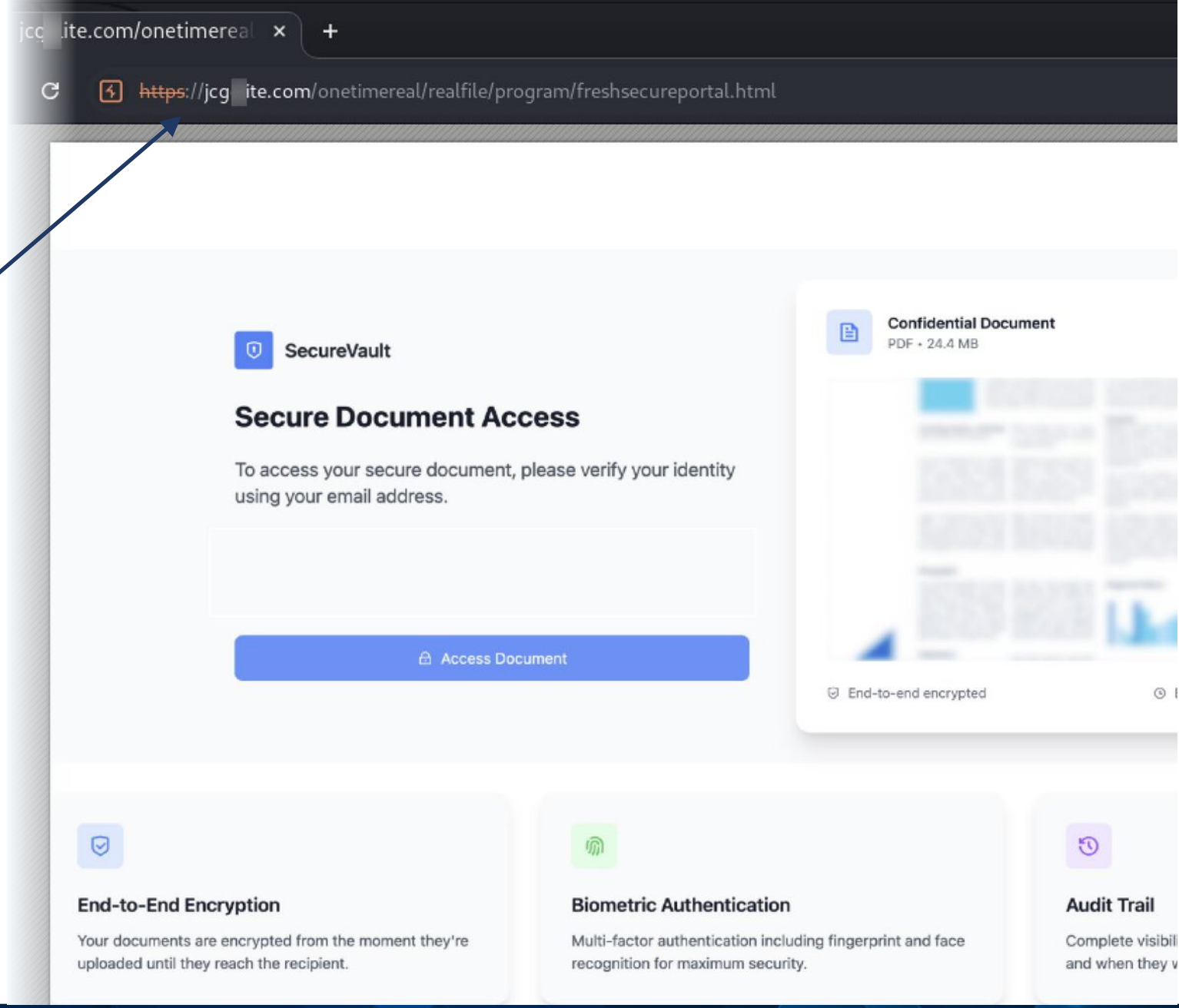
Hover over icon (don't click)



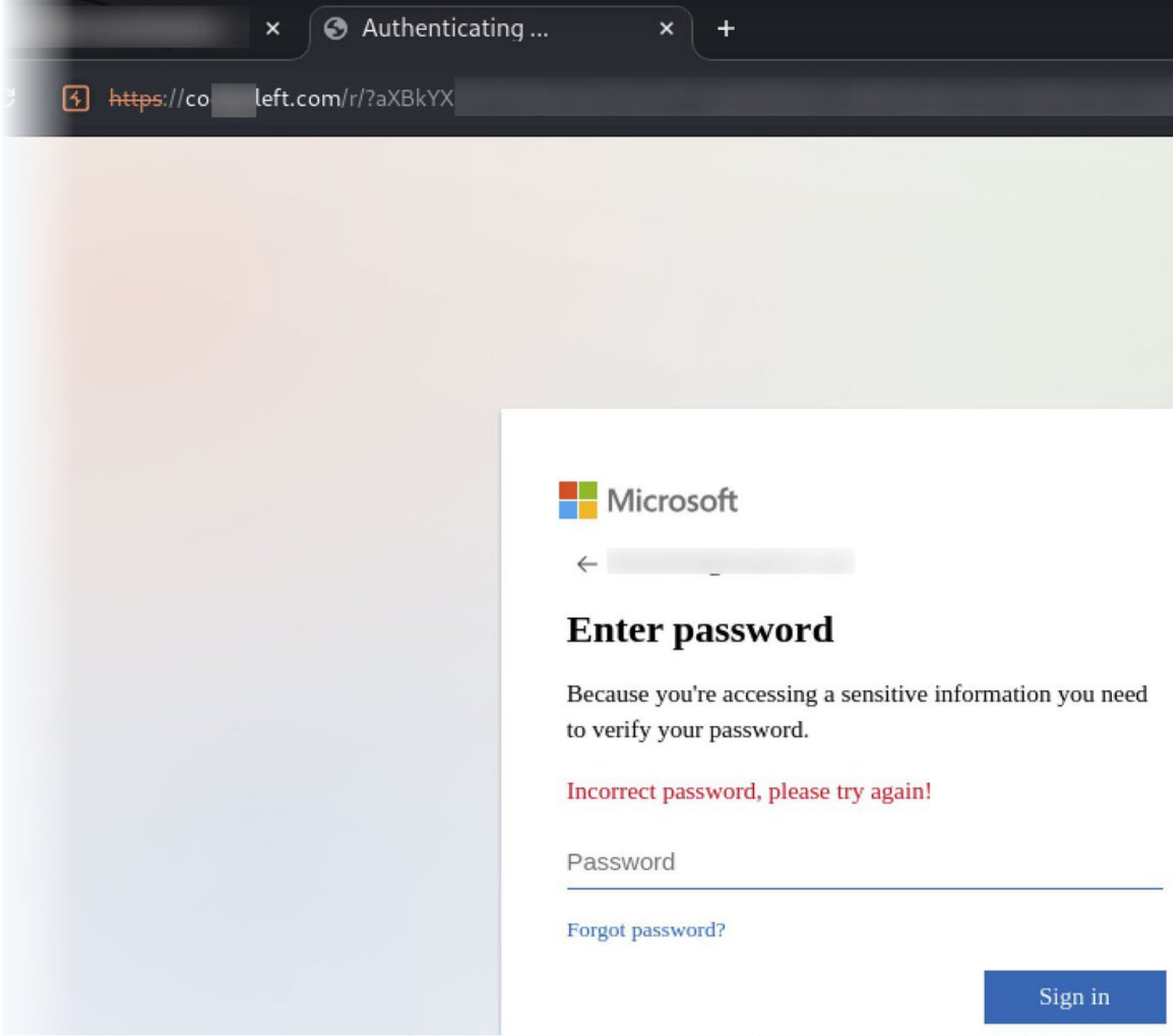
Site and method for file retrieval not expected

Credential Harvesting

Link looks suspicious

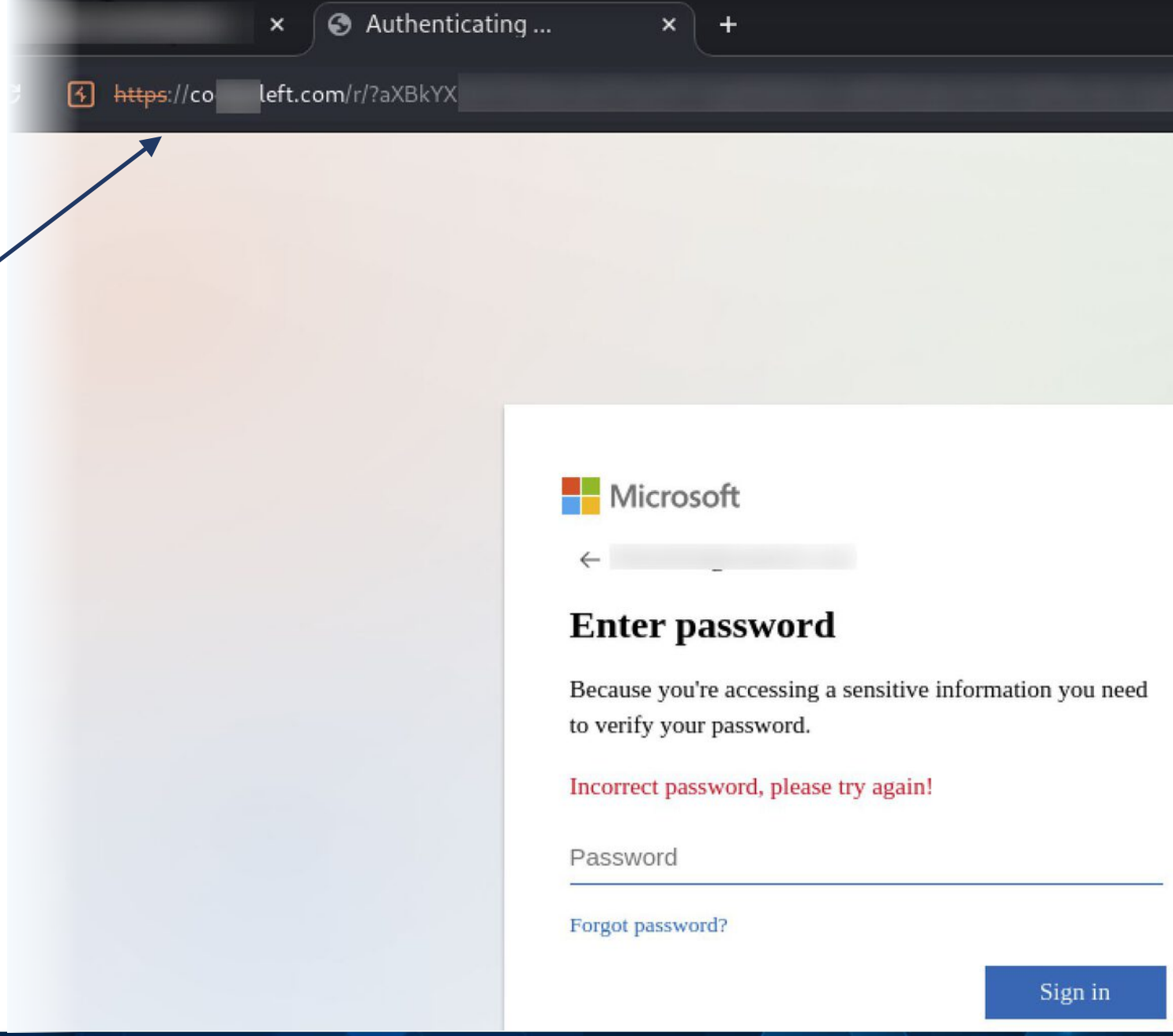


Credential Harvesting



Credential Harvesting

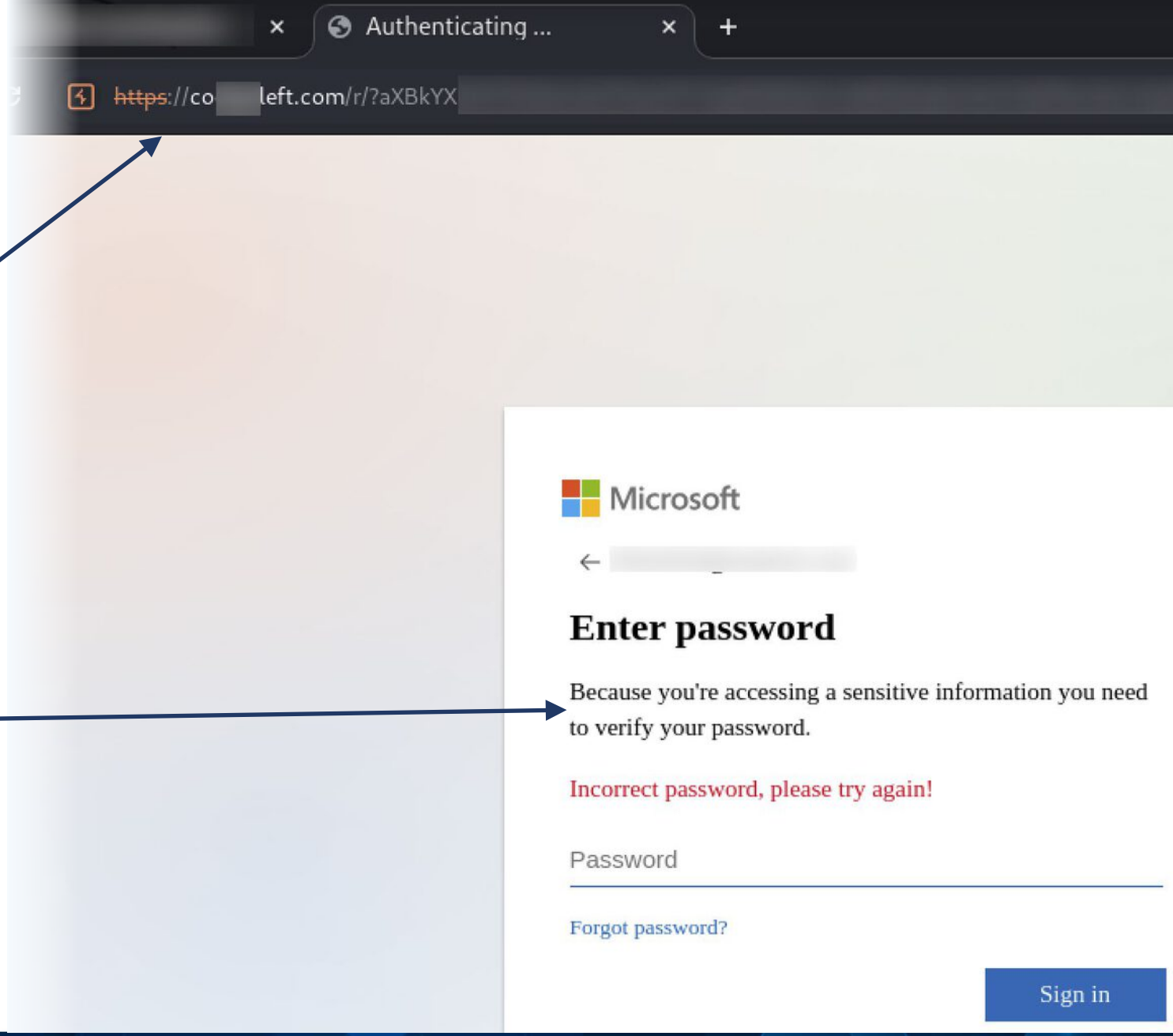
Not a Microsoft domain



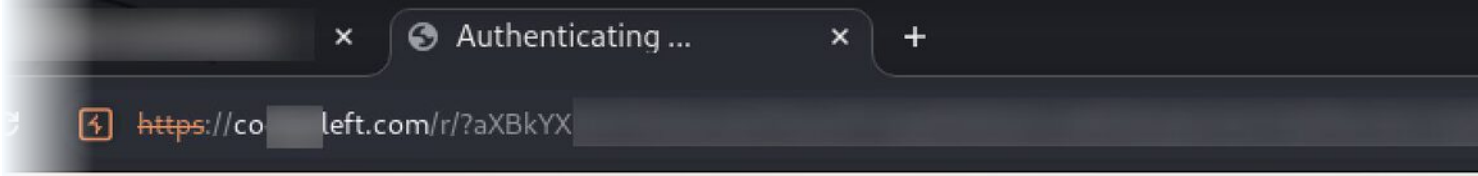
Credential Harvesting

Not a Microsoft domain

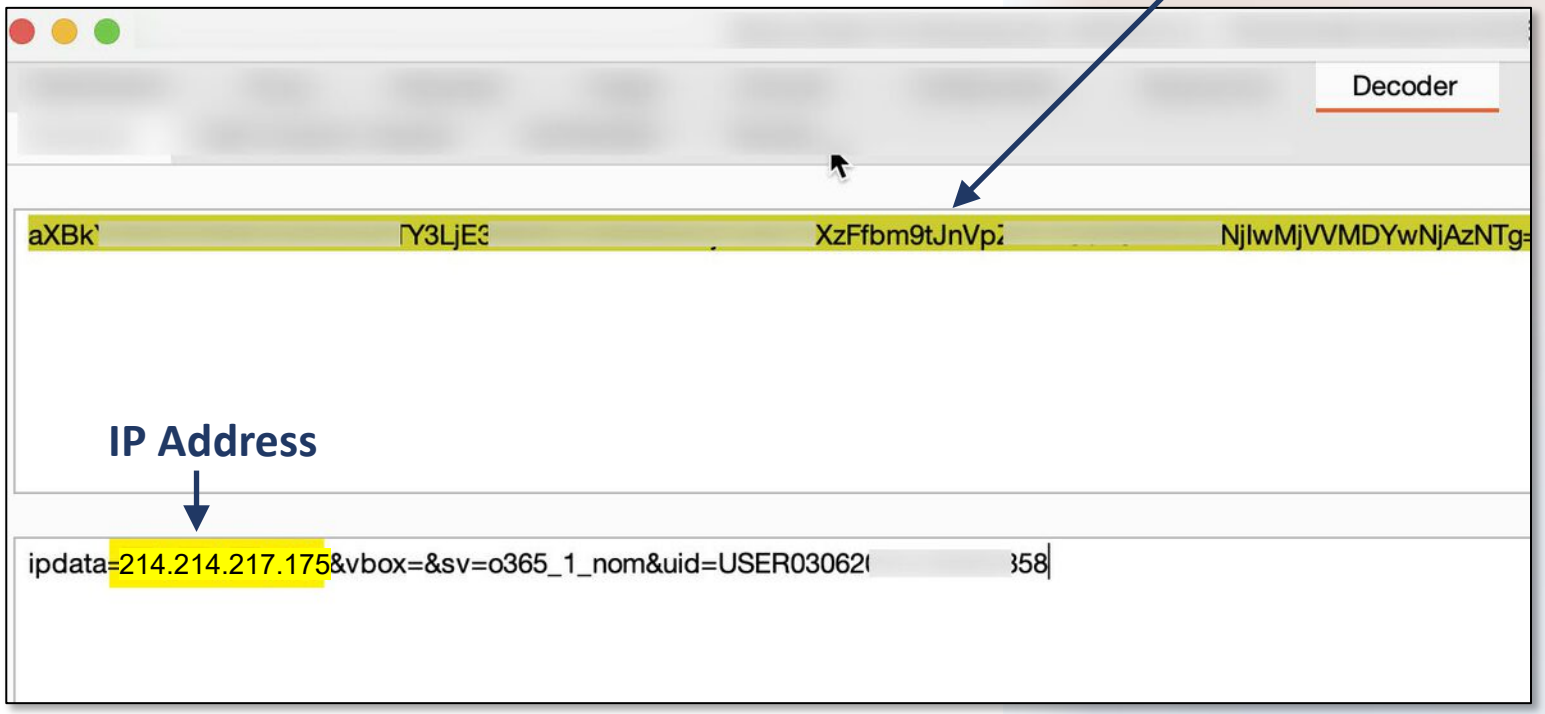
Font does not look right

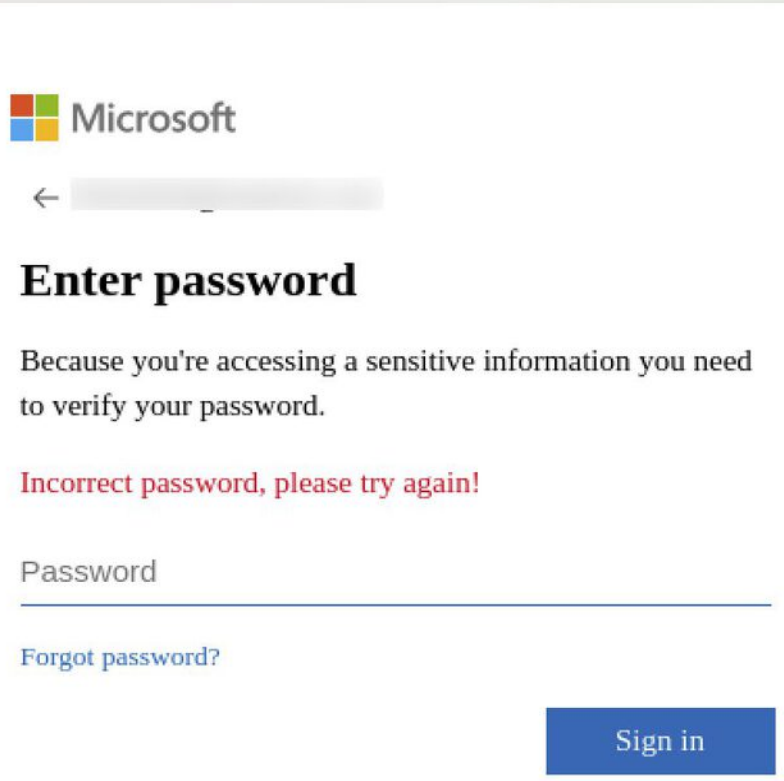


Credential Harvesting



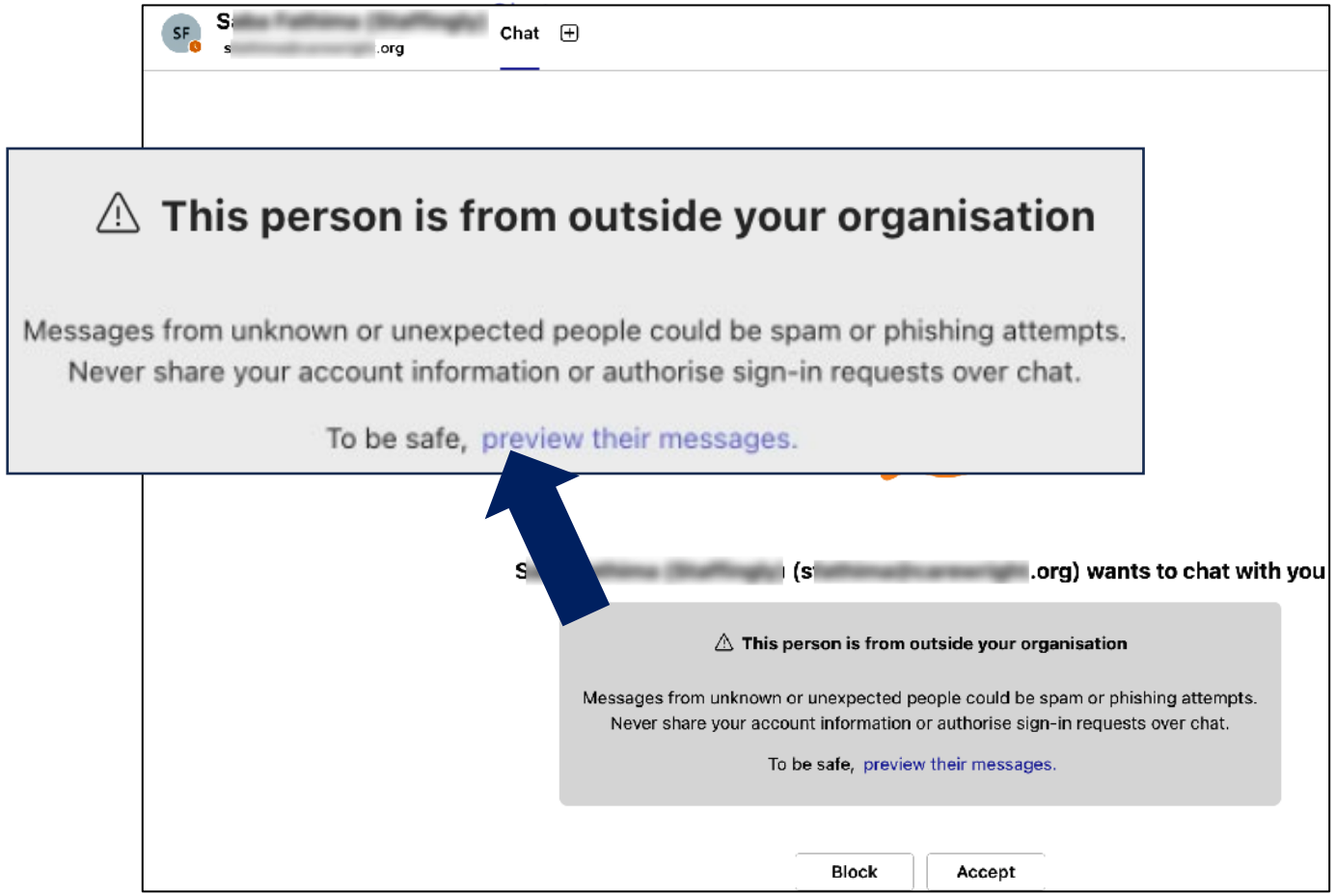
Decode Base64 in URL



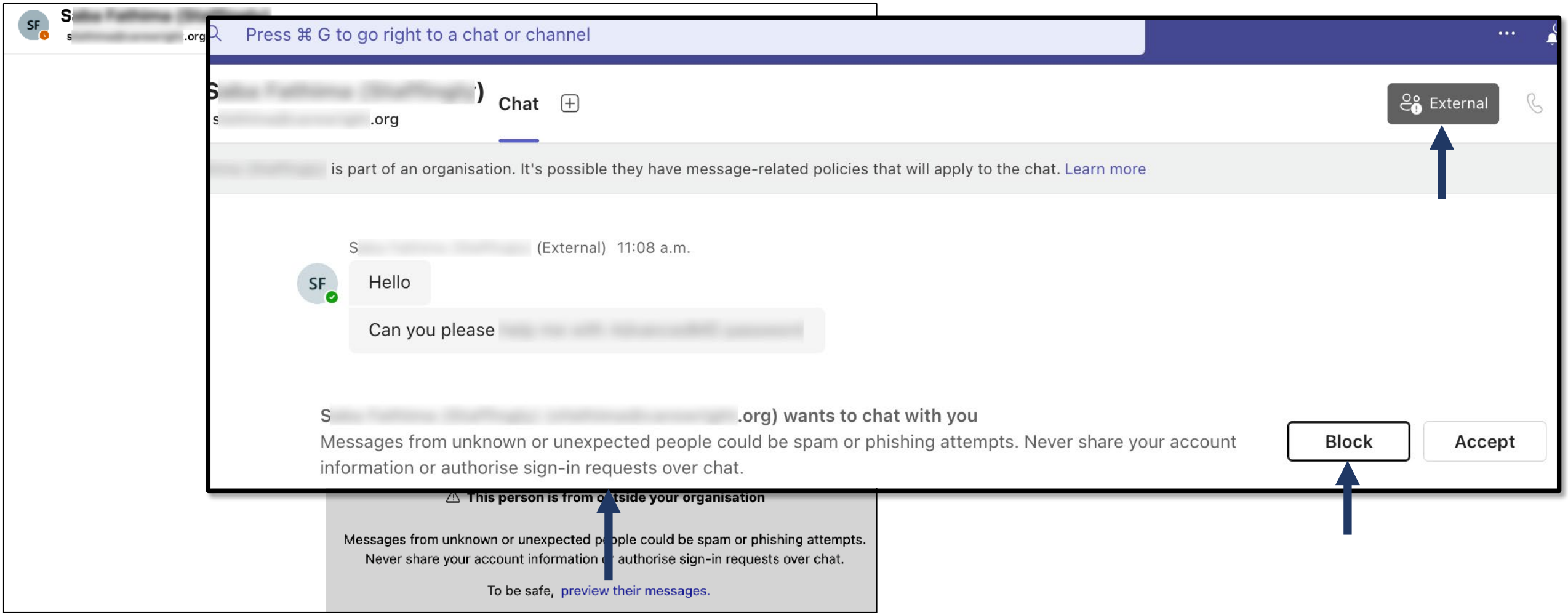


(External) Reaching Out From MS Teams

Message

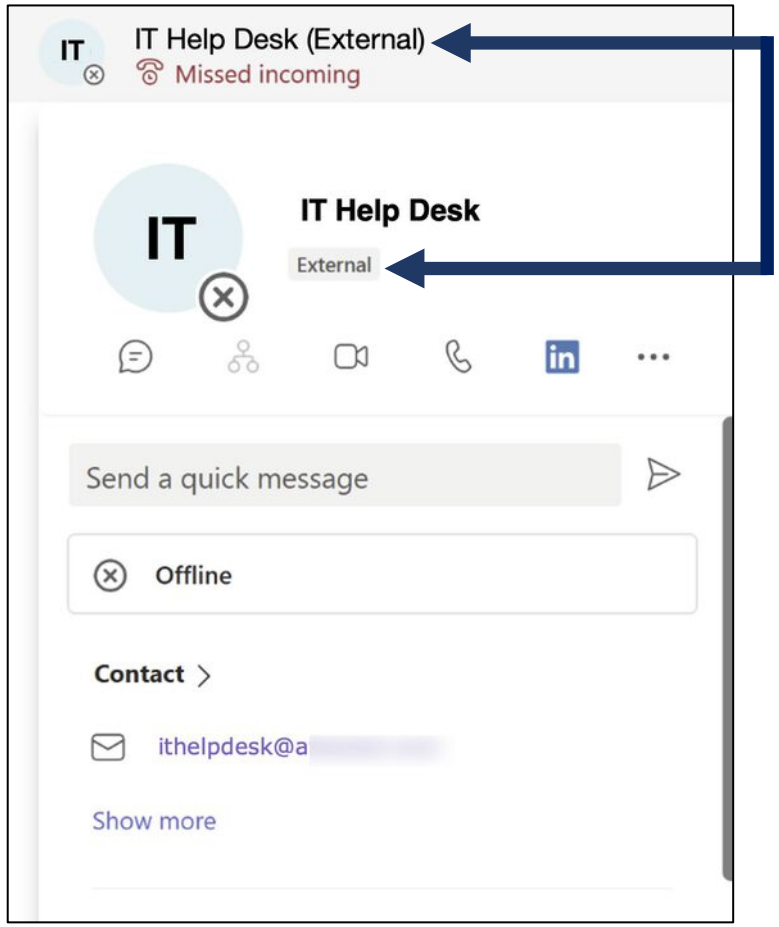


(External) Reaching Out From MS Teams



(External) Reaching Out From MS Teams

Call



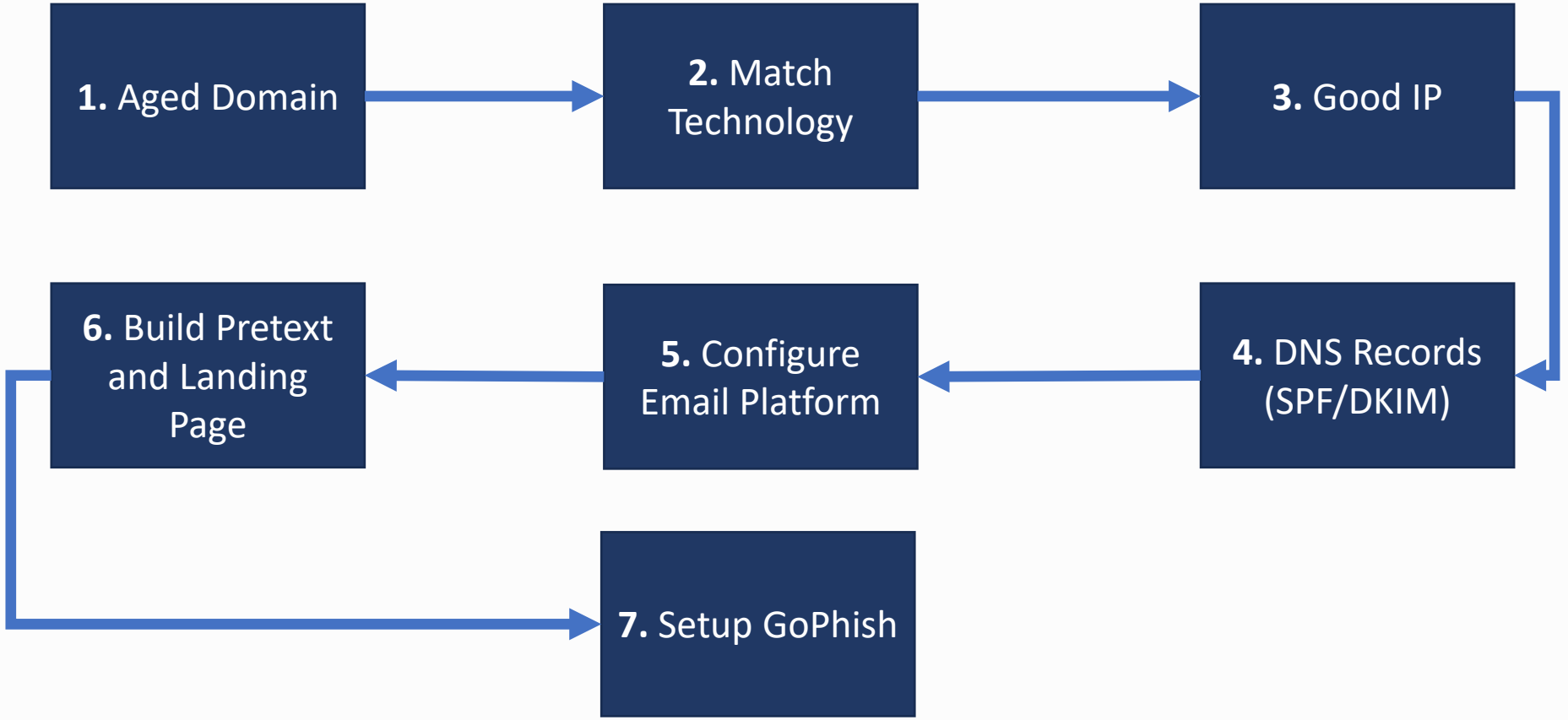
External

EMAIL PHISHING

"PHISHING EMAILS BAIT WITH TRUST, BUT REEL IN WITH DECEPTION."

Email Phishing

Steps to build a platform to get email into inbox without whitelisting

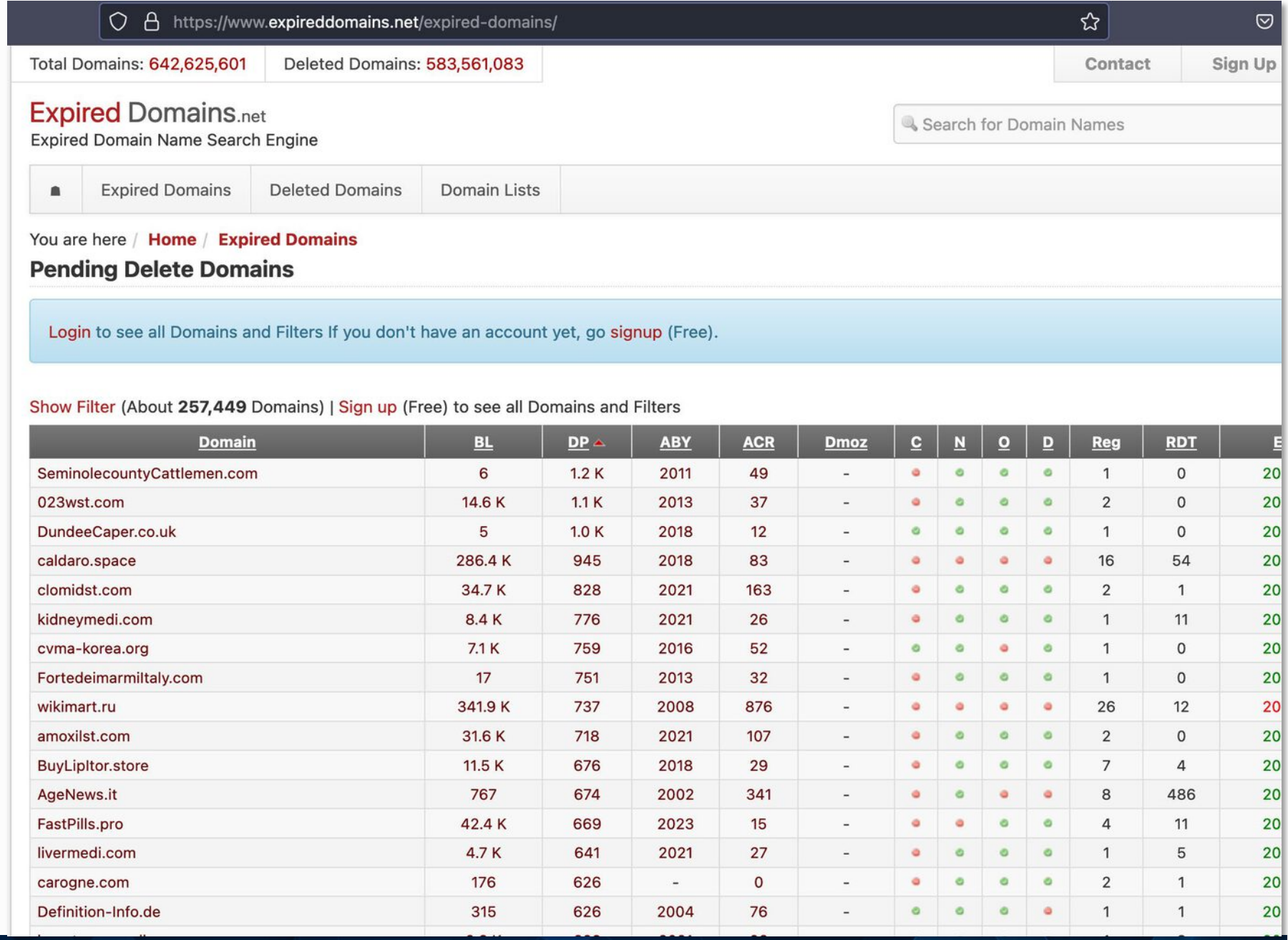


Email Phishing

Choose an aged domain with a neutral or good reputation

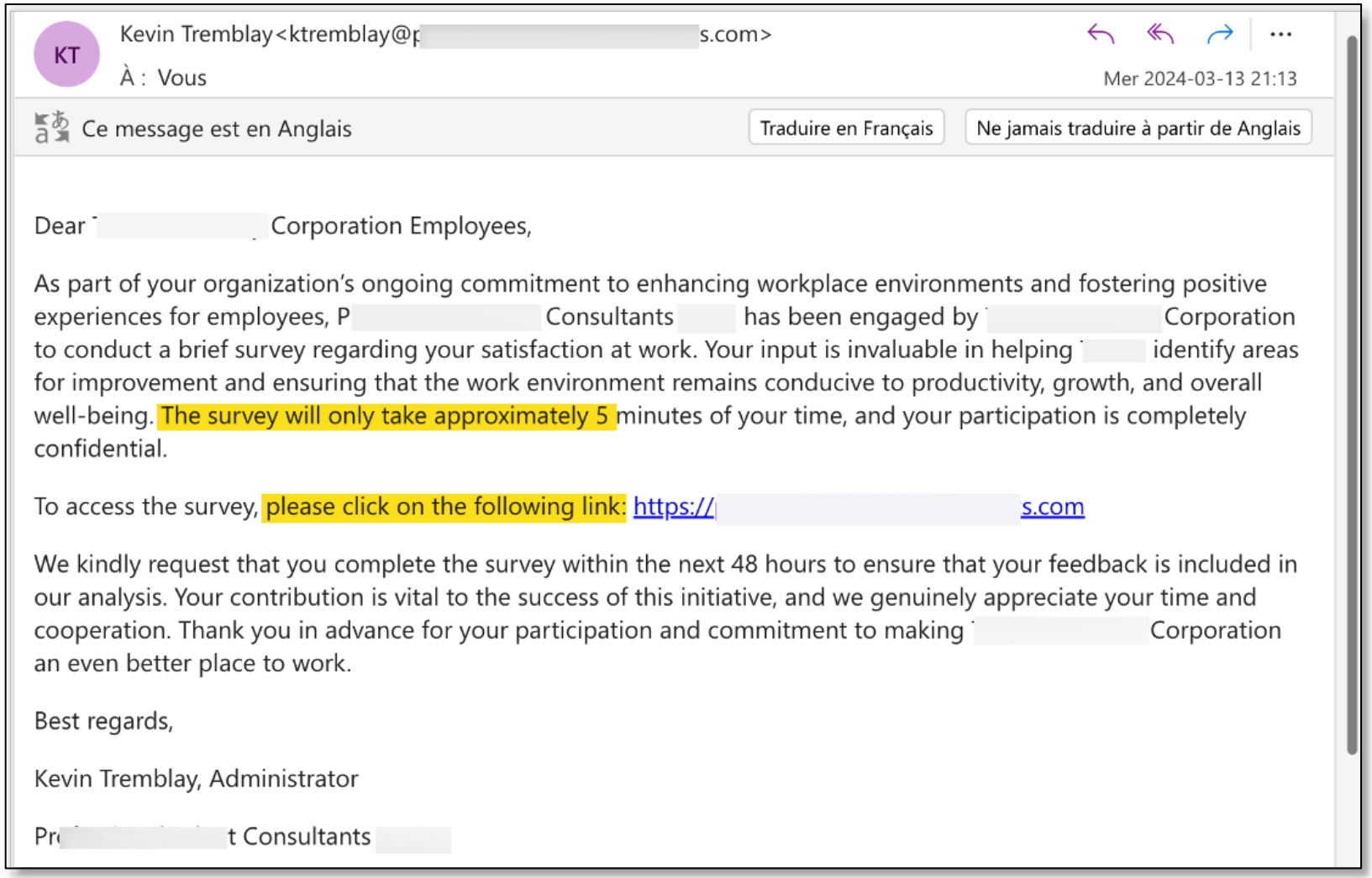
- Choose something that closely matches client's context
- URLs to check
  - Aged Domains: https://www.expireddomains.net
  - Reputation Check: https://www.talosintelligence.com/reputation_center
  - Domain Classification: https://www.fortiguard.com/webfilter

Email Phishing



Domain	BL	DP	ABY	ACR	Dmoz	C	N	O	D	Reg	RDT	E
SeminolecountyCattlemen.com	6	1.2 K	2011	49	-					1	0	20
023wst.com	14.6 K	1.1 K	2013	37	-					2	0	20
DundeeCaper.co.uk	5	1.0 K	2018	12	-					1	0	20
caldaro.space	286.4 K	945	2018	83	-					16	54	20
clomidst.com	34.7 K	828	2021	163	-					2	1	20
kidneymedi.com	8.4 K	776	2021	26	-					1	11	20
cvma-korea.org	7.1 K	759	2016	52	-					1	0	20
Fortedeimarmiltaly.com	17	751	2013	32	-					1	0	20
wikimart.ru	341.9 K	737	2008	876	-					26	12	20
amoxilst.com	31.6 K	718	2021	107	-					2	0	20
BuyLipItor.store	11.5 K	676	2018	29	-					7	4	20
AgeNews.it	767	674	2002	341	-					8	486	20
FastPills.pro	42.4 K	669	2023	15	-					4	11	20
livermedi.com	4.7 K	641	2021	27	-					1	5	20
carogne.com	176	626	-	0	-					2	1	20
Definition-Info.de	315	626	2004	76	-					1	1	20

Email Phishing



KT

Kevin Tremblay<ktremblay@p s.com>

À : Vous

Mer 2024-03-13 21:13

Ce message est en Anglais | Traduire en Français | Ne jamais traduire à partir de Anglais

Dear Corporation Employees,

As part of your organization's ongoing commitment to enhancing workplace environments and fostering positive experiences for employees, P Consultants has been engaged by Corporation to conduct a brief survey regarding your satisfaction at work. Your input is invaluable in helping identify areas for improvement and ensuring that the work environment remains conducive to productivity, growth, and overall well-being. The survey will only take approximately 5 minutes of your time, and your participation is completely confidential.

To access the survey, please click on the following link: https:// s.com

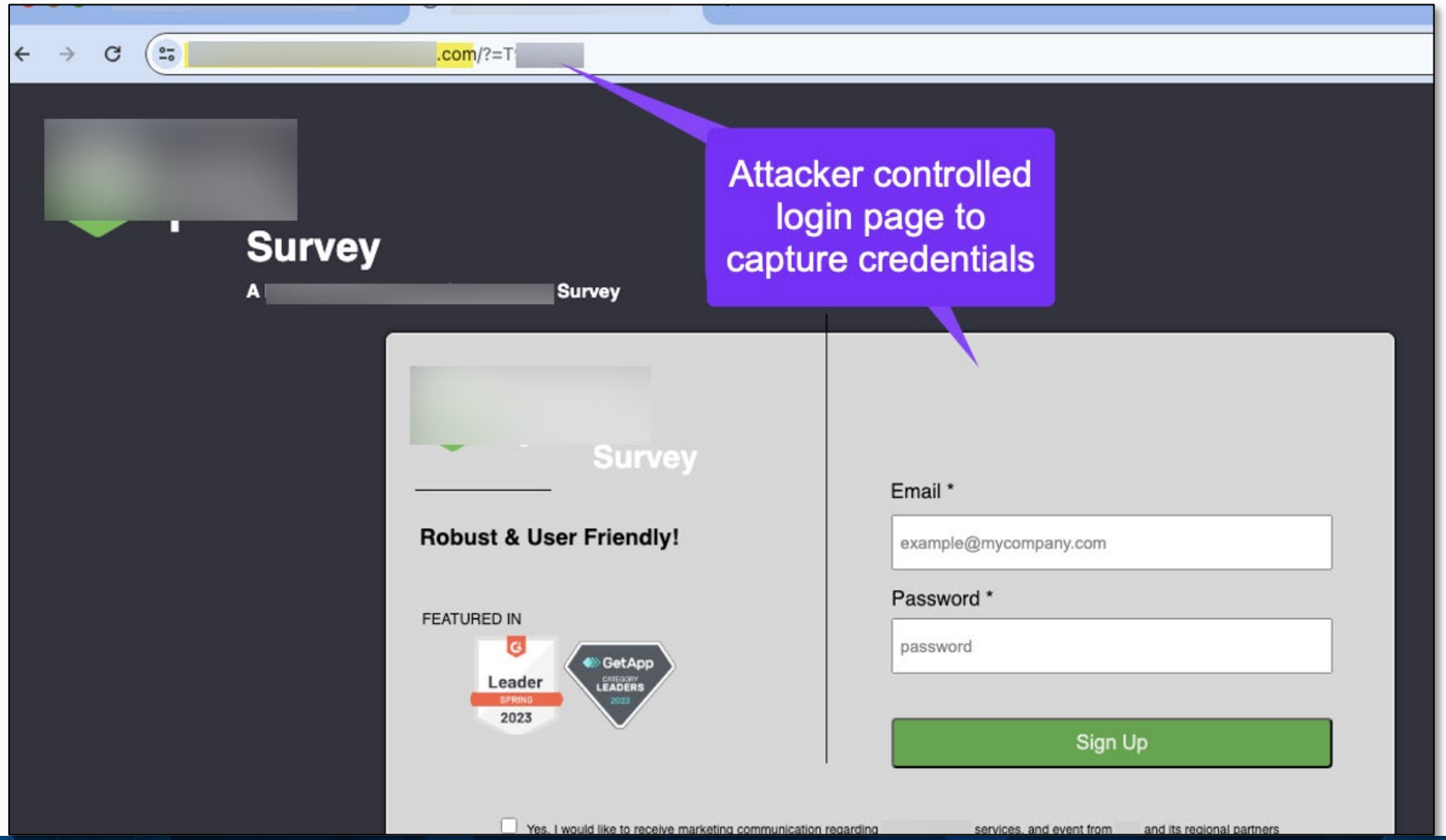
We kindly request that you complete the survey within the next 48 hours to ensure that your feedback is included in our analysis. Your contribution is vital to the success of this initiative, and we genuinely appreciate your time and cooperation. Thank you in advance for your participation and commitment to making Corporation an even better place to work.

Best regards,

Kevin Tremblay, Administrator

Pr t Consultants

Email Phishing

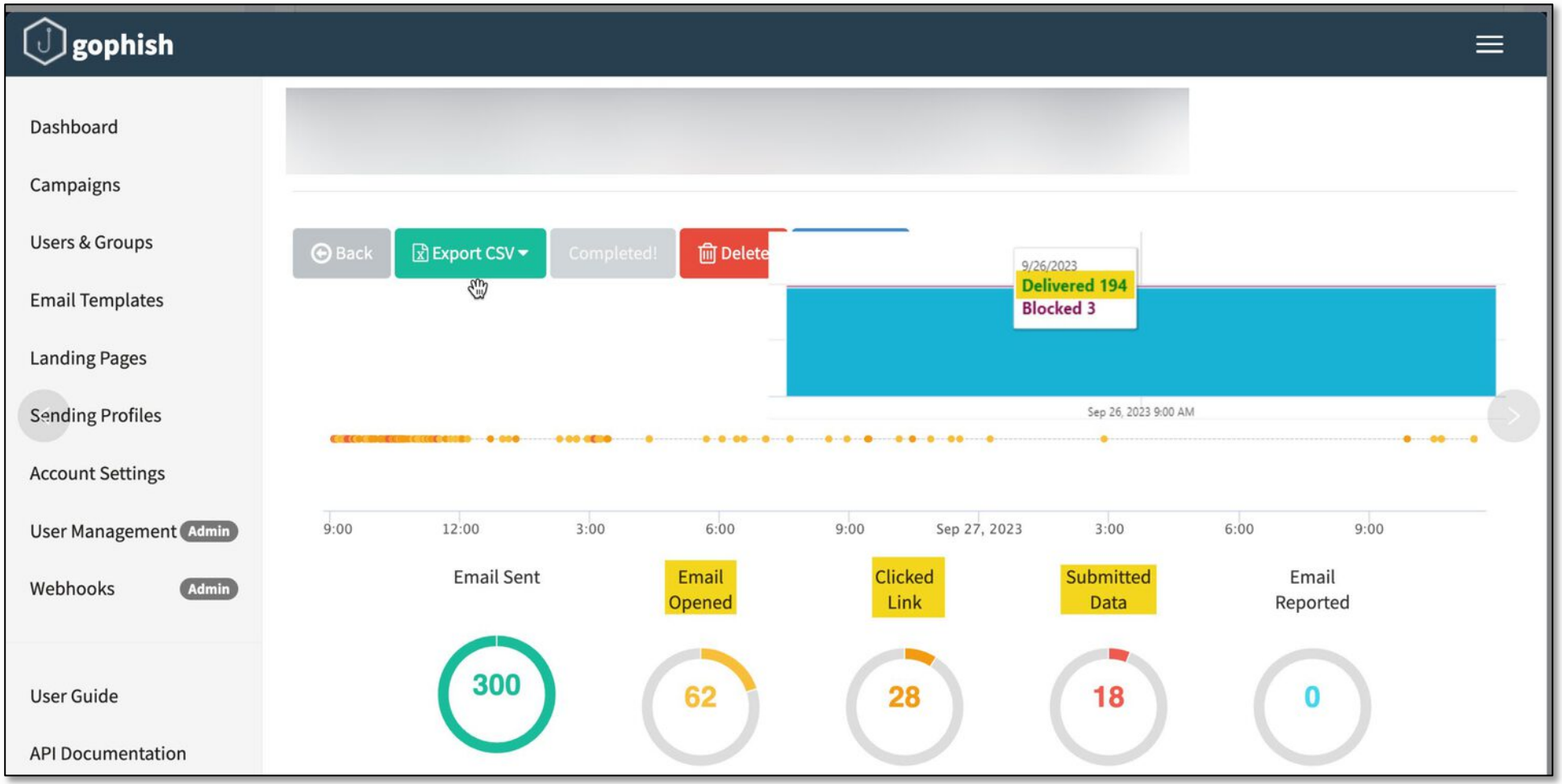


Email Phishing

Setup GoPhish

- Remove signatures
  - https://www.redteam.cafe/phishing/gophish-mods
- Setup the following
  - Landing page
  - Email template
  - Sending profile
- https://getgophish.com

Email Phishing



PHONE SOCIAL ENGINEERING

"PHONE PHISHING DISGUISES A VOICE OF TRUST, BUT IT'S A TRAP WAITING TO BE ANSWERED."

Phone Social Engineering

Hands on Cases

- Calling Customer Support Numbers for Internal Information
- Account Takeover via Tech Support
- Account Takeover Gone Wrong
- Convincing Staff to Enter MFA Authentication Codes

Phone Social Engineering

Preparation

- New cellphone number for the region you want to operate in
  - Prepaid phone card: $5 SIM + $20 credit
  - Create accounts with cloud telephony vendors
- Targets to call
- Pretext

Phone Social Engineering

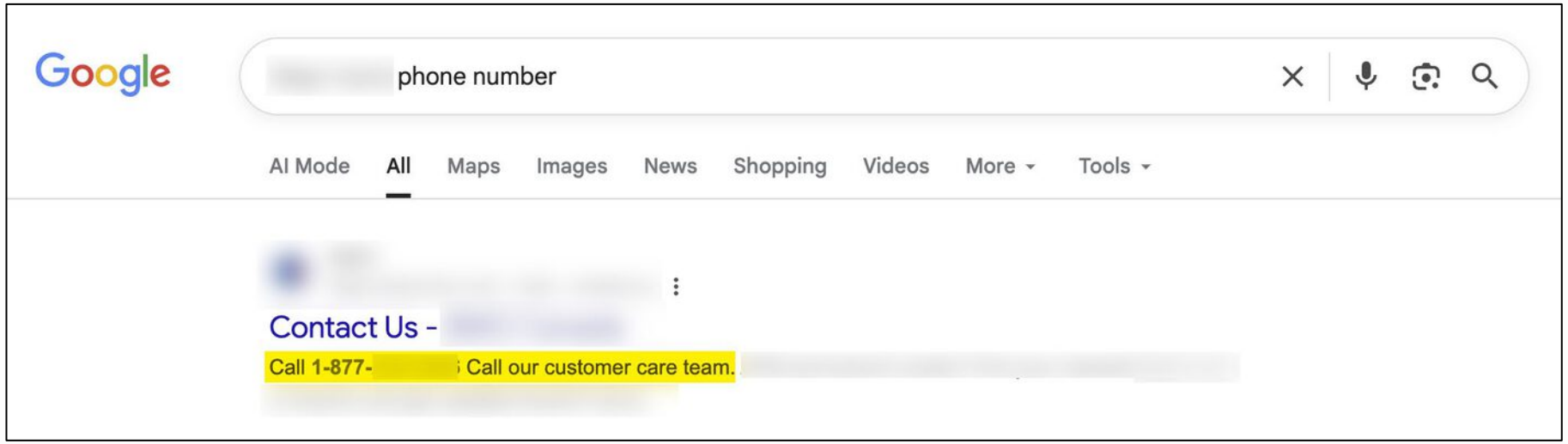
Calling Customer Support Numbers for Internal Information

Phone Social Engineering

Goal: Obtain Internal IT Support Number

Background: Internal tech support number not found via OSINT

- Collect all publicly disclosed phone numbers



- Call the numbers
    - **"I am an ABC employee. I forgot the internal support line number. My laptop is not working. Do you have the internal tech support number?"**

Phone Social Engineering

Outcomes

NUMBER FOUND ON THE INTERNET	SUPPORT ASKED FOR NAME?	SUPPORT ASKED FOR EMPLOYEE NUMBER?	PROVIDED INTERNAL IT SUPPORT NUMBER?
1 (800) 444-XXXX			
1 (888) 888-XXXX			
1 (800) 555-XXXX			

Phone Social Engineering

Outcomes

NUMBER FOUND ON THE INTERNET	SUPPORT ASKED FOR NAME?	SUPPORT ASKED FOR EMPLOYEE NUMBER?	PROVIDED INTERNAL IT SUPPORT NUMBER?
1 (800) 444-XXXX	YES	YES	NO
1 (888) 888-XXXX			
1 (800) 555-XXXX			

Phone Social Engineering

Outcomes

NUMBER FOUND ON THE INTERNET	SUPPORT ASKED FOR NAME?	SUPPORT ASKED FOR EMPLOYEE NUMBER?	PROVIDED INTERNAL IT SUPPORT NUMBER?
1 (800) 444-XXXX	YES	YES	NO
1 (888) 888-XXXX	YES	NO	YES
1 (800) 555-XXXX			

Phone Social Engineering

Outcomes

NUMBER FOUND ON THE INTERNET	SUPPORT ASKED FOR NAME?	SUPPORT ASKED FOR EMPLOYEE NUMBER?	PROVIDED INTERNAL IT SUPPORT NUMBER?
1 (800) 444-XXXX	YES	YES	NO
1 (888) 888-XXXX	YES	NO	YES
1 (800) 555-XXXX	NO	NO	YES

Phone Social Engineering

Account Takeover via Tech Support

Phone Social Engineering

Account Takeover via Tech Support

Goal: Account Takeover

To complete the objective the help desk will need to be convinced to do the following:

- Reset the account password.
- Reset MFA (i.e “Google Authenticator”, “MS Authenticator”) and/or update the account holder’s phone number to the attacker-controller phone number.

Phone Social Engineering

Account Takeover via Tech Support

Pretext:

- "I'm a contractor. I set stuff up a long time ago. I don't know my password. My password is not working. I can't login."

- "I'm a contractor. I'm not able to access my email. I changed phones. I need my password reset and also need MFA to be setup on a new phone. "

Phone Social Engineering

Account Takeover via Tech Support

Questions Commonly Asked to Verify Identity:

- Who do you report to?
  - **If asked:** Make sure this information is on hand before the call.
- What is your employee number?
  - **If asked:** “I don’t have that on me. I recently moved. I just need to get access”
- When was the last time you logged in?
  - **If asked:** “It’s been a while. I’m not to sure”
- What was your previous phone number
  - **If asked:** “I moved around recently. I don’t have it anymore. I have my new number”

Task as assessor: Provided minimum information [only first name and last name if possible]

Phone Social Engineering

	OUTCOMES
Day	
Night	

Phone Social Engineering

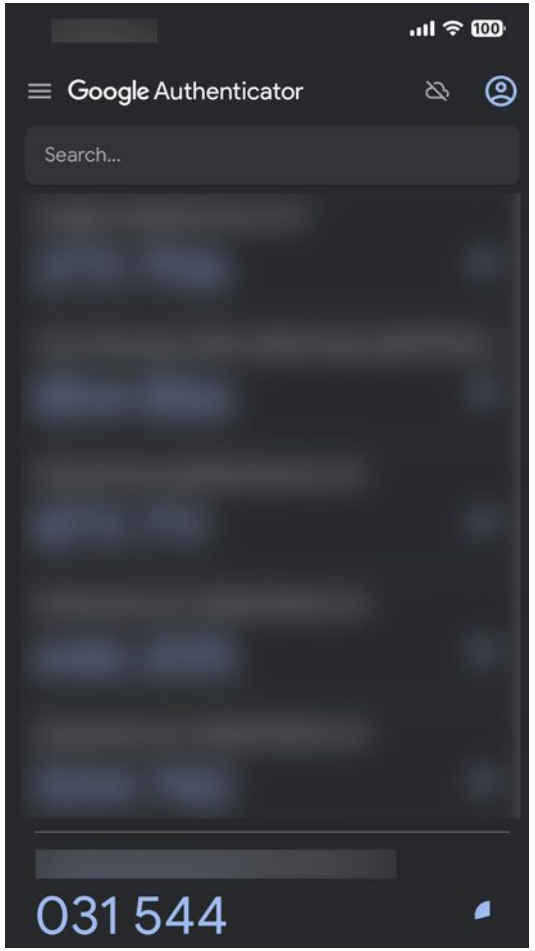
	OUTCOMES
Day	• Attacker provides name when asked. • Support asks when last logged in. • Support asks for employee number (Attacker did **NOT** provide).
Night	

Phone Social Engineering

	OUTCOMES
Day	• Attacker provides name when asked. • Support asks when last logged in. • Support asks for employee number (Attacker did **NOT** provide). • **OUTCOME:** Support asks attacker to send an email of request
Night	

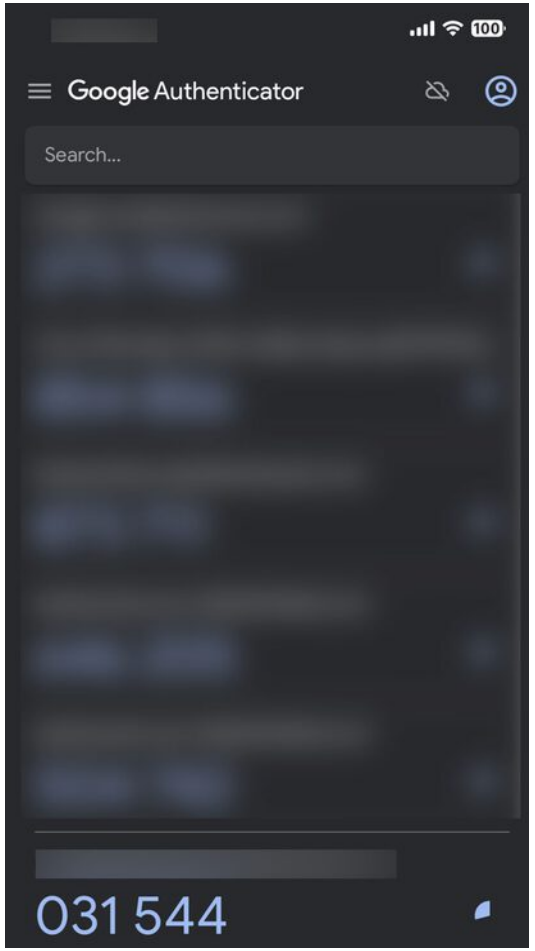
Phone Social Engineering

	OUTCOMES
Day	• Attacker provides name when asked. • Support asks when last logged in. • Support asks for employee number (Attacker did **NOT** provide). • **OUTCOME:** Support asks attacker to send an email of request
Night	• Attacker provides name when asked. • Support asks for employee number (Attacker did **NOT** provide). • **Support provides the employee number to attacker** • **Transfer of MFA to new phone.**



Phone Social Engineering

	OUTCOMES
Day	• Attacker provides name when asked. • Support asks when last logged in. • Support asks for employee number (Attacker did **NOT** provide). • **OUTCOME:** Support asks attacker to send an email of request
Night	• Attacker provides name when asked. • Support asks for employee number (Attacker did **NOT** provide). • **Support provides the employee number to attacker** • **Transfer of MFA to new phone.** • **OUTCOME:** Attacker takes over account.



Phone Social Engineering

Account Takeover Gone Wrong

Phone Social Engineering

Account Takeover Gone Wrong

Background:

- Email phishing campaign was able to capture the credentials (Username, Password).
- However, MFA is still required to login.

Objective:

- Have tech support walk through adding multi-factor authentication (MFA) to the attacker-controlled phone.

Pretext:

- "Hello. This is A--- B---."
- "I'm not able to get into my account."
- "I recently switched phone and phone numbers"
- "I need MFA to be setup on my new phone."

Phone Social Engineering

Tech support did NOT perform rigorous identity validation checks

Only asked for first name, last name, and email address

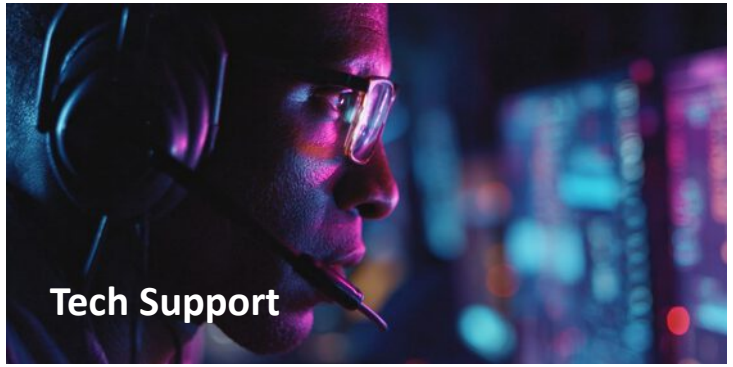
MFA was setup on a new phone.....

Phone Social Engineering

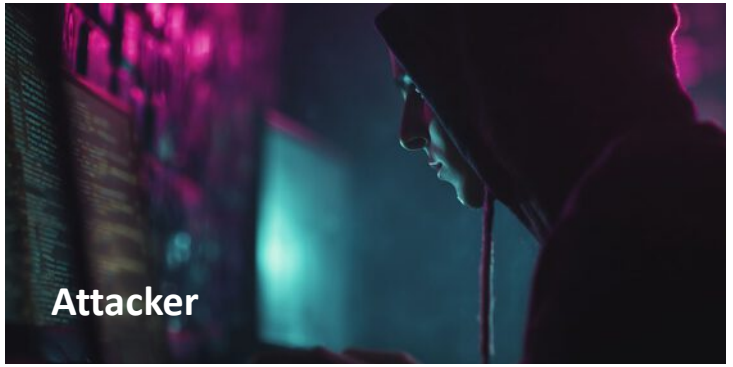
Tech support did NOT perform rigorous identity validation checks

Only asked for first name, last name, and email address

MFA was setup on a new phone.....



- Eager to help



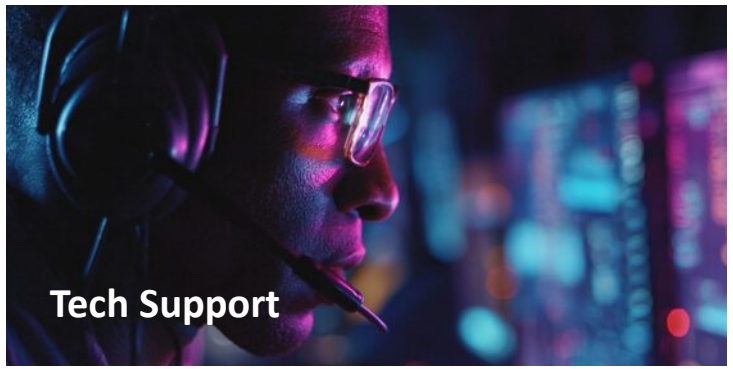
- Was able to get creds from phishing email campaign
- Was able to get MFA enable

Phone Social Engineering

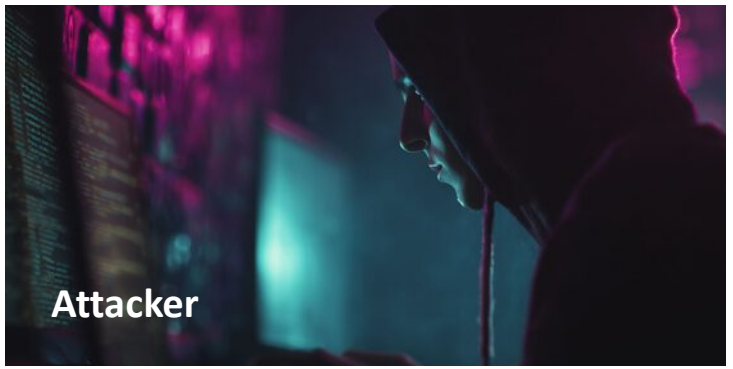
Tech support did NOT perform rigorous identity validation checks

Only asked for first name, last name, and email address

MFA was setup on a new phone..... BUT



- Eager to help
- **Went beyond setting up MFA**
- **Communicates through alternative methods (i.e. wants to send links)**



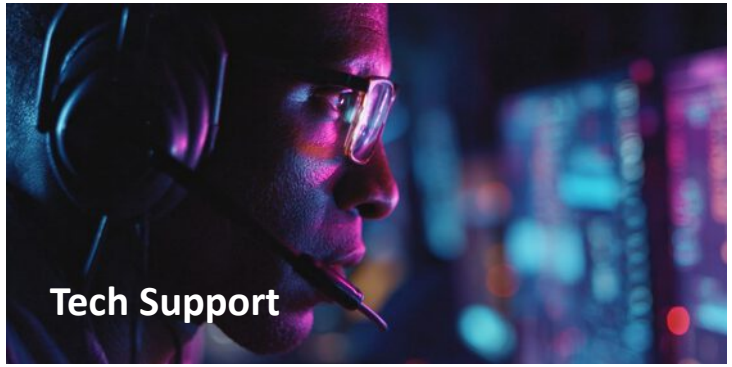
- Was able to get creds from phishing email campaign
- Was able to get MFA enable

Phone Social Engineering

Tech support did NOT perform rigorous identity validation checks

Only asked for first name, last name, and email address

MFA was setup on a new phone..... BUT



- Eager to help
- Went beyond setting up MFA
- Communicates through alternative methods (i.e. wants to send links)

- Was able to get creds from phishing email campaign
- Was able to get MFA enable

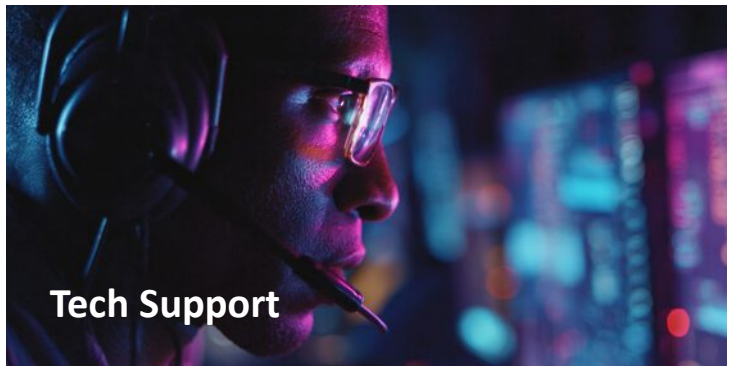
- **Remembers providing credentials for survey**
- **Notices suspicious behavior**
- **Escalates to security team**

Phone Social Engineering

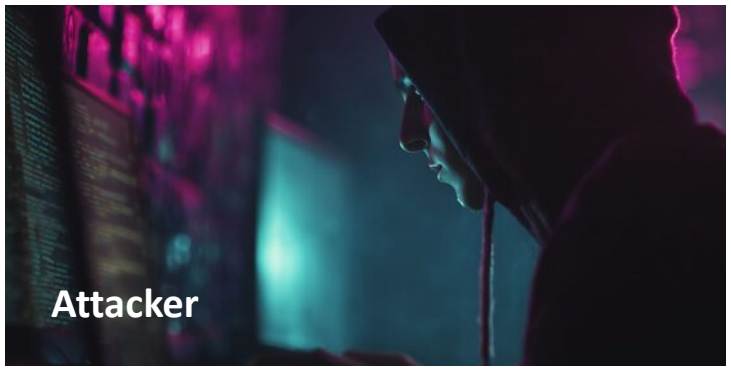
Tech support did NOT perform rigorous identity validation checks

Only asked for first name, last name, and email address

MFA was setup on a new phone..... BUT



- Eager to help
- Went beyond setting up MFA
- Communicates through alternative methods (i.e. wants to send links)



- Was able to get creds from phishing email campaign
- Was able to get MFA enable
- **Account disabled during social engineering call**

- Remembers providing credentials for survey
- Notices suspicious behavior
- Escalates to security team

Phone Social Engineering

Attacker Suggestions

- Perform social engineering activities during after hours if possible
  - Support staff might be less vigilant
  - Target might not be available if alerts occur
- Stick to immediate goals
  - Being too greedy might be risky

Phone Social Engineering

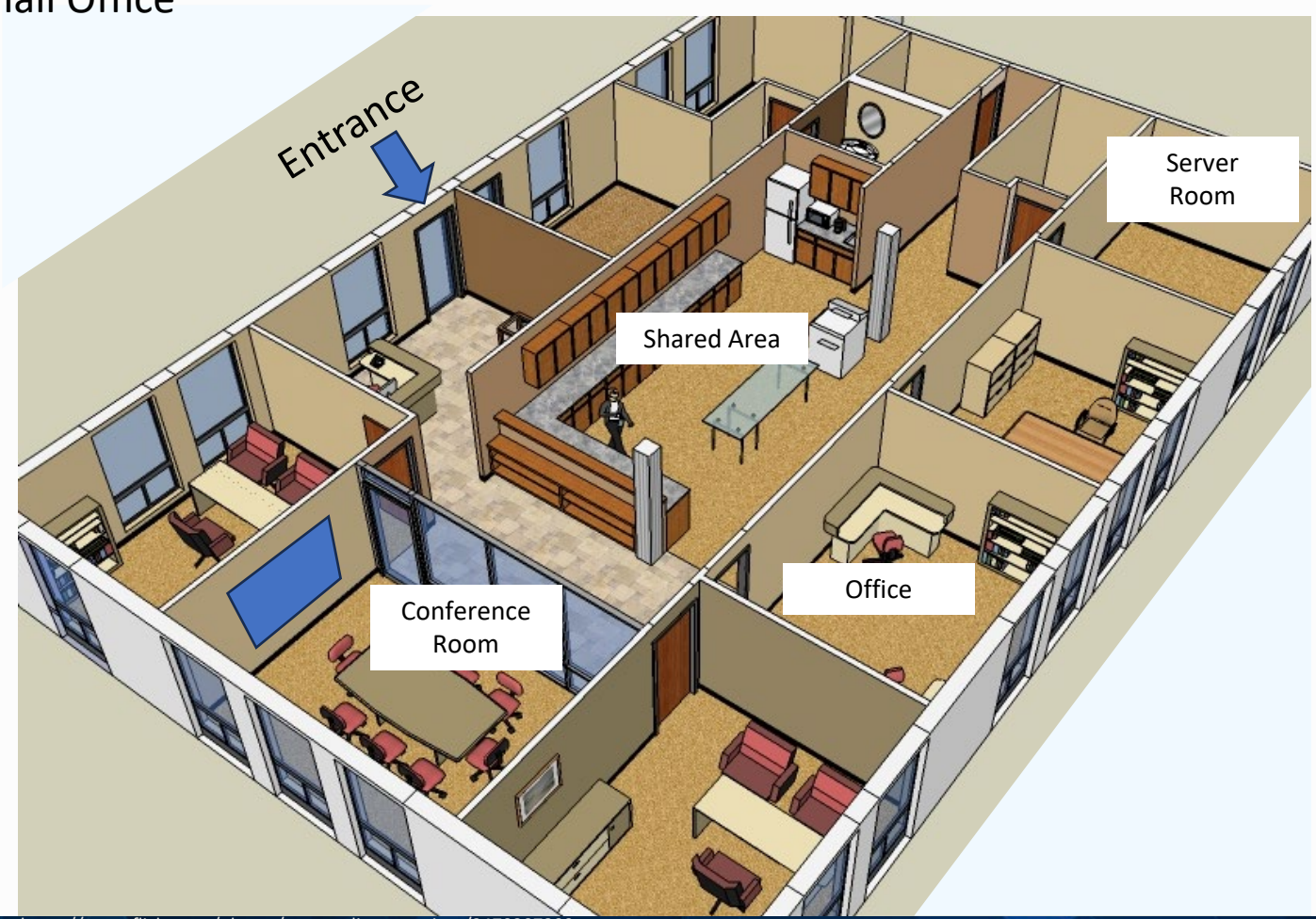
Defense Suggestions

- **Vigilance:** Make sure staff follows validations checklists
  - Check employee number, who they report to, ext...
- **Information Leaks:**
  - Make sure customer support staff are trained to not provide insider information
- **Training & Awareness**:
  - Staff should be made aware of the dangers of social engineering and trained to identify and report common tactics.
- **MFA**:
  - If MFA needs to be reset and transferred to a new phone, consider requiring technical staff to contact the hiring manager to confirm the situation before it is transferred to a new phone.

PHYSICAL SECURITY

Physical Security

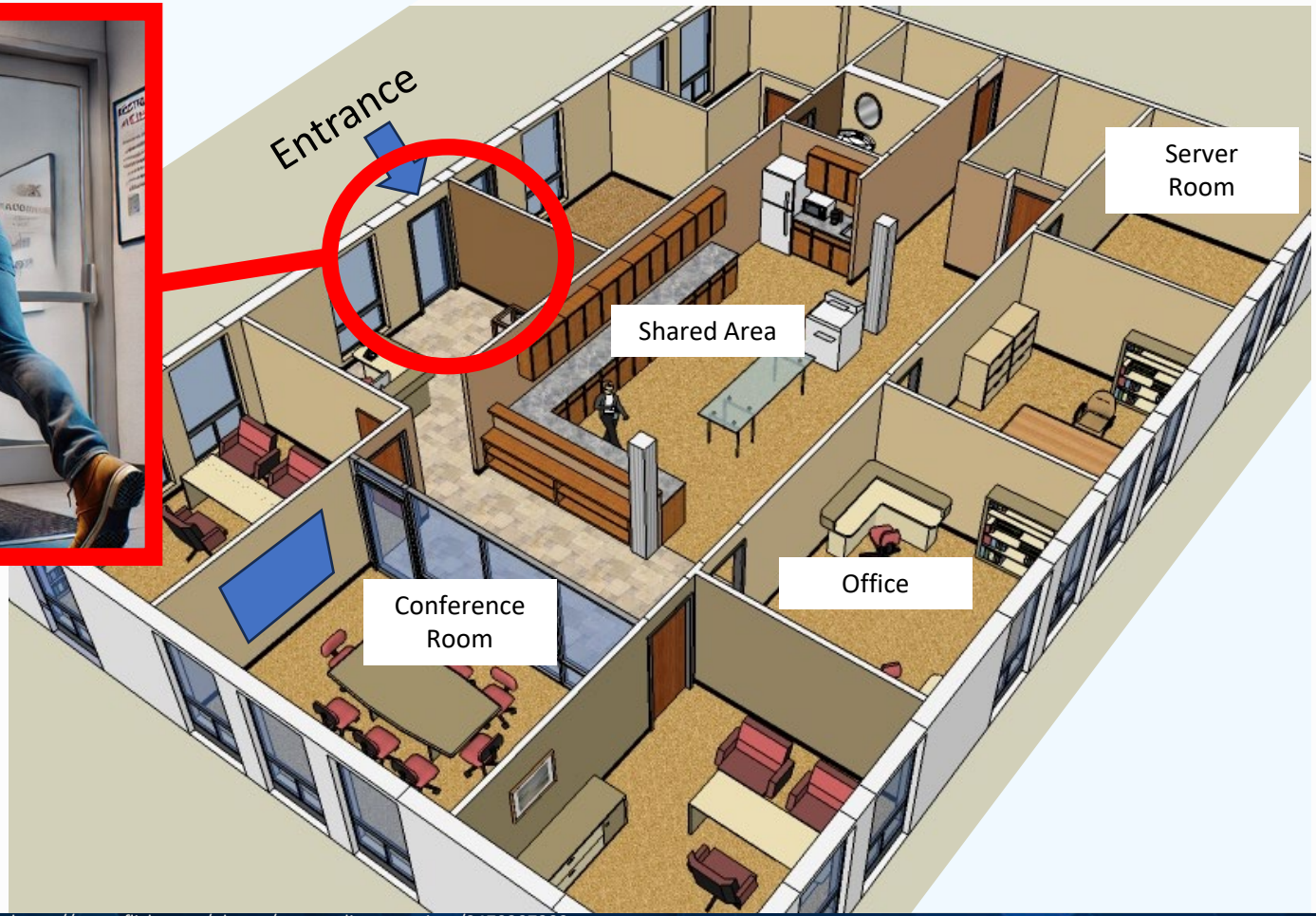
Typical Small Office



https://www.flickr.com/photos/newmediaconsortium/2479307399

Physical Security

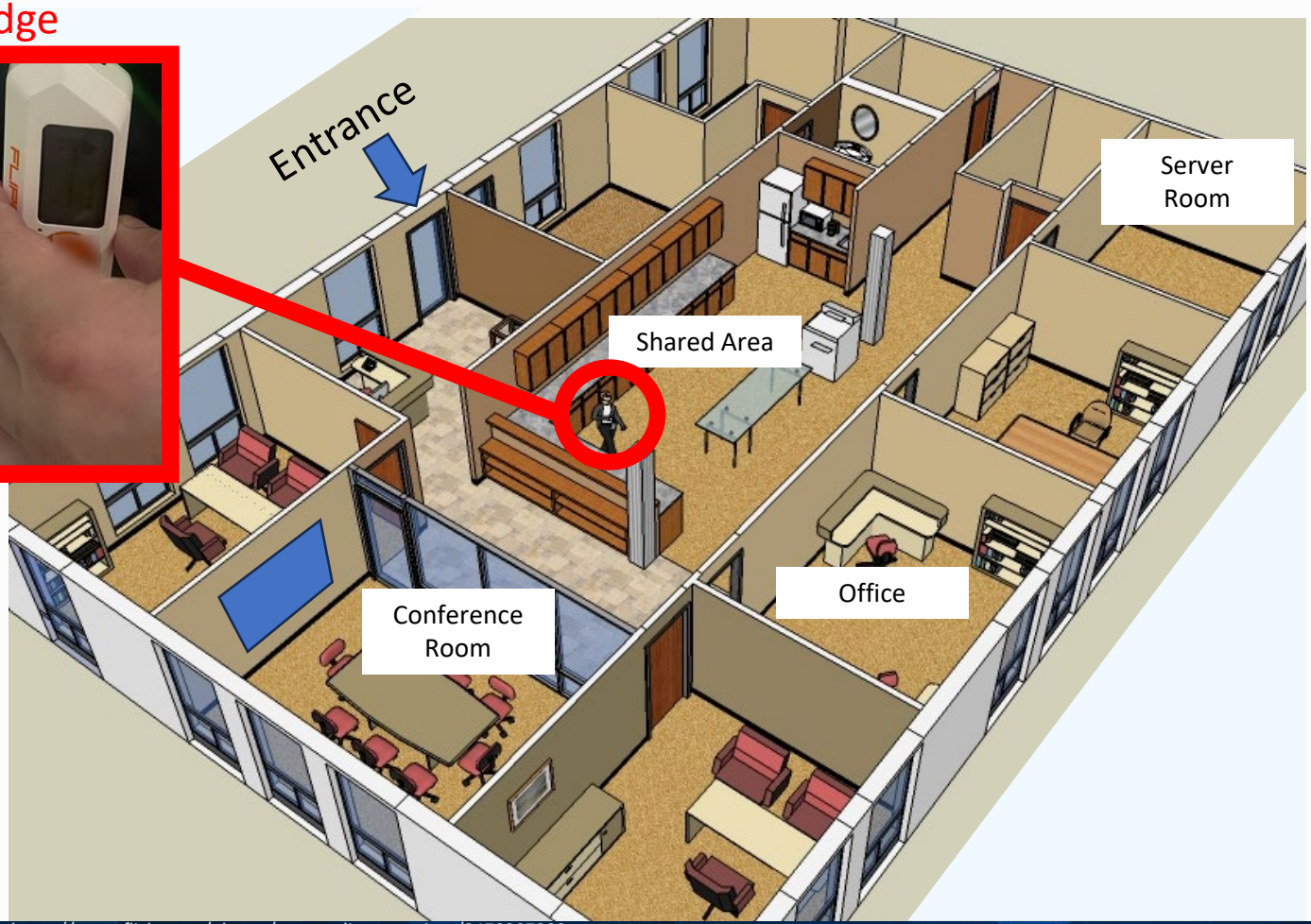
Tailgating Front Entrance



https://www.flickr.com/photos/newmediaconsortium/2479307399

Physical Security

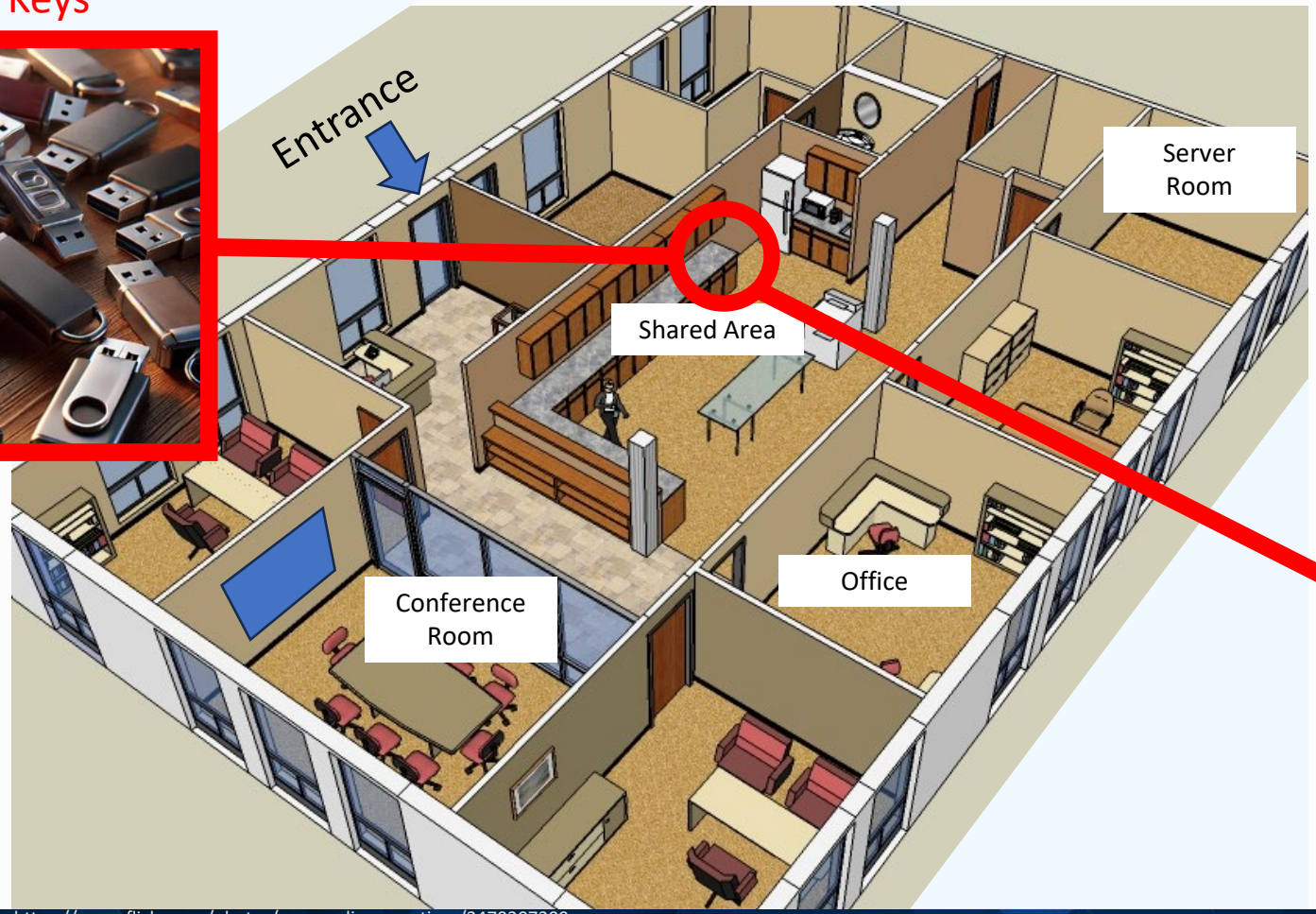
Cloning RFID Badge



https://www.flickr.com/photos/newmediaconsortium/2479307399

Physical Security

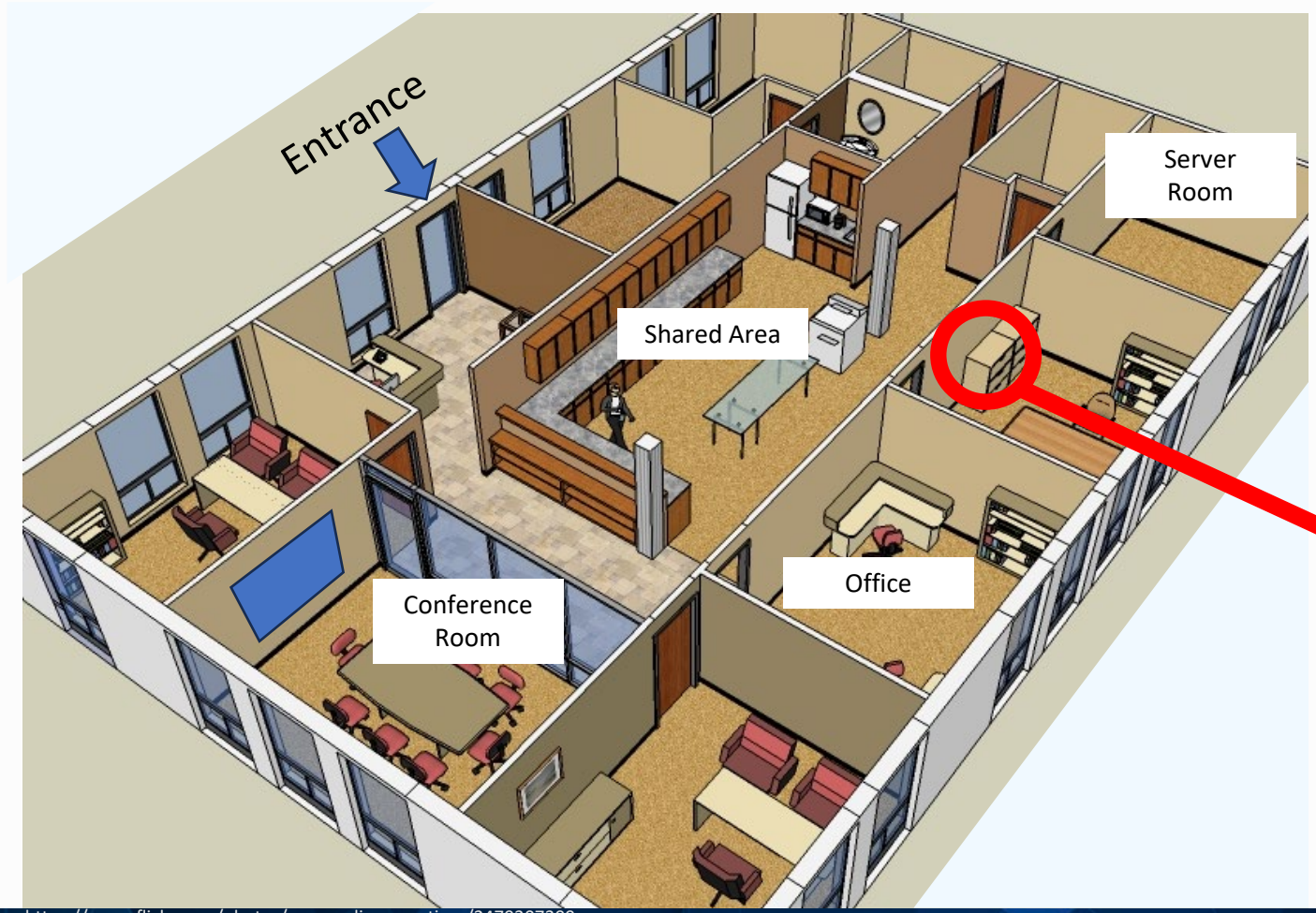
Malicious USB Keys



Remote Access USB Cables

https://www.flickr.com/photos/newmediaconsortium/2479307399

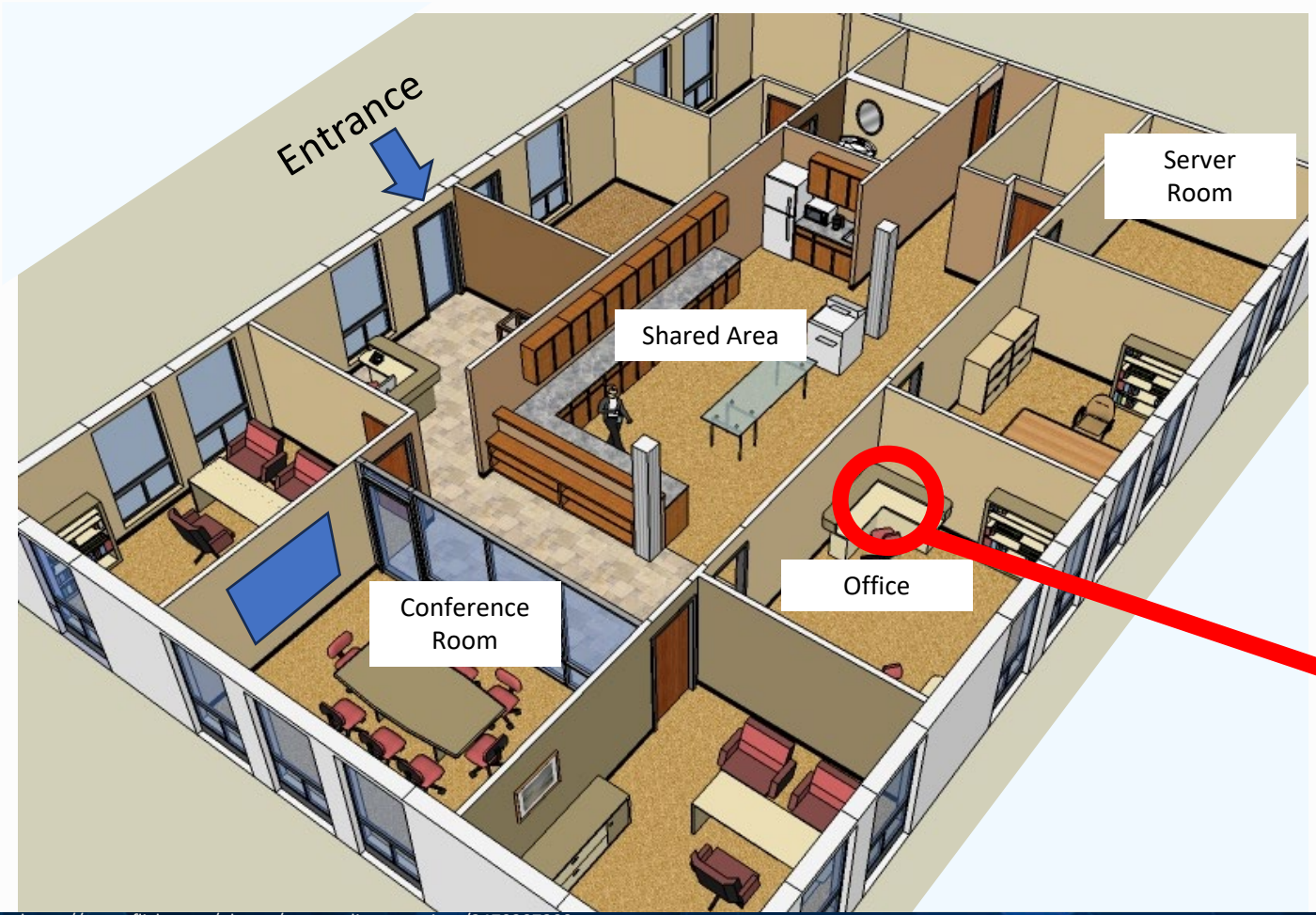
Physical Security



Filling Cabinets Left Unlocked

https://www.flickr.com/photos/newmediaconsortium/2479307399

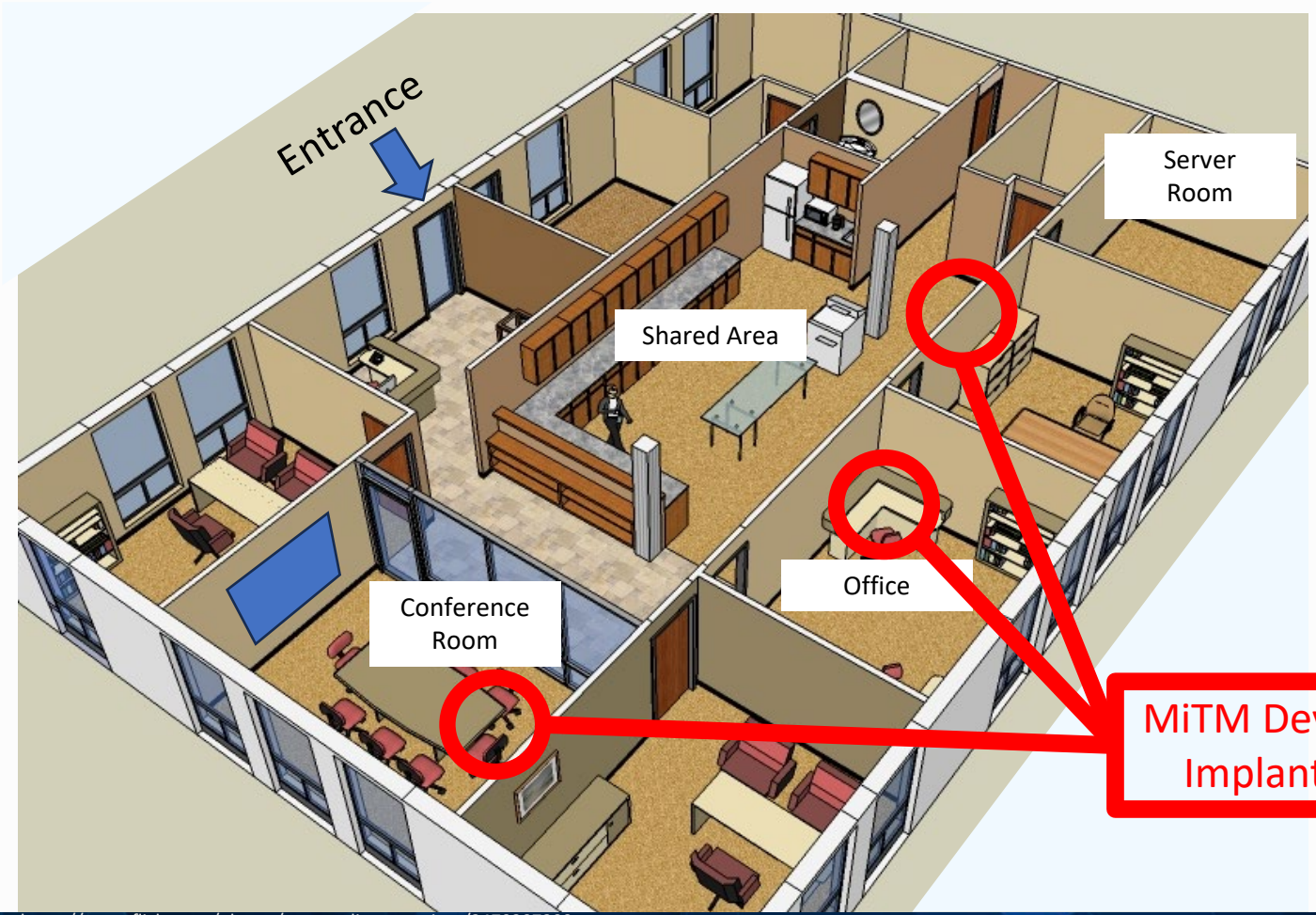
Physical Security



https://www.flickr.com/photos/newmediaconsortium/2479307399

Laptop Not Cable Locked

Physical Security



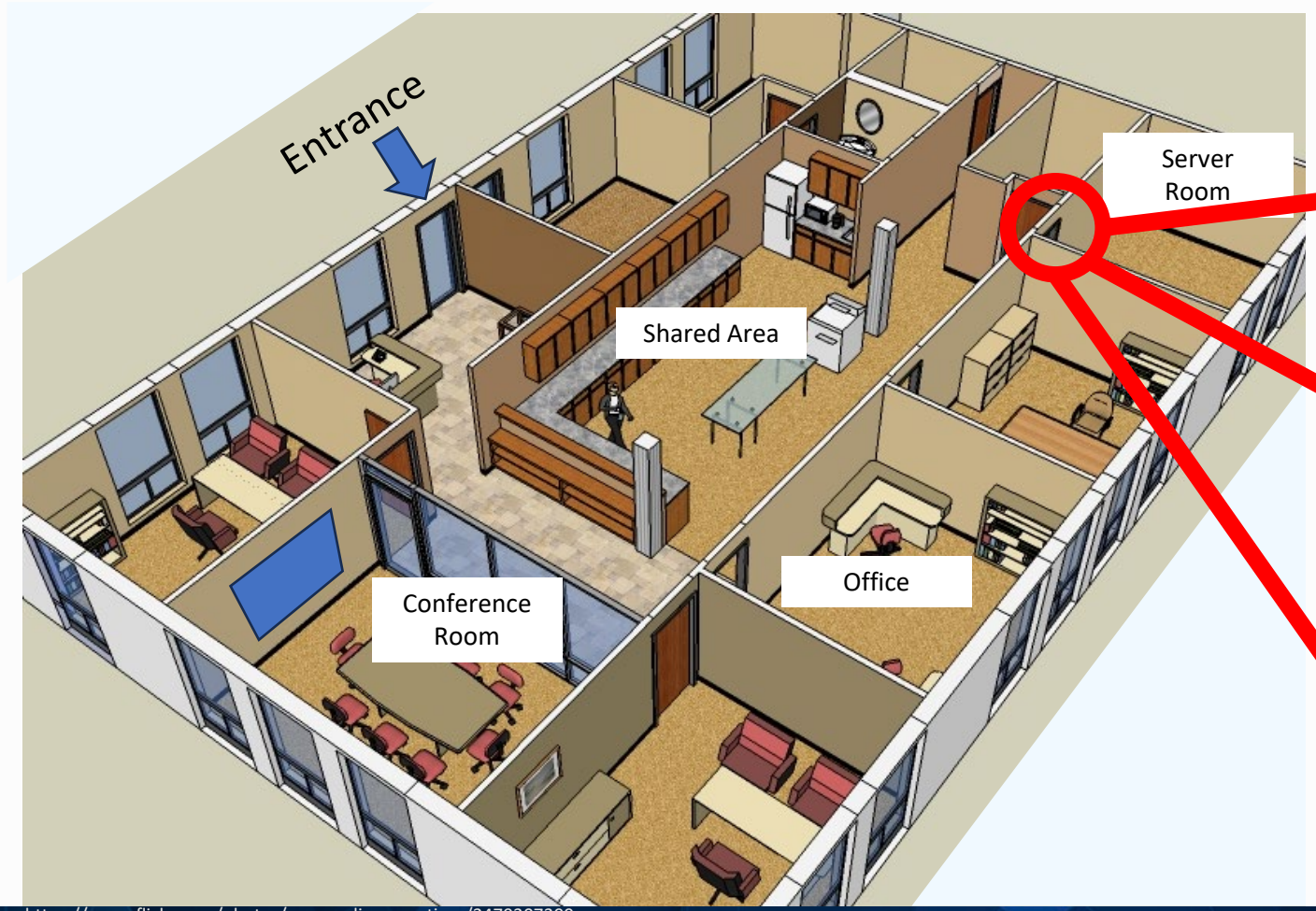
https://www.flickr.com/photos/newmediaconsortium/2479307399

MiTM Device Implants

Remote HDMI Monitoring

Lan Tap for Printers, PCs, Docking Stations

Physical Security



https://www.flickr.com/photos/newmediaconsortium/2479307399

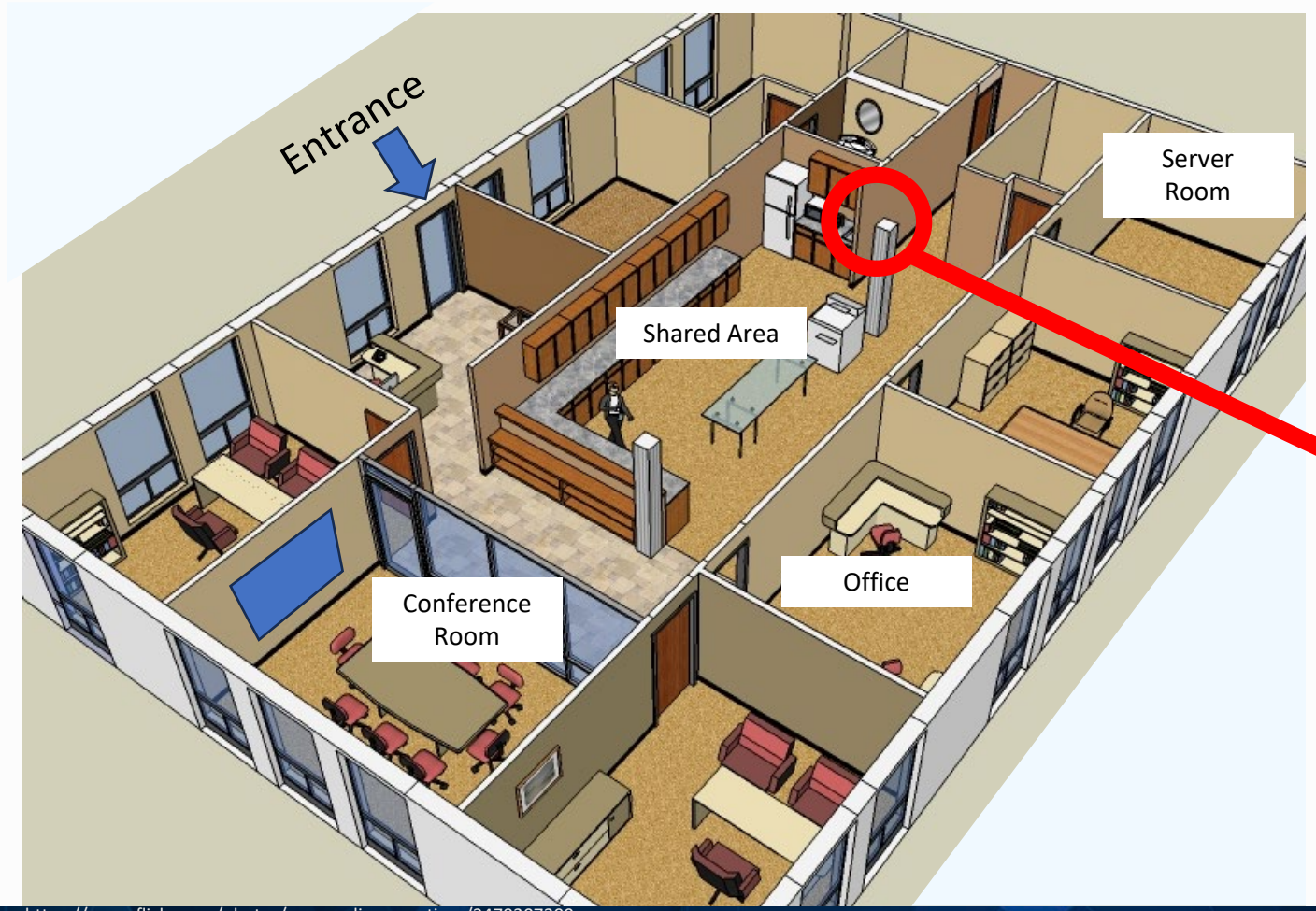
Server Room Door Propped Open

https://www.flickr.com/photos/chris_radcliff/172619346

Lack of CCTV

Easy to Pick Locks

Physical Security



https://www.flickr.com/photos/newmediaconsortium/2479307399

Wi-Fi Evil Twin

Thanks

Malleum
THE POWER TO KNOW AHEAD

300-116 Albert Street, Ottawa, ON, Canada, K1P 5G3

ashah@malleum.com

+1-877-RED-TEAM