

A complex network diagram with numerous nodes and connections, rendered in shades of blue and purple. The nodes are represented by small squares and circles, some containing numerical values like 48.15, 45.79, 69.23, 26.37, 67.44, 27.15, 56.10, 31.75, and 79.93. The connections are thin lines forming a dense web.

Martin Haller

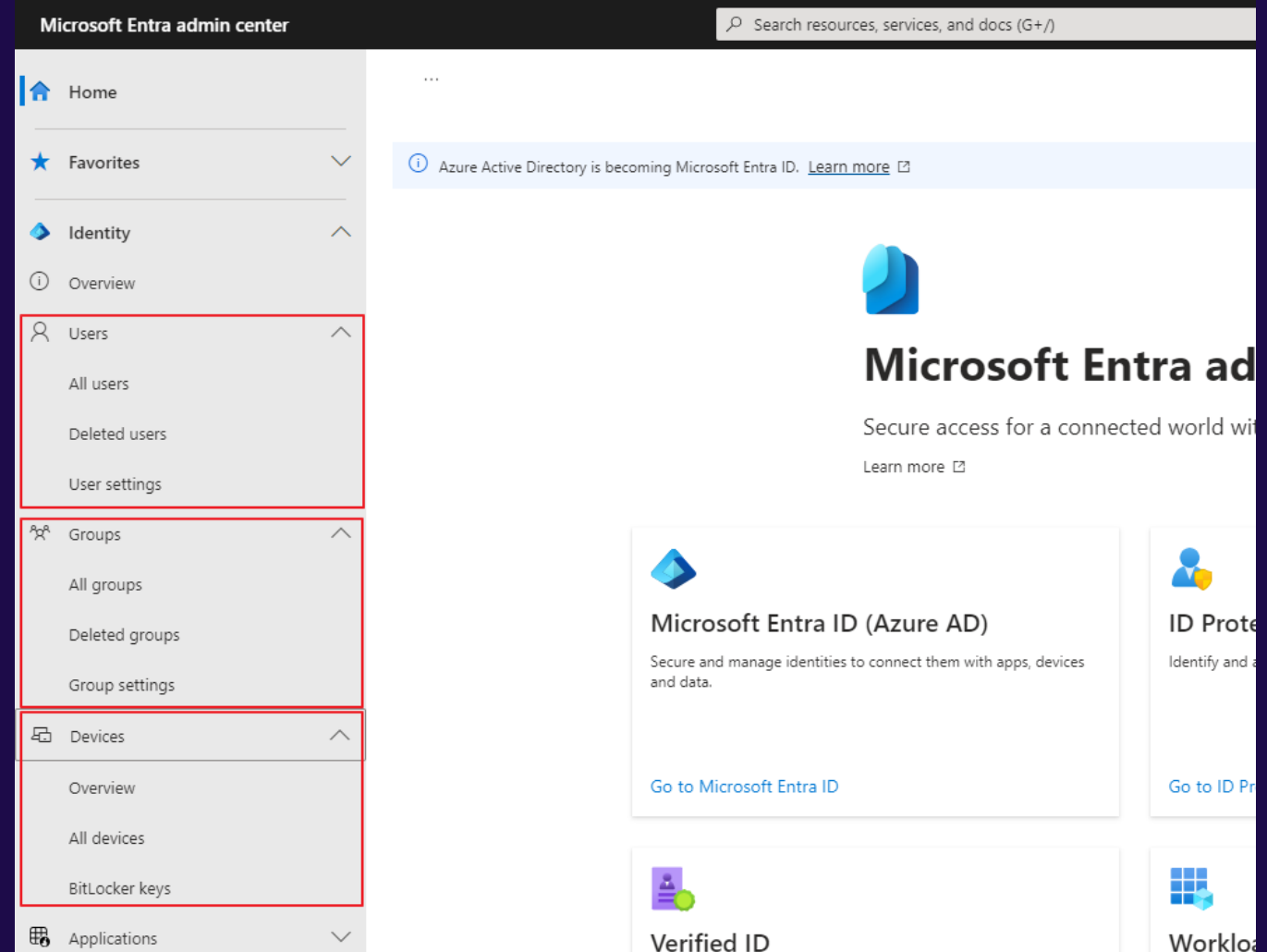
Microsoft Entra ID Attack surface

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 Access (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

The screenshot shows the Microsoft Entra admin center interface. The main content area displays the 'Overview' tab for the tenant 'MSFT'. A notification banner at the top states: 'Azure Active Directory is becoming Microsoft Entra ID. Learn more'. Below this, there are tabs for 'Overview', 'Monitoring', 'Properties', 'Recommendations', and 'Tutorials'. A search bar for the tenant is present. The 'Basic information' section contains the following data:

Property	Value	Property	Value
Name	MSFT	Users	17
Tenant ID	06cc7d68-ad59-4943-958e-c5f5b80baf53	Groups	8
Primary domain	mhlab.cz	Applications	1
License	Azure AD Premium P2	Devices	1
Workload License	Azure AD Workload Free		

Below the basic information, there is an 'Alerts' section with a notification: 'Upcoming Azure AD rename. Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you. Learn more'.

The screenshot shows the 'Active Directory Users and Computers' console window. The left pane shows a tree view of the directory structure for 'ad.patron-it.cz', with 'Users' selected. The right pane displays a list of users and groups with the following columns: Name, Type, and Description.

Name	Type	Description
Administrator	User	Built-in account for a...
Allowed RODC Password Replication Group	Security Group...	Members in this grou...
Cert Publishers	Security Group...	Members of this grou...
Cloneable Domain Controllers	Security Group...	Members of this grou...
ForeignSecurityPrincipals	Security Group...	Members of this grou...
Denied RODC Password Replication Group	Security Group...	Members in this grou...
DHCP Administrators	Security Group...	Members who have a...
DHCP Users	Security Group...	Members who have v...
DnsAdmins	Security Group...	DNS Administrators C...
DnsUpdateProxy	Security Group...	DNS clients who are p...
Domain Admins	Security Group...	Designated administr...
Domain Computers	Security Group...	All workstations and ...
Domain Controllers	Security Group...	All domain controller...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administr...
Enterprise Key Admins	Security Group...	Members of this grou...
Enterprise Read-only Domain Controllers	Security Group...	Members of this grou...
Group Policy Creator Owners	Security Group...	Members in this grou...
Guest	User	Built-in account for g...
Key Admins	Security Group...	Members of this grou...
krbtgt	User	Key Distribution Cent...
Protected Users	Security Group...	Members of this grou...
RAS and IAS Servers	Security Group...	Servers in this grou...
Read-only Domain Controllers	Security Group...	Members of this grou...
Schema Admins	Security Group...	Designated administr...
WinRMRemoteWMIUsers_...	Security Group...	Members of this grou...

Microsoft Entra ID vs Active Directory



Microsoft Entra ID

- » Oauth
- » SAML



Active Directory

- » NTLM
- » Kerberos

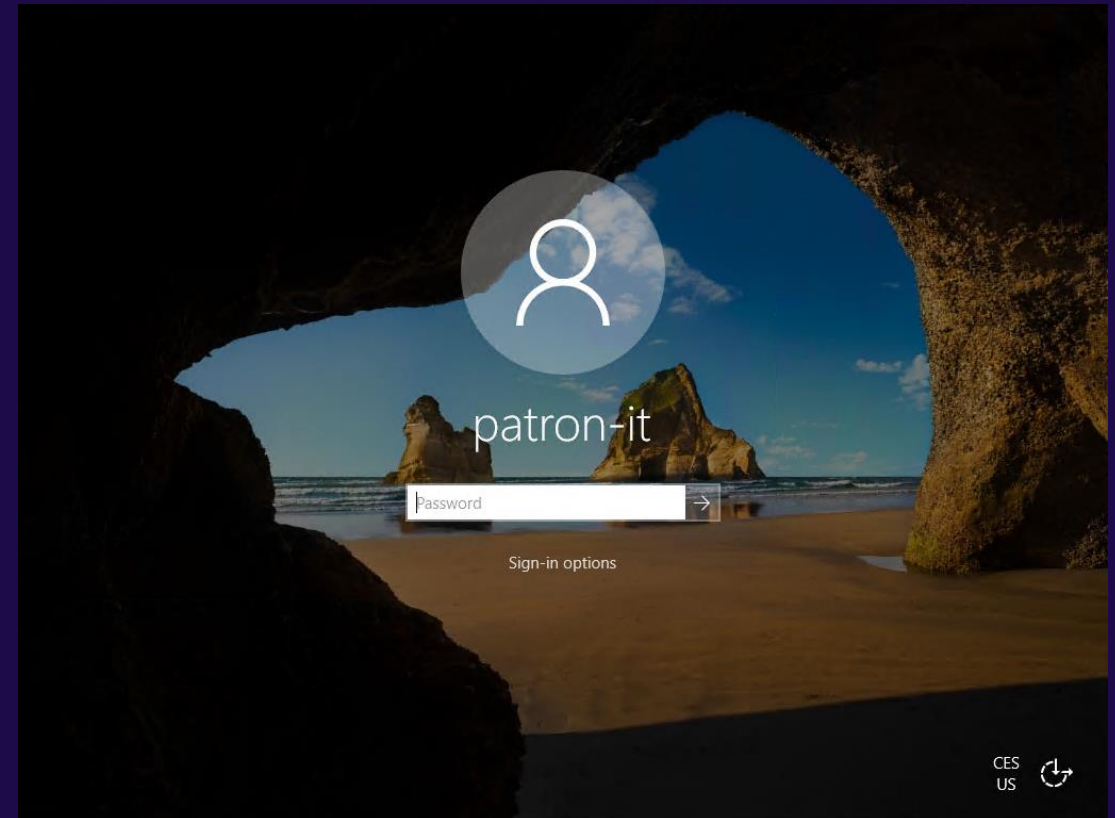
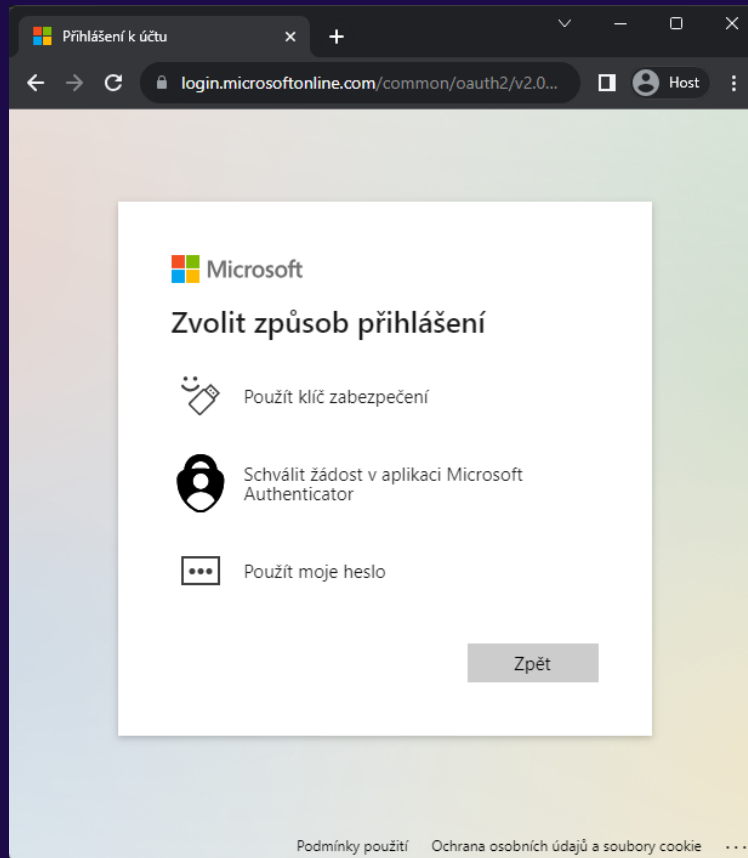
Microsoft Entra ID vs Active Directory



Microsoft Entra ID



Active Directory



Microsoft Entra ID vs Active Directory



Microsoft Entra ID



Active Directory

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	

- » Password
- » Smart card

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

Entra ID: Attack surface

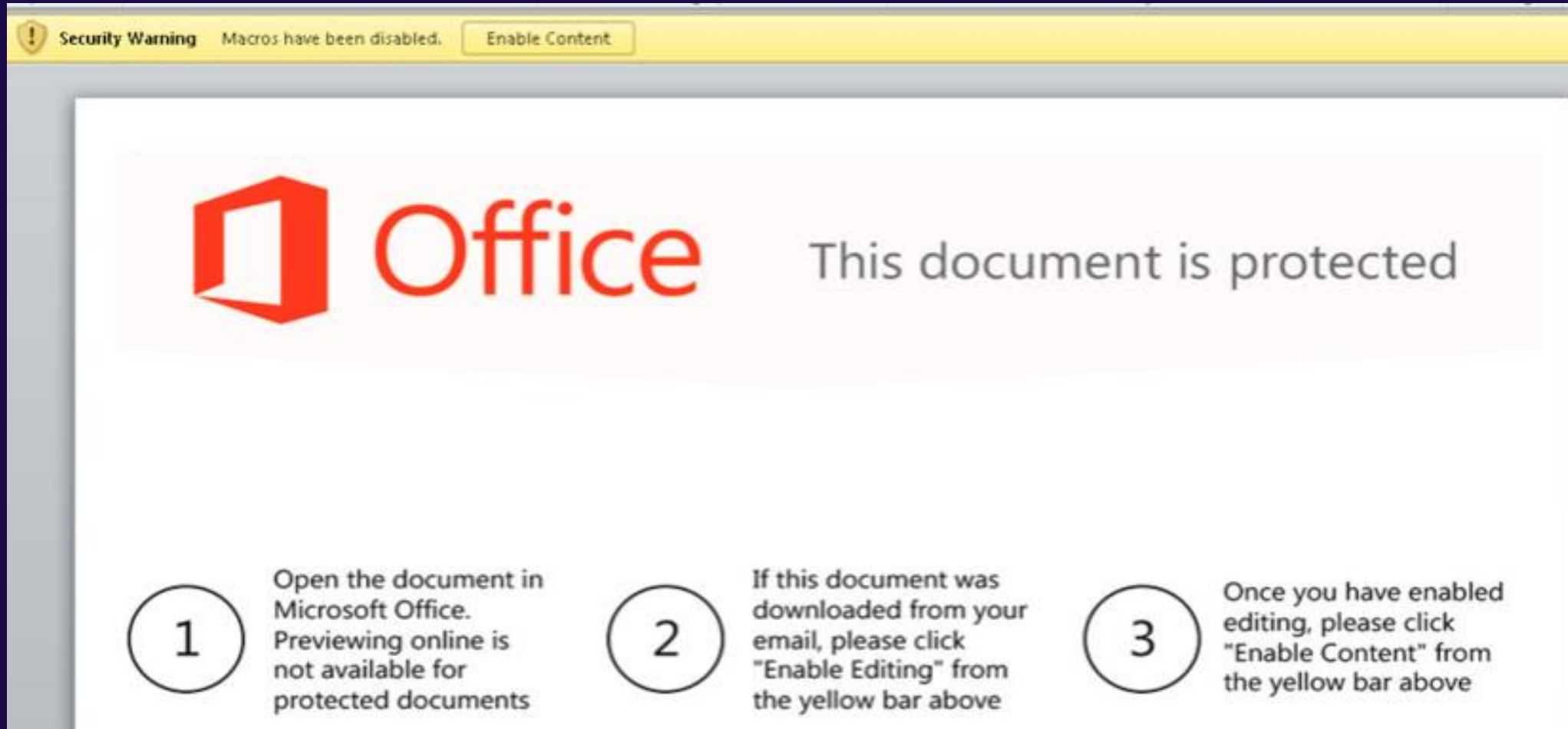
Today's agenda?

- » 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

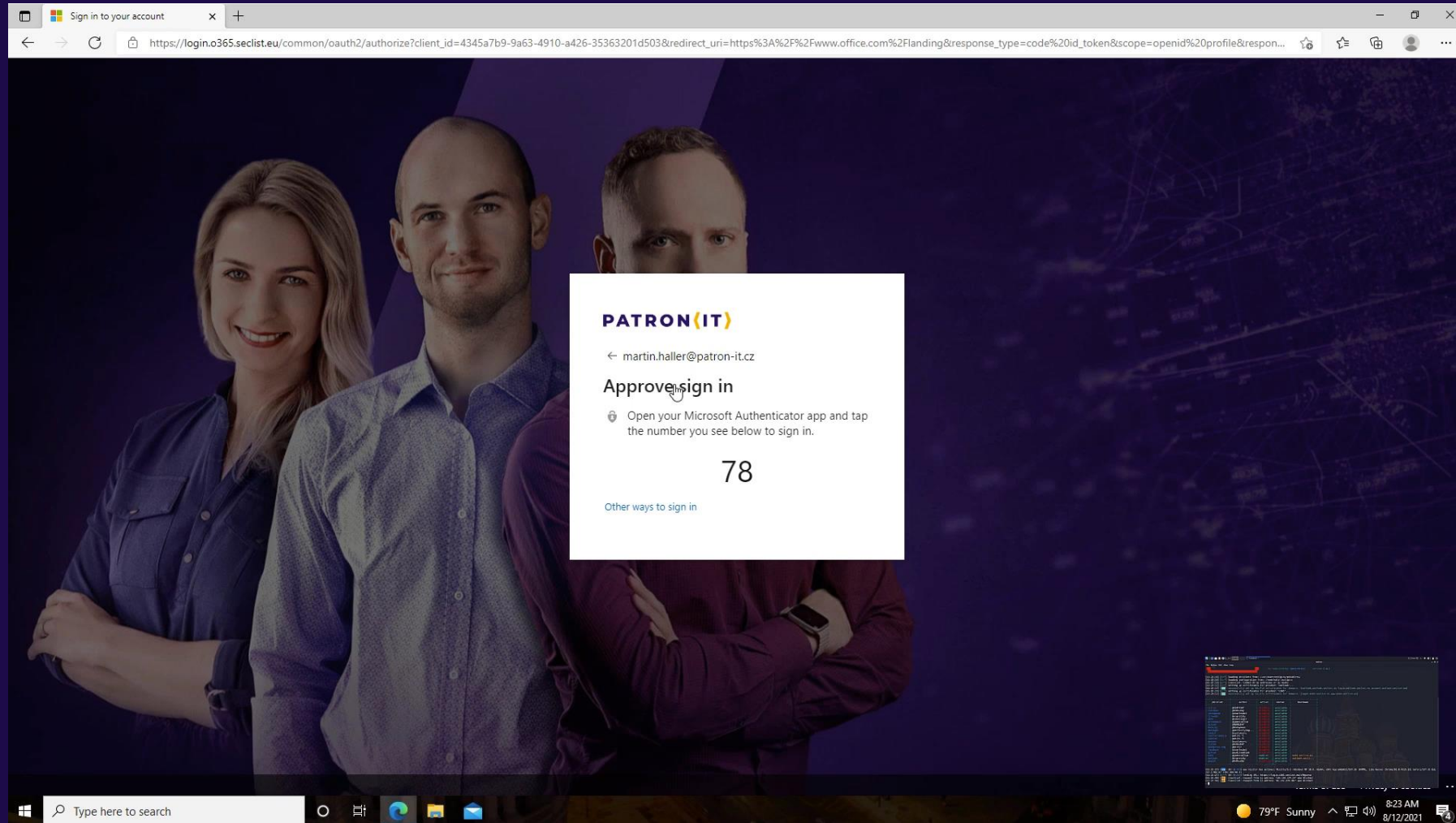


The image shows a screenshot of a Microsoft Office document preview page. At the top, there is a yellow security warning bar that reads "Security Warning Macros have been disabled." with an "Enable Content" button. Below the bar, the Microsoft Office logo is displayed on the left, and the text "This document is protected" is on the right. At the bottom, there are three numbered steps in a list:

- 1 Open the document in Microsoft Office. Previewing online is not available for protected documents
- 2 If this document was downloaded from your email, please click "Enable Editing" from the yellow bar above
- 3 Once you have enabled editing, please click "Enable Content" from the yellow bar above

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

Cloud -> Phishing: 🎯 Steal credentials

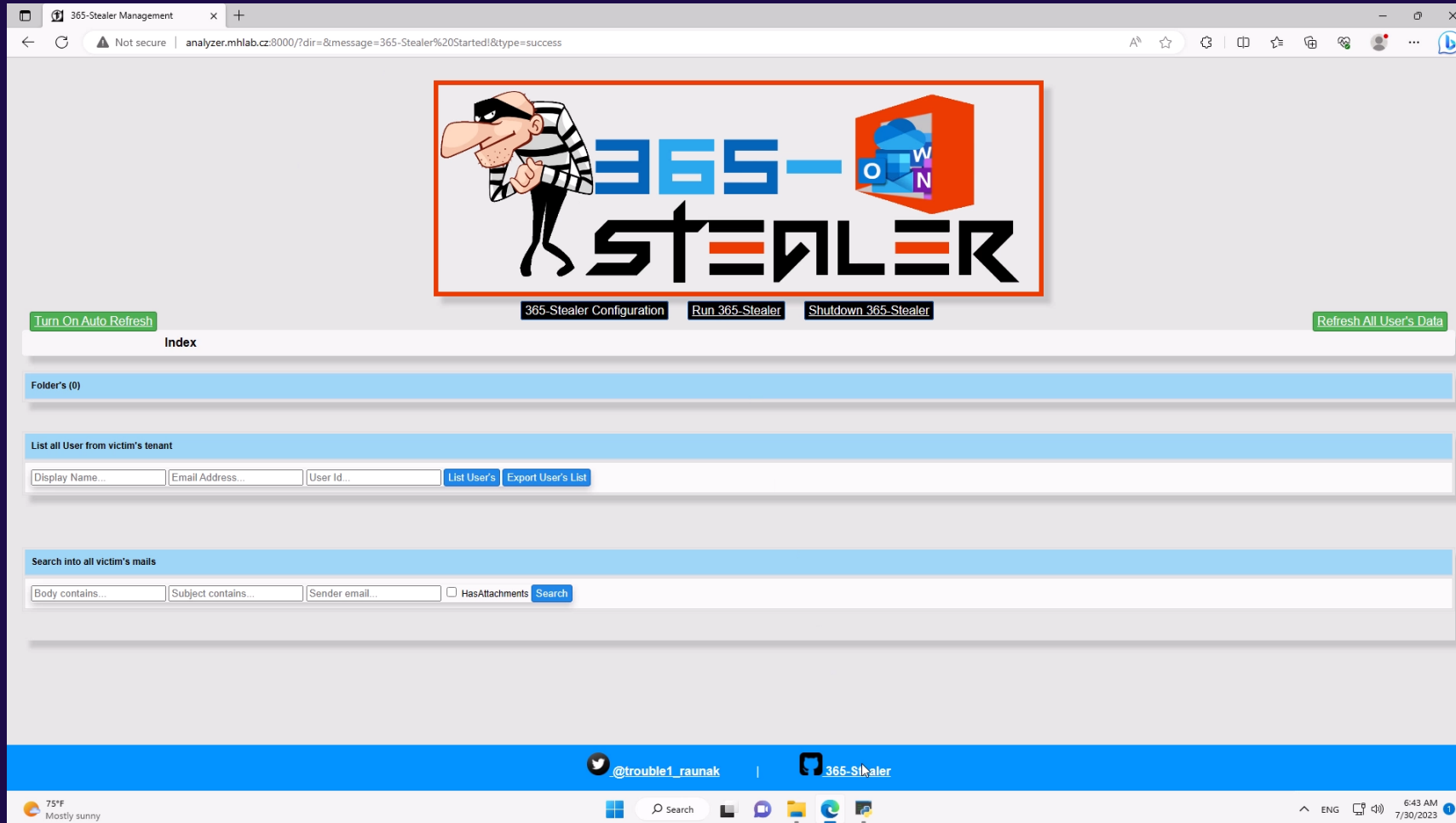


Cloud -> Phishing: 🎯 Steal credentials

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



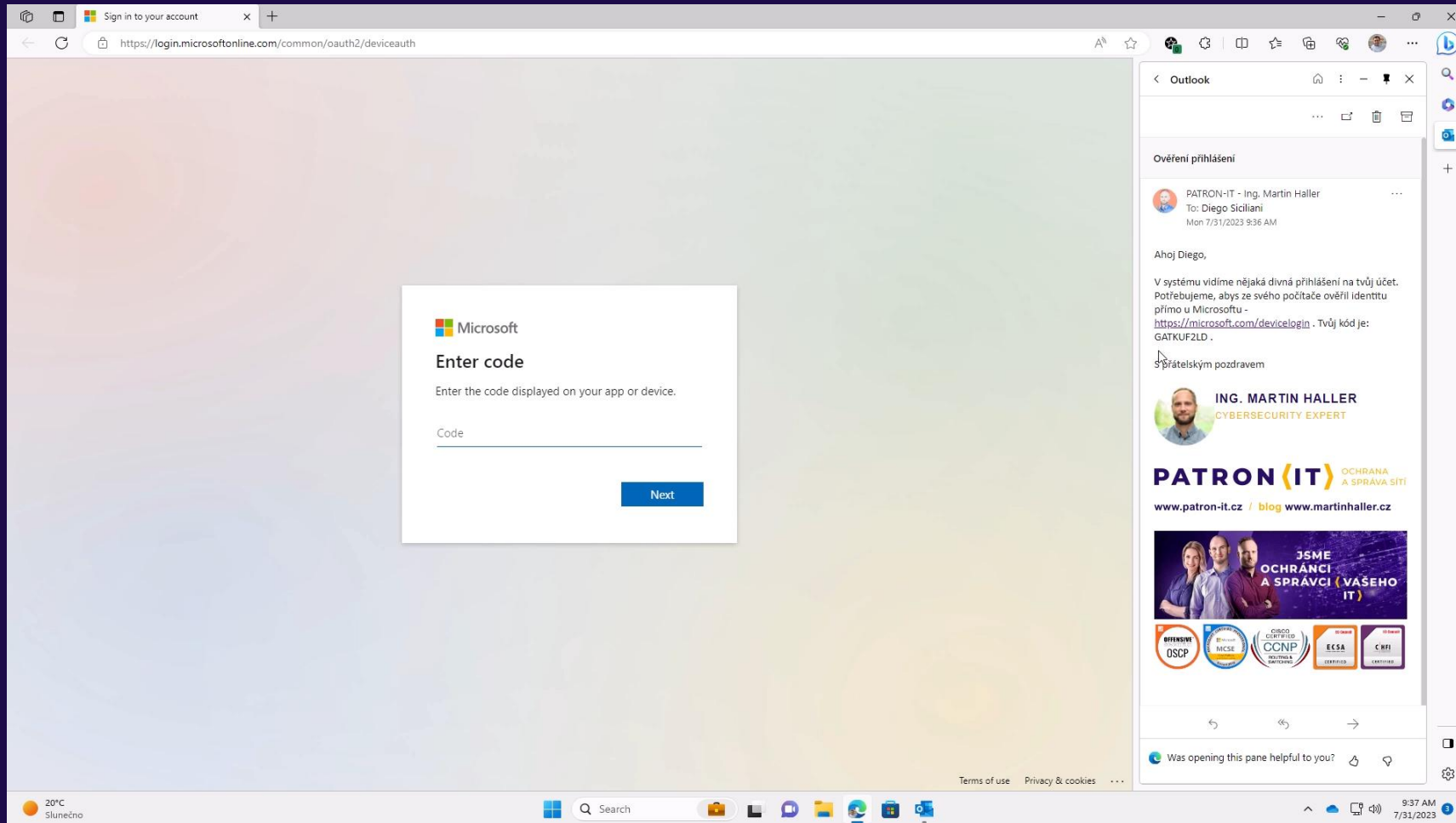
Cloud -> Phishing: 🎯 Illicit Consent Grant

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



The screenshot shows a web browser window with a Microsoft login page on the left and a phishing email on the right. The login page is titled "Enter code" and asks the user to enter a code displayed on their app or device. The email is from "PATRON-IT - Ing. Martin Haller" and contains a link to a Microsoft login page with a device code: "https://microsoft.com/devicelogin . Tvůj kód je: GATKUF2LD .". The email also includes a profile picture of Ing. Martin Haller, a "CYBERSECURITY EXPERT", and a logo for "PATRON (IT) OCHRANA A SPRÁVA SÍTI". The browser's address bar shows the URL "https://login.microsoftonline.com/common/oauth2/deviceauth". The Windows taskbar at the bottom shows the date and time as 9:37 AM on 7/31/2023.

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:

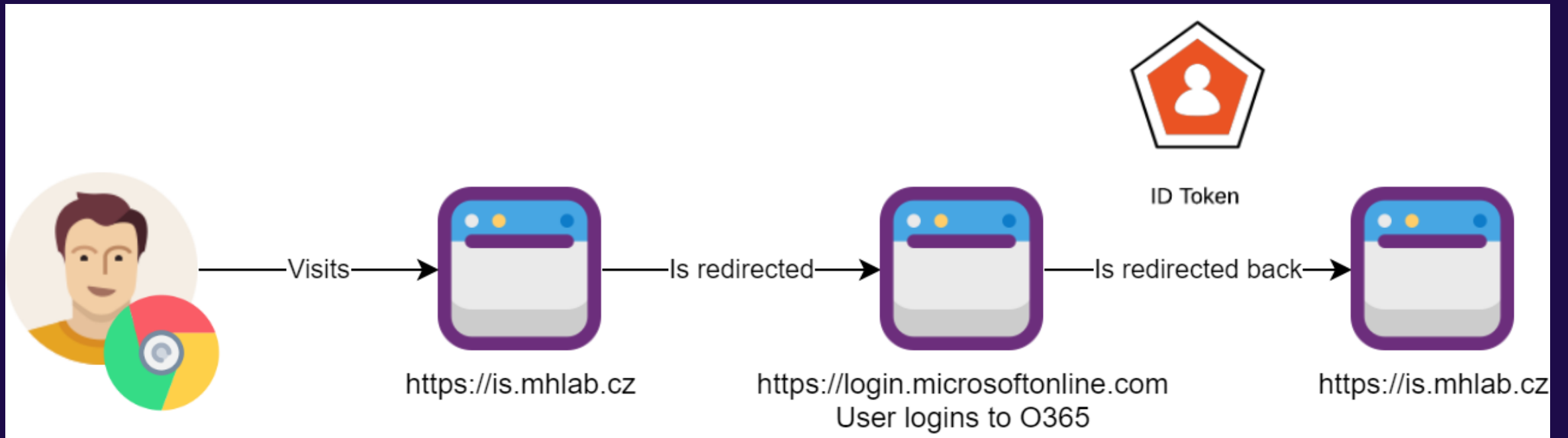
- » **Login credentials** (Plaintext creds)
- » **NT Hash** (NTLM)
- » **TGT a TGS** (Kerberos)

```
Authentication Id : 0 ; 2858340 <00000000:002b9d64>
Session           : Service from 0
User Name         : svc-SQLDBEngine01
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-2222329127-1607

msv :
00000000 Primary
* Username : svc-SQLDBEngine01
* Domain   : ADSECLAB
* NTLM     : d0abfc0cb689f4cdc8959a1411499096
* SHA1     : 467f0516e6155eed60668827b0a4dab5eecefacd
tspkg :
* Username : svc-SQLDBEngine01
* Domain   : ADSECLAB
* Password : ThisIsAGoodPassword99!
wdigest :
* Username : svc-SQLDBEngine01
* Domain   : ADSECLAB
* Password : ThisIsAGoodPassword99!
kerberos :
* Username : svc-SQLDBEngine01
* Domain   : LAB.ADSECURITY.ORG
* Password : ThisIsAGoodPassword99!
ssp :
credman :
```

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

Oauth 2.0 – principle simplified



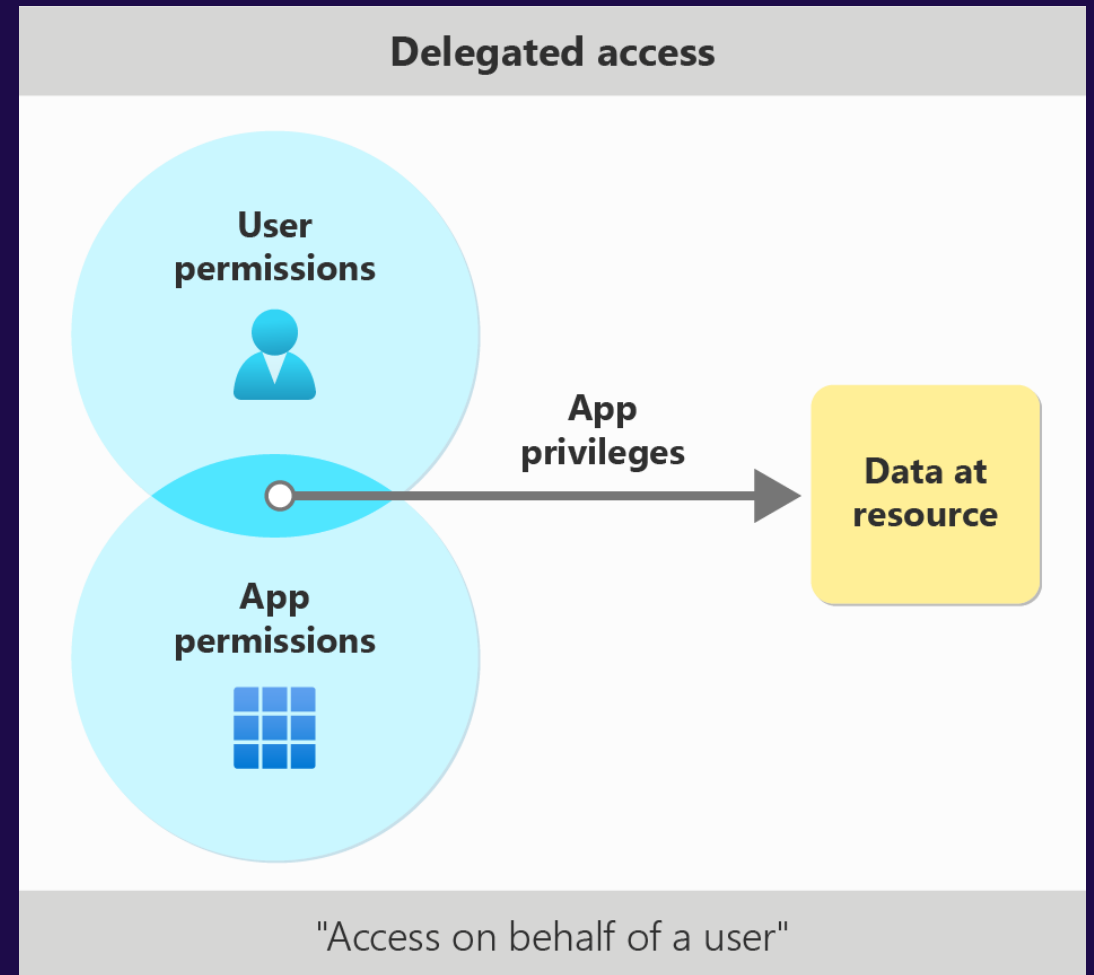
Token icon source: <https://auth0.com/blog/ultimate-guide-nextjs-authentication-auth0/>

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)?

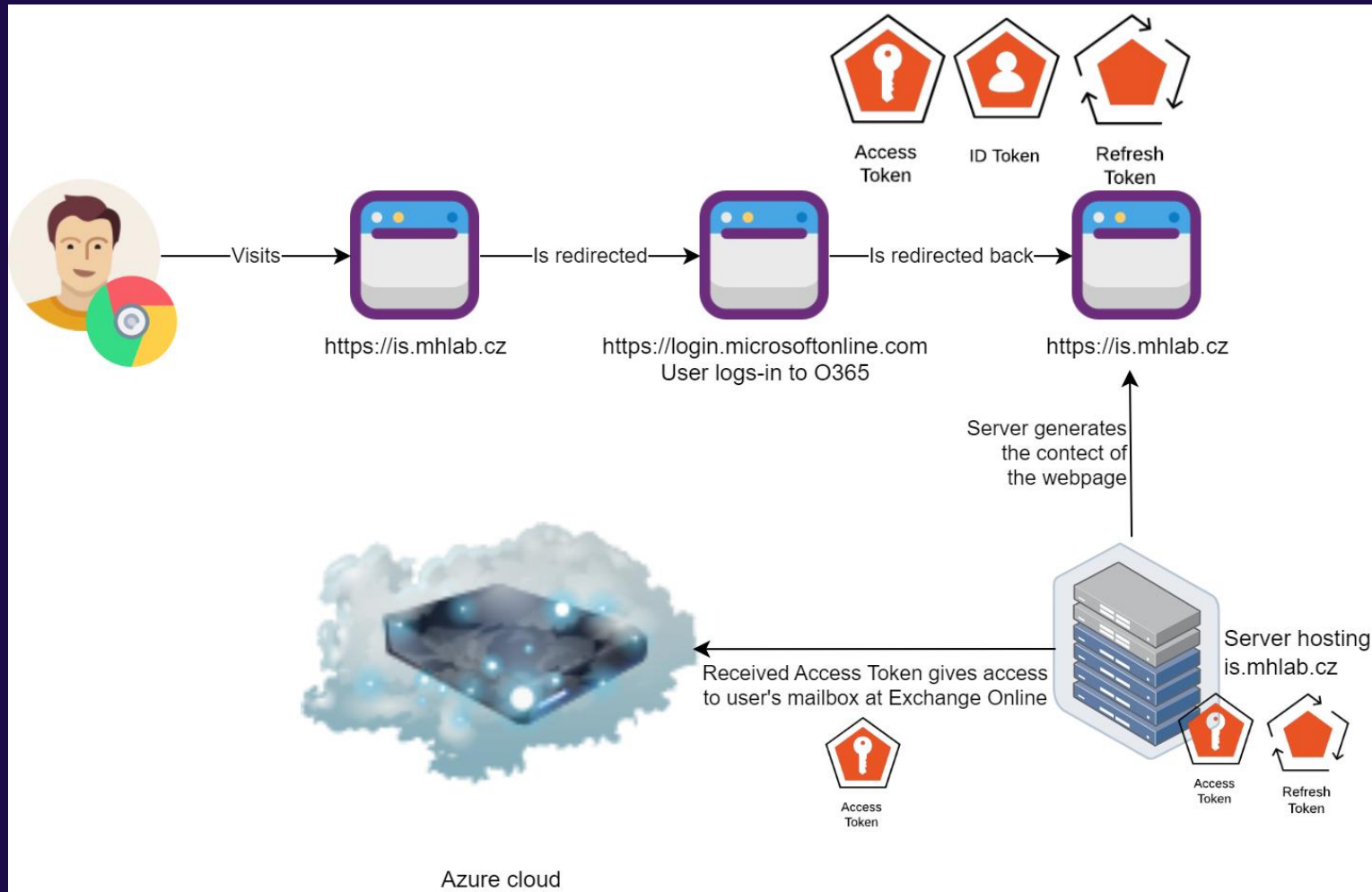
Oauth 2.0: tokens

- » **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).



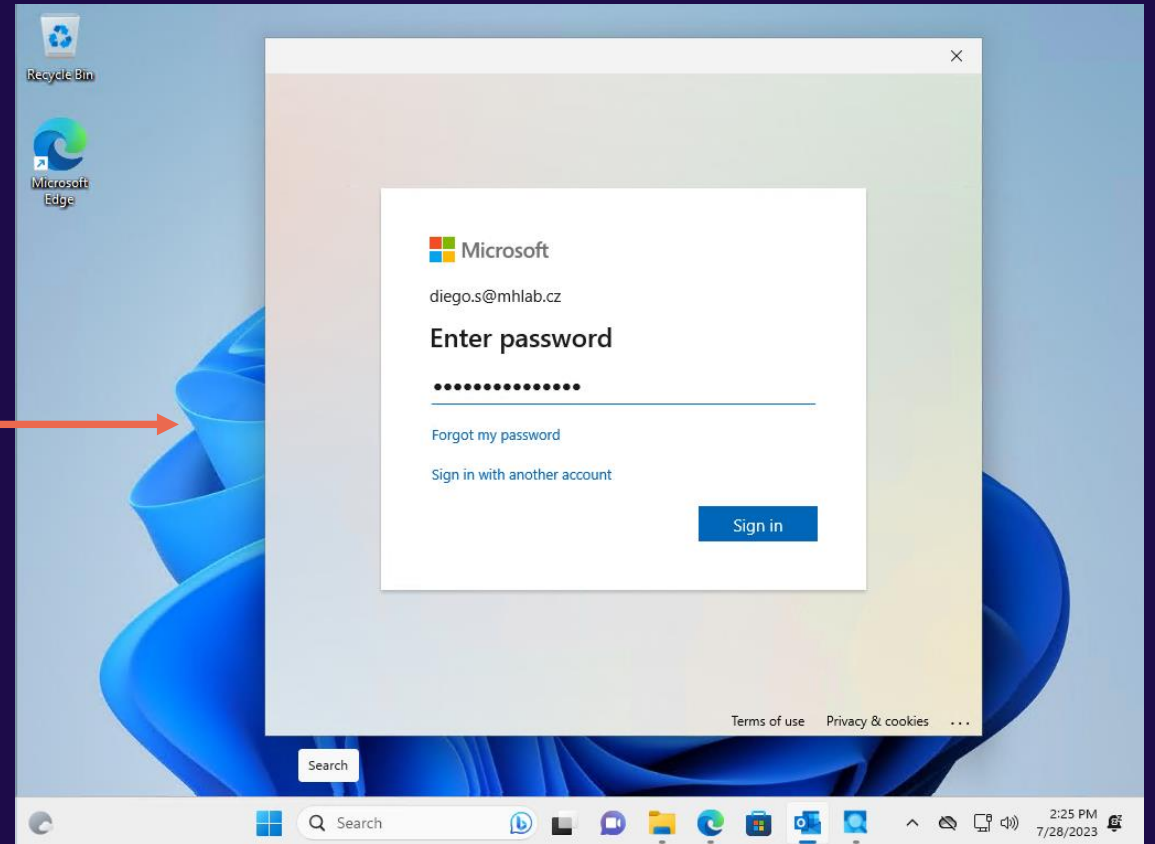
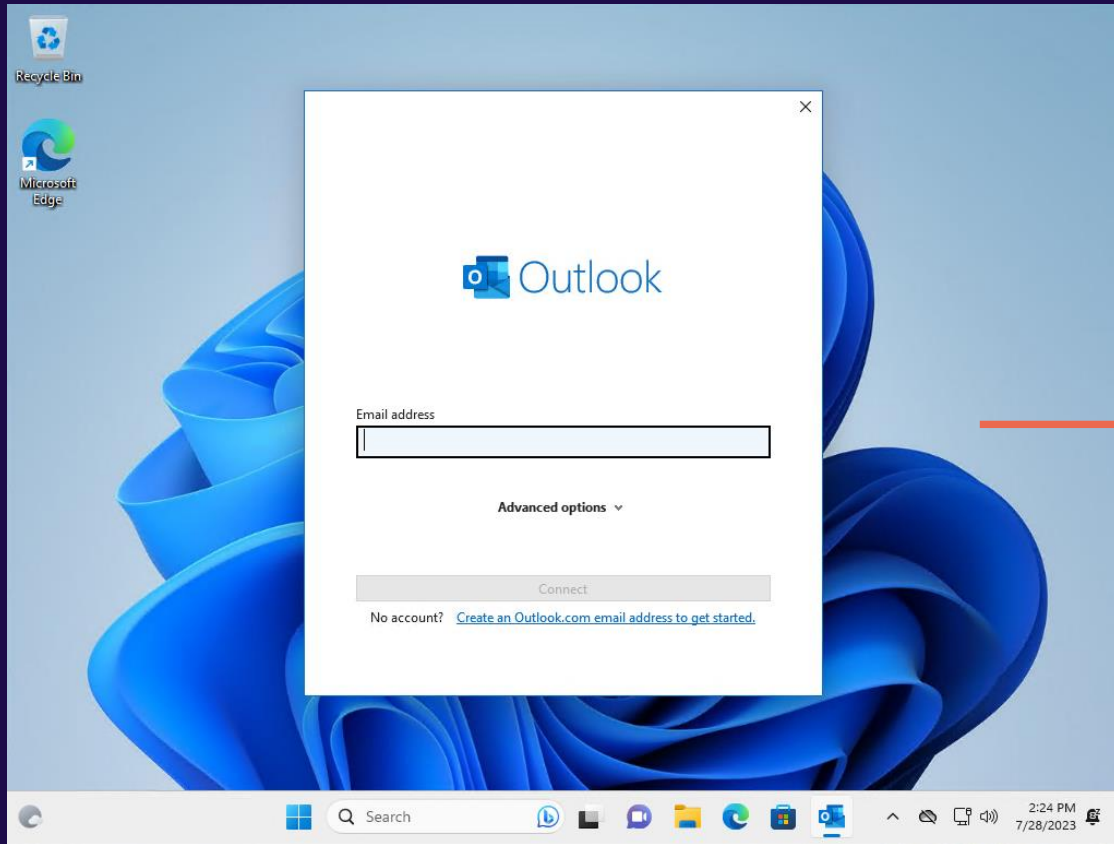
Source: <https://learn.microsoft.com/en-us/azure/active-directory/develop/permissions-consent-overview>

Oauth 2.0 – zjednodušený princip

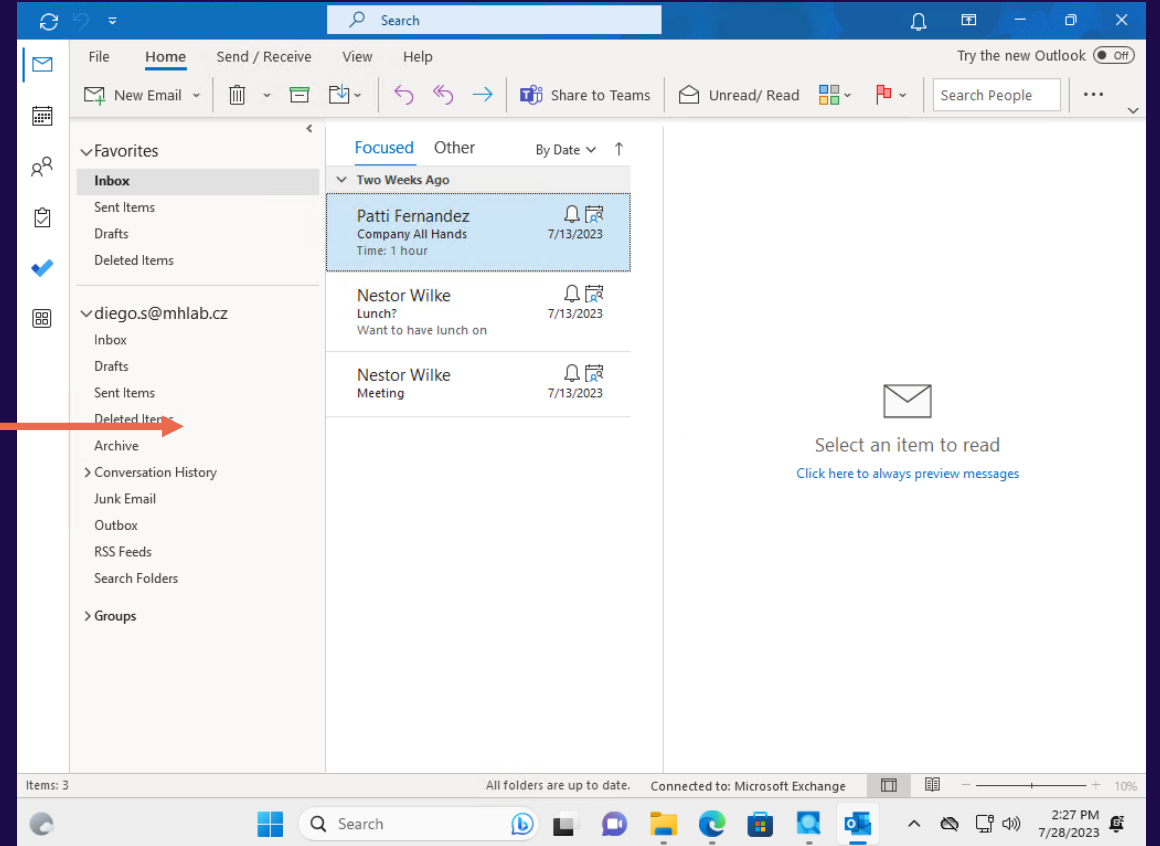
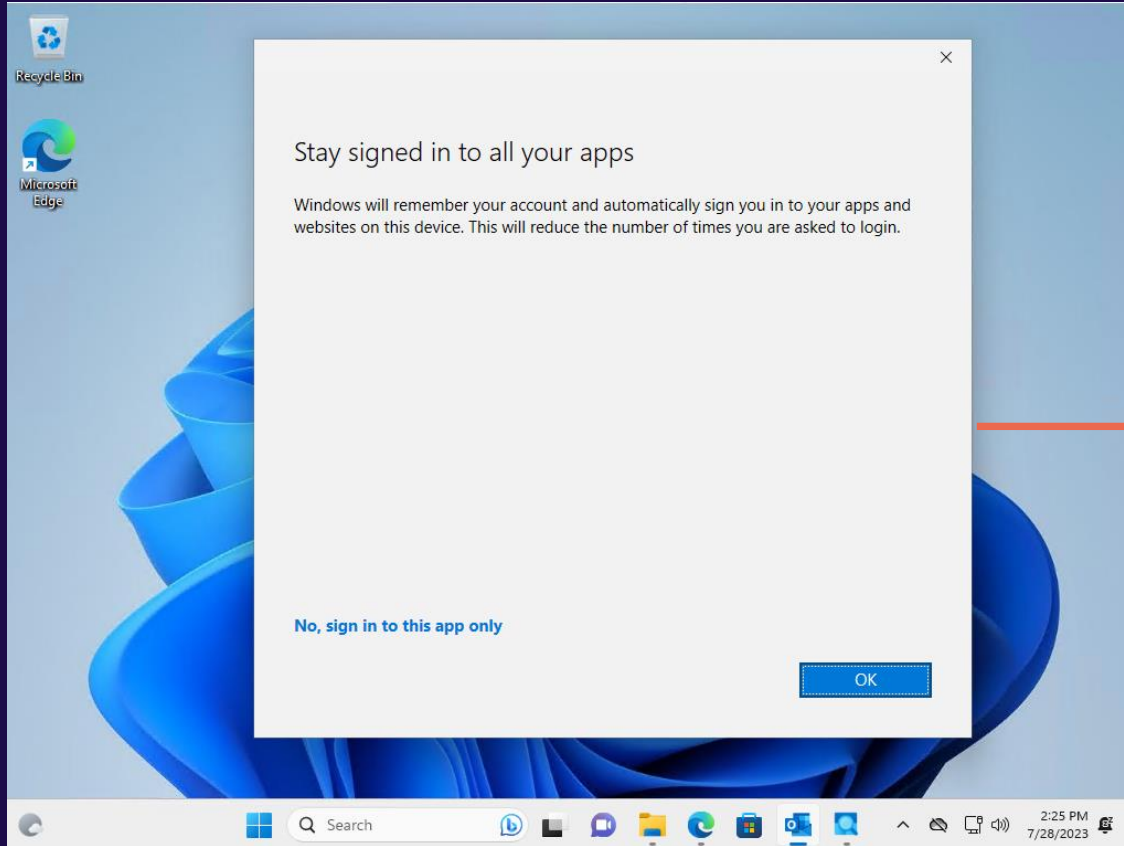


Token icon source : <https://auth0.com/blog/ultimate-guide-nextjs-authentication-auth0/>

Oauth 2.0: Outlook



Oauth 2.0: Outlook



Oauth 2.0: Tokens demonstration

The screenshot shows a web browser window with the URL `https://jwt.ms`. The page title is "jwt.ms". A text input field contains a long JWT token. Below the input, a message states: "This token was issued by Azure Active Directory." Below that, there are two tabs: "Decoded Token" (selected) and "Claims". The "Decoded Token" tab shows the following JSON structure:

```
{
  "typ": "JWT",
  "nonce": "11fP52gYGmOy1eYcouBP4MKRVvOECZ6dcPbFzvfTI8",
  "alg": "RS256",
  "x5t": "-KI3Q9nNR7bRofxmeZoXqbHZGew",
  "kid": "-KI3Q9nNR7bRofxmeZoXqbHZGew"
}.- {
  "aud": "https://graph.microsoft.com/",
  "iss": "https://sts.windows.net/06cc7d68-ad59-4943-958e-c5f5b80baf53/",
  "iat": 1690725321,
  "nbf": 1690725321,
  "exp": 1690730484,
  "acct": 0,
  "acr": "1",
  "aio": "AYOAE/8UAAAAItEh/f6n8+1IAPT36aaEOvuedswI/Ph6PD605m4e0Aaioxb59niekxYUo10mDduT2Mh0zzZvhC2x0/fG2vh1IV069eoe6MwZr2nMUNDeWou1UeY1hsD1P"
```

Oauth 2.0: PRT

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

Oauth 2.0: Tokens

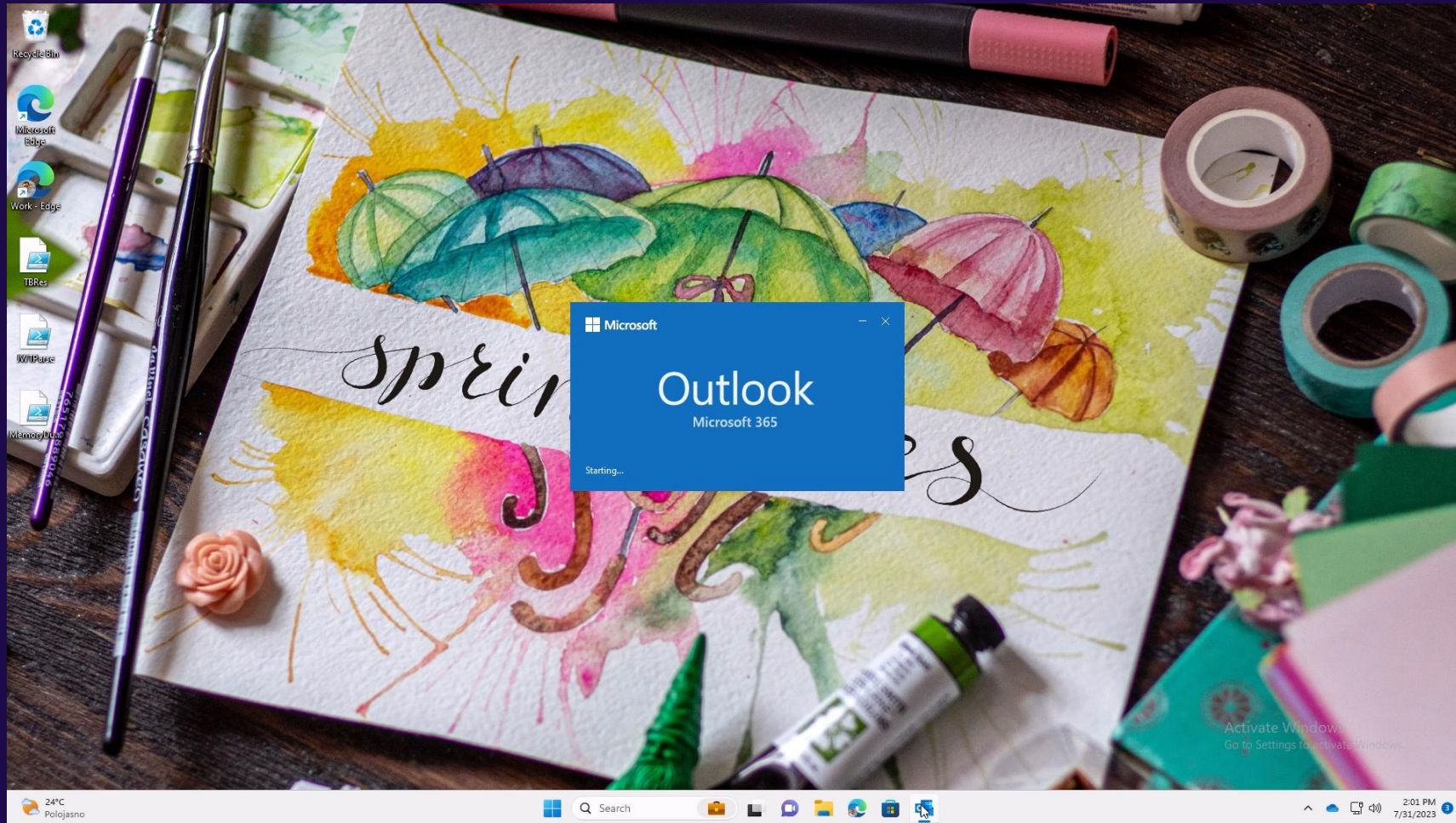
- » We don't save passwords to app no more, but tokens.
- » What is the benefit on company's PC?

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

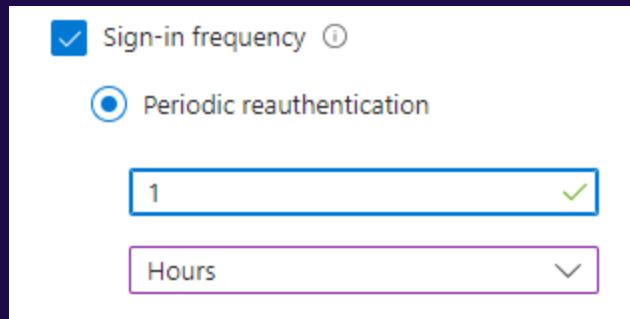
- » The same is valid for RT (refresh token)
- » Misuse of PRT (primary refresh token)
- » Safety of a token is not related to authentication method (password, MS Authenticator, WHfB, FIDO2)
- » Conditional Access is evaluated only during Access Token issuance

BYOD: token stealing



BYOD: cookie stealing

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



Sign-in frequency ⓘ

Periodic reauthentication

1 ✓

Hours ▼

Identity as perimeter?



Password



Authenticator
(Phone Sign-in)



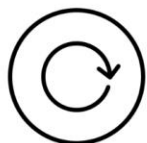
Window
Hello



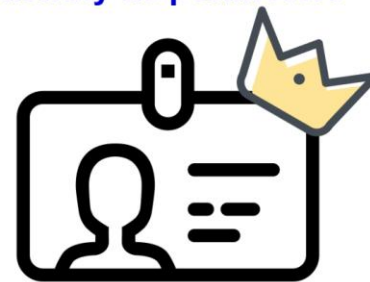
FIDO2 security key



Certificates



Self-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)

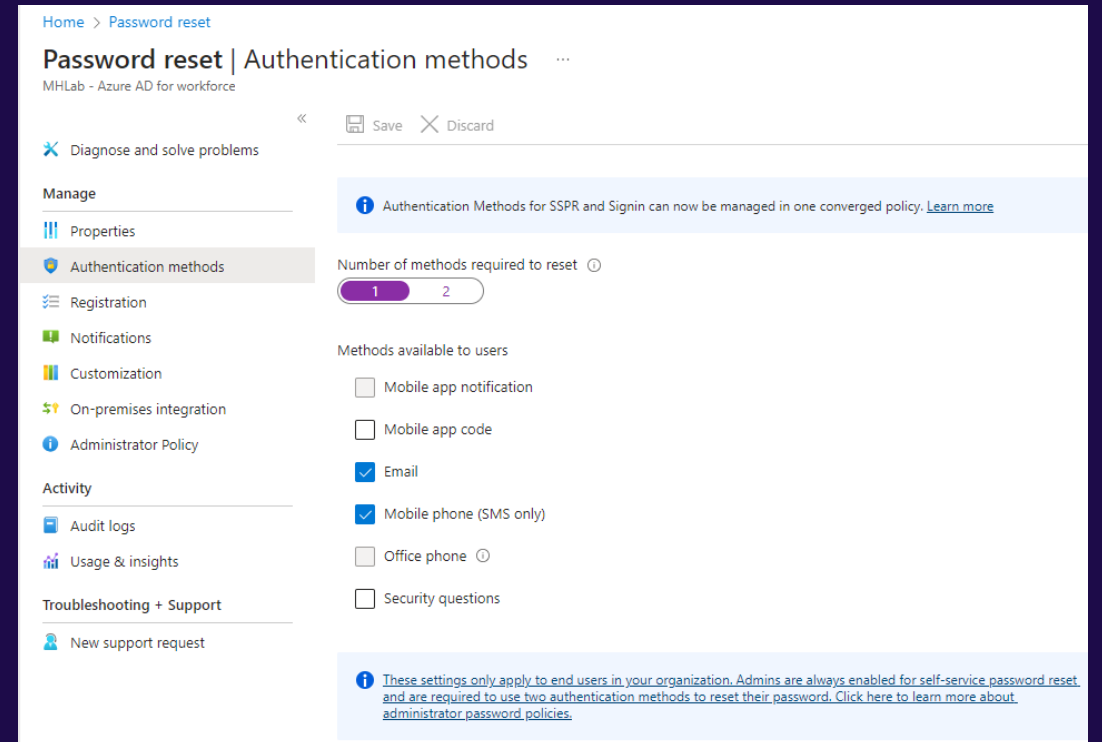
SAML Token(s)

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⟩