Everything you want to know about authentication (MFA and other) at UNM

…but are afraid to ask

Neil Sabol (Enterprise Managed Systems and Services)

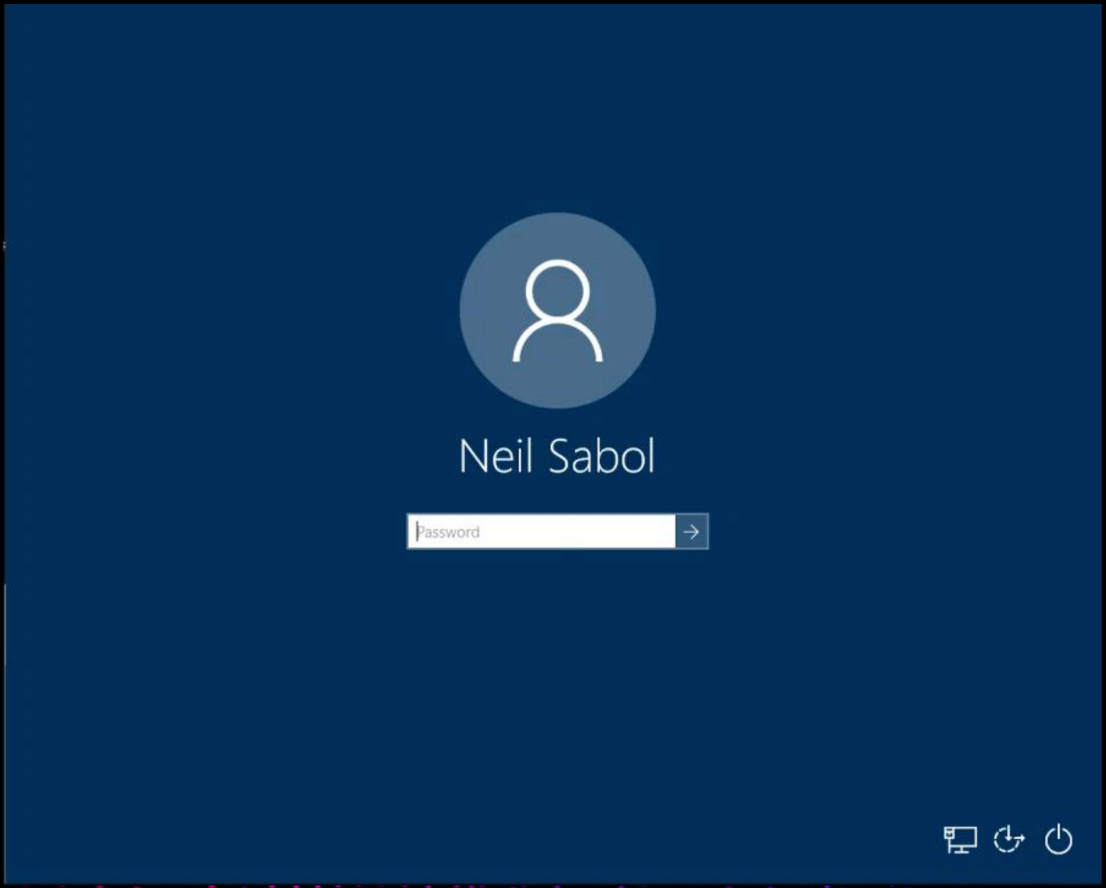
4/30/2020

Agenda

- The Authentication road map (parts 1 – 4)
- What about MFA
- MFA current state (Duo Security)
- MFA future state (Azure MFA)
- MFA road map for 2020-2021
- Azure MFA tips and usage
  - General (enrollment, Authenticator app, etc.)
  - Stay Signed in
  - MFA without a phone (OATH-TOTP)
  - Opting into the O365 MFA pilot
  - Use Azure MFA for your custom or vendor provided app

Authentication Road Map – part 1

In short, “true single sign on.” Not the following (what we have today):



Neil Sabol

Authentication Road Map – part 2

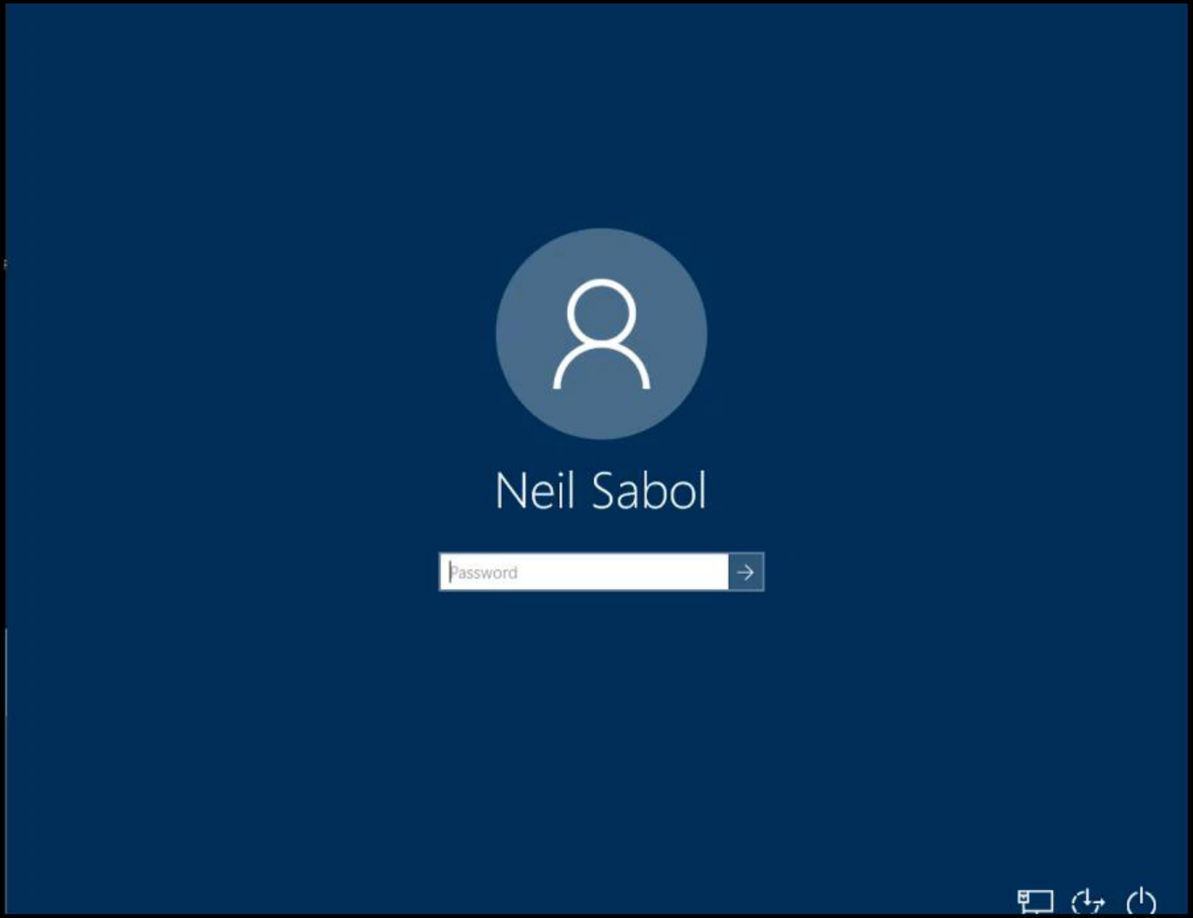
UNM has 2 underlying directories (Active Directory and LDAP), 4 identity providers (Azure AD, ADFS, CAS, and Shibboleth) and 2 MFA providers (Duo Security and Microsoft). Additionally, many applications do not even use 1 of the 4 IdPs – they use directory binds or other means to authenticate users.

This equates to a poor sign on experience for users (as demonstrated in the previous slide). Additionally, we are duplicating effort maintaining directories and IdPs and there is no “one directory/IdP to rule them all” in terms of security and logging.

“True SSO” (powered by Azure AD) will eventually allow a user’s workstation login to carry through to all subsequent applications accessed. That is one login per user per day and unlimited access to UNM apps and services.

Authentication Road Map – part 3

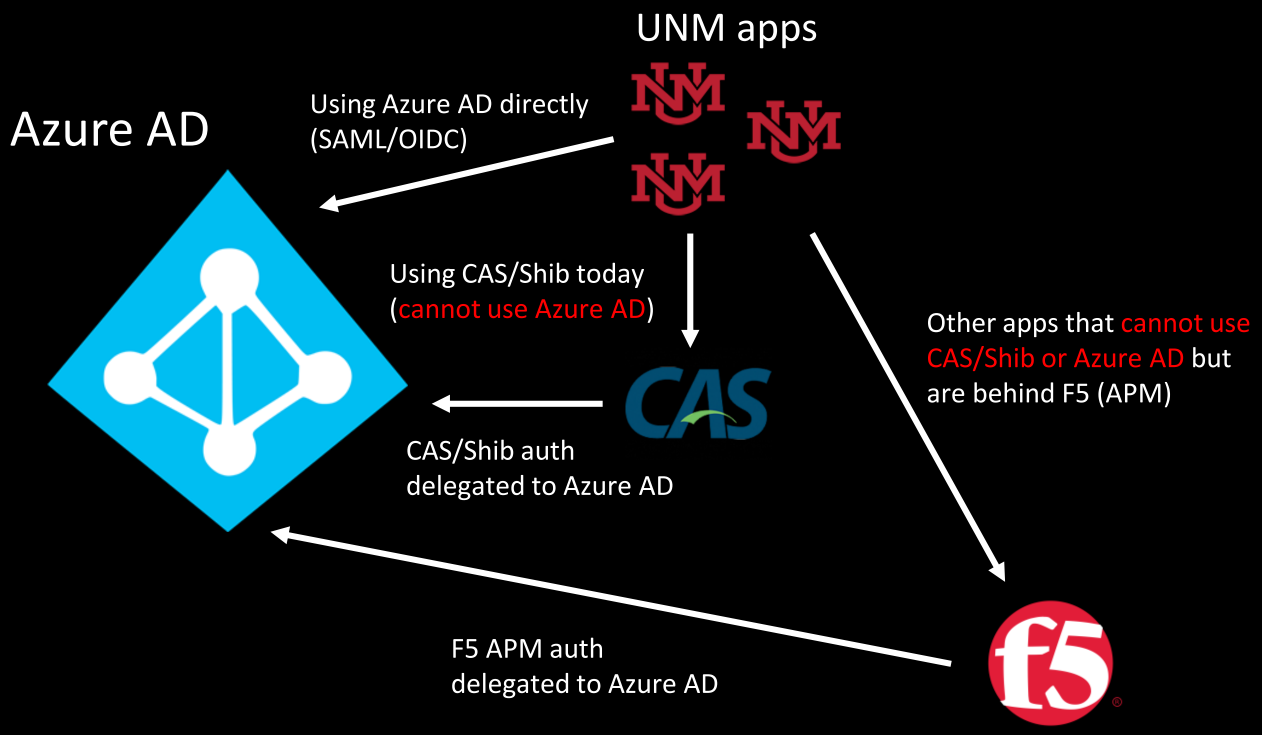
What "true single sign on" could look like:



Neil Sabol

Authentication Road Map – part 4

Azure AD as the primary IdP – “one IdP to rule them all”



UNM apps

Azure AD

Using Azure AD directly (SAML/OIDC)

Using CAS/Shib today (cannot use Azure AD)

CAS/Shib auth delegated to Azure AD

Other apps that cannot use CAS/Shib or Azure AD but are behind F5 (APM)

F5 APM auth delegated to Azure AD

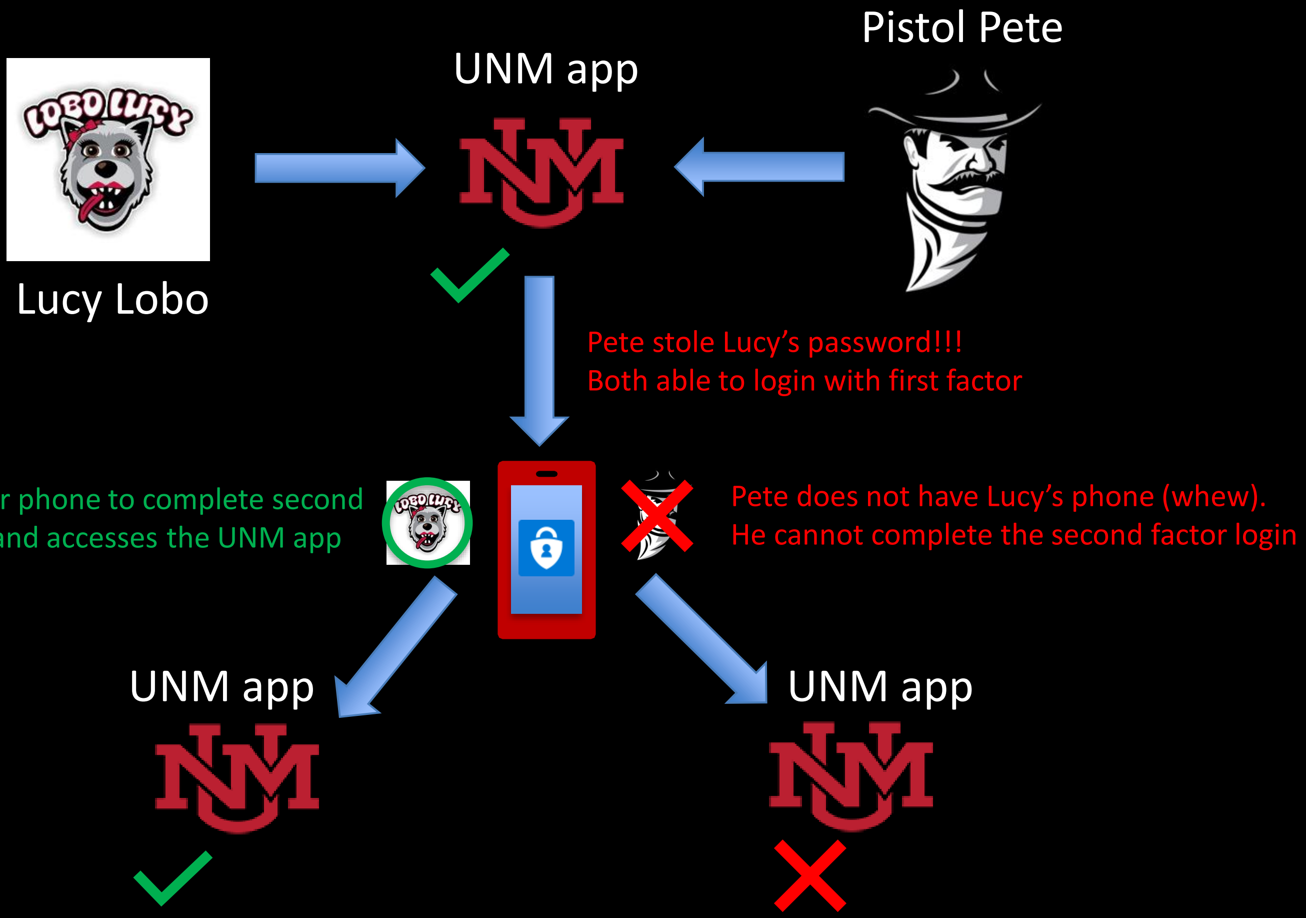
What about MFA?

"Multi factor authentication" or MFA refers to the security process needed to access certain UNM systems. With MFA, users must not only provide their NetID/password to login to their account, but must also provide a second authentication in the form of a push notification, code, SMS message or phone call.

Something you know (username/password) + something you have (device)

- MFA adds a second layer of security to your online accounts. Verifying your identity using a second factor (like your phone or other mobile device) helps prevent anyone but you from logging in, even if they know your password.
- The first time you access certain UNM services, you will be prompted to enroll a device- you can use a smart phone, feature phone, desk phone (land line), or Authenticator app depending on the situation.
- Once enrolled, you will use your device to complete the MFA login process each time you access certain systems. You can also “remember” or “trust” your personal computer to forgo MFA for a period of time.

What is MFA anyway? In practice.



Lucy Lobo

UNM app

Pistol Pete

Pete stole Lucy’s password!!!
Both able to login with first factor

Lucy uses her phone to complete second factor login and accesses the UNM app

Pete does not have Lucy’s phone (whew).
He cannot complete the second factor login

UNM app

UNM app

Current state (Duo Security): History

In Spring 2016, Duo Security was implemented as the MFA provider for specific Loboweb modules (Direct Deposit) to improve the security of sensitive employee information. It was subsequently applied to other modules (Benefits, W2/W4).

Why?

- Convenience: there was previously no way to update your direct deposit online (required a visit to the Business Center)
- Security: The reason online direct deposit changes were stopped was due to a breach and the malicious redirection of some employee’s paychecks

Current state (Duo Security): Usage

- Authentications by factor: 65% phone call, 27% SMS message, 8% other
- Average authentication cost per day (telephony): $10
- Authentication failure rate: 10% for phone calls, 20% for SMS
  - Worth noting, UNM pays for the authentication attempt whether it succeeds or fails.
- Top causes of authentication failures: “User not in permitted group” and “Invalid passcode”
  - *User not in permitted group* is likely caused by the 48 hour provisioning issue
  - *Invalid passcode* is likely caused by the nuances to SMS authentications

Future State (Azure MFA): Why?

- NO 48 HOUR DELAY FOR NEW USERS!!!
- Lays ground work for true SSO in the future (Azure AD)
- Enhances user experience (more MFA options like push notifications and authenticator apps, easier SMS experience, better "Remember me" experience)
- Centralized logging in Azure AD
- Granular conditions to trigger MFA only in some scenarios
- Reduced cost (no ongoing telephony charges)

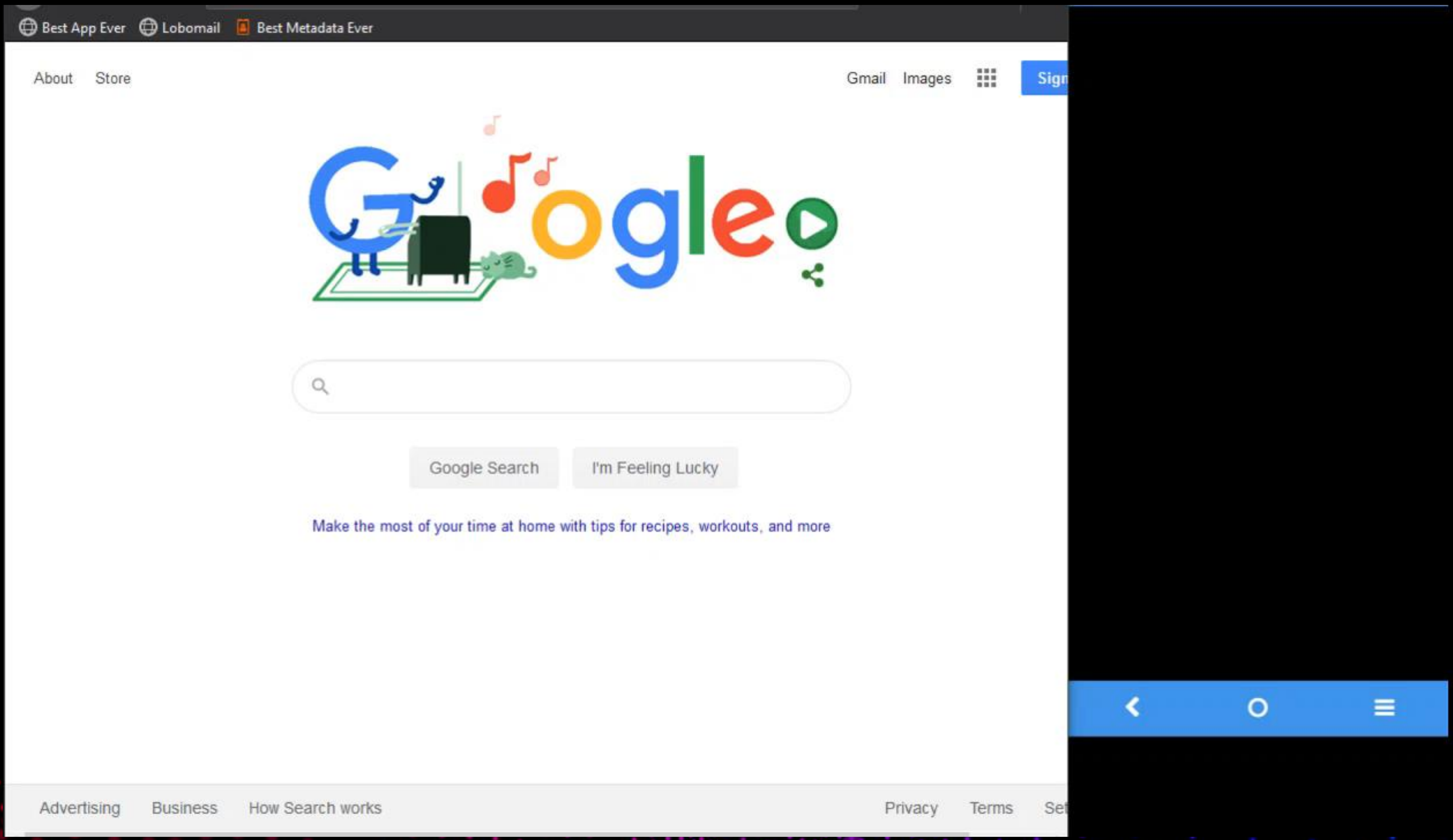
MFA Road Map for 2020-2021

- TouchNet (Bursar Account Suite) – May 2020
  - Just like the original Direct Deposit use case – prevent malicious redirection of student’s financial awards (scholarships, grants, etc.)
- Loboweb Direct Deposit/Benefits/W2/W4 – June 2020
  - Moving what currently uses Duo to Azure MFA
- Office 365 – by end of year 2020
  - SPAM/Phishing issues – look familiar?

    "NOTICES! ! !", "RELY", "RE: Assistant Intern!"

Azure MFA tips and usage: General

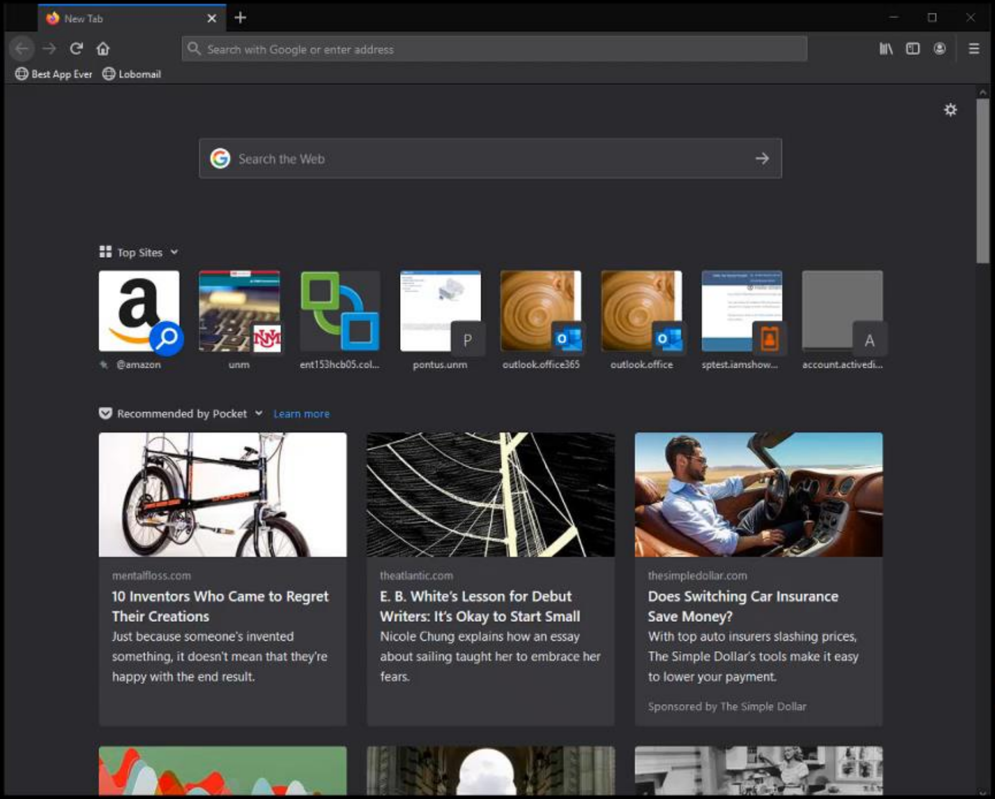
Initial enrollment



Make the most of your time at home with tips for recipes, workouts, and more

Azure MFA tips and usage: General

Ongoing authentication



mentalfloss.com

10 Inventors Who Came to Regret Their Creations

Just because someone's invented something, it doesn't mean that they're happy with the end result.

theatlantic.com

E. B. White's Lesson for Debut Writers: It's Okay to Start Small

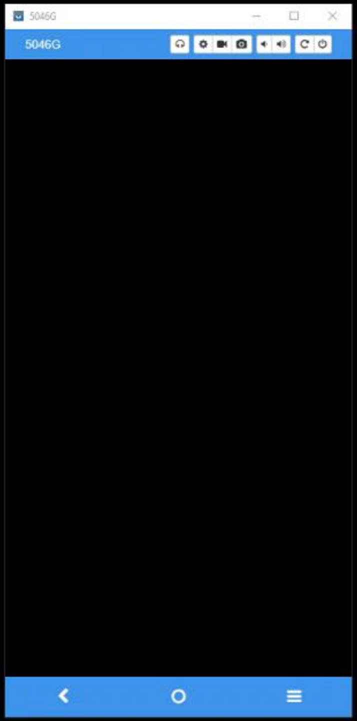
Nicole Chung explains how an essay about sailing taught her to embrace her fears.

thesimpledollar.com

Does Switching Car Insurance Save Money?

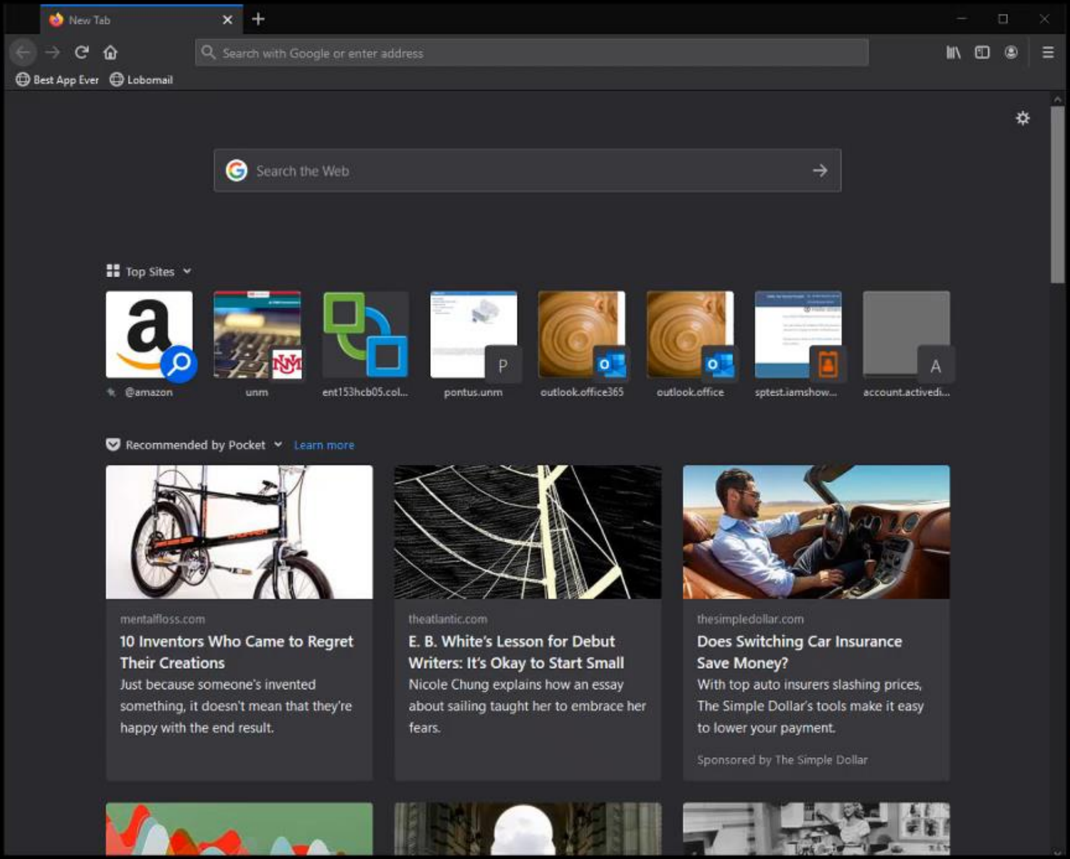
With top auto insurers slashing prices, The Simple Dollar's tools make it easy to lower your payment.

Sponsored by The Simple Dollar



Azure MFA tips and usage: General

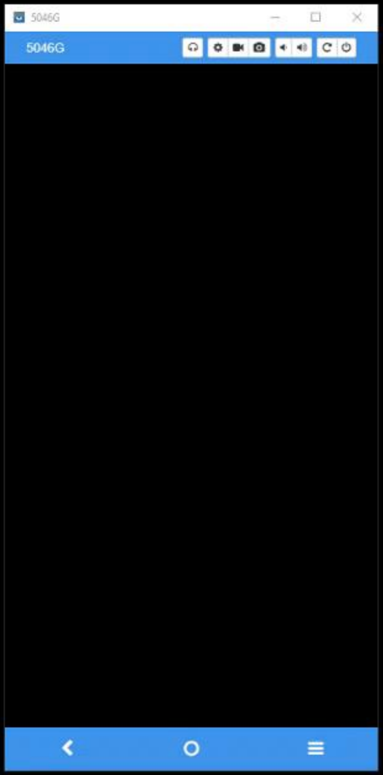
Stopping a hacking attempt



mentalfloss.com
10 Inventors Who Came to Regret Their Creations
Just because someone's invented something, it doesn't mean that they're happy with the end result.

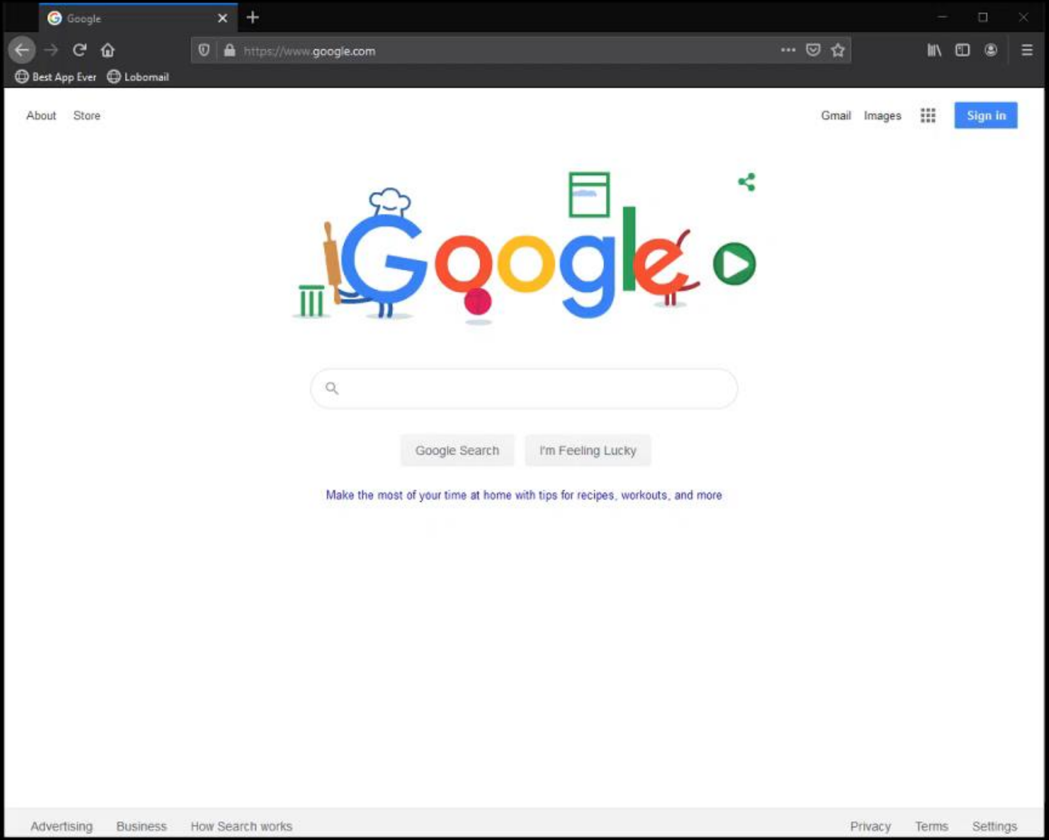
theatlantic.com
E. B. White's Lesson for Debut Writers: It's Okay to Start Small
Nicole Chung explains how an essay about sailing taught her to embrace her fears.

thesimpledollar.com
Does Switching Car Insurance Save Money?
With top auto insurers slashing prices, The Simple Dollar's tools make it easy to lower your payment.
Sponsored by The Simple Dollar

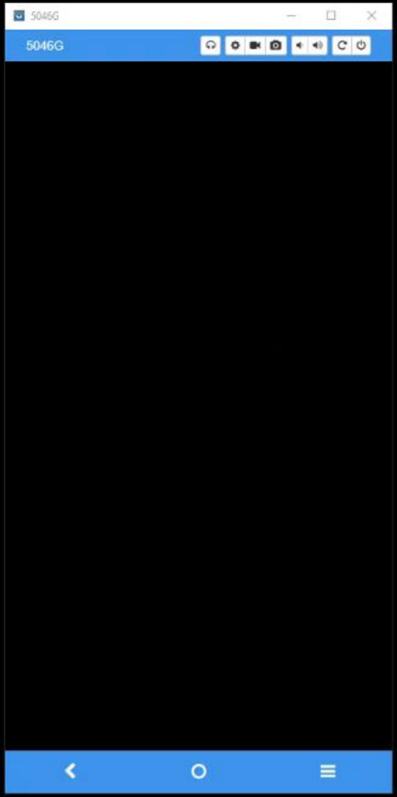


Azure MFA tips and usage: “Stay signed in”

Remember me for trusted devices

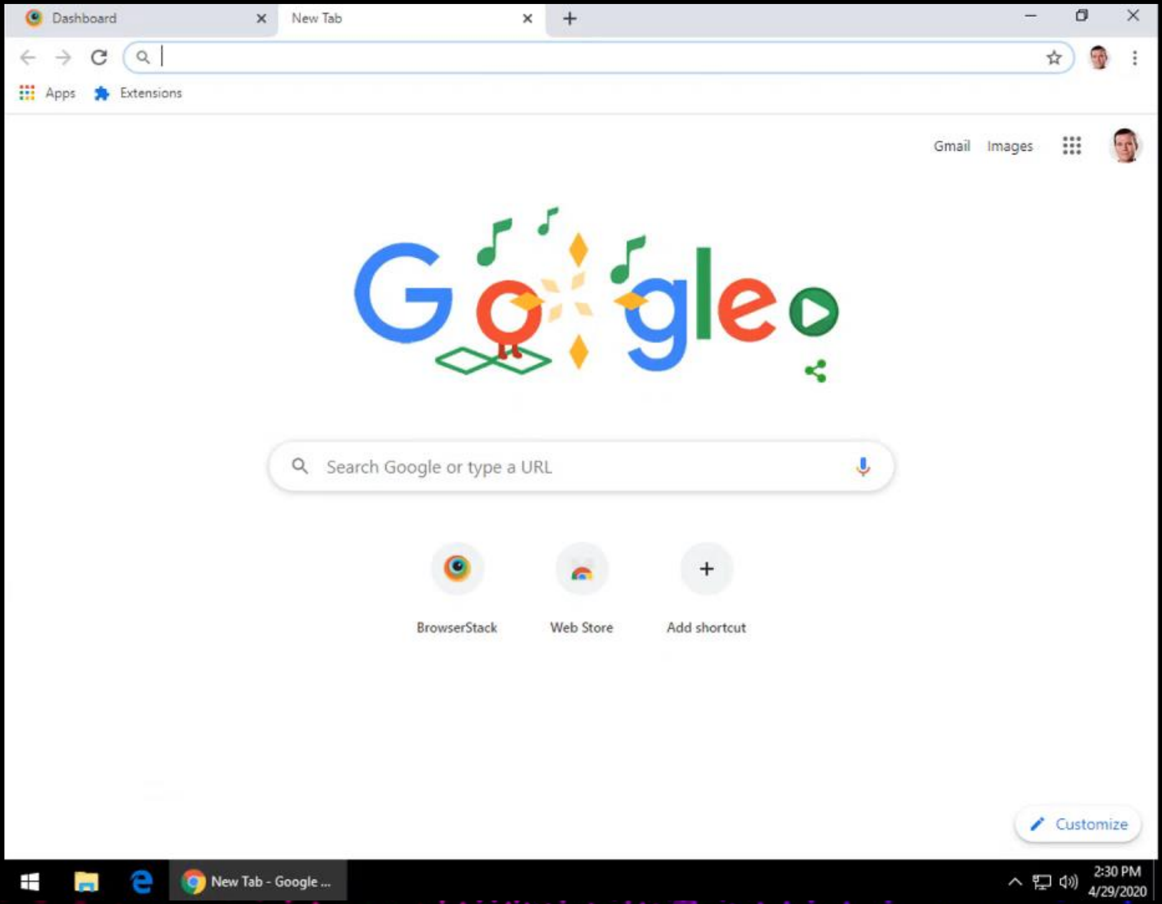


Make the most of your time at home with tips for recipes, workouts, and more



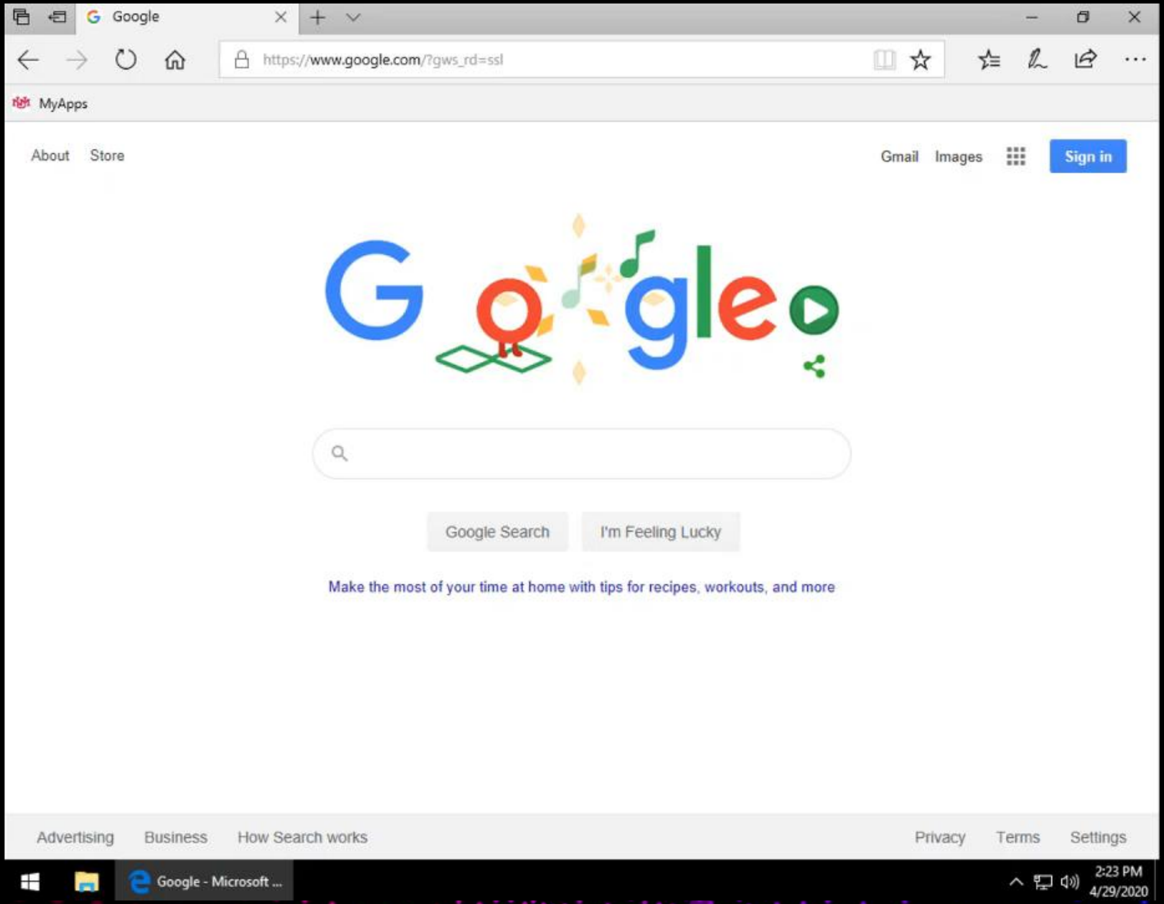
Azure MFA tips and usage: MFA without a phone

Technically without a phone or data plan - for computers or tablets



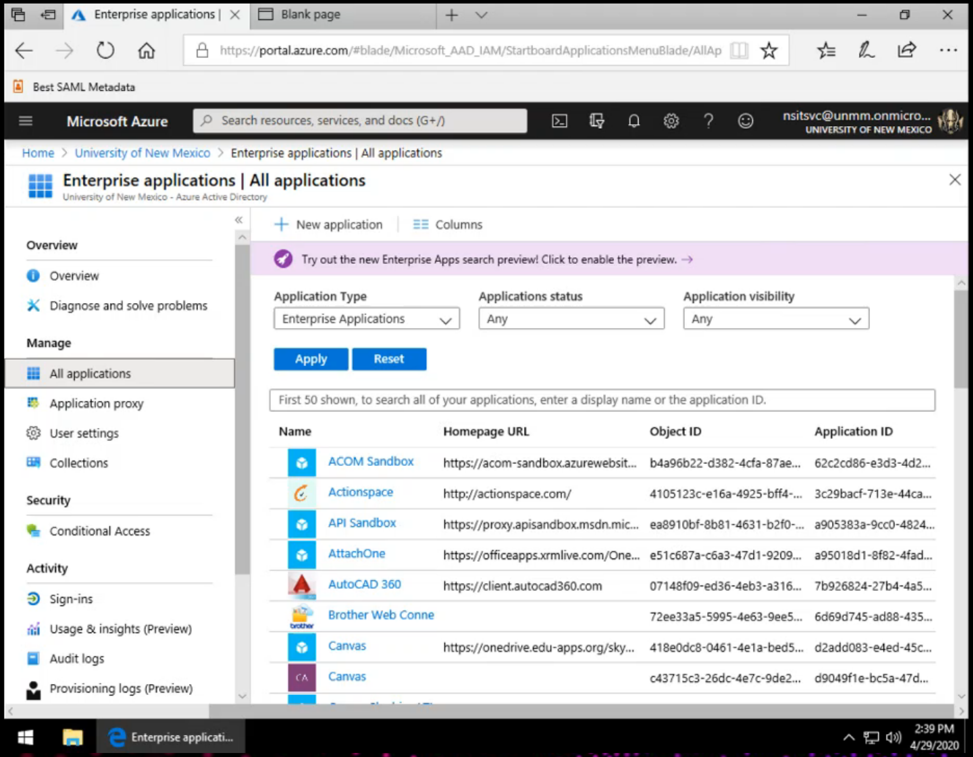
Azure MFA tips and usage: Opting into the O365 MFA pilot

You can opt in or opt out anytime – great for the security conscious



Azure MFA tips and usage: Azure MFA for your app

Developing or deploying an app that needs MFA? Using Azure MFA is a matter of delegating your app’s authentication to Azure AD with SAML or OIDC (Open ID Connect/OATH).


Enterprise applications |
Blank page
https://portal.azure.com/#blade/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/AllAp
Best SAML Metadata
Microsoft Azure
Search resources, services, and docs (G+/)
nsitsvc@unmm.onmicro...
UNIVERSITY OF NEW MEXICO
Home > University of New Mexico > Enterprise applications | All applications
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
Collections
Security
Conditional Access
Activity
Sign-ins
Usage & insights (Preview)
Audit logs
Provisioning logs (Preview)
New application
Columns
Apply
Reset
Enterprise applicati...
2:39 PM
4/29/2020

Enterprise applications | All applications

University of New Mexico - Azure Active Directory

Try out the new Enterprise Apps search preview! Click to enable the preview. →

Application Type: Enterprise Applications

Applications status: Any

Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL	Object ID	Application ID
ACOM Sandbox	https://acom-sandbox.azurewebsit...	b4a96b22-d382-4cfa-87ae...	62c2cd86-e3d3-4d2...
Actionspace	http://actionspace.com/	4105123c-e16a-4925-bff4-...	3c29bacf-713e-44ca...
API Sandbox	https://proxy.apisandbox.msdn.mic...	ea8910bf-8b81-4631-b2f0-...	a905383a-9cc0-4824...
AttachOne	https://officeapps.xrmlive.com/One...	e51c687a-c6a3-47d1-9209...	a95018d1-8f82-4fad...
AutoCAD 360	https://client.autocad360.com	07148f09-ed36-4eb3-a316...	7b926824-27b4-4a5...
Brother Web Conne		72ee33a5-5995-4e63-9ee5...	6d69d745-ad88-435...
Canvas	https://onedrive.edu-apps.org/sky...	418e0dc8-0461-4e1a-bed5...	d2add083-e4ed-45c...
Canvas		c43715c3-26dc-4e7c-9de2...	d9049f1e-bc5a-47d...

Thank You

Questions? Comment on this video.