Martin Haller

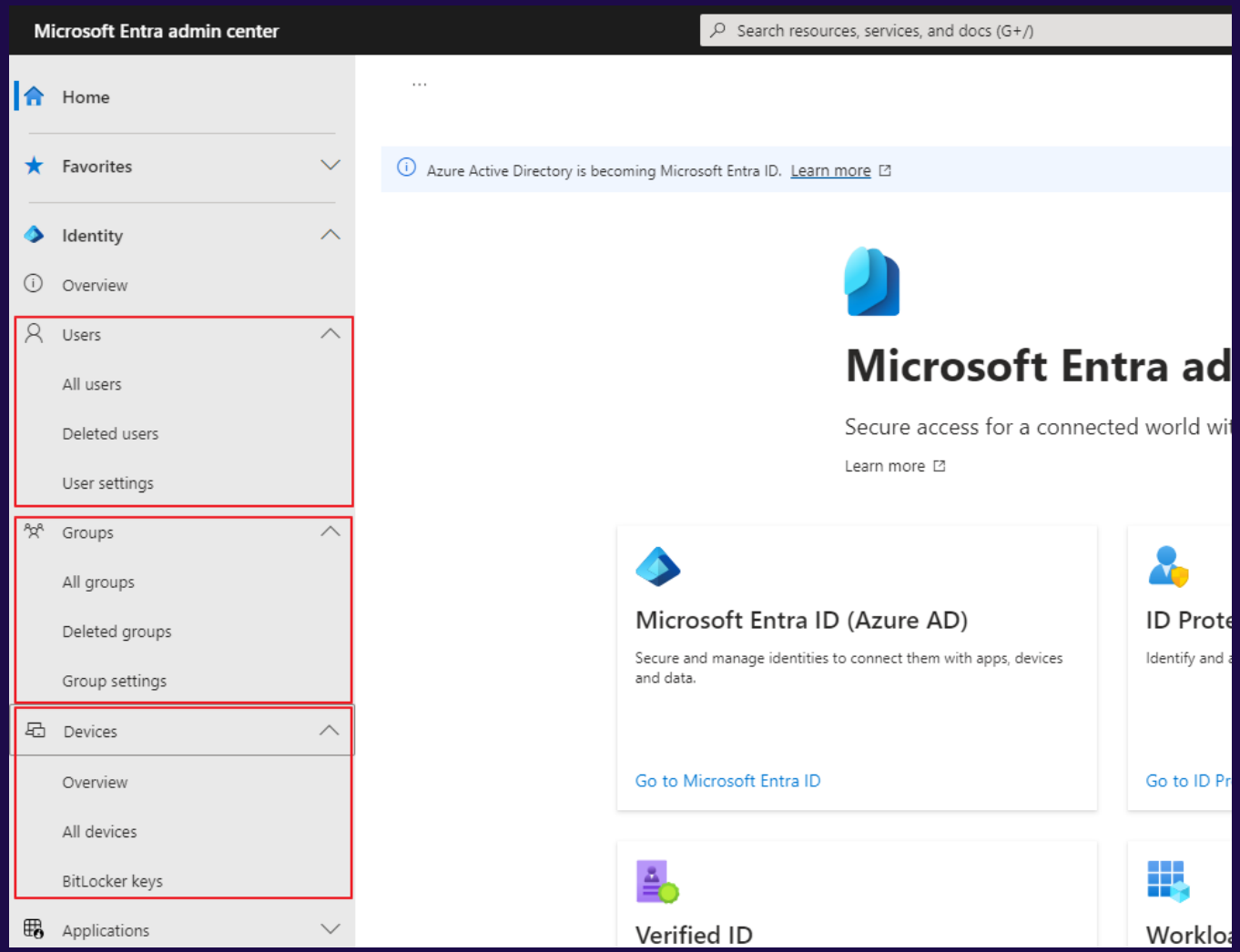
⟨ Microsoft Entra ID Attack surface ⟩

PATRON ⟨IT⟩ OCHRANA A SPRÁVA SÍTÍ

Entra ID: Introduction

Microsoft Entra ID: What is it?

- New name for Azure AD
- Cloud version of Active Directory?
- Higher level of protection



Microsoft Entra ID: Why to care?

- Ransomware groups know AD better than defenders
- Entra ID is more recent than AD
- Almost everyone has Entra ID tenant

Future problem

Microsoft Entra ID: identity provider (IdP)?

- Single sign-on (SSO)
- Single logon credentials (user onboarding / offboarding)
- Logs at one place (audit, security)
- Native MFA support
- Conditional Acces (CA) – controls WHO can access WHAT (data / applications) under which CONDITIONS and PRIVILEGES.

Microsoft Entra ID: other characteristics

» SSO for cloud and on-prem apps

Accompanying products :

» Intune (~GPO)

» Information Protection for M365

» Defender for * (AV, EDR, cloud apps, identity)

» Privileged Identity Management (PIM)

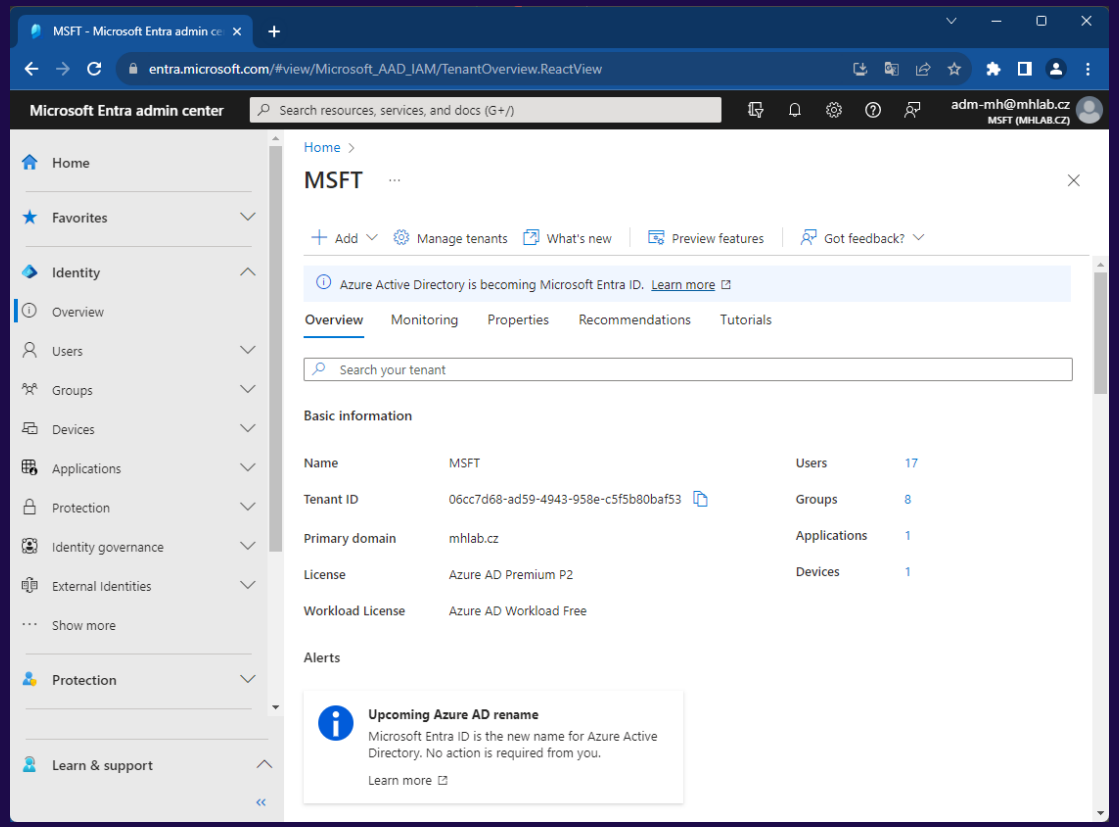
Microsoft Entra ID vs Active Directory

Same features:

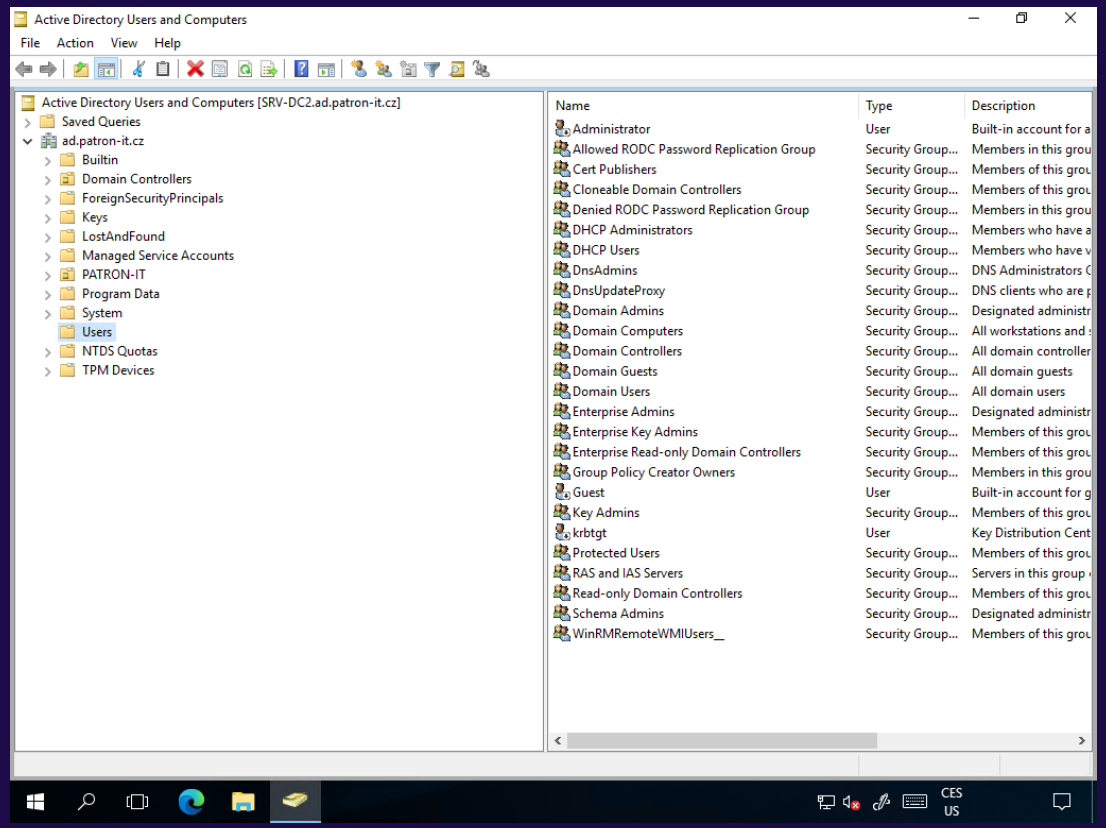
- Users
- Groups
- Devices
- +/- GPO

Microsoft Entra ID vs Active Directory

Microsoft Entra ID



Active Directory



Microsoft Entra ID vs Active Directory

Microsoft Entra ID

- Oauth
- SAML

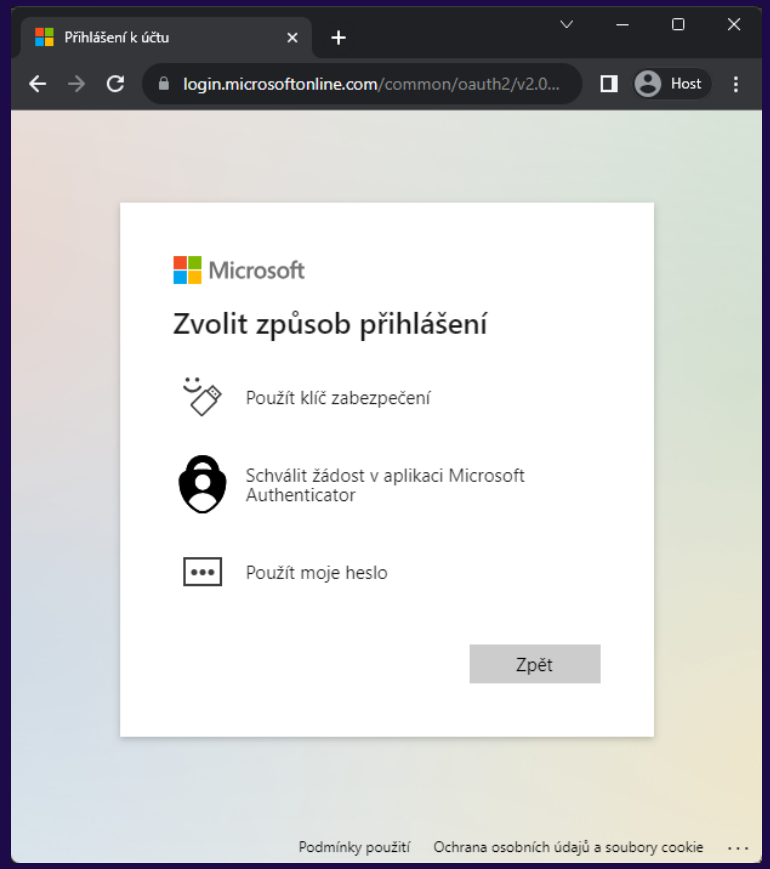
Active Directory

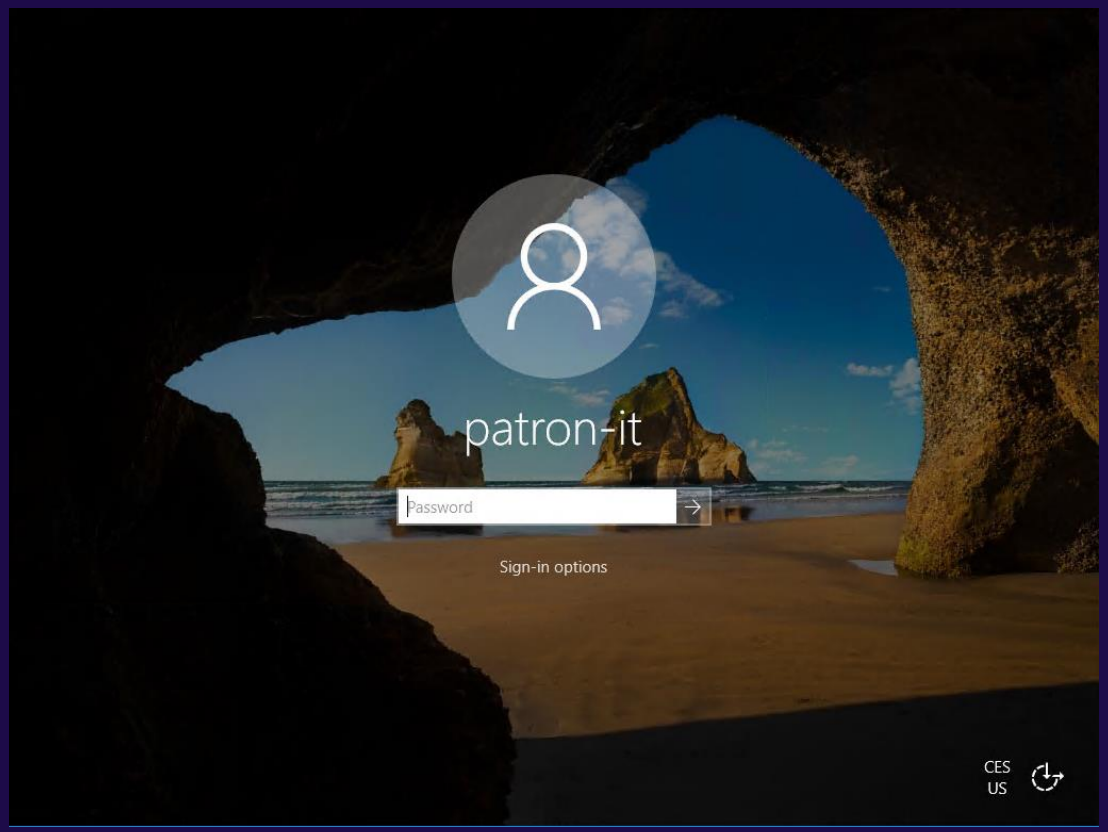
- NTLM
- Kerberos

Microsoft Entra ID vs Active Directory

Microsoft Entra ID

Active Directory





Microsoft Entra ID vs Active Directory

Microsoft Entra ID

Method	Primary authentication	Secondary authentication
Windows Hello for Business	Yes	MFA*
Microsoft Authenticator (Push)	No	MFA and SSPR
Microsoft Authenticator (Passwordless)	Yes	No
Authenticator Lite	No	MFA
FIDO2 security key	Yes	MFA
Certificate-based authentication	Yes	No
OATH hardware tokens (preview)	No	MFA and SSPR
OATH software tokens	No	MFA and SSPR
SMS	Yes	MFA and SSPR
Voice call	No	MFA and SSPR
Password	Yes	

Active Directory

- Password
- Smart card

Source: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

Entra ID:
Attack surface

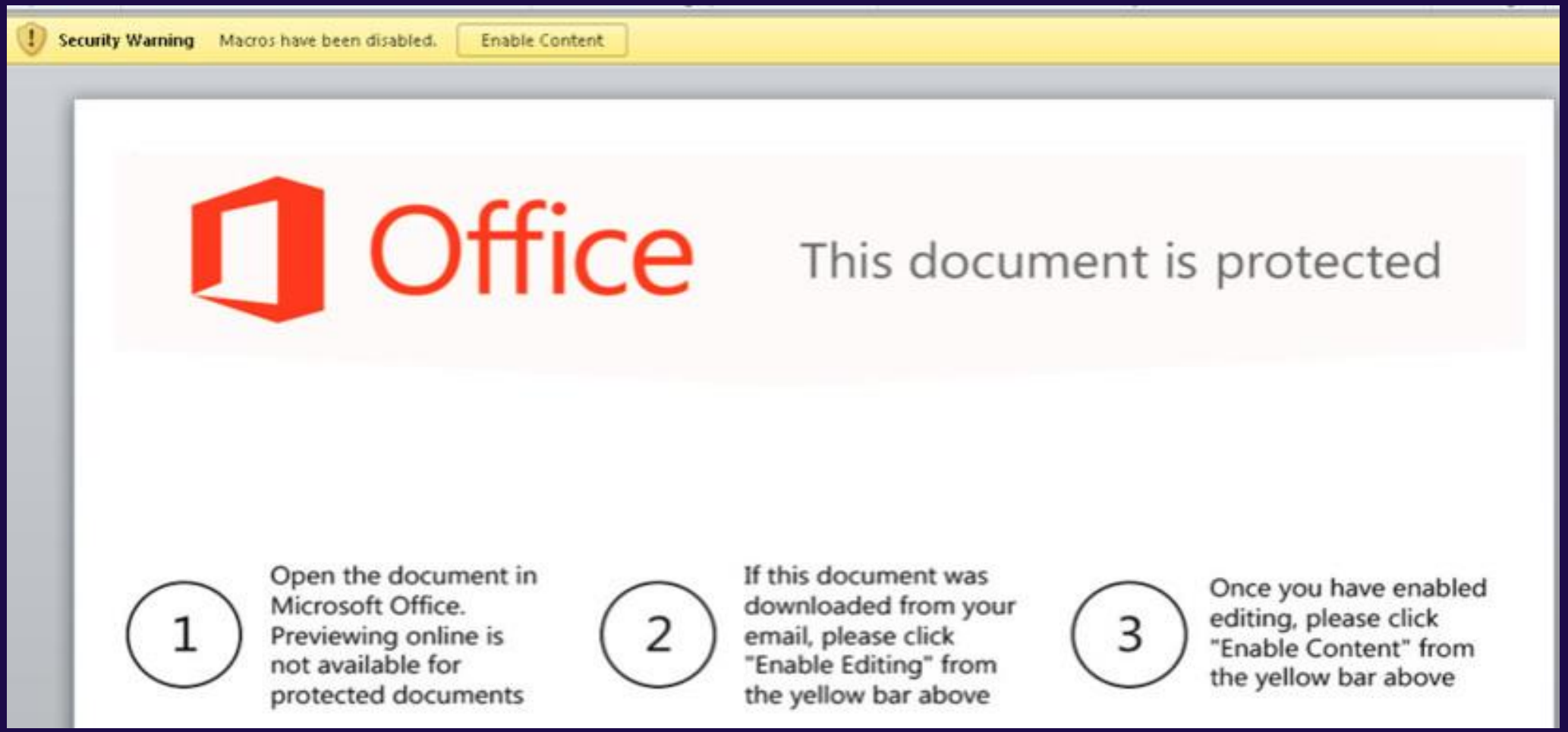
Today's agenda?

- Initial foothold
- Summary of present cloud and on-prem threats
- Cloud-only (no hybrid, for simplicity)

Microsoft Entra ID is safer, right?

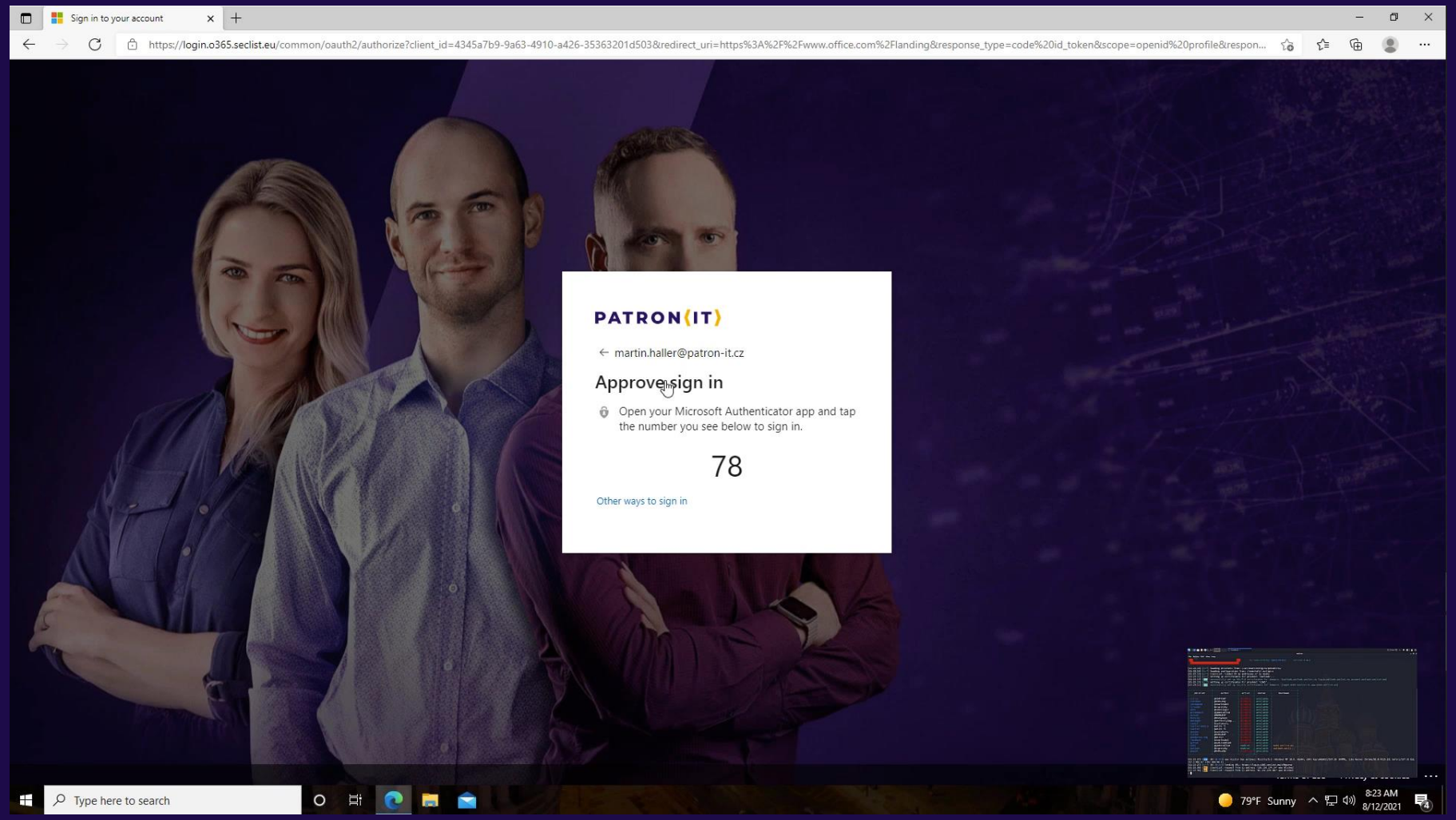
- **Cloud** – work from everywhere (vs. AD epoch)
- **BYOD** – work from any device (vs. AD epoch)

Cloud -> Phishing: 🎯 Malware



Source: https://www.linkedin.com/pulse/how-dridex-threat-actors-craft-phishing-attacks-exploits-jitendra-das/

Cloud -> Phishing: 🎯 Steal credentials

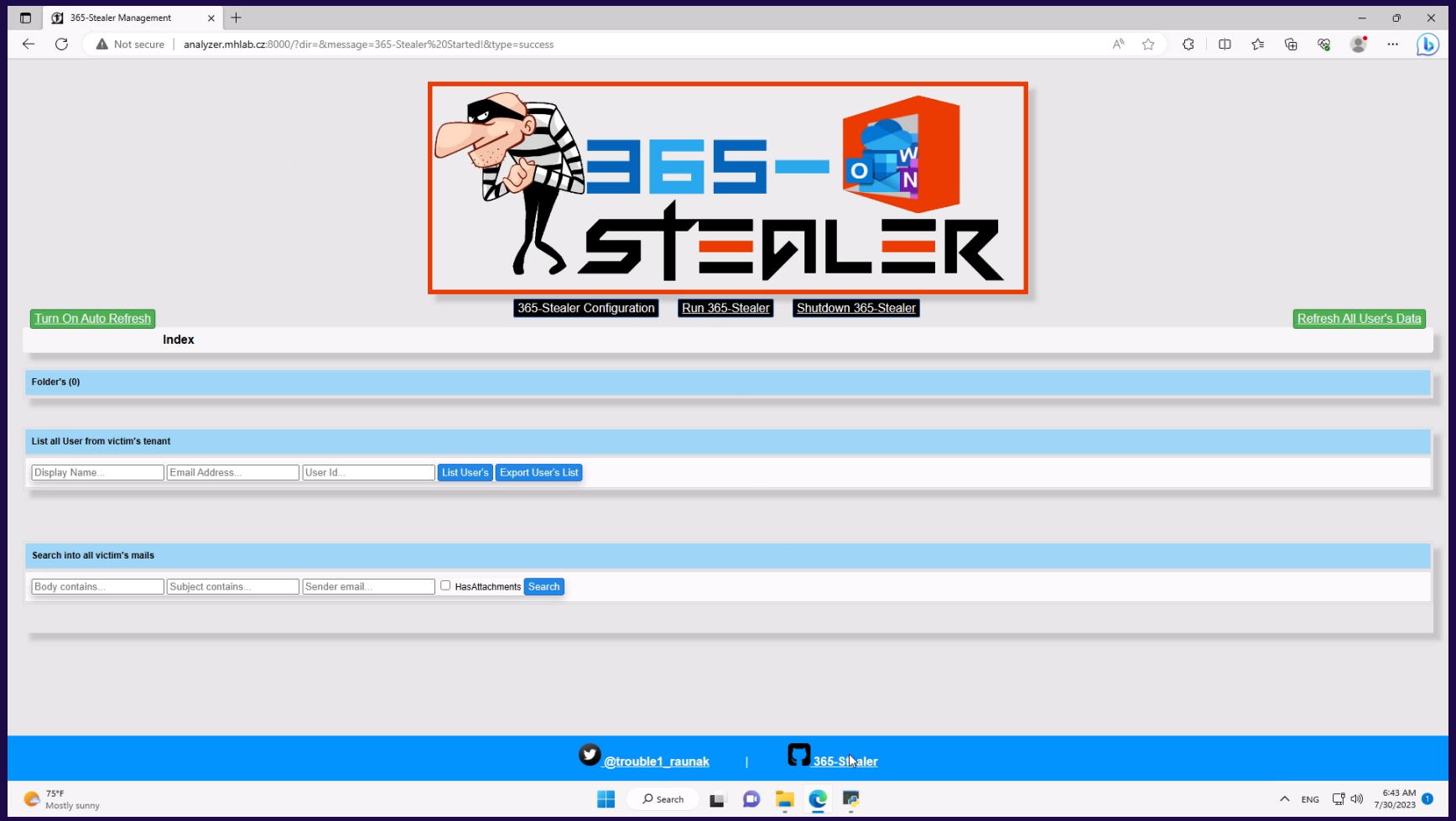


Cloud -> Phishing: 🎯 Steal credentials

Authentication method combination	MFA strength	Passwordless MFA strength	Phishing-resistant MFA strength
FIDO2 security key	✅	✅	✅
Windows Hello for Business	✅	✅	✅
Certificate-based authentication (Multi-Factor)	✅	✅	✅
Microsoft Authenticator (Phone Sign-in)	✅	✅	
Temporary Access Pass (One-time use AND Multi-use)	✅		
Password + something you have[1]	✅		
Federated single-factor + something you have[1]	✅		
Federated Multi-Factor	✅		

Source: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths

Cloud -> Phishing: 🎯 Illicit Consent Grant



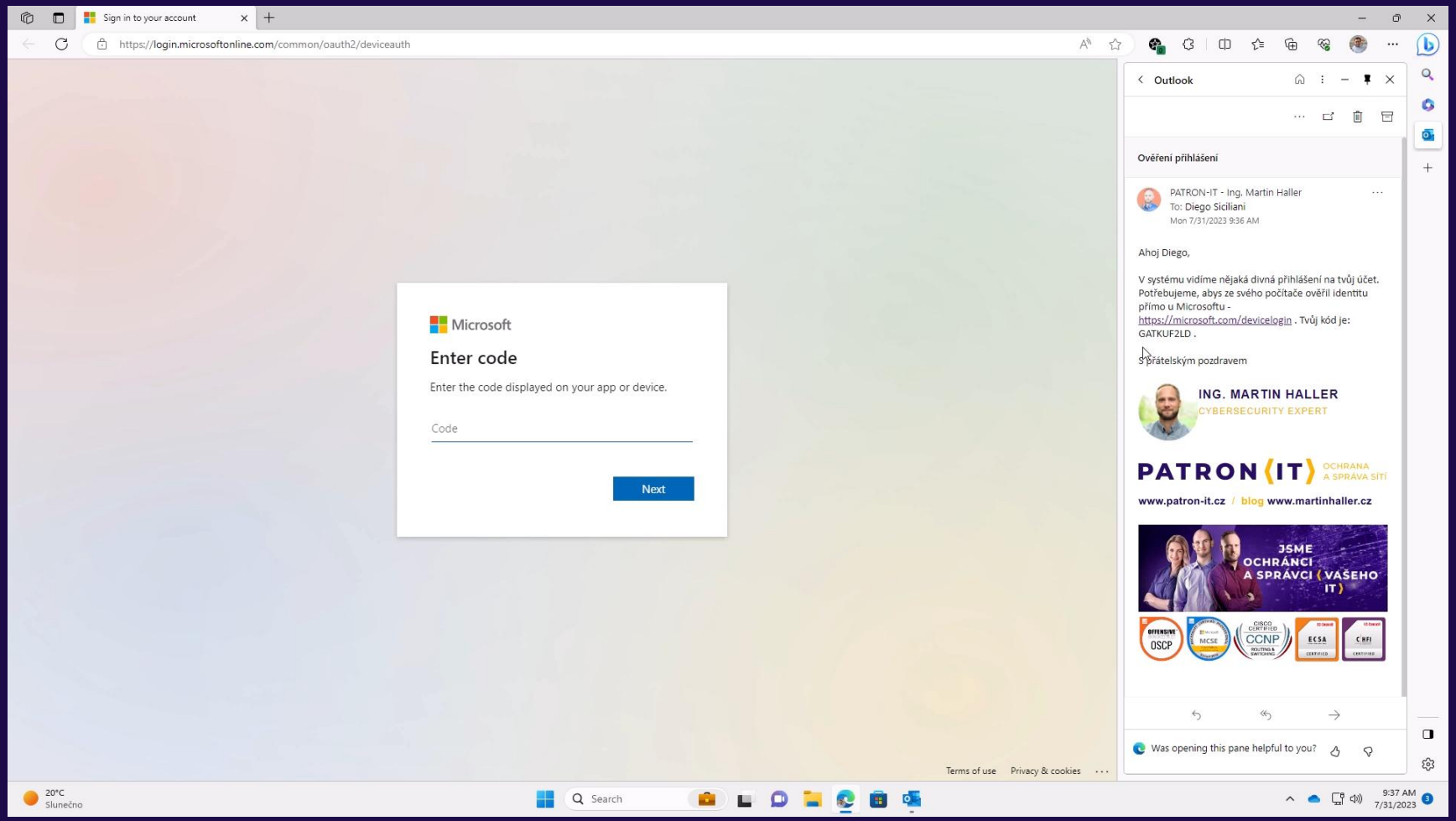
Cloud -> Phishing: 🎯 Illicit Consent Grant

What doesn't help

- URL inspection
- MFA
- Phishing resistant authentication
- Conditional Access (except default deny)

It is longterm access

Cloud -> Phishing: 🎯 OAuth Device code flow



Cloud -> Phishing: 🎯 OAuth Device code flow

What doesn't help

- URL inspection
- MFA
- Phishing resistant
- Conditional Access (except require Hybrid/Compliant Device)

It is longterm access

Oauth 2.0 Excursion

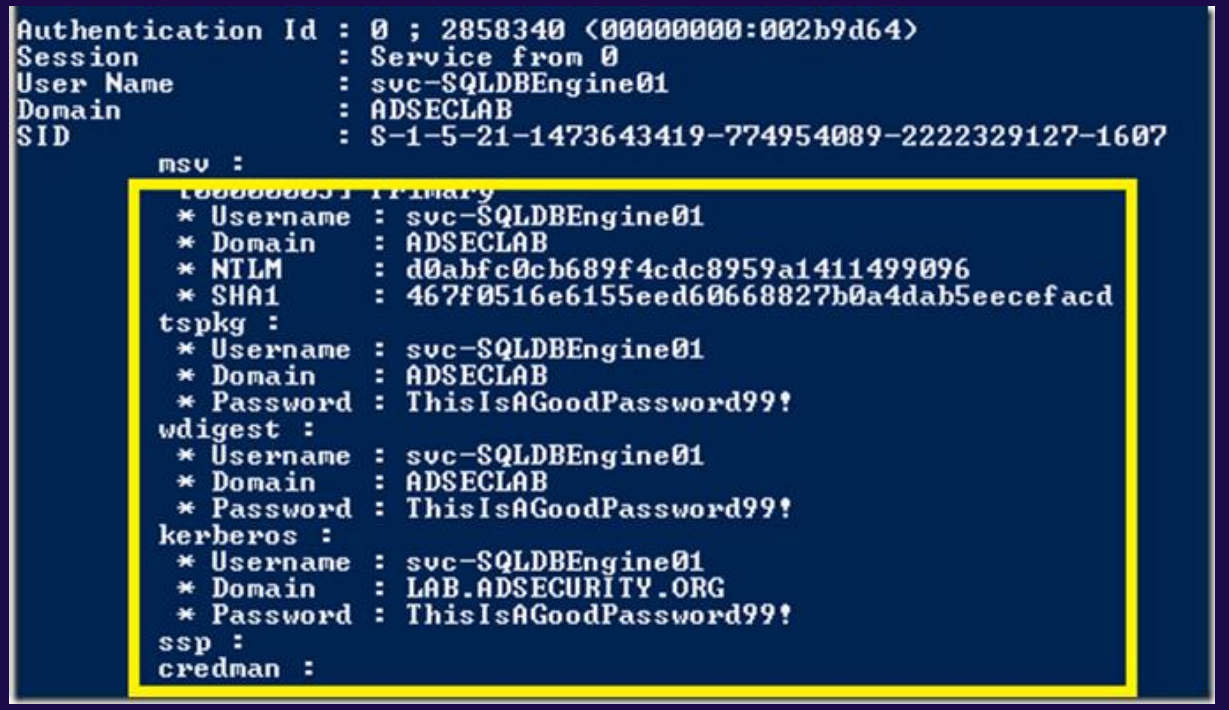
Active Directory Excursion

Attacker's gold:

» **Login credentials** (Plaintext creds)

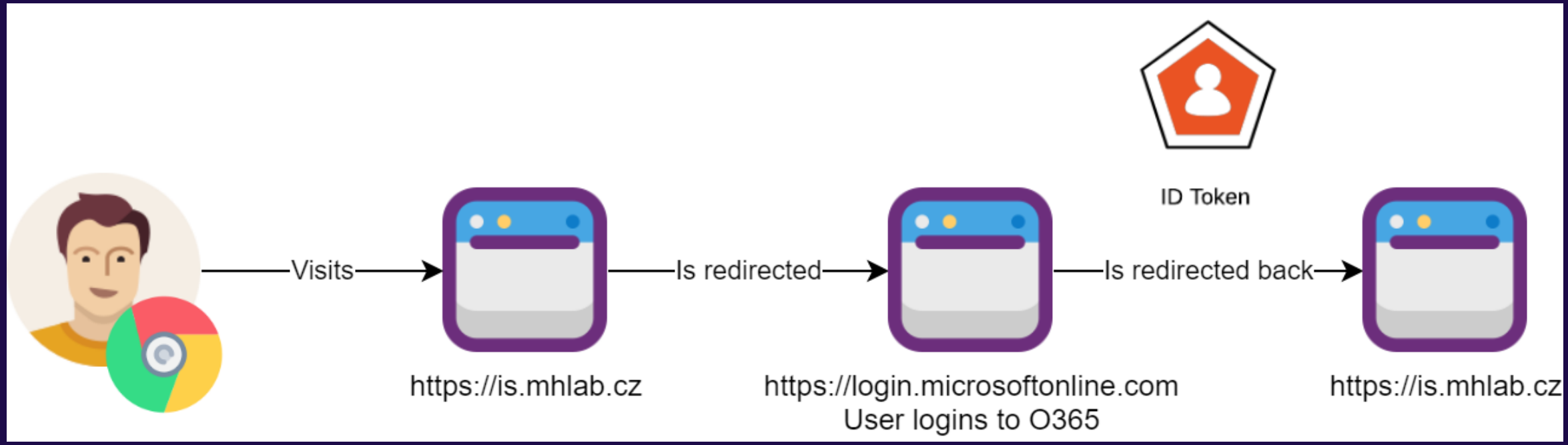
» **NT Hash** (NTLM)

» **TGT a TGS** (Kerberos)



Source: https://adsecurity.org/?page_id=1821

Oauth 2.0 – principle simplified



Token icon source: https://auth0.com/blog/ultimate-guide-nextjs-authentication-auth0/

Oauth 2.0 – principle simplified

» Authentication to https://is.mhlab.cz without password disclosure

» But what if we want to allow (authorize) the app to access data at other service (e.g. Outlook to Exchange Online)?

Oauth 2.0: tokens

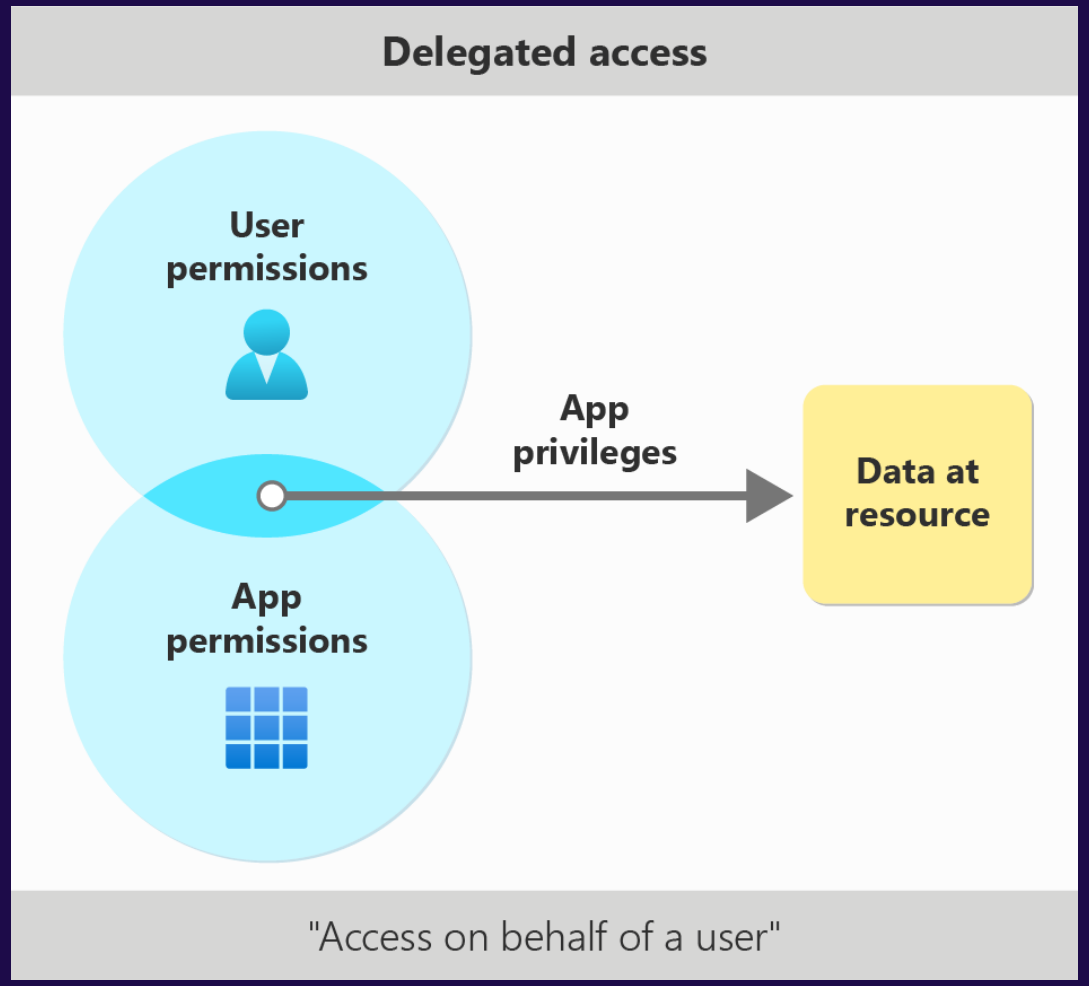
» **ID Token:** proofs who we are

» **Access Token –** the bearer can access „defined“ resources. Validity 60-90 minuts.

» **Refresh Token** – allows to request new Access Token. Validity 90 days to inifinity.

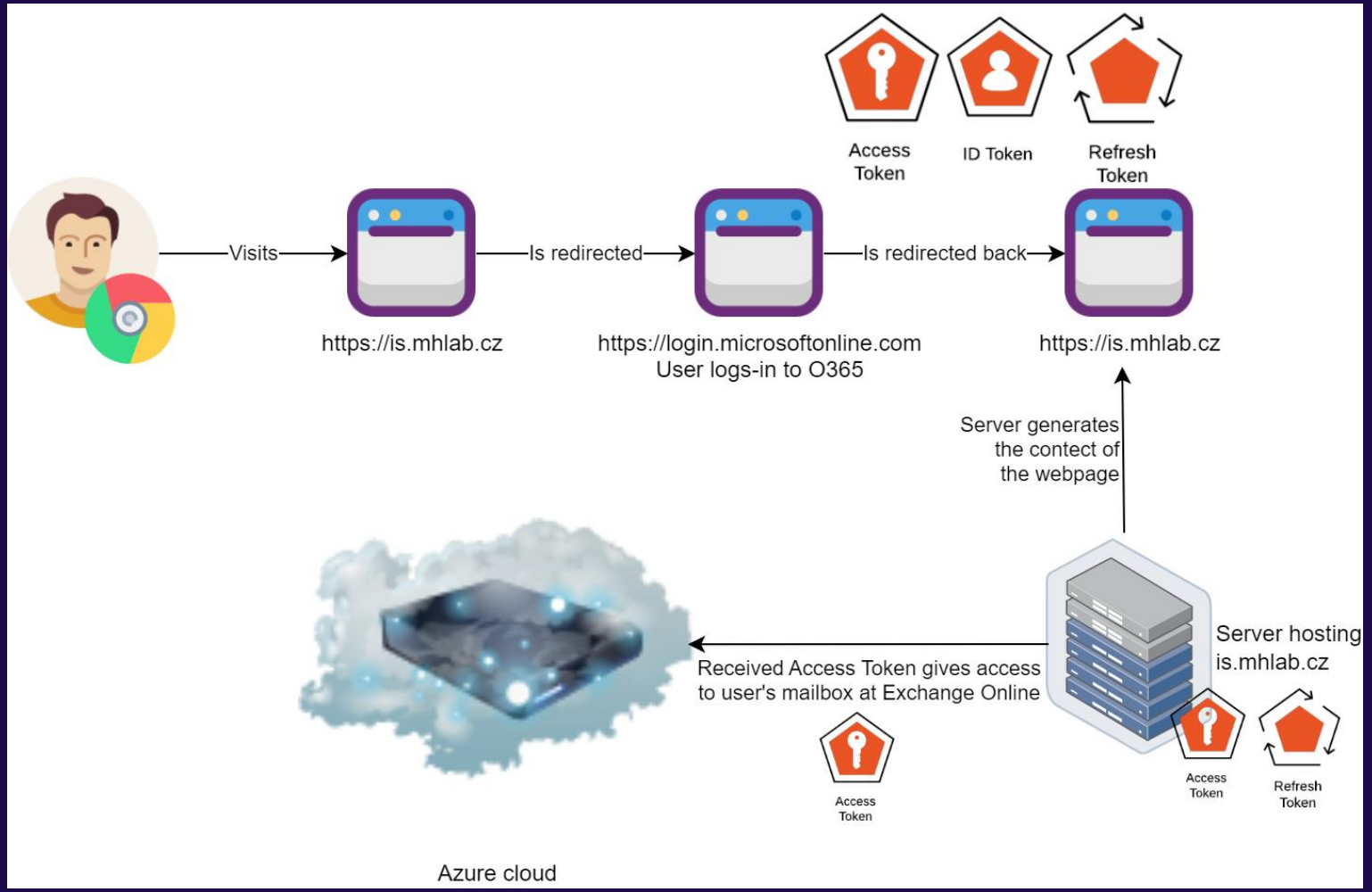
» Access and Refresh tokens are tight to specific application and scoped to set of privileges.

» All the tokens are sensitive informations (same as credentials).



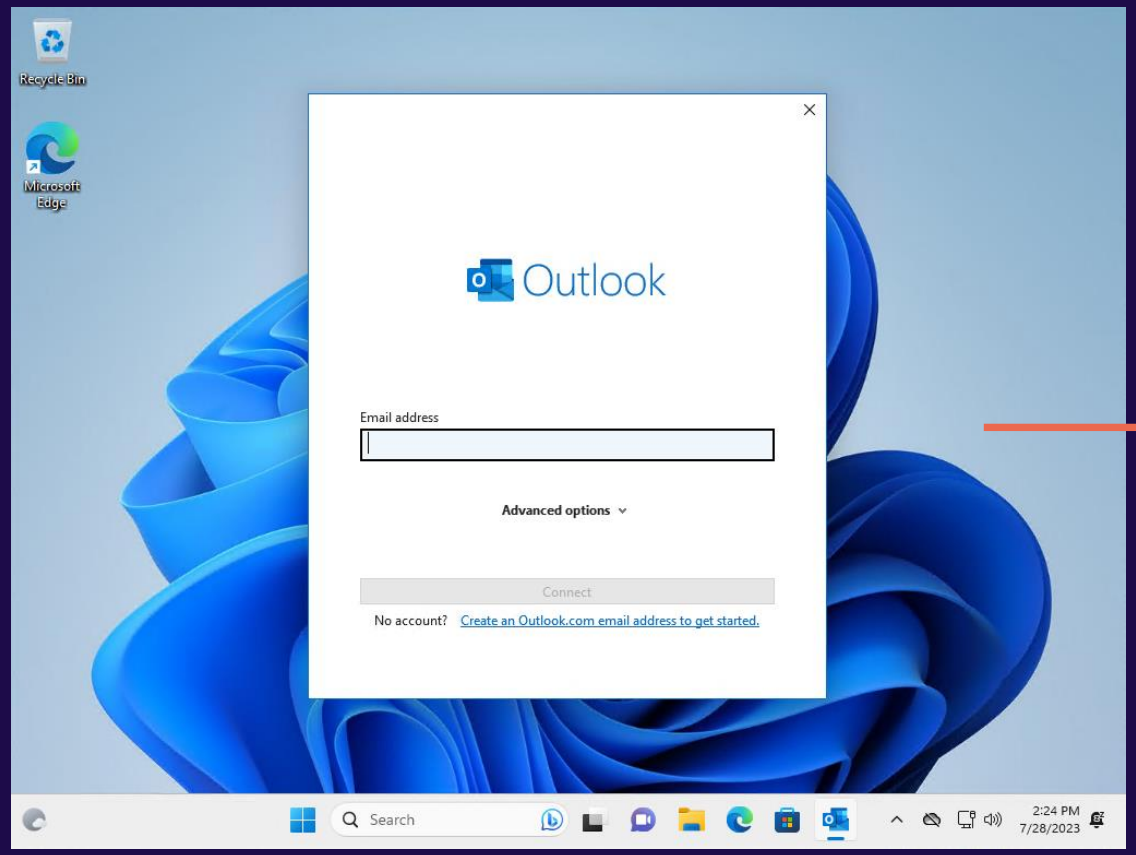
Source: https://learn.microsoft.com/en-us/azure/active-directory/develop/permissions-consent-overview

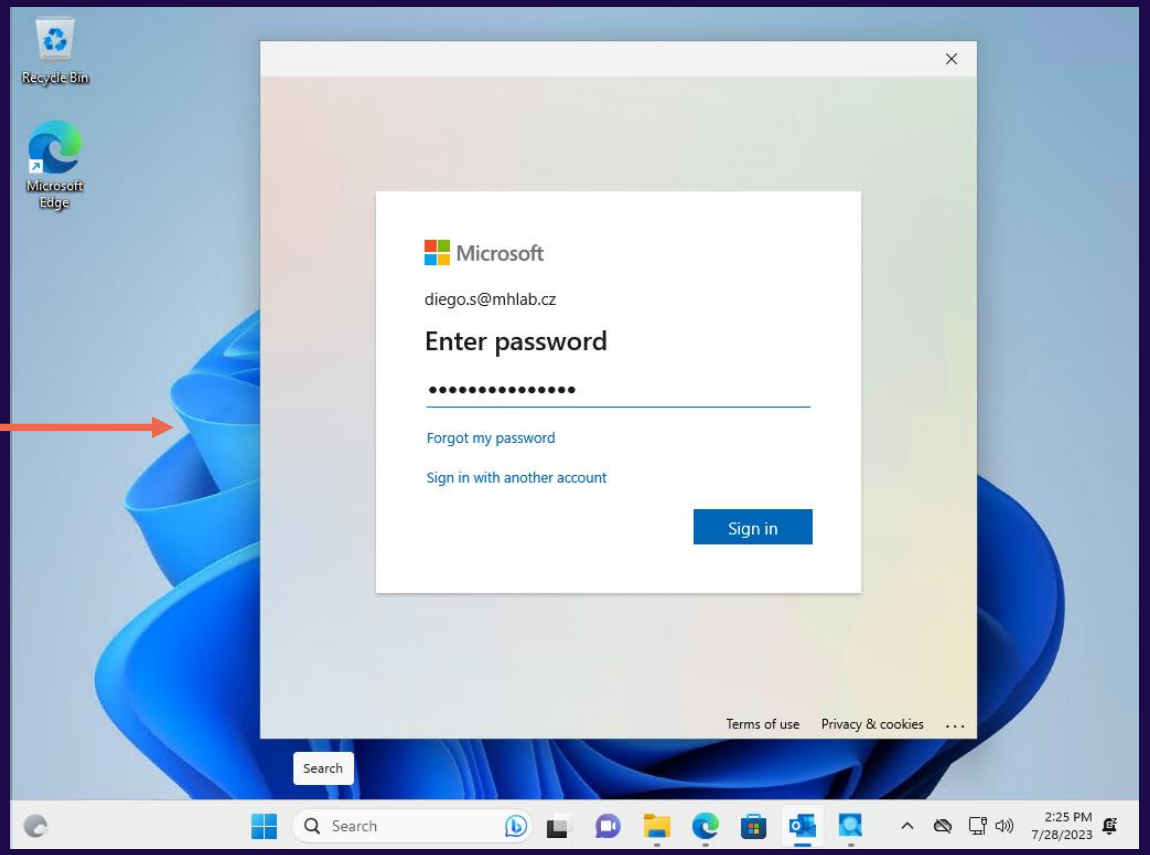
Oauth 2.0 – zjednodušený princip



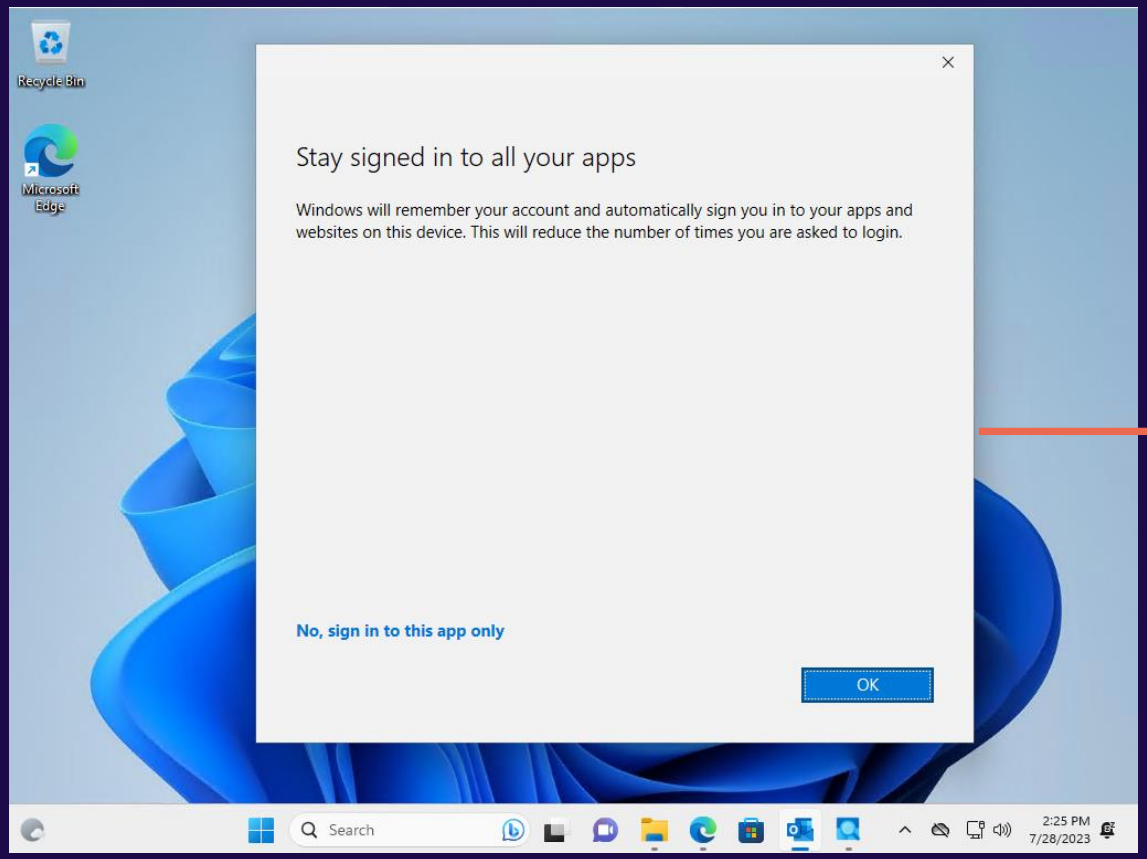
Token icon source : https://auth0.com/blog/ultimate-guide-nextjs-authentication-auth0/

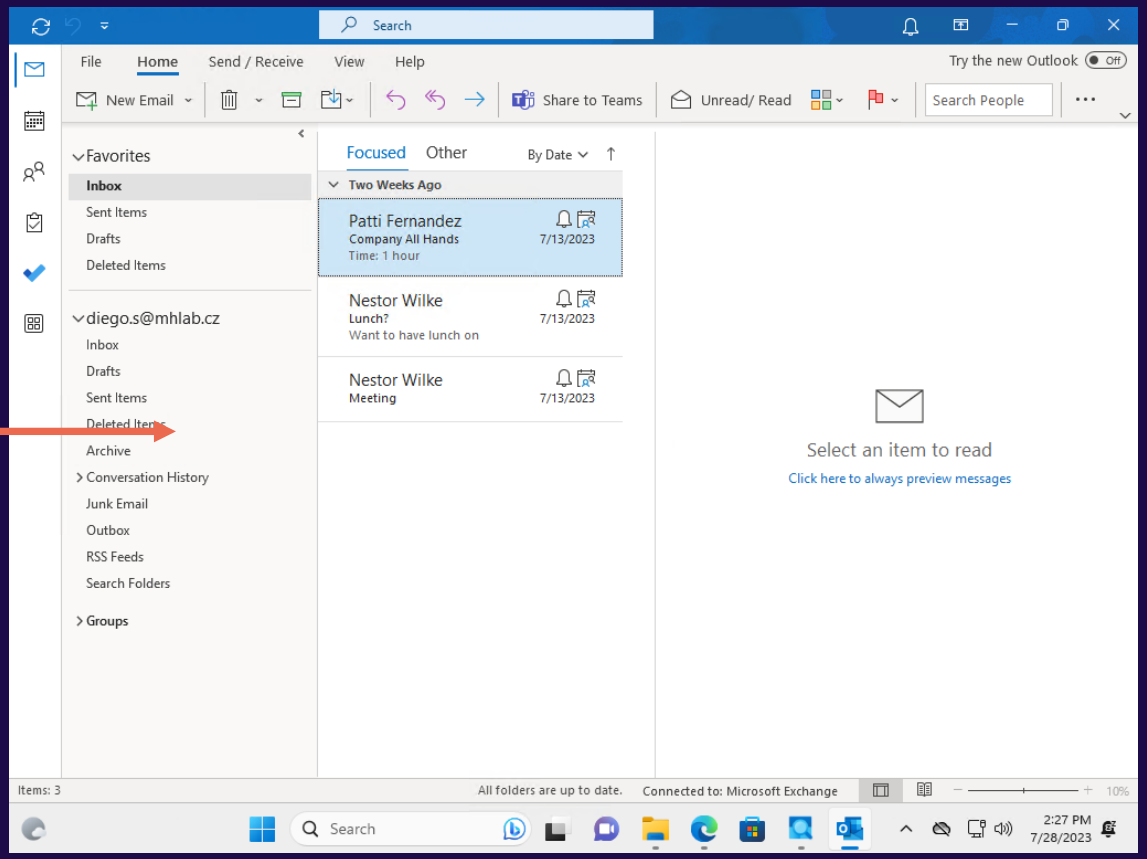
Oauth 2.0: Outlook



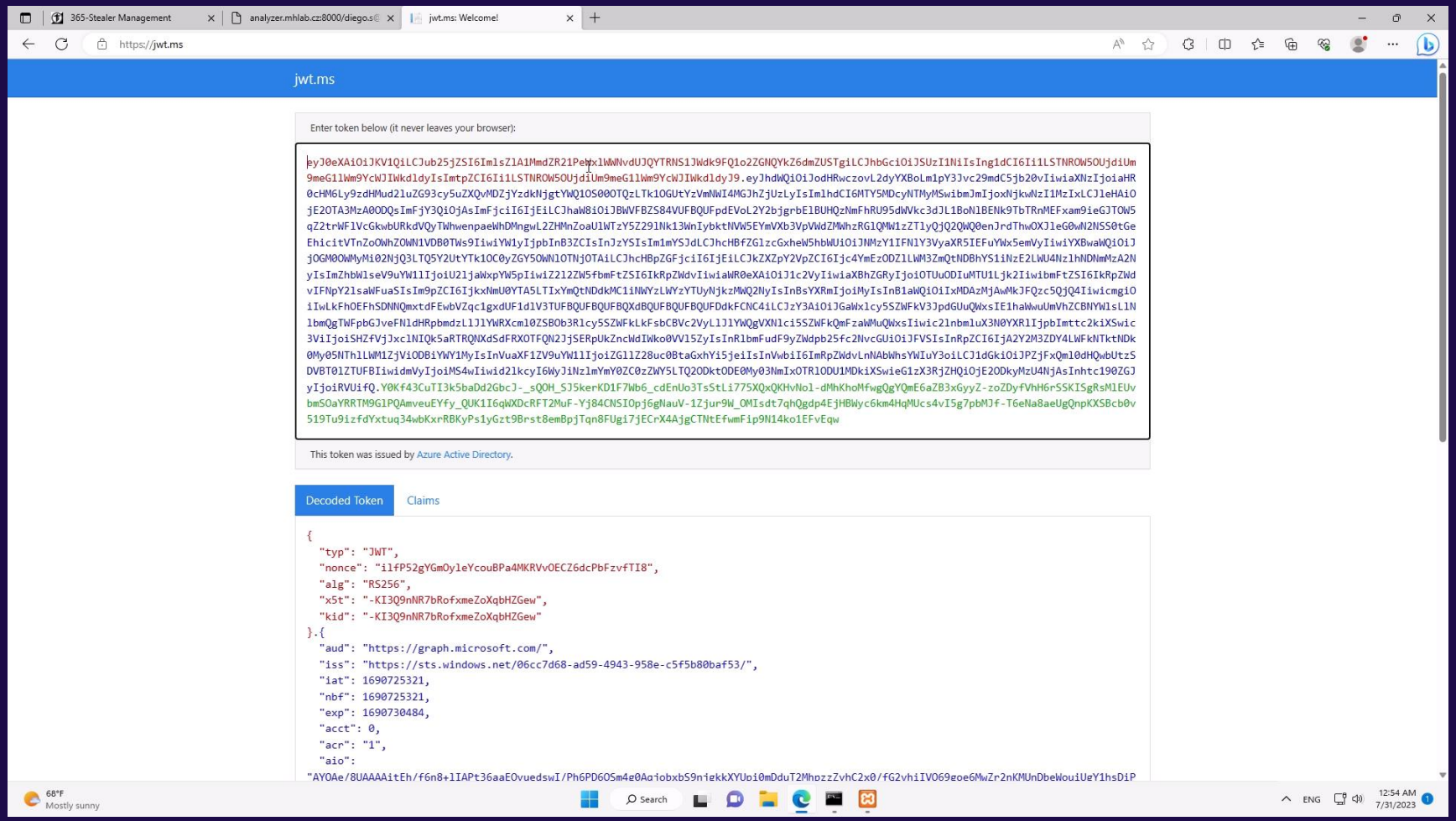


Oauth 2.0: Outlook





Oauth 2.0: Tokens demonstration



Oauth 2.0: PRT

- Primary Refresh Token (rules them all)
- Entra ID Joined, Hybrid, Registered devices
- Chráněn TPM

Oauth 2.0: Tokens

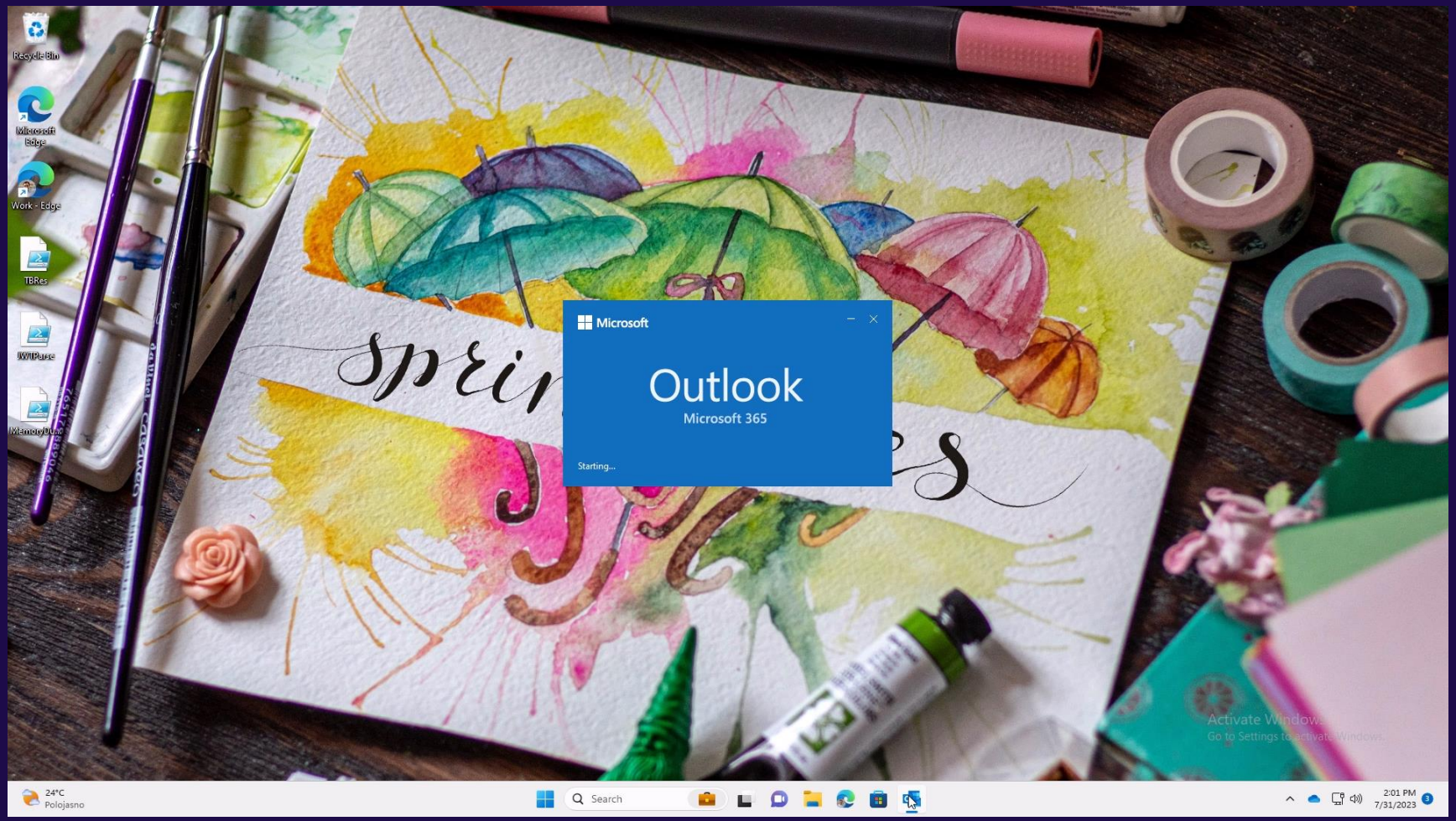
- We don’t save passwords to app no more, but tokens.
- What is the benefit on company’s PC?

Back to BYOD

BYOD: what's the problem?

- Devices are not under company's management (hardening and monitoring)
- Often compromised (https://www.bleepingcomputer.com/news/security/over-400-000-corporate-credentials-stolen-by-info-stealing-malware/)
- Contains company's credentials, tokens (PRT, RT, AT), cookies.

BYOD: token stealing



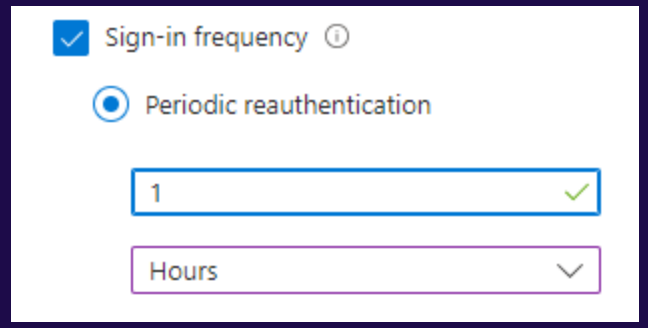
BYOD: token stealing

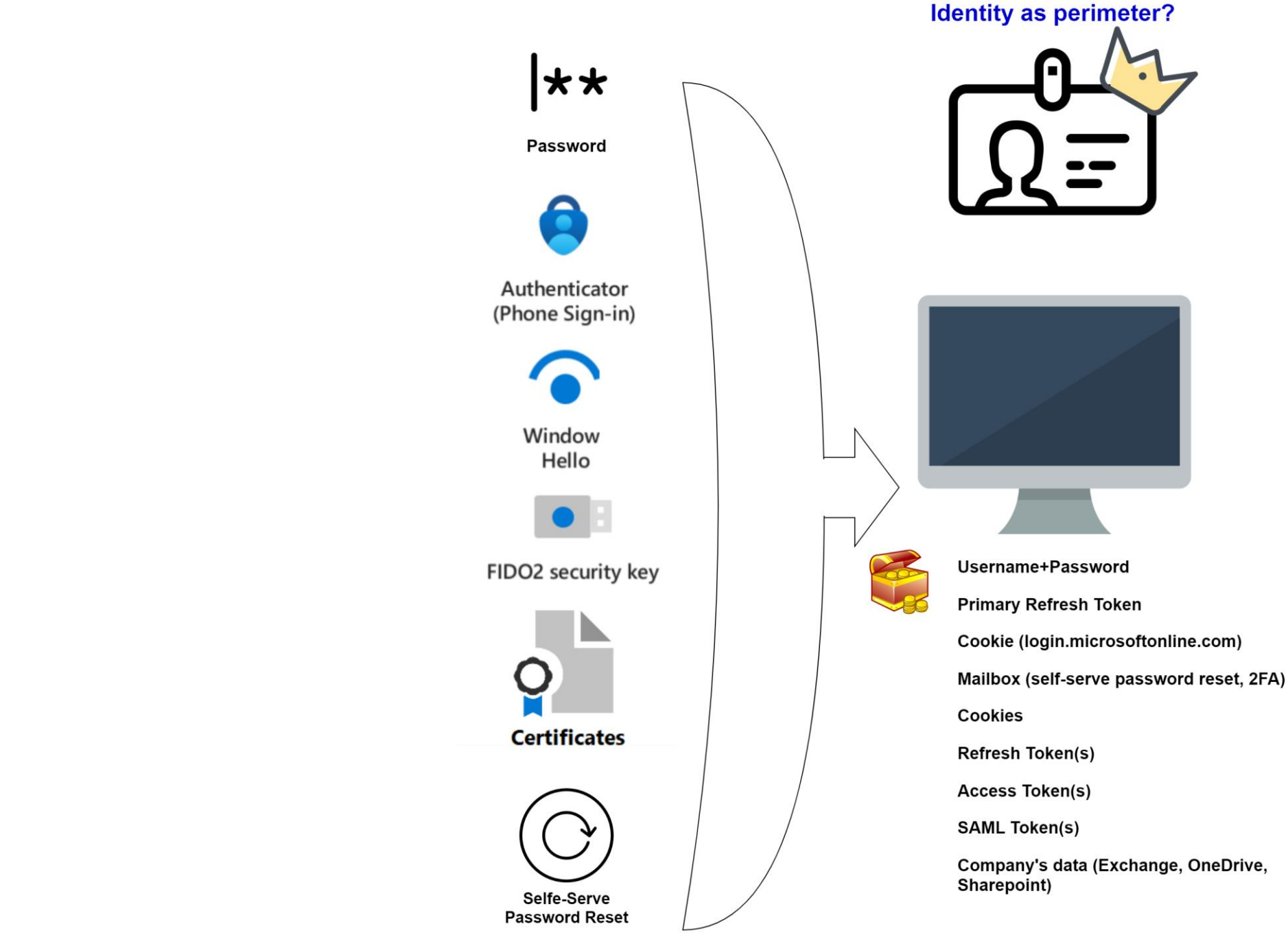
- The same is valid for RT (refresh token)
- Misuse of PRT (primary refresh token)
- Safety of a token is not related to authentication method (password, MS Authenticator, WHfB, FIDO2)
- Conditonal Acces is evaluated only during Access Token issuance

BYOD: token stealing

BYOD: cookie stealing

- Sing-in to one app compromise whole identity
- CA Sign-in frequency

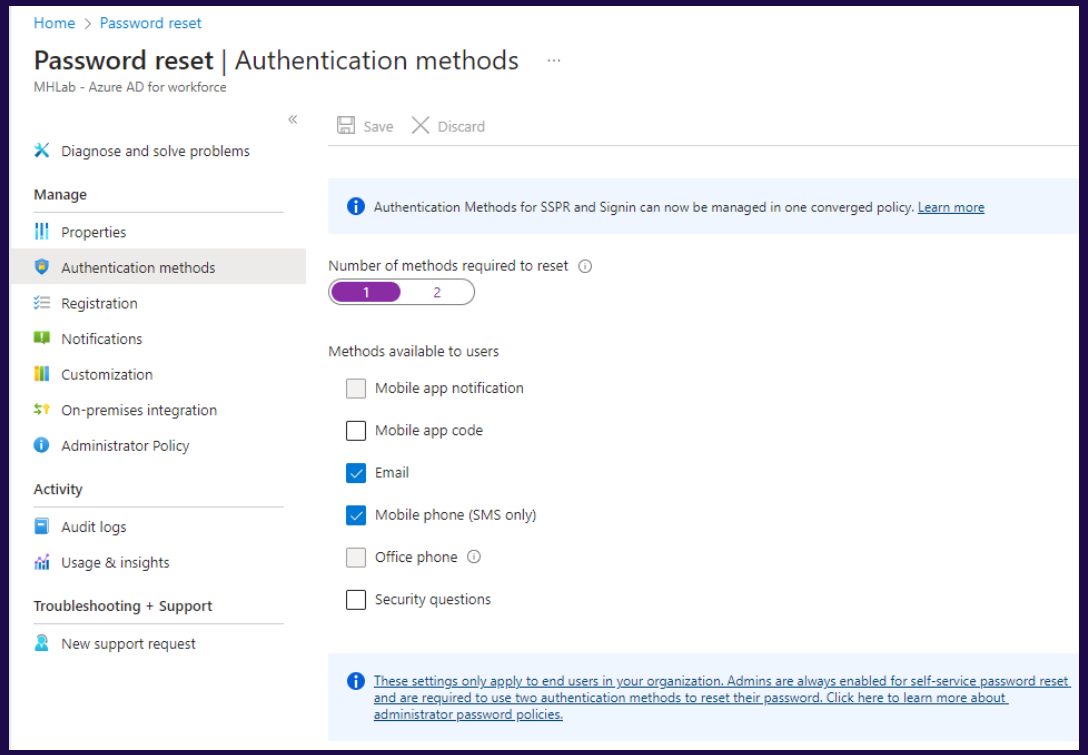



Identity as perimeter?
Password
Authenticator
(Phone Sign-in)
Window
Hello
FIDO2 security key
Certificates
Selfe-Serve
Password Reset
Username+Password
Primary Refresh Token
Cookie (login.microsoftonline.com)
Mailbox (self-serve password reset, 2FA)
Cookies
Refresh Token(s)
Access Token(s)
SAML Token(s)
Company's data (Exchange, OneDrive,
Sharepoint)

Other threats

Other threats

- Threats outside of our control – exploitation of MS
  - Incident from 07/2023 – leak of token signing keys https://www.wiz.io/blog/storm-0558-compromised-microsoft-key-enables-authentication-of-countless-micr
- Compromising of mobile phone (passwordless, tokens [PRT,RT,AT])
- Self-serve password reset portal



Summary

Initial vector

- Credentials leak from other service
- Phishing
  - Malware execution
  - Theft of credentials
  - Illicit Consent Grant
  - Device code flow
- Threats on PC/device (particularly BYOD)
  - Keylogger / theft of credentials
  - Theft of artefacts (tokens)
  - Abuse of PC to issue new tokens (benefit from PRT)
- Login credentials
  - Physical theft (e.g. token, smart phone)
  - Control of authentication device (e.g. smart phone, passwordless)
- Mistakes on Microsoft side

Resources

Where to find more knowledge

» OAuth 2.0 and OpenID Connect (in plain English) - https://www.youtube.com/watch?v=996OiexHze0

» Tokens, everywhere! - https://www.youtube.com/watch?v=8qEh1pc0tT8&t=3584s

» https://aadinternals.com/

» https://dirkjanm.io/

» https://github.com/WillOram/AzureAD-incident-response

» https://www.alteredsecurity.com/post/Introduction-To-365-Stealer

Děkuji za ⟨pozornost⟩