From Lift-Off to Landing

Simple Security Improvements That Make a Big Difference

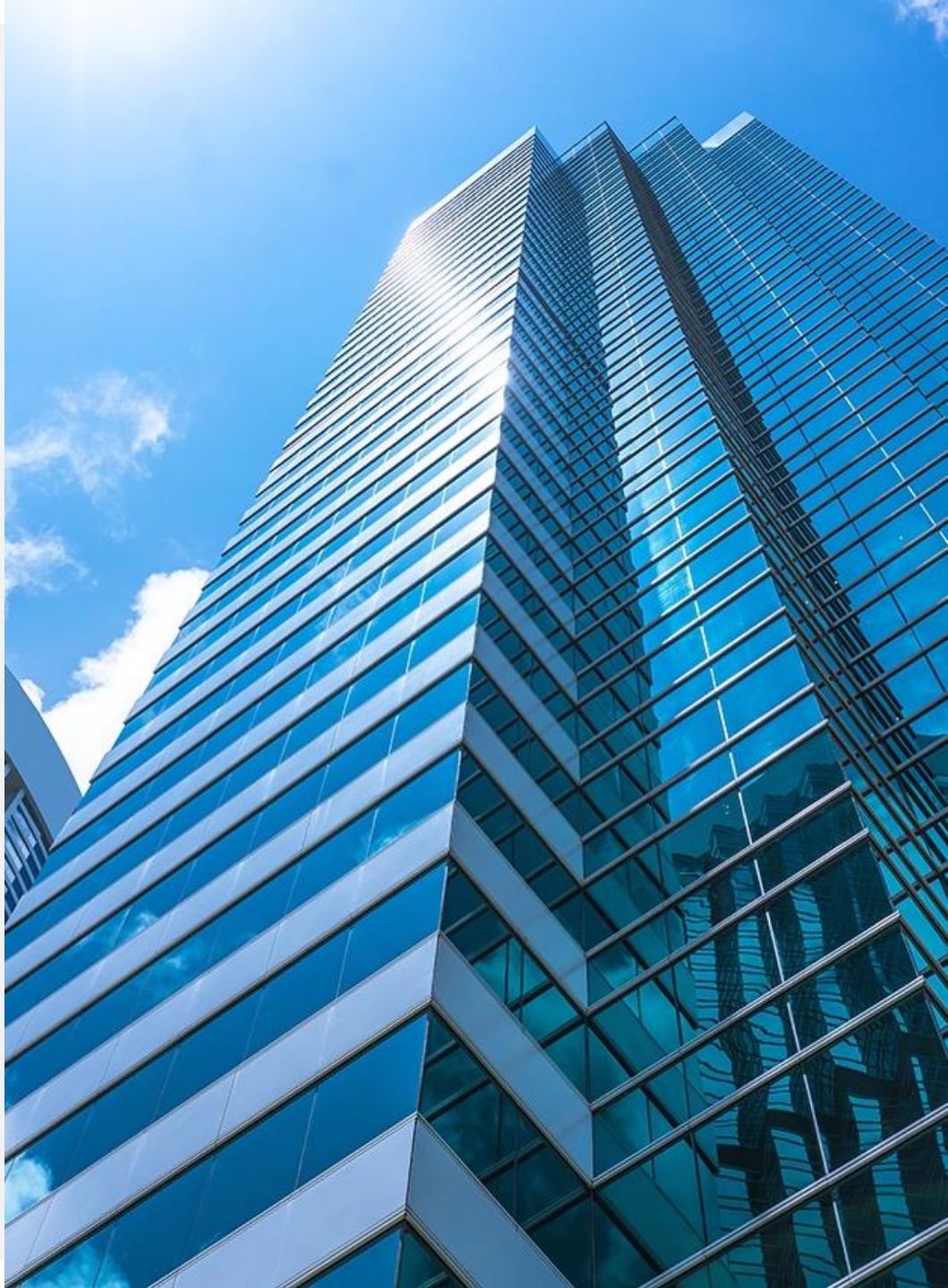
Nick Lloyd

Head of Modern Work & Security Pre-Sales

Callum Butler

Principal Security Engineer

Two Forces Reshaping the Threat Landscape

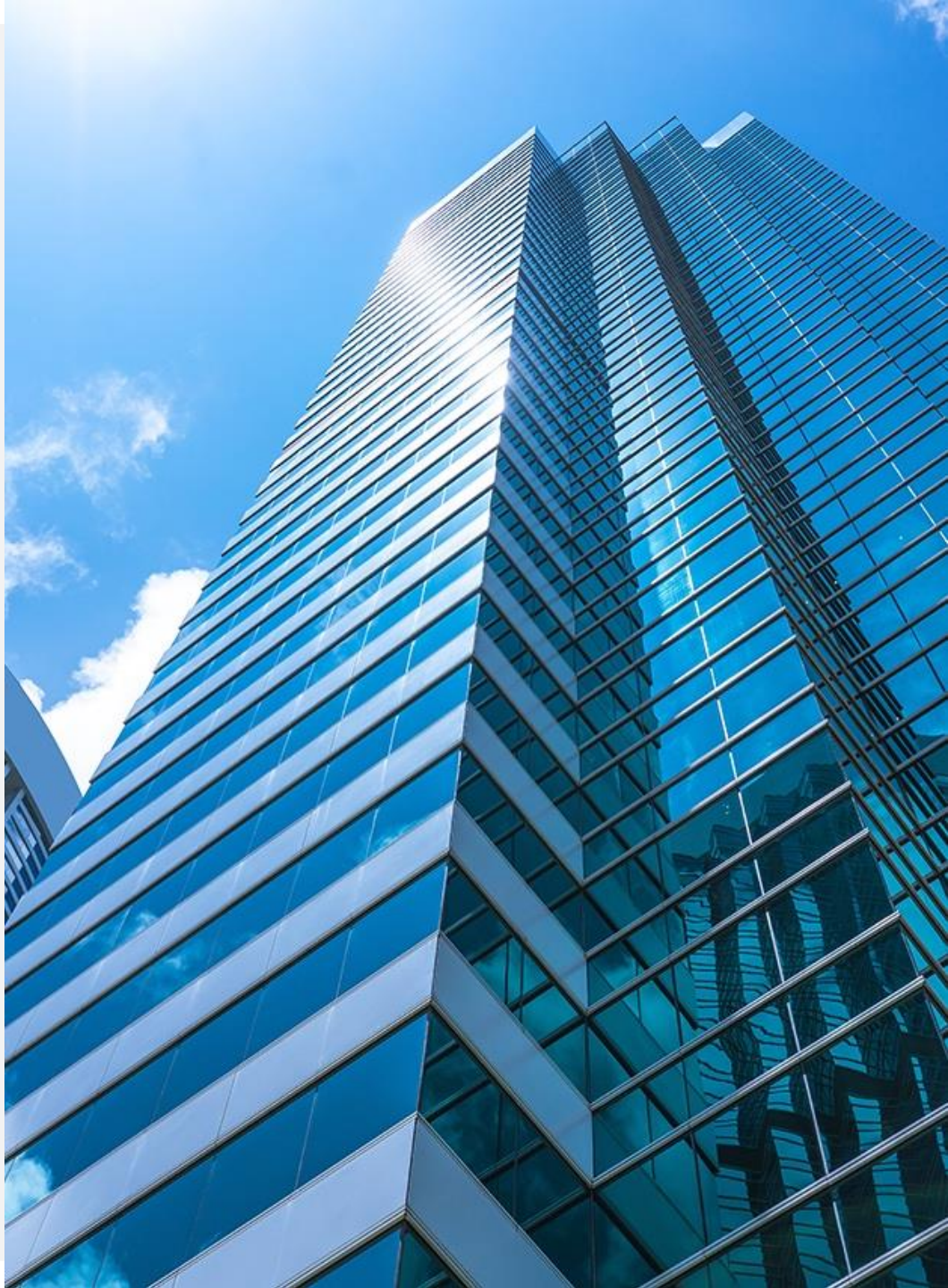


1

Two Forces Reshaping the Threat Landscape

Geopolitical Conflict

The Iran conflict (Operation Epic Fury / Roaring Lion, February 2026) has triggered a wave of retaliatory cyber operations targeting Western businesses and critical infrastructure.

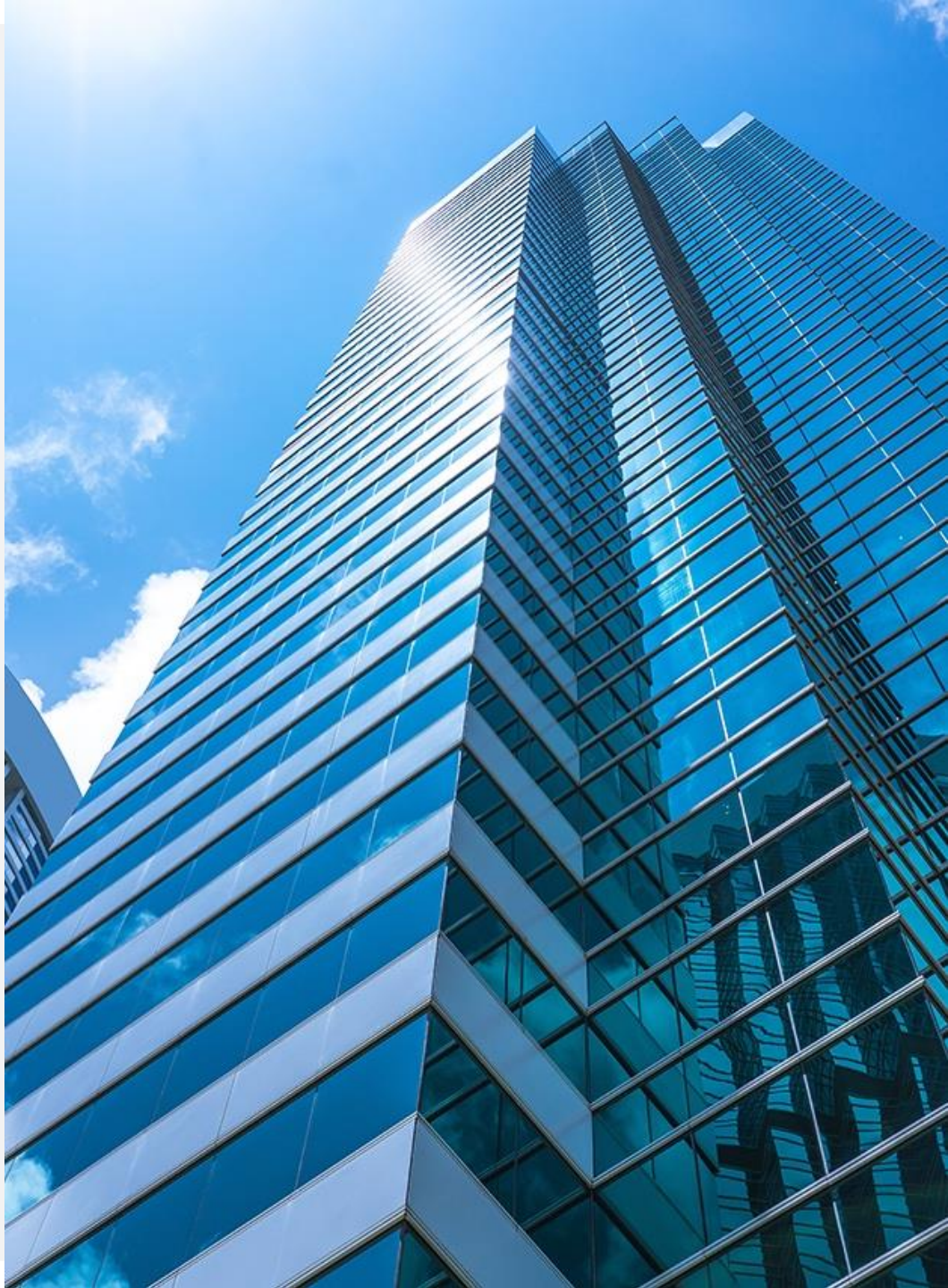


2

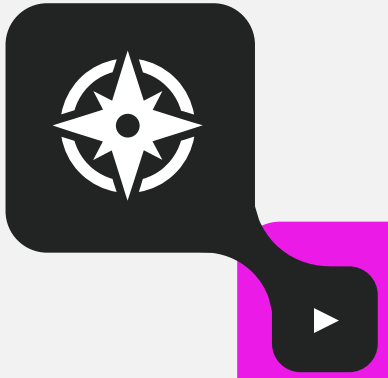
Two Forces Reshaping the Threat Landscape

AI-Powered Adversaries

Threat actors are weaponizing AI to operate faster, at greater scale, and with higher precision than ever before. Attack campaigns that once took weeks now take hours.

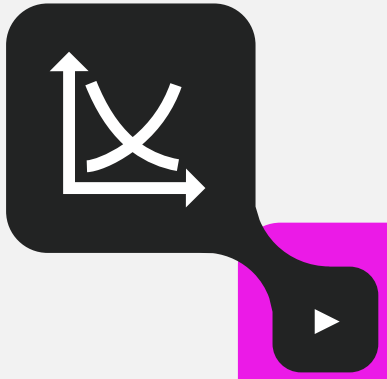


Understanding the Adversary



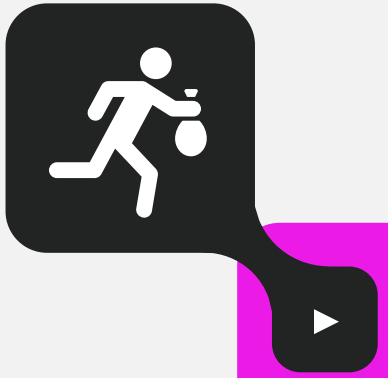
Nation-State Retaliation

Cyber is cheaper, deniable, and hits harder than traditional warfare



Financial Gain

Ransomware, data extortion, Cybercrime-as-a-Service



Espionage & IP Theft

State actors target trade secrets, defence data, and intelligence

Hacktivism & Influence

DDoS, defacement, hack-and-leak to shift public opinion

AI: The Adversary's New Force Multiplier

44% increase in attacks on public facing applications, driven by AI-Enabled Vulnerability Scanning, then publishing false content.

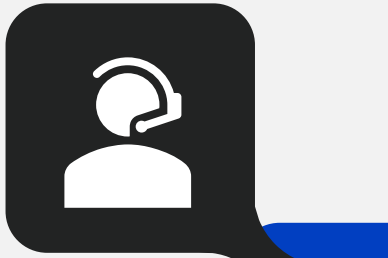
Death of “Spot the Phish”

AI Phishing Strips Away Old Tells

No typos, perfect branding, contextually relevant content

Deepfake Video Calls

Used to impersonate CFOs, CEOs, and senior leadership



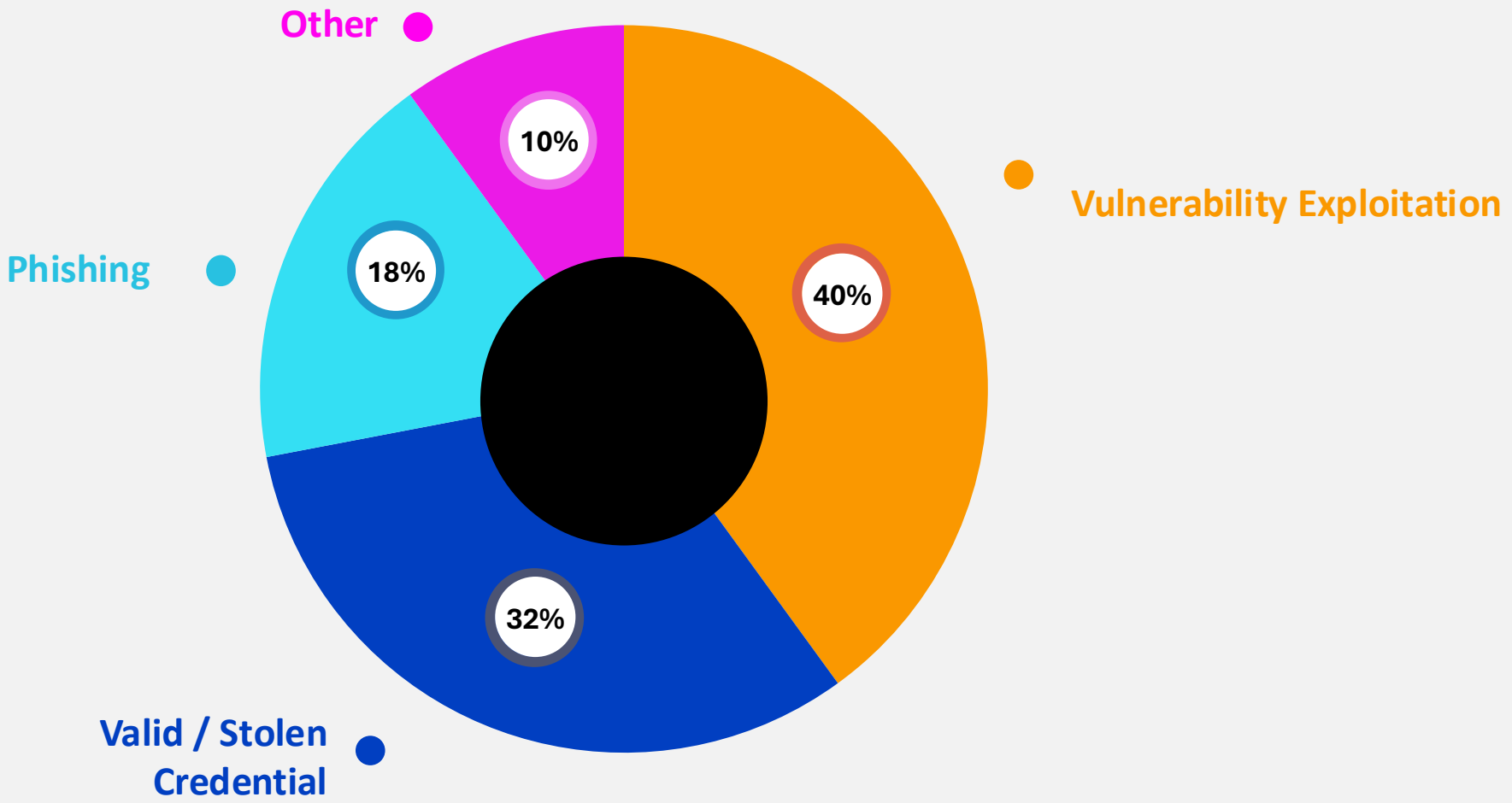
Voice Cloning

Enables real-time phone-based social engineering

Staff Training Alone is no Longer Sufficient

Layered technical controls are essential

How Attackers Get In



So how is this happening?

Your Domain

Is Their Weapon

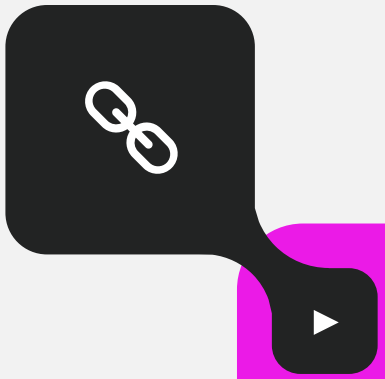
In plain terms: the signpost is still up, but the destination is empty — and anyone can move in and put their own content there, under the a trusted brand.

Subdomain Takeovers

"Its free real estate"

You decommission a cloud service

Azure, AWS, Github – Resource Deleted



You forget to remove the DNS Record

CNAME still pointing at nothing, dangling

Attacker claim it. Now it’s theirs

No Hacking. No access to your systems needed. Captured in less than 5 minutes

The Trust Problem

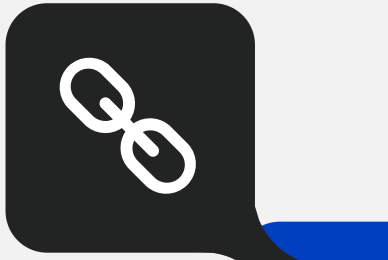
https://login-micr0s0ft-secure.xyz

Emails filters will catch this. Browser flags, and even Dave from accounts is going to catch this one

https://portal.yourcompany.com/login

Trust domain. Your Domain. Email Gateway waves it through, no one will question it.

Now Add AI

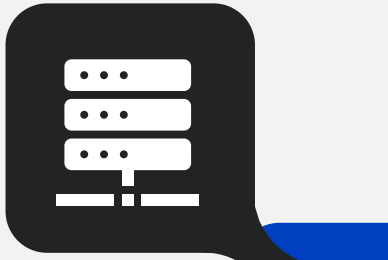


1. Takeover

Adversary claims the forgotten subdomain

2. Prompt

AI Builds login replica with logging mechanism



3. Deploy

Application is deployed to the captured instance

4. Harvest

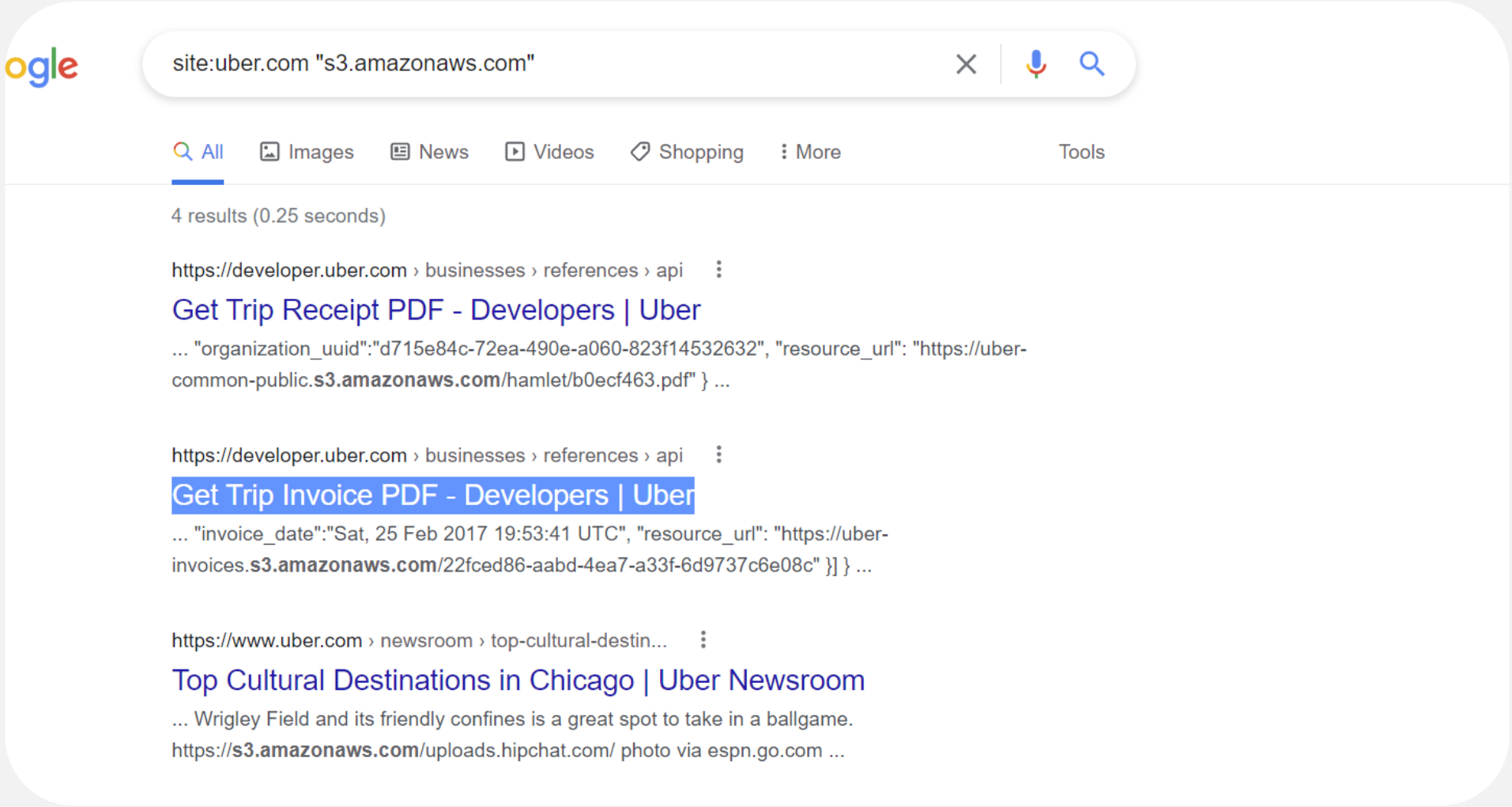
Data is fed back to a command and control. Credentials, Payment details etc.

This Isn’t Theoretical

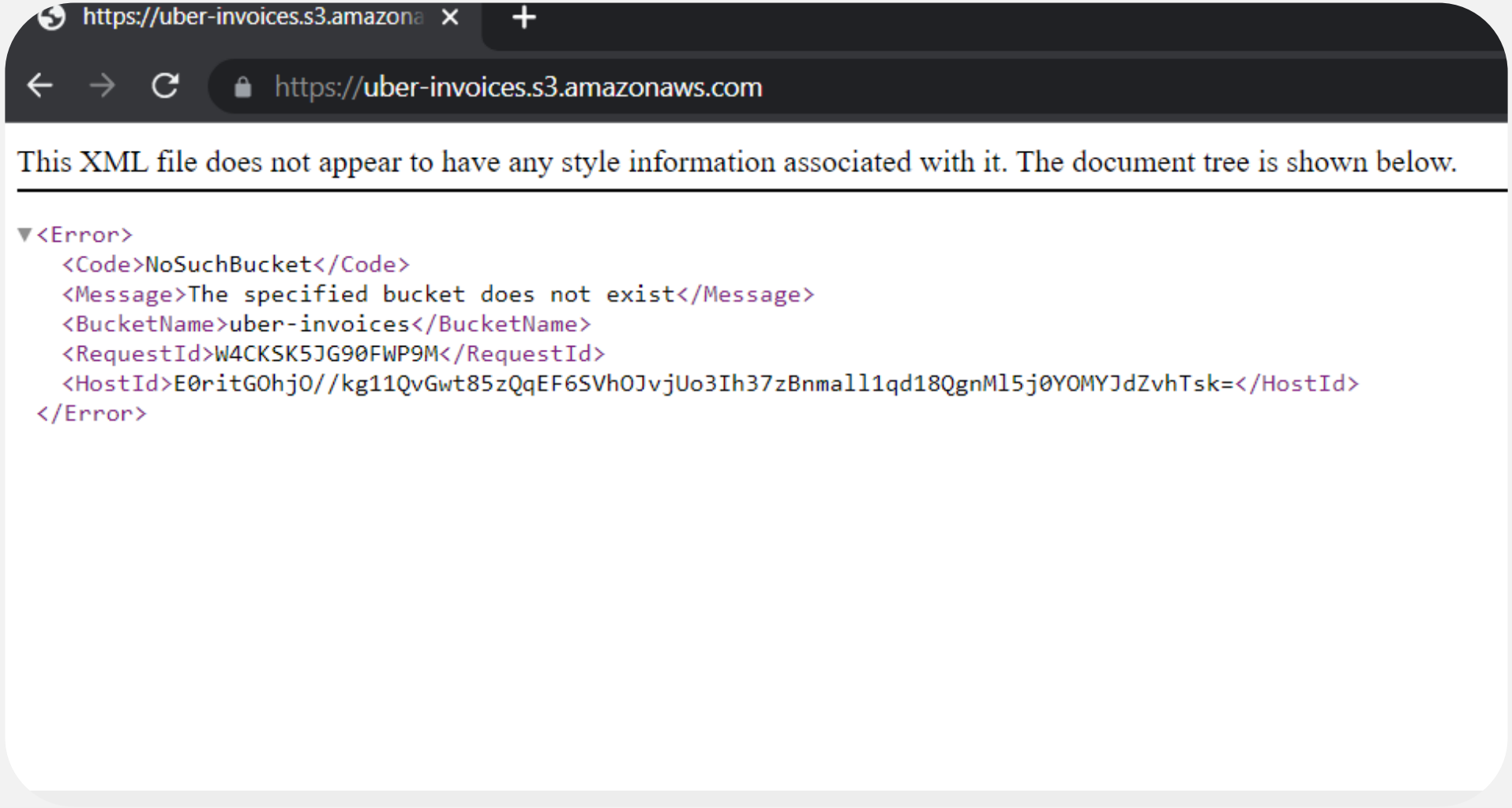
It’s a wide problem, only growing as business grow

- 34x US Universities Compromised
- 2,000+ exploitable DNS records at ONE organisation
- Attacks are happening, now

Let’s See It For Real



Let’s See It For Real



Register > Upload > Serve

Let’s See It For Real

Only a S3 bucket… What’s the harm… Right?

Ooh no……

er	operation	useragent	request_uri
	REST.GET.OBJECT	"MobileSafari/604.1 CFNetwork/978.0.7 Darwin/18.7.0"	"GET /favicon.ico HTTP/1.1"
	REST.GET.OBJECT	"MobileSafari/604.1 CFNetwork/978.0.7 Darwin/18.7.0"	"GET /favicon.ico HTTP/1.1"
	REST.GET.OBJECT	"Mozilla/5.0 (iPad; CPU OS 12_5_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.2 Mobile/15E148 Safari/604.1"	"GET /d2a15e04-7c2d-41fc-81b2-9abb4ec98e8d?Signature=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX&Expires=1474815844&AWSAccessl
	REST.GET.OBJECT	"MobileSafari/604.1 CFNetwork/978.0.7 Darwin/18.7.0"	"GET /apple-touch-icon.png HTTP/1.1"
	REST.GET.OBJECT	"MobileSafari/604.1 CFNetwork/978.0.7 Darwin/18.7.0"	"GET /apple-touch-icon.png HTTP/1.1"
	REST.GET.OBJECT	"MobileSafari/604.1 CFNetwork/978.0.7 Darwin/18.7.0"	"GET /apple-touch-icon-precomposed.png HTTP/1.1"
	REST.GET.OBJECT	"MobileSafari/604.1 CFNetwork/978.0.7 Darwin/18.7.0"	"GET /apple-touch-icon-precomposed.png HTTP/1.1"
	REST.GET.OBJECT	"MobileSafari/604.1 CFNetwork/978.0.7 Darwin/18.7.0"	"GET /apple-touch-icon-152x152.png HTTP/1.1"
	REST.GET.OBJECT	"MobileSafari/604.1 CFNetwork/978.0.7 Darwin/18.7.0"	"GET /apple-touch-icon-152x152.png HTTP/1.1"
	REST.GET.OBJECT	"MobileSafari/604.1 CFNetwork/978.0.7 Darwin/18.7.0"	"GET /apple-touch-icon-152x152-precomposed.png HTTP/1.1"
	REST.GET.OBJECT	"MobileSafari/604.1 CFNetwork/978.0.7 Darwin/18.7.0"	"GET /apple-touch-icon-152x152-precomposed.png HTTP/1.1"

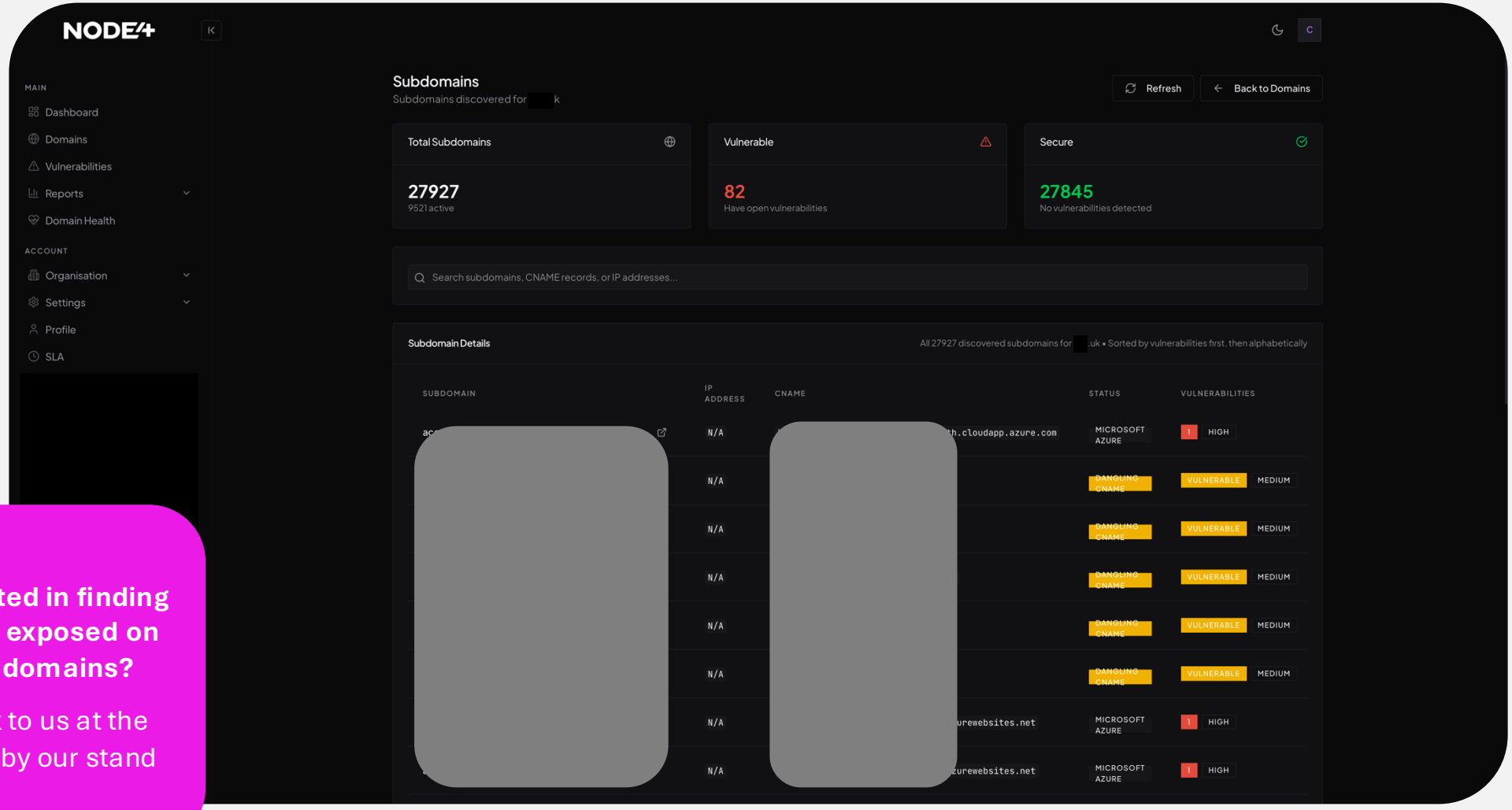
We often see these services be linked to a lot more…

That’s not good….

[redacted].53	"https://uber-invoices.s3.amazonaws.com/"	REST.GET.OBJECT	"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36"
[redacted].53	"https://t3.uberinternal.com/"	REST.GET.BUCKET	"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36"
	"https://uber-invoices.s3.amazonaws.com/"	REST.GET.OBJECT	"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36"
	"https://t3.uberinternal.com/"	REST.GET.BUCKET	"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36"

Now imagine this being your business… what could an adversary get?

The Scale Of The Problem



Interested in finding what's exposed on your domains?

Speak to us at the end or by our stand

Detection Isn’t Enough

Detect The Risk

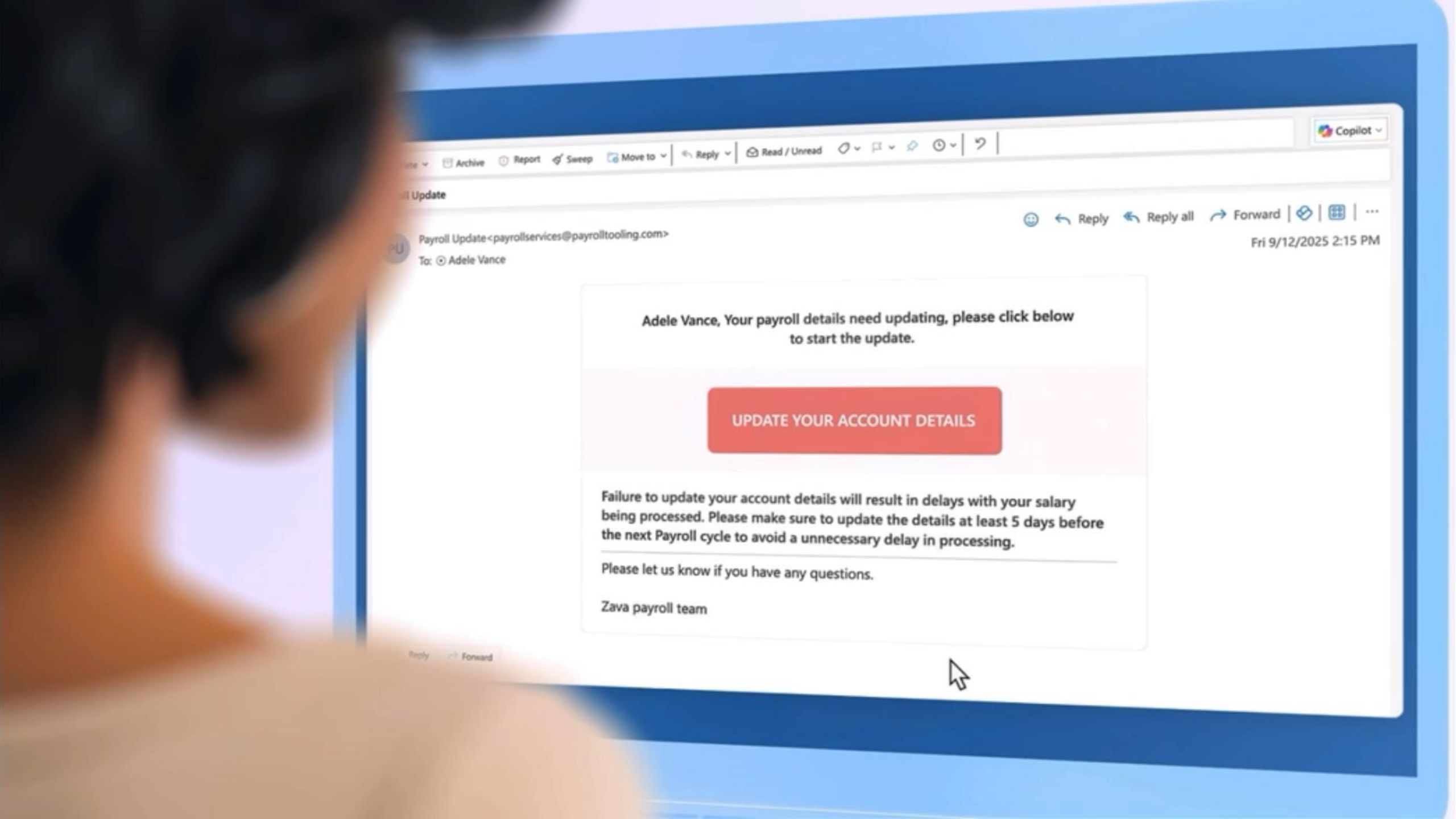
- Monitor Attack Surface
- Find Dangling DNS
- Watch CT Logs

Make Credentials Worthless

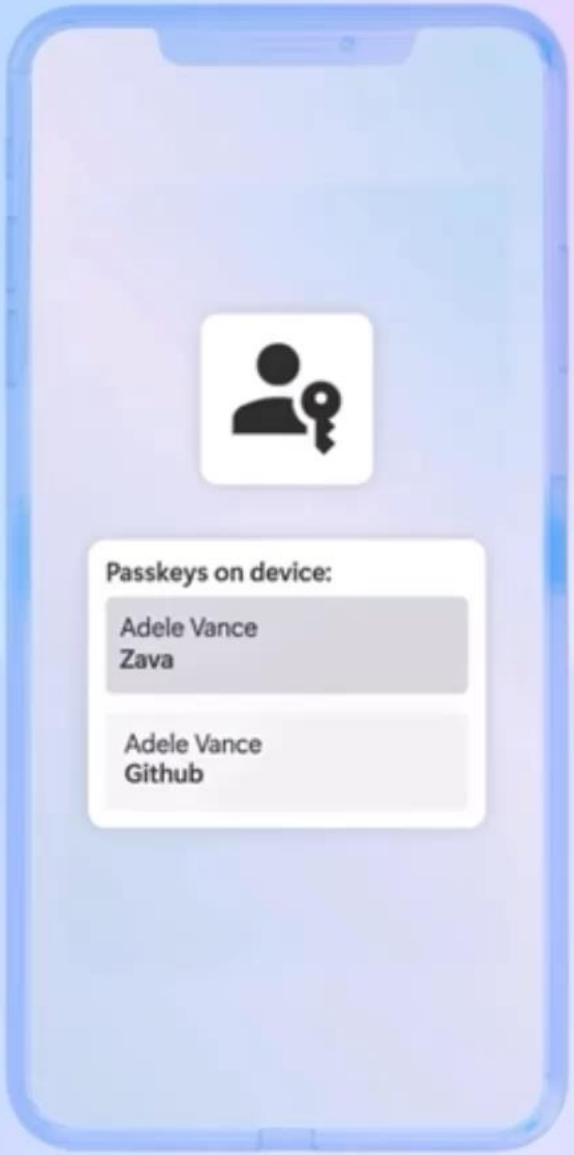
- SSO & Passkeys
- Conditional Access
- Device Compliance

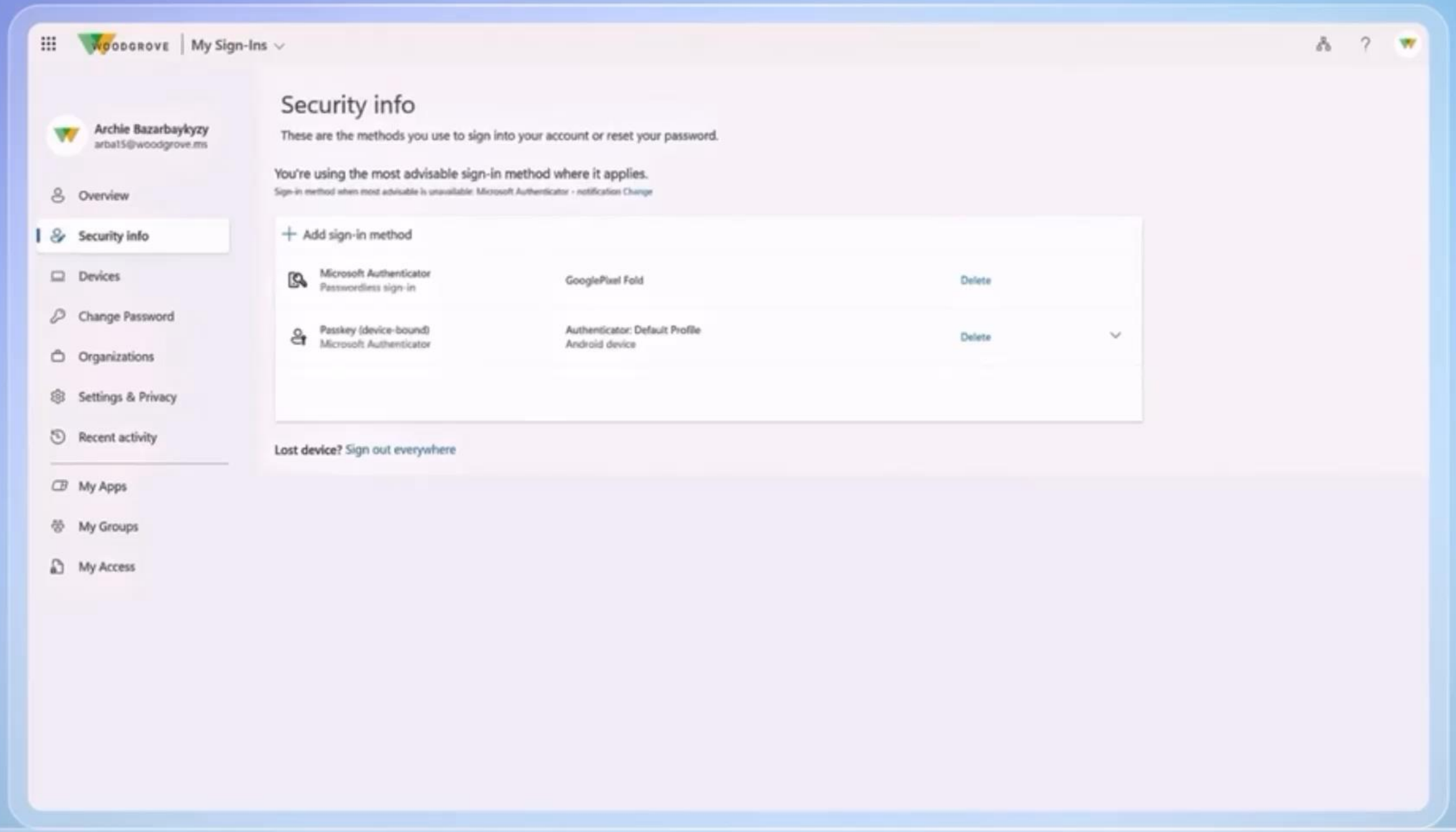
Demo Time

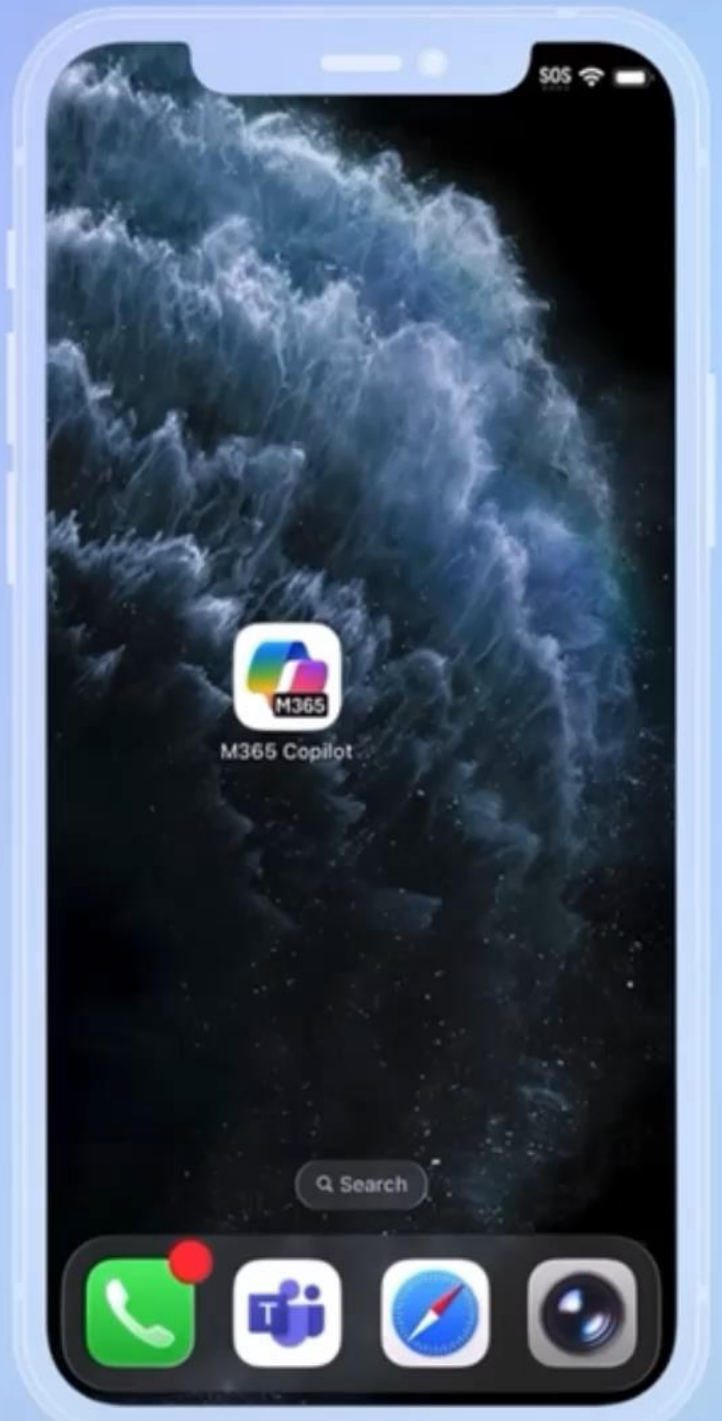
Beyond MFA

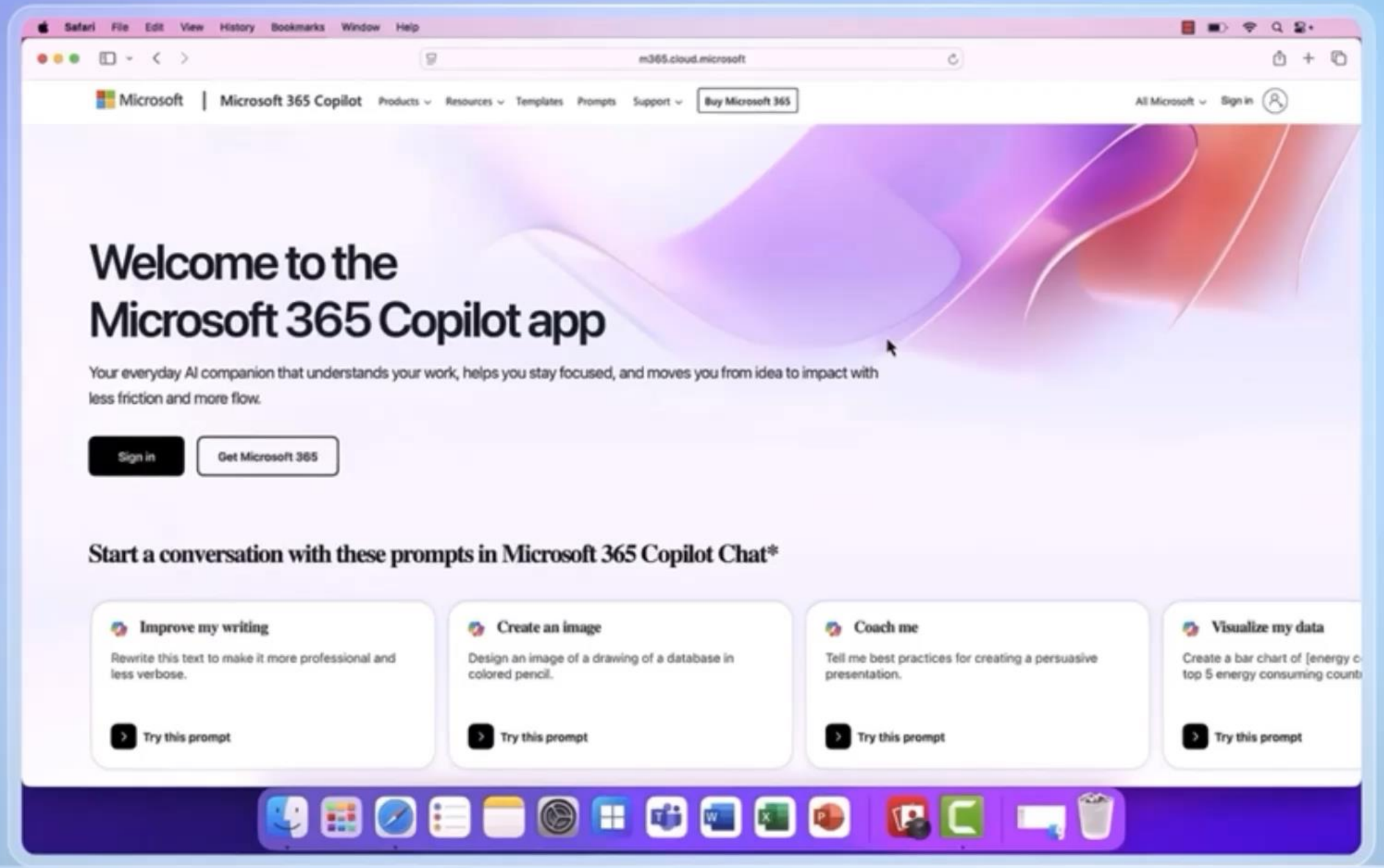

Archive
Report
Sweep
Move to
Reply
Read / Unread
Copilot
Update
Reply
Reply all
Forward
Payroll Update<payrollservices@payrolltooling.com>
To: Adele Vance
Fri 9/12/2025 2:15 PM
Adele Vance, Your payroll details need updating, please click below to start the update.
UPDATE YOUR ACCOUNT DETAILS
Failure to update your account details will result in delays with your salary being processed. Please make sure to update the details at least 5 days before the next Payroll cycle to avoid a unnecessary delay in processing.
Please let us know if you have any questions.
Zava payroll team

Device-bound passkeys

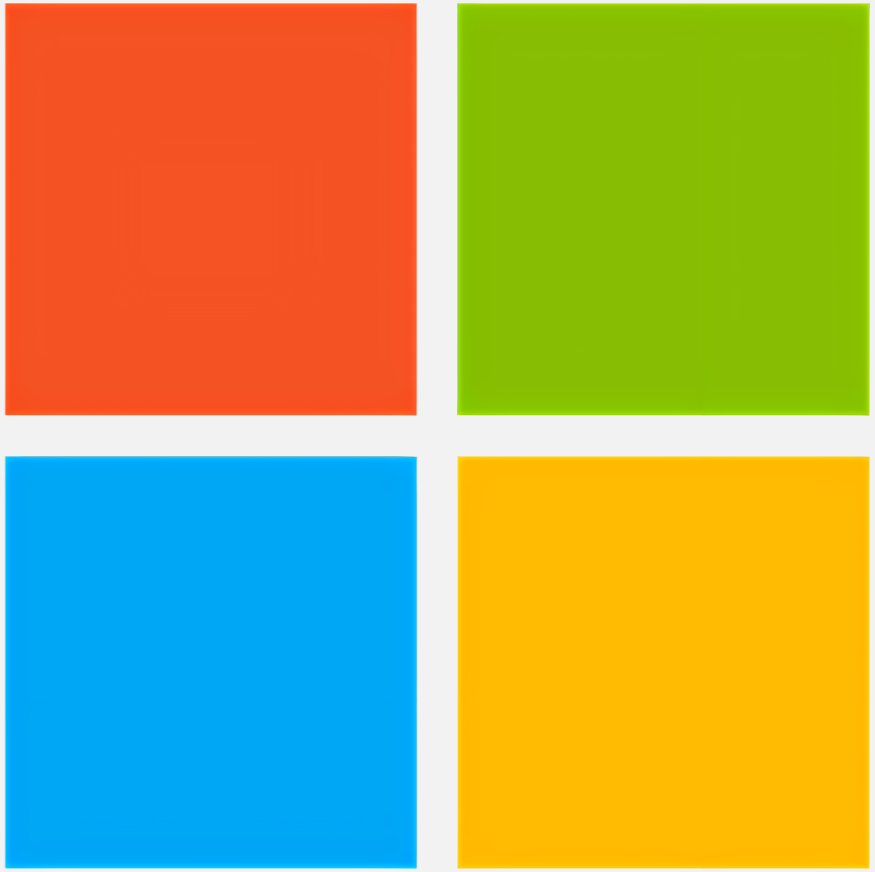



WOODGROVE
My Sign-Ins
Archie Bazarbaykyzy
arba15@woodgrove.ms
Overview
Security info
Devices
Change Password
Organizations
Settings & Privacy
Recent activity
My Apps
My Groups
My Access
Security info
These are the methods you use to sign into your account or reset your password.
You're using the most advisable sign-in method where it applies.
Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification Change
Add sign-in method
Microsoft Authenticator
Passwordless sign-in
GooglePixel Fold
Delete
Passkey (device-bound)
Microsoft Authenticator
Authenticator: Default Profile
Android device
Delete
Lost device? Sign out everywhere

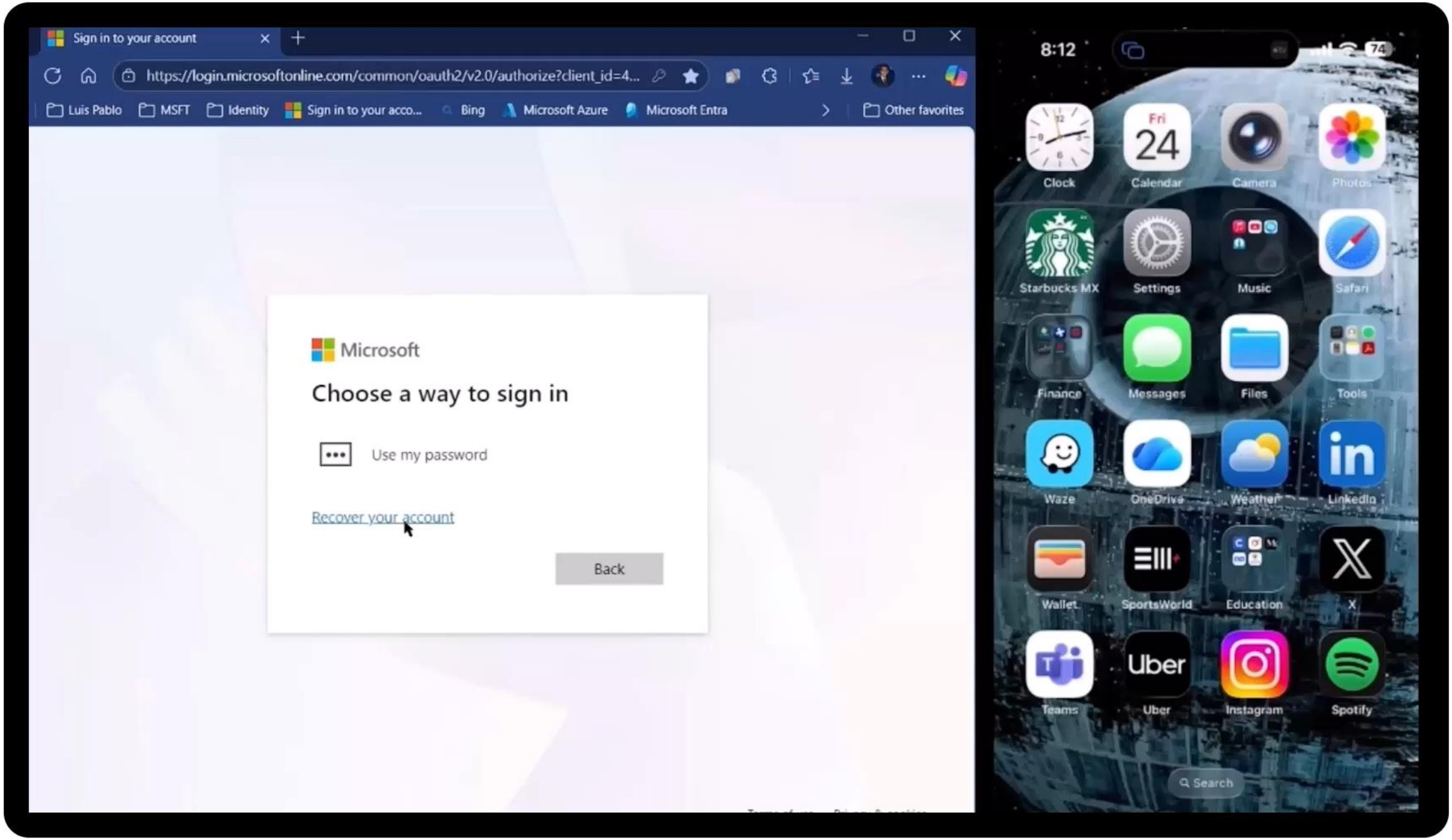

SOS
M365
M365 Copilot
Search

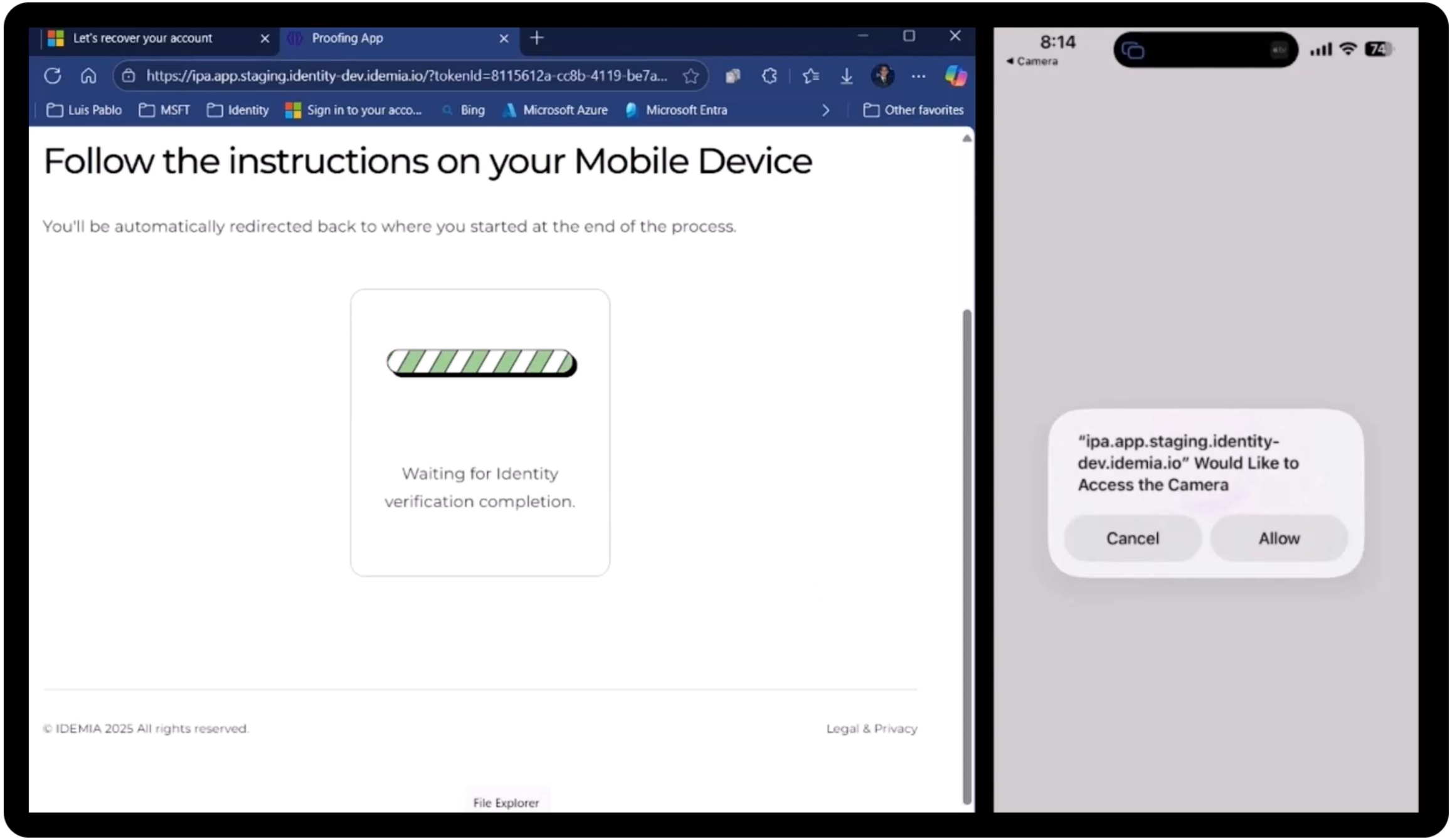

Safari File Edit View History Bookmarks Window Help
m365.cloud.microsoft
Microsoft | Microsoft 365 Copilot
Products Resources Templates Prompts Support
Buy Microsoft 365
All Microsoft
Sign in
Welcome to the Microsoft 365 Copilot app
Your everyday AI companion that understands your work, helps you stay focused, and moves you from idea to impact with less friction and more flow.
Sign in
Get Microsoft 365
Start a conversation with these prompts in Microsoft 365 Copilot Chat*
Improve my writing
Rewrite this text to make it more professional and less verbose.
Try this prompt
Create an image
Design an image of a drawing of a database in colored pencil.
Try this prompt
Coach me
Tell me best practices for creating a persuasive presentation.
Try this prompt
Visualize my data
Create a bar chart of [energy c
top 5 energy consuming count
Try this prompt

VS



Face ID


Sign in to your account
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4...
Luis Pablo
MSFT
Identity
Sign in to your acco...
Bing
Microsoft Azure
Microsoft Entra
Other favorites
Microsoft
Choose a way to sign in
Use my password
Recover your account
Back
8:12
Clock
Calendar
Camera
Photos
Starbucks MX
Settings
Music
Safari
Finance
Messages
Files
Tools
Waze
OneDrive
Weather
LinkedIn
Wallet
SportsWorld
Education
X
Teams
Uber
Instagram
Spotify
Search


Let's recover your account
Proofing App
https://ipa.app.staging.identity-dev.idemia.io/?tokenId=8115612a-cc8b-4119-be7a...
Luis Pablo
MSFT
Identity
Sign in to your acco...
Bing
Microsoft Azure
Microsoft Entra
Other favorites
Follow the instructions on your Mobile Device
You'll be automatically redirected back to where you started at the end of the process.
Waiting for Identity verification completion.
© IDEMIA 2025 All rights reserved.
Legal & Privacy
File Explorer
8:14
Camera
"ipa.app.staging.identity-dev.idemia.io" Would Like to Access the Camera
Cancel
Allow

Let's recover your account | Proofing App

https://ipa.app.staging.identity-dev.idemia.io/?tokenId=8115612a-cc8b-4119-be7a...

Luis Pablo | MSFT | Identity | Sign in to your acco... | Bing | Microsoft Azure | Microsoft Entra | Other favorites

Follow the instructions on your Mobile Device

You'll be automatically redirected back to where you started at the end of the process.

Waiting for Identity verification completion.

Legal & Privacy

File Explorer

8:14

Camera

EN

BY IDEMIA

Review the results.

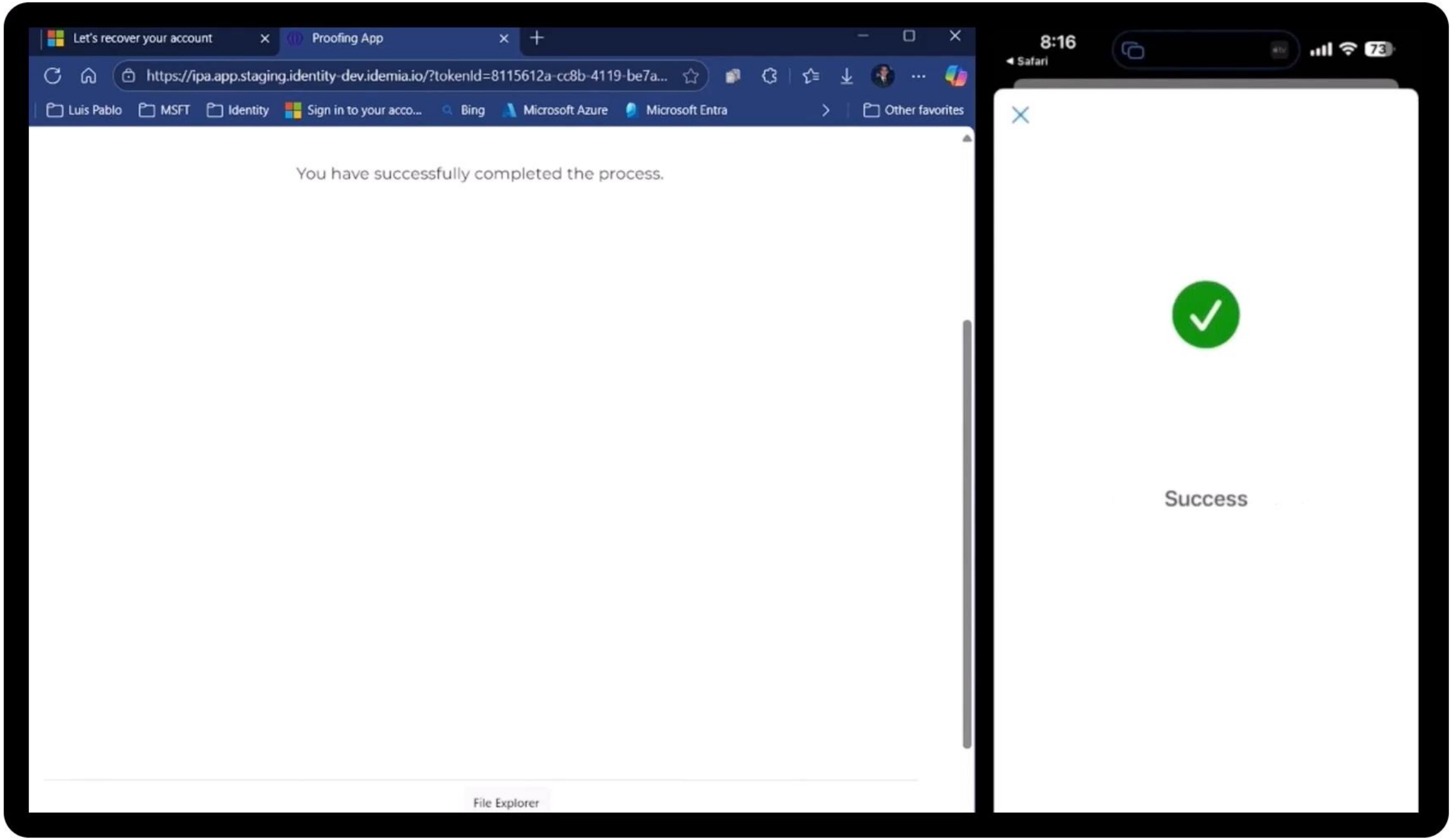
Before submitting photos, make sure that:

- **All corners are visible**
- **All data is visible (nothing is covered)**
- **No glares and shadows**

Front

Submit photos

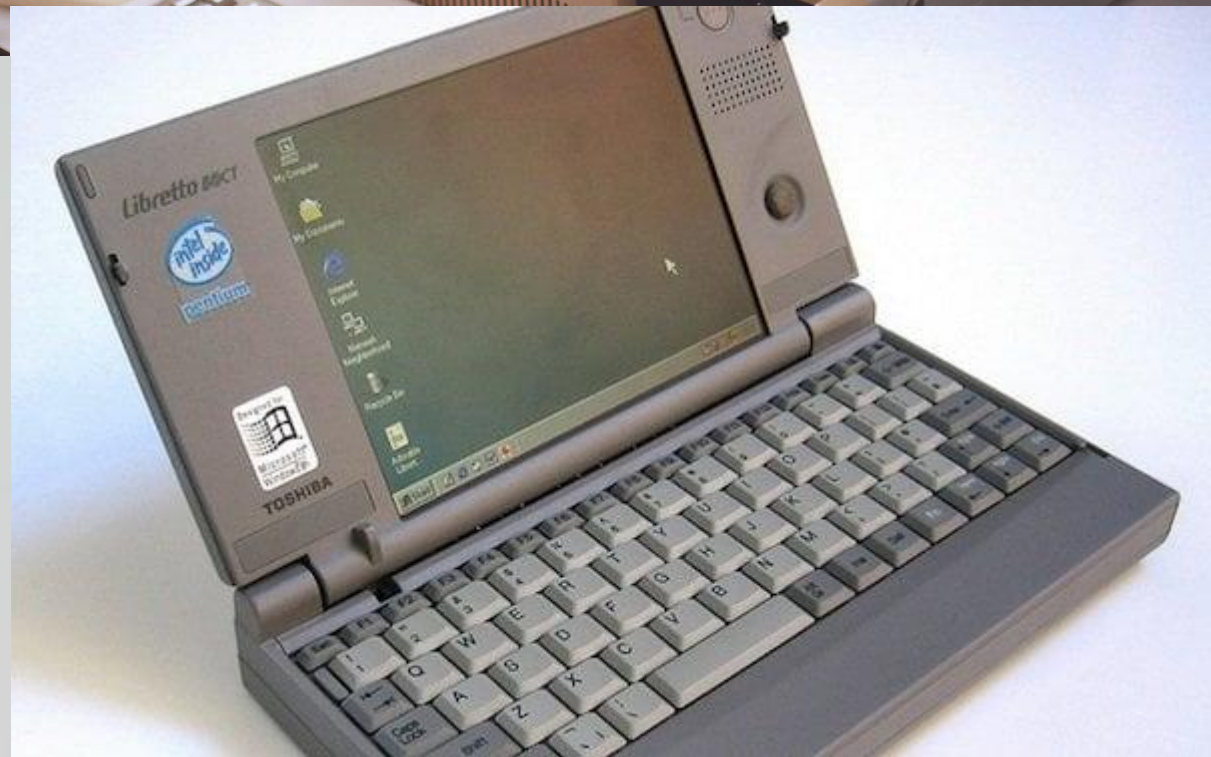
Retake photo

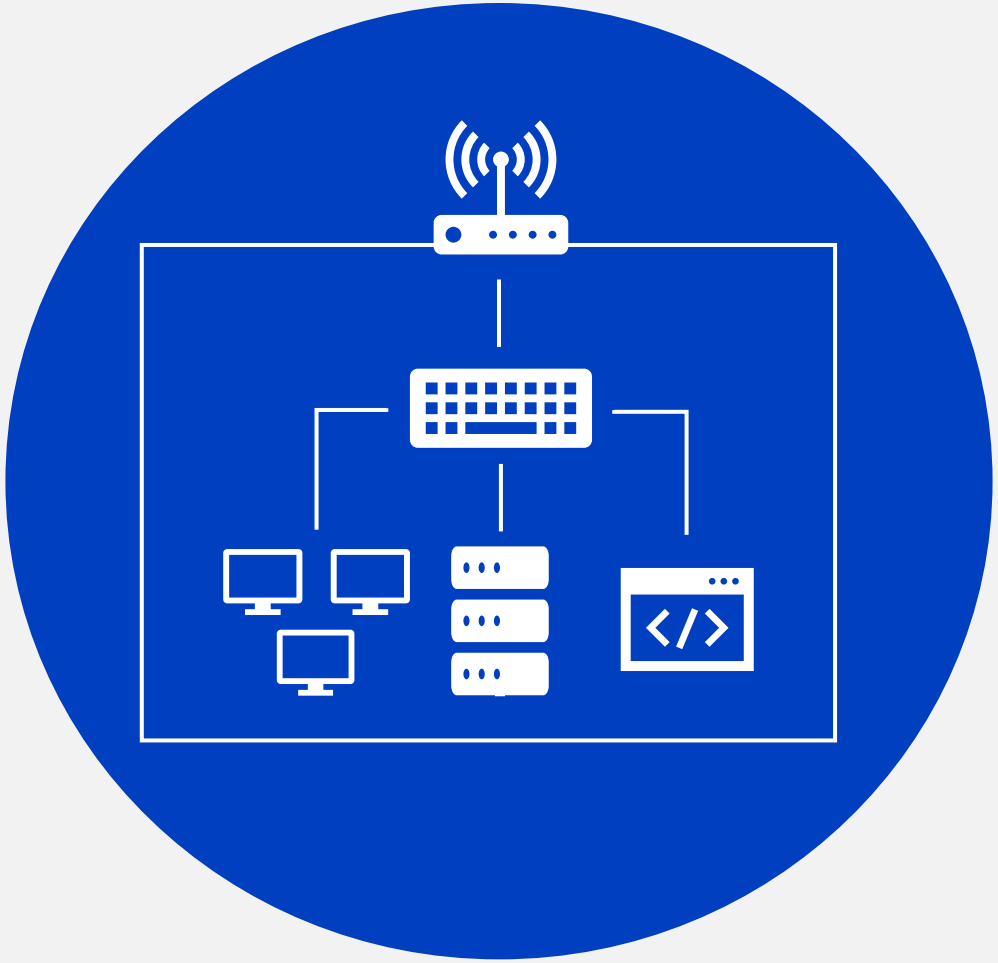

Let's recover your account
Proofing App
https://ipa.app.staging.identity-dev.idemia.io/?tokenId=8115612a-cc8b-4119-be7a...
Luis Pablo
MSFT
Identity
Sign in to your acco...
Bing
Microsoft Azure
Microsoft Entra
Other favorites
You have successfully completed the process.
File Explorer
8:16
Safari
Success

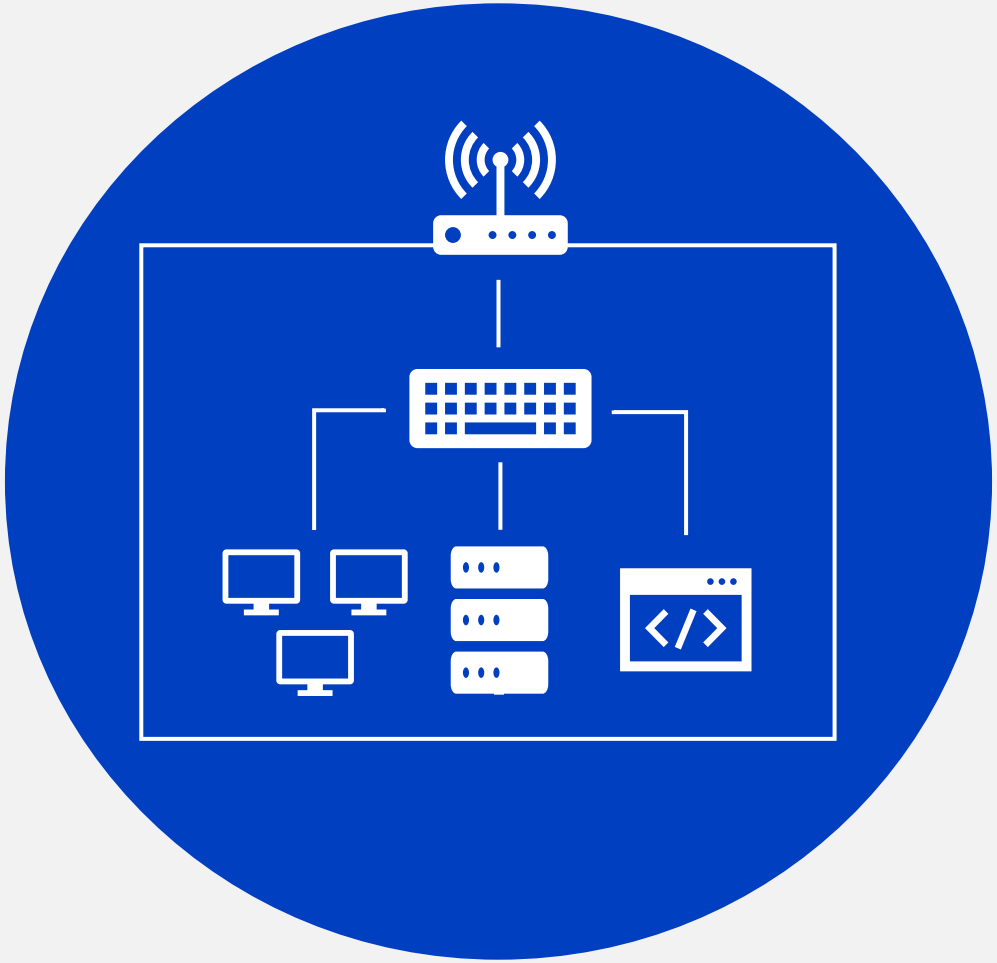
Trust is King


NOKIA
NOKIA
GSM
ABC
MENU
C
R
M
1
2 abc
3 def
4 ghi
5 jkl
6 mn
7 prs
8 tuv
9 wxy
0 oqz
#


MOTOROLA


Libretto 80CT
intel inside
centrino
TOSHIBA

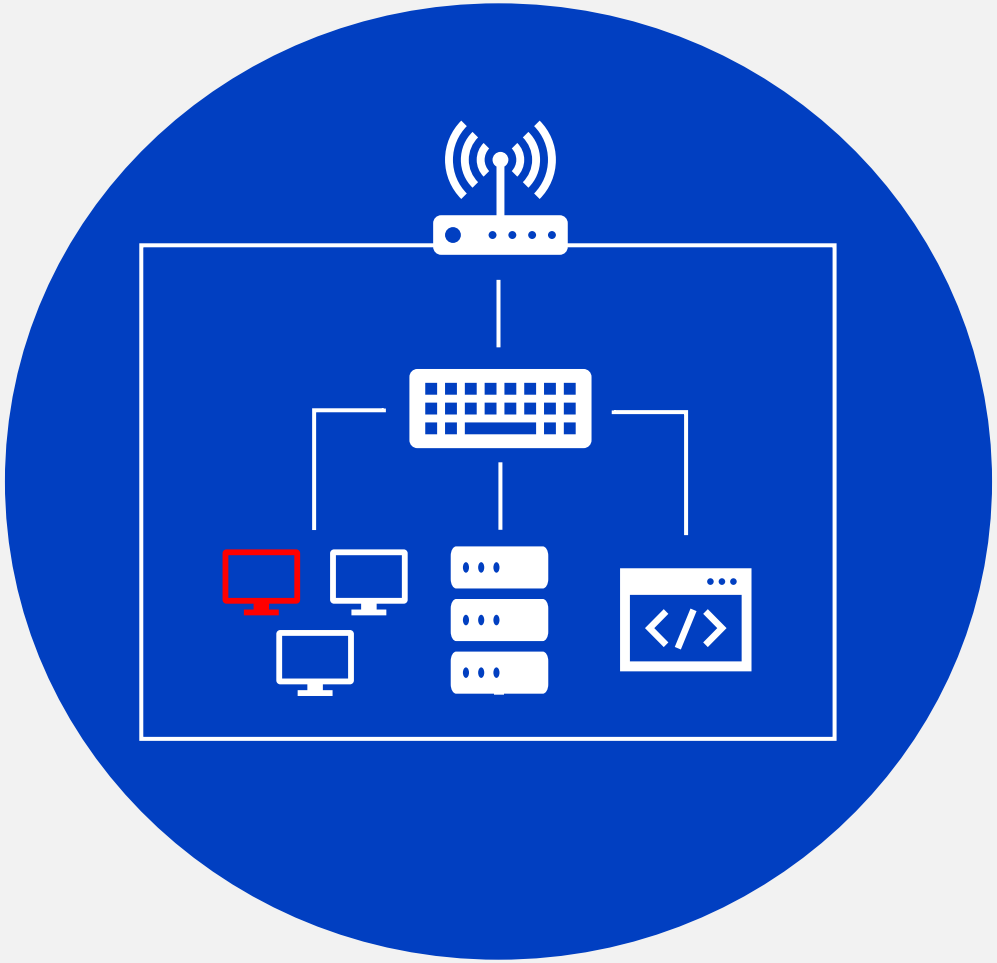




Cloud Apps & Services

Remote Working

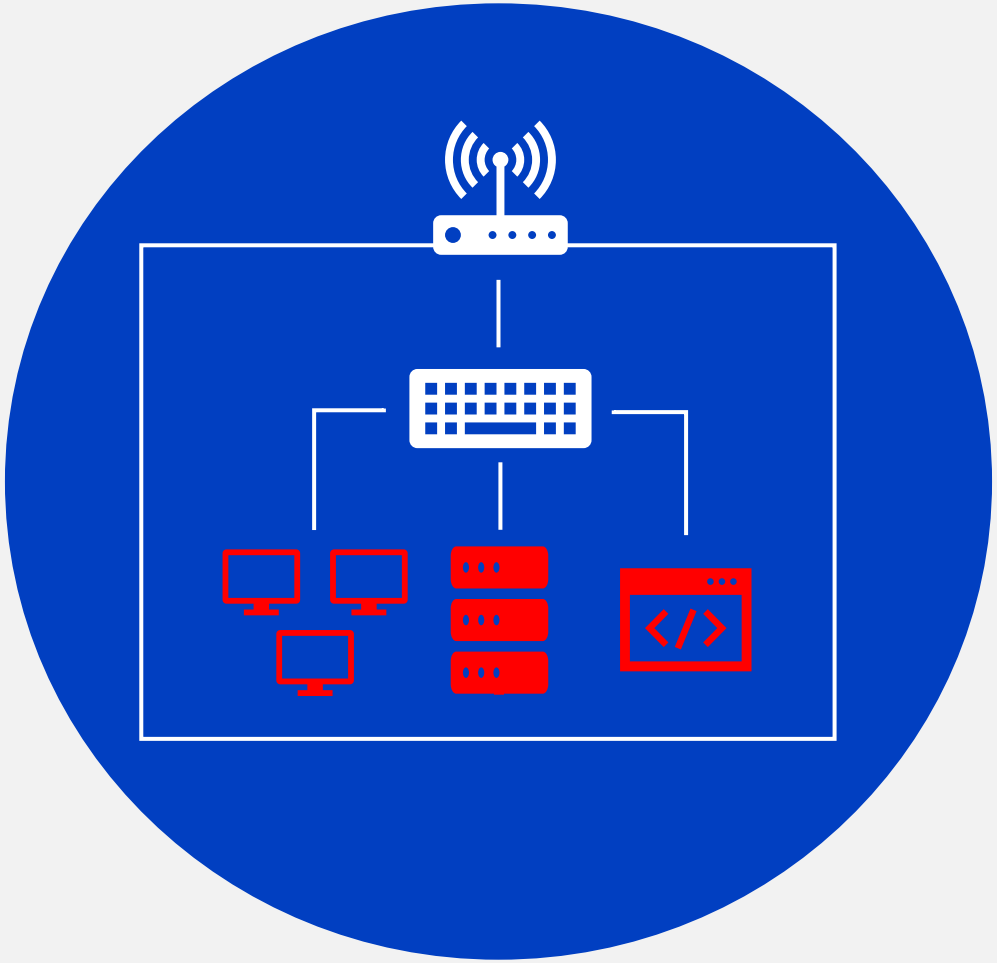
User Owned Devices



Cloud Apps & Services

Remote Working

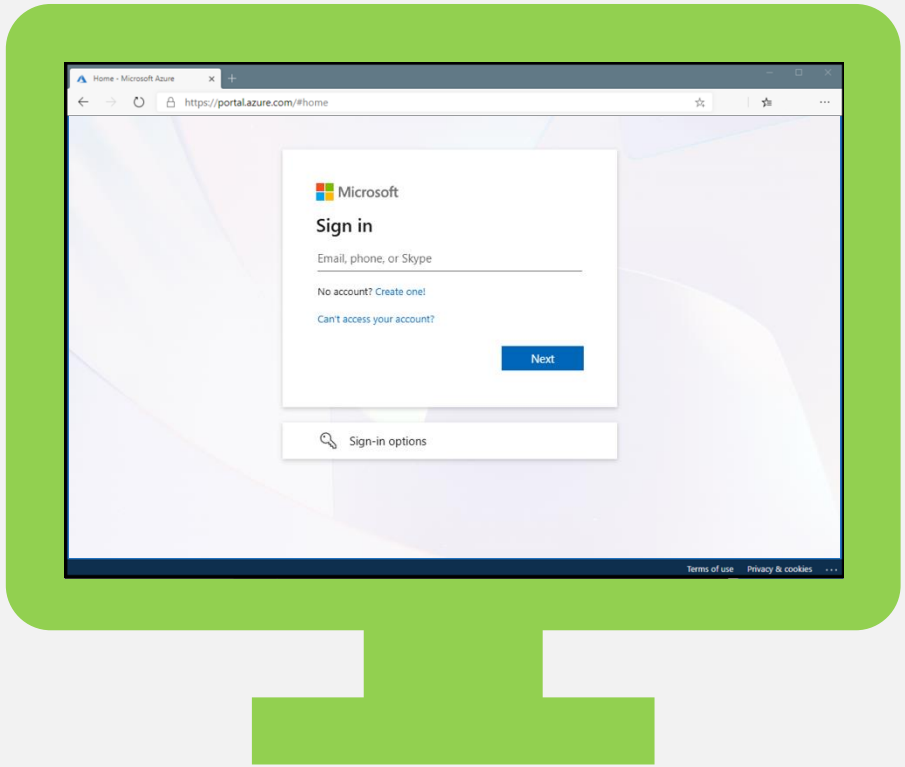
User Owned Devices

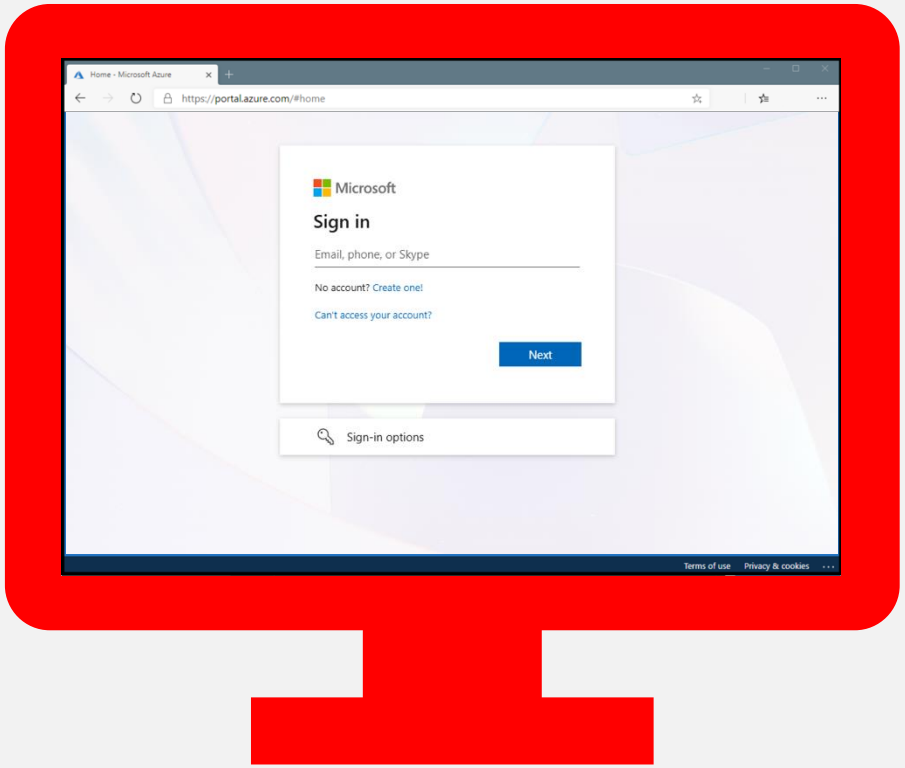


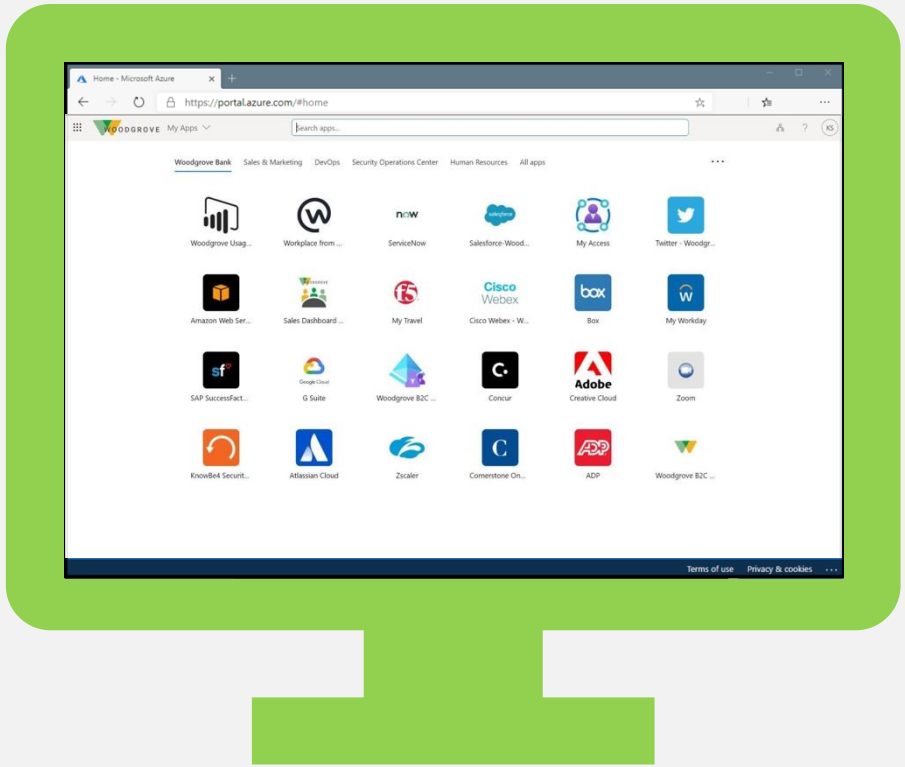
Cloud Apps & Services

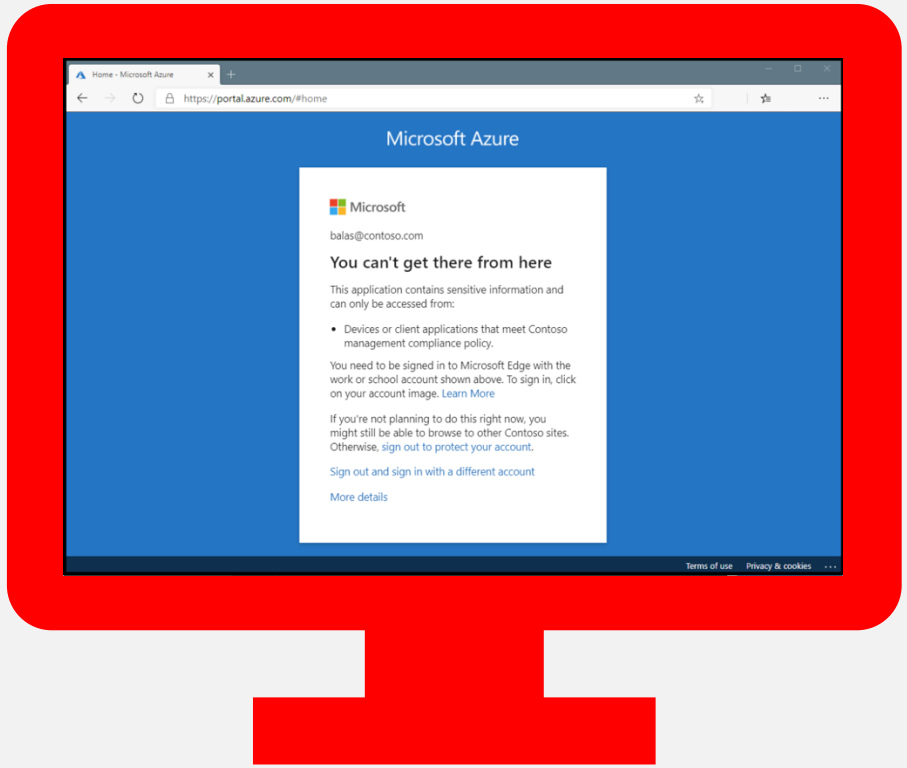
Remote Working

User Owned Devices


Home - Microsoft Azure
https://portal.azure.com/#home
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Next
Sign-in options
Terms of use
Privacy & cookies


Home - Microsoft Azure
https://portal.azure.com/#home
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Next
Sign-in options
Terms of use
Privacy & cookies


Home - Microsoft Azure
https://portal.azure.com/#home
My Apps
Search apps...
Woodgrove Bank
Sales & Marketing
DevOps
Security Operations Center
Human Resources
All apps
Woodgrove Usag...
Workplace from ...
ServiceNow
Salesforce-Wood...
My Access
Twitter - Woodgr...
Amazon Web Ser...
Sales Dashboard ...
My Travel
Cisco Webex - W...
Box
My Workday
SAP SuccessFact...
G Suite
Woodgrove B2C ...
Concur
Creative Cloud
Zoom
KnowBe4 Securit...
Atlassian Cloud
Zscaler
Cornerstone On...
ADP
Woodgrove B2C ...
Terms of use
Privacy & cookies


Home - Microsoft Azure
https://portal.azure.com/#home
Microsoft Azure
Microsoft
balas@contoso.com
You can't get there from here
This application contains sensitive information and can only be accessed from:
Devices or client applications that meet Contoso management compliance policy.
You need to be signed in to Microsoft Edge with the work or school account shown above. To sign in, click on your account image. Learn More
If you're not planning to do this right now, you might still be able to browse to other Contoso sites. Otherwise, sign out to protect your account.
Sign out and sign in with a different account
More details
Terms of use
Privacy & cookies

Wrap Up

You’re Only as Strong as Your Weakest Supplier

Takeaways

The Threat Landscape Has Shifted

Geopolitical conflict and AI have changed the speed, scale, and sophistication of attacks. This is not business as usual.

01

Identity is the New Battleground

Cloud identity infrastructure (Entra ID, Intune, IAM) is where the most impactful attacks are happening.

02

The Basics Still Matter the Most

MFA, patching, backups, and incident planning prevent the vast majority of successful attacks.

03

Any Questions?

Thank You.

node4.co.uk

linkedin.com/in/ncdlloyd

linkedin.com/in/callumrbutler