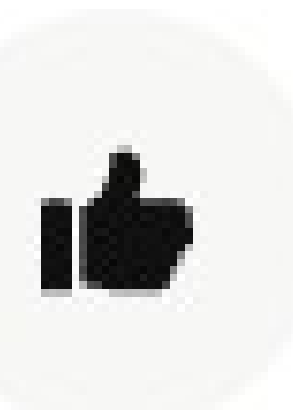


# Stopping Session Theft

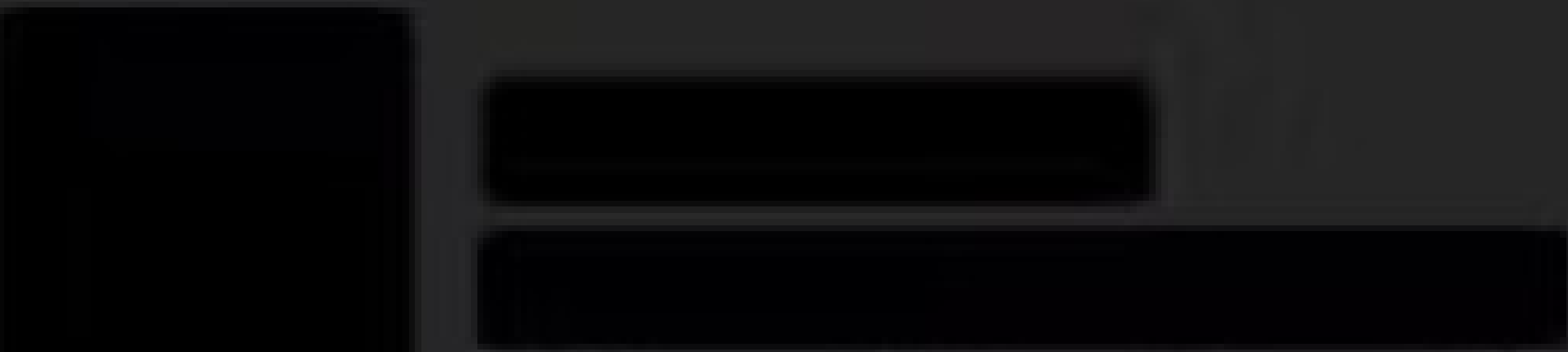
**Your MFA is futile if I have your cookie**

Anthony Castano

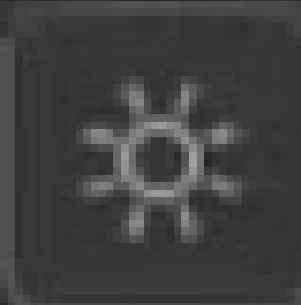




RE: Brandon [redacted] shared [redacted] with you



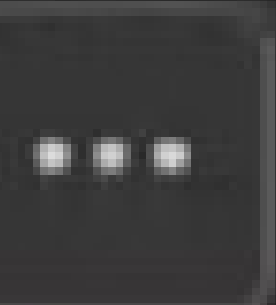
Retention Policy Delete After 11 Years (11 years)



Reply

Reply All

Forward



Thu 1/16/2025 10:09 AM

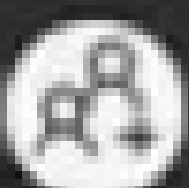
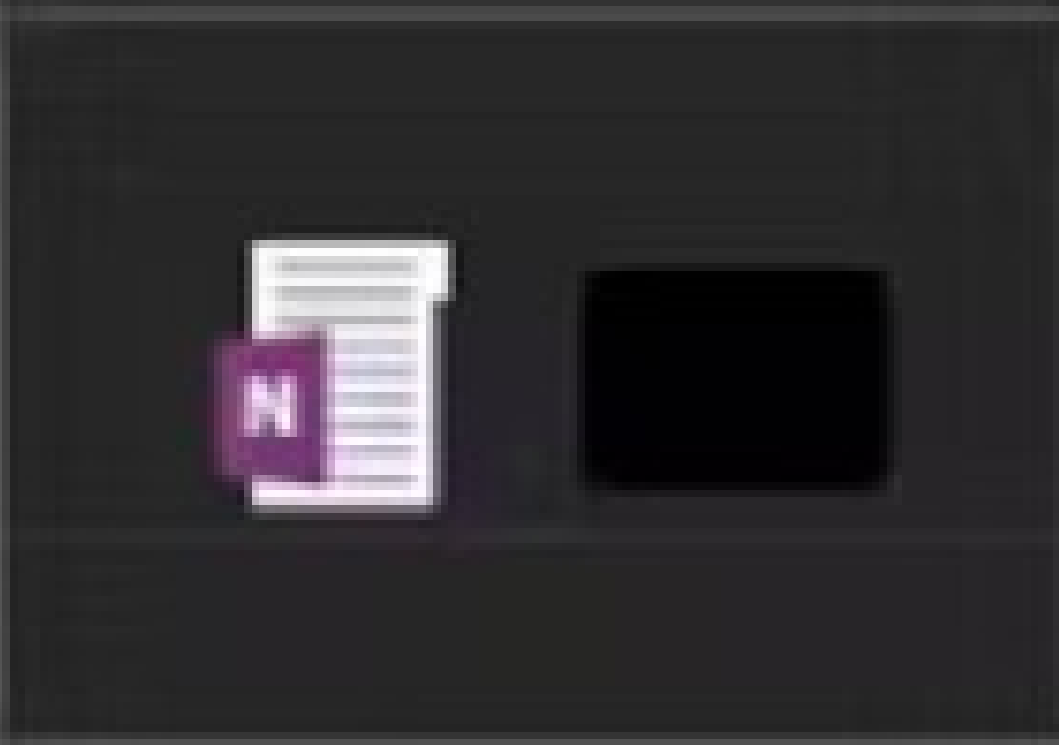
Expires 1/14/2036

From: Brandon [redacted]  
Sent: Thursday, January 16, 2025 6:59 AM  
To: [redacted]  
Subject: Brandon [redacted] shared [redacted] with you



Brandon [redacted] shared a file with you

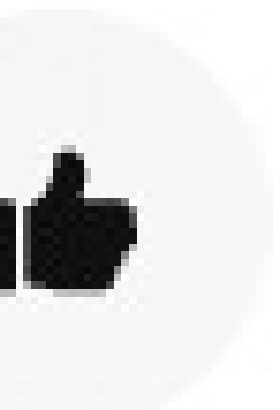
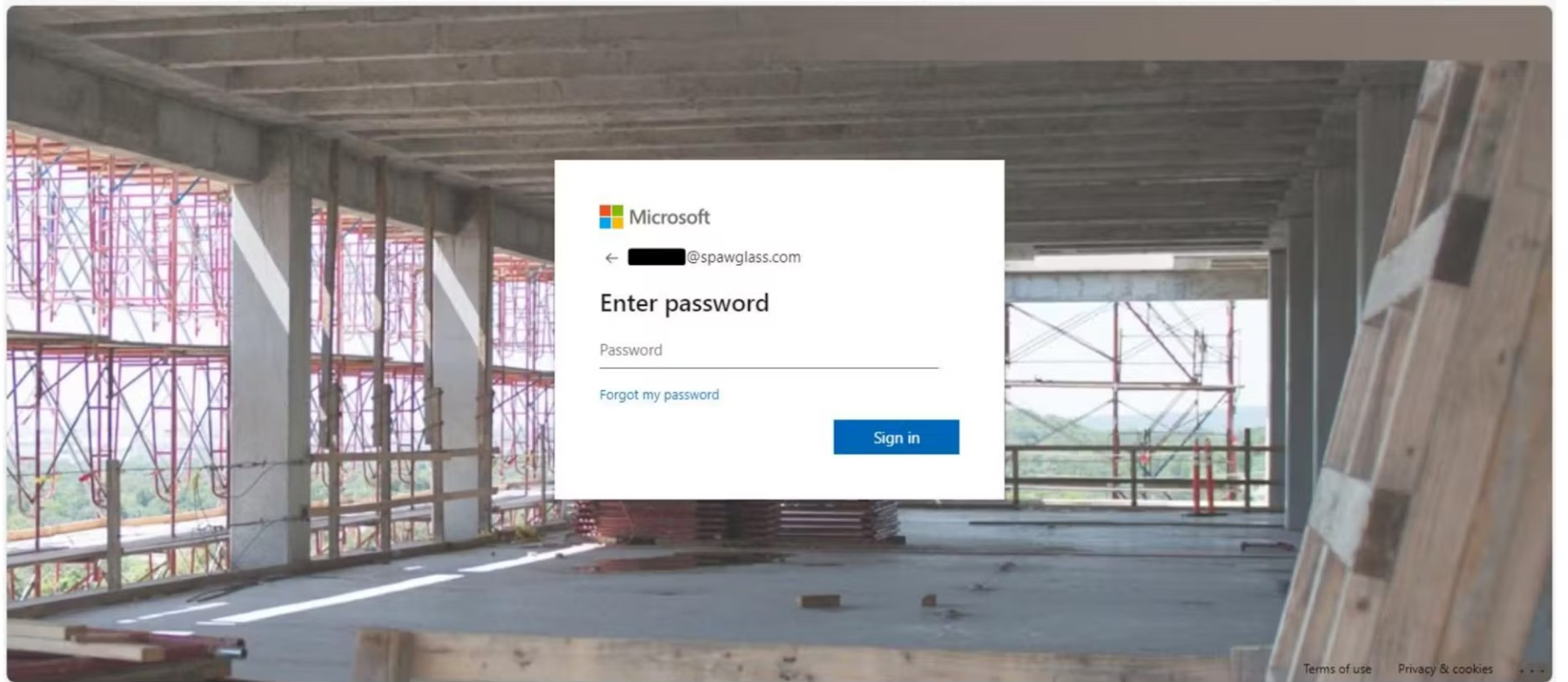
Here's the document that [redacted] shared with you.

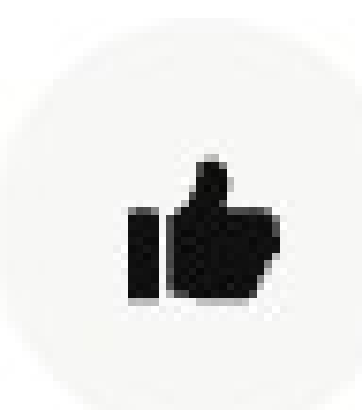


This link only works for the direct recipients of this message.

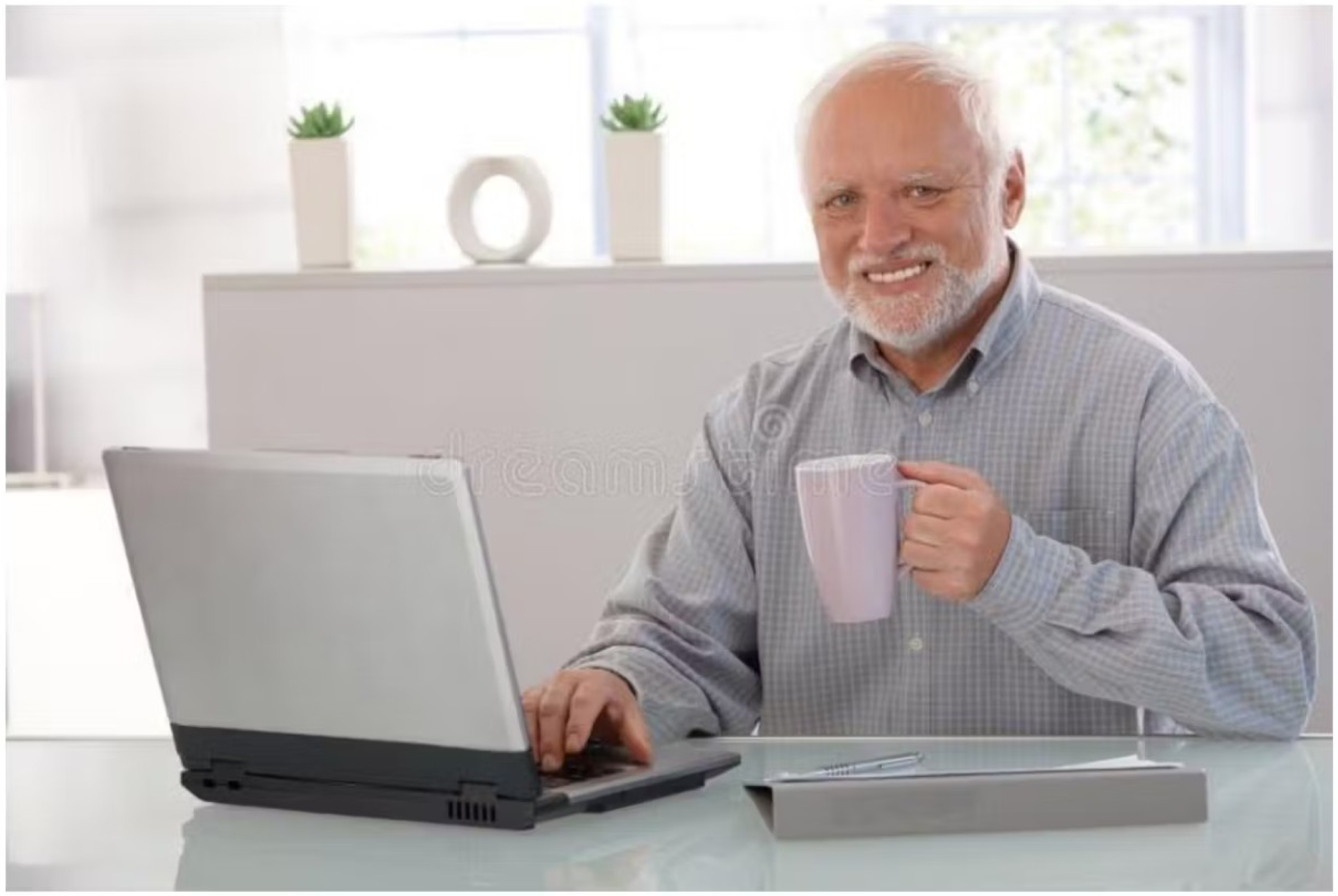
Open














Microsoft

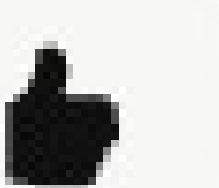
Hacker



# Understanding The Problem

Phishing-as-a-Service for \$350 month Features:

- Two-factor authentication (2FA) bypass
- 2FA cookie harvesting
- Status of phishing campaigns



# Understanding The Problem Pt. 2

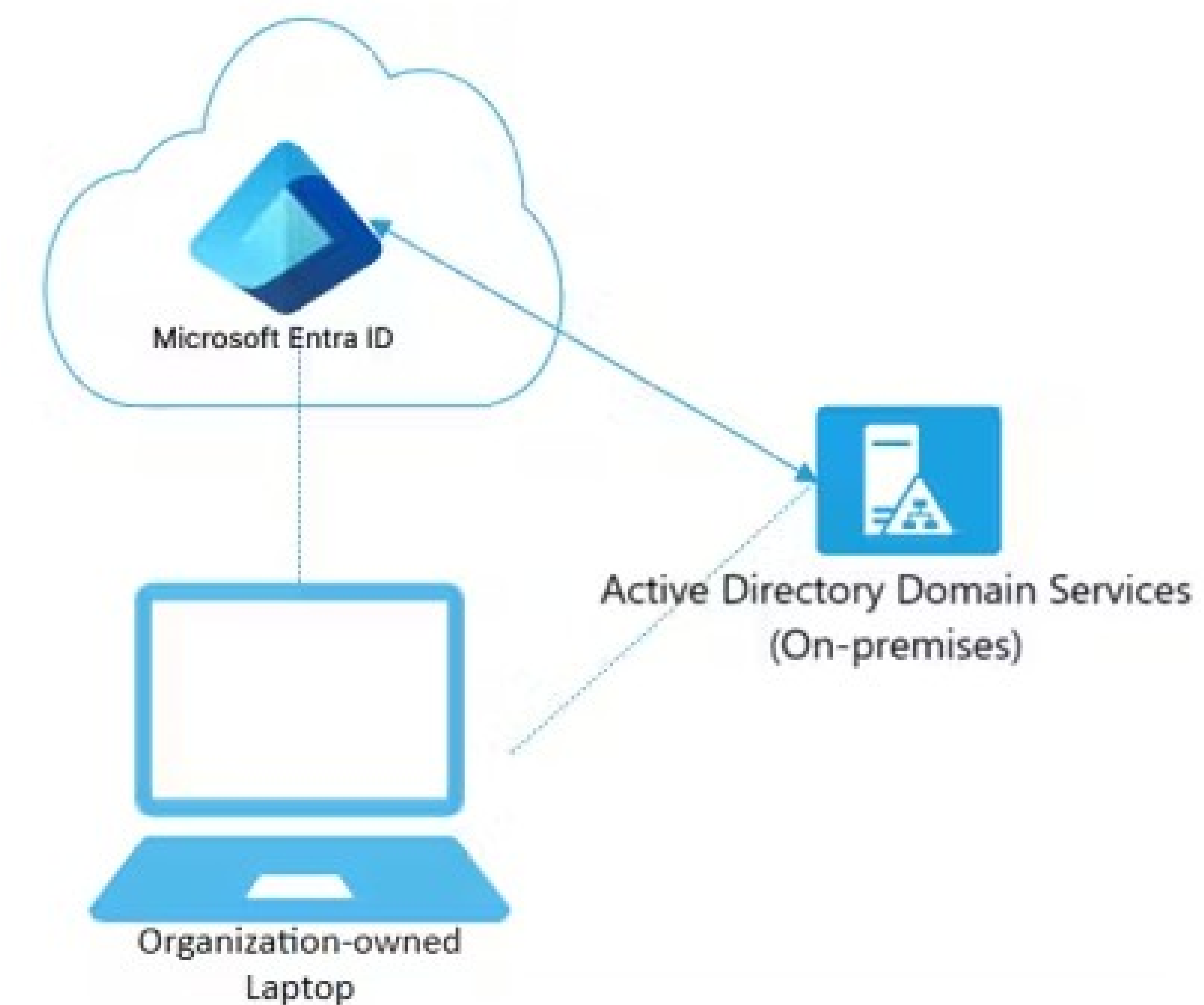
- Microsoft – delayed alerting
- Third-party security – delayed alerting
- No 2FA is enough
- Email Security
- Firewall
- Awareness Training

# Solution: Authorizing Devices

## Prerequisites:

- E3 license
- On-prem AD and Entra ID
- Hybrid joined devices
- Chrome for enterprise (free)
- Auditing 3rd-party apps for support
- Hybrid-join policy and protecting cookies
- Exceptions to policy

Hybrid-join policy and protecting cookies





# In Scope Devices

- Windows
- Linux
- MacOS
- Unknown OS (ChromeOS)

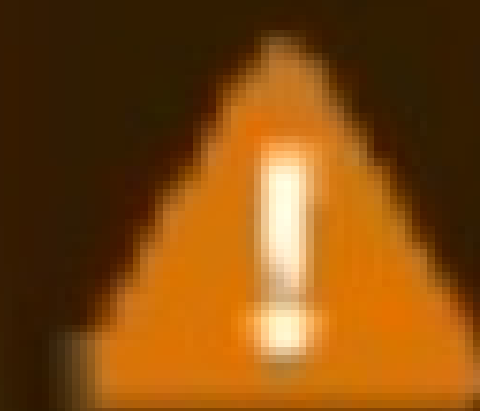
## **Out of Scope**

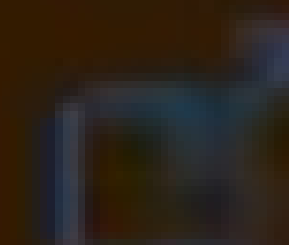
- Android
- iOS (iPhone and iPad)

# Grant



Require Microsoft Entra  
hybrid joined device



Don't lock yourself out! Make  
sure that your device is  
Microsoft Entra hybrid joined.  
[Learn more](#) 

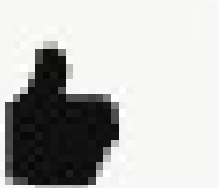
# Impact and Results

- STOPPED session stealing
- Users didn't notice change
- Upset personal PCs didn't work
- Reduced risk of infostealers



# Key takeaways

1. Monitor Entra ID Risky sign-ins
2. Geo and IP restrictions
3. Limit Browser Extensions
4. Risk-based reporting (requires license)
5. Hybrid-restriction policy



# Resources

- <https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-grant#require-microsoft-entra-hybrid-joined-device>
- <https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk>
- <https://thehackernews.com/2025/05/russian-hackers-breach-20-ngos-using.html>
- <https://thehackernews.com/2025/05/how-browser-in-middle-attacks-steal.html>
- <https://www.bleepingcomputer.com/news/security/chainlink-phishing-how-trusted-domains-become-threat-vectors/>
- <https://thehackernews.com/2025/05/100-fake-chrome-extensions-found.html>