Going beyond MFA PASSWORDLESS in the real world

Ward van Besien
Merill Fernando

AGENDA

- Passwordless overview
- Passwordless Journey
- Passkeys
- Implementing Passwordless

Passwordless Overview

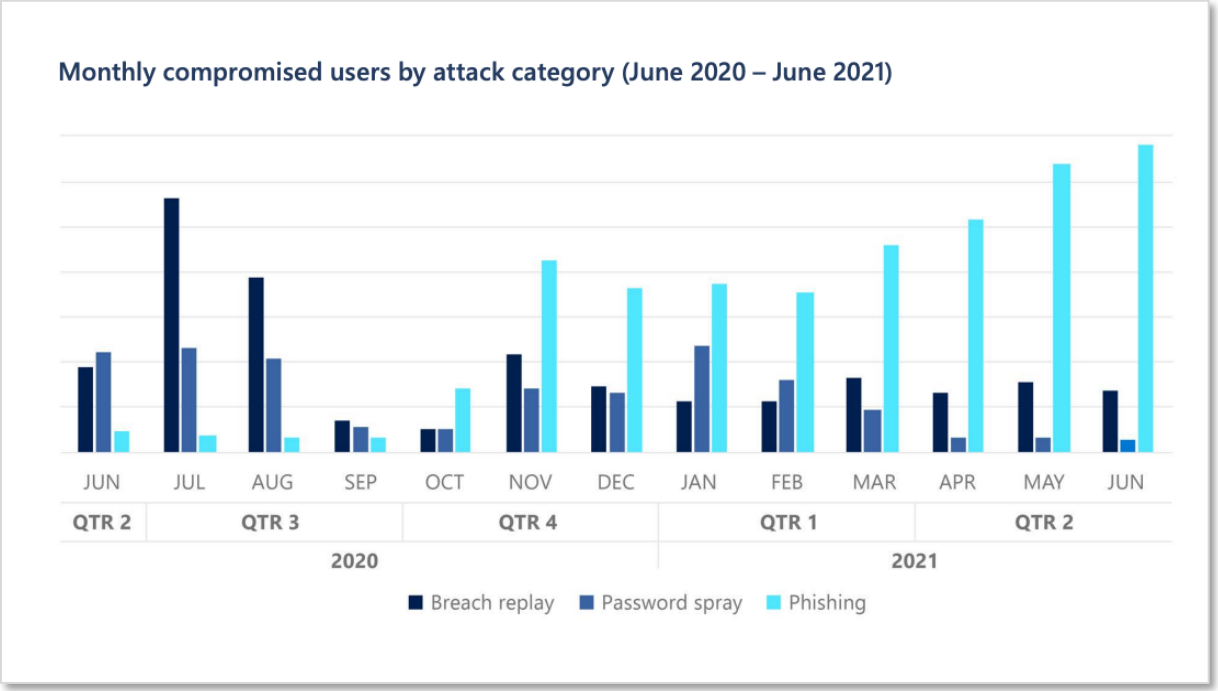
Why passwordless?

- Password are one of your biggest risks
- Depends on users (human nature is significant risk factor)
- Complex password policies may do more damage than good
- People are not good at picking passwords
- Only strong password is completely random

Cybersecurity Challenges

We're seeing a massive increase in phishing

Phishing is responsible for 70%+ of data breaches



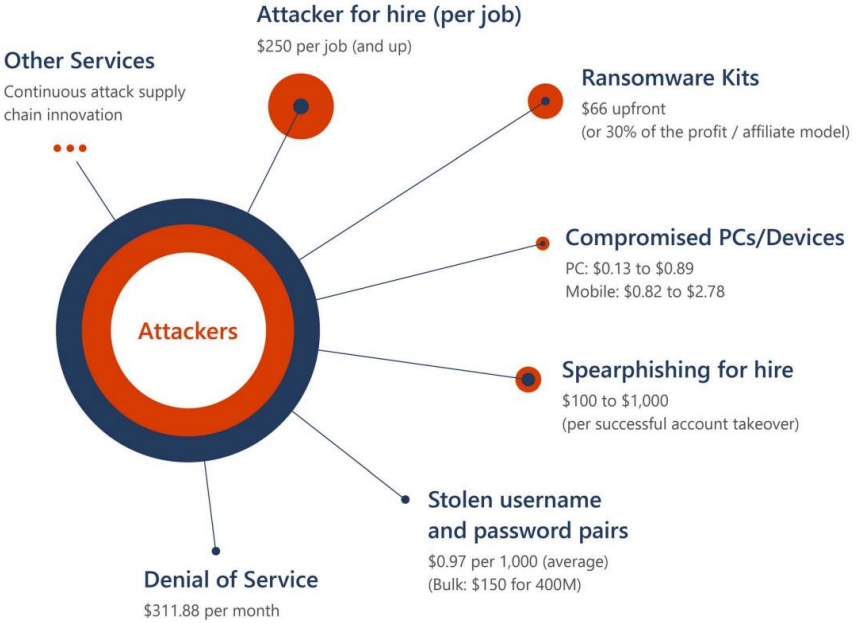
Recent Lapsus$ attacks relied on MFA prompt-bombing end users which highlights the importance of "phish resistant" credentials

Cybersecurity Challenges

220% increase in strong authentication usage in the last 18 months.

Basic security hygiene protects against 98% of attacks.

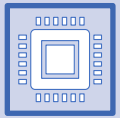
Average prices of cybercrime services for sale



The passwordless promise

Promise to remove attack vector of standalone passwords

A better user experience than **Passwords** + MFA **(Multi-Factor Authentication)**



Strong, device-based authentication methods

- Windows Hello for Business
- Microsoft Authenticator – Passwordless phone sign-in
- FIDO2 security keys (platform and external)

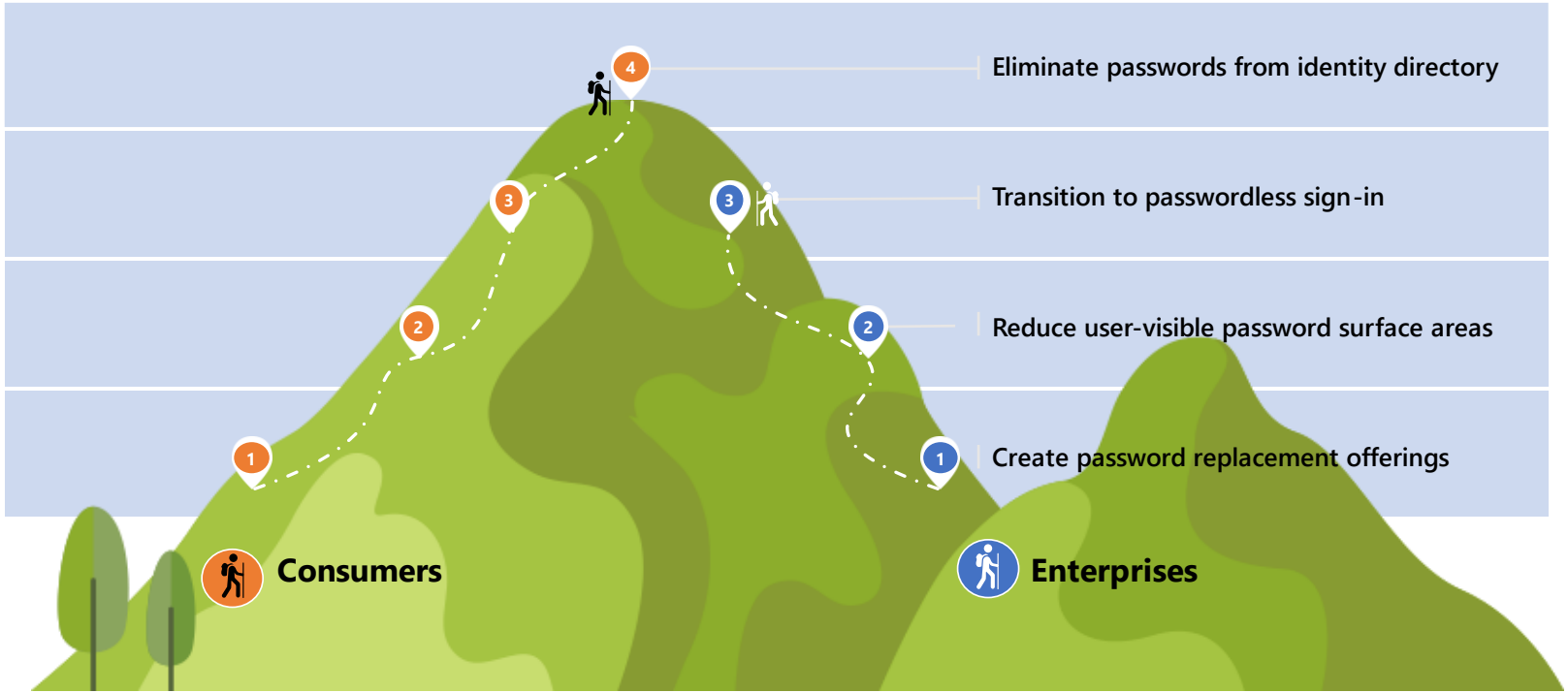
https://aka.ms/PhishResistantExplained

ACSC Maturity levels for authentication

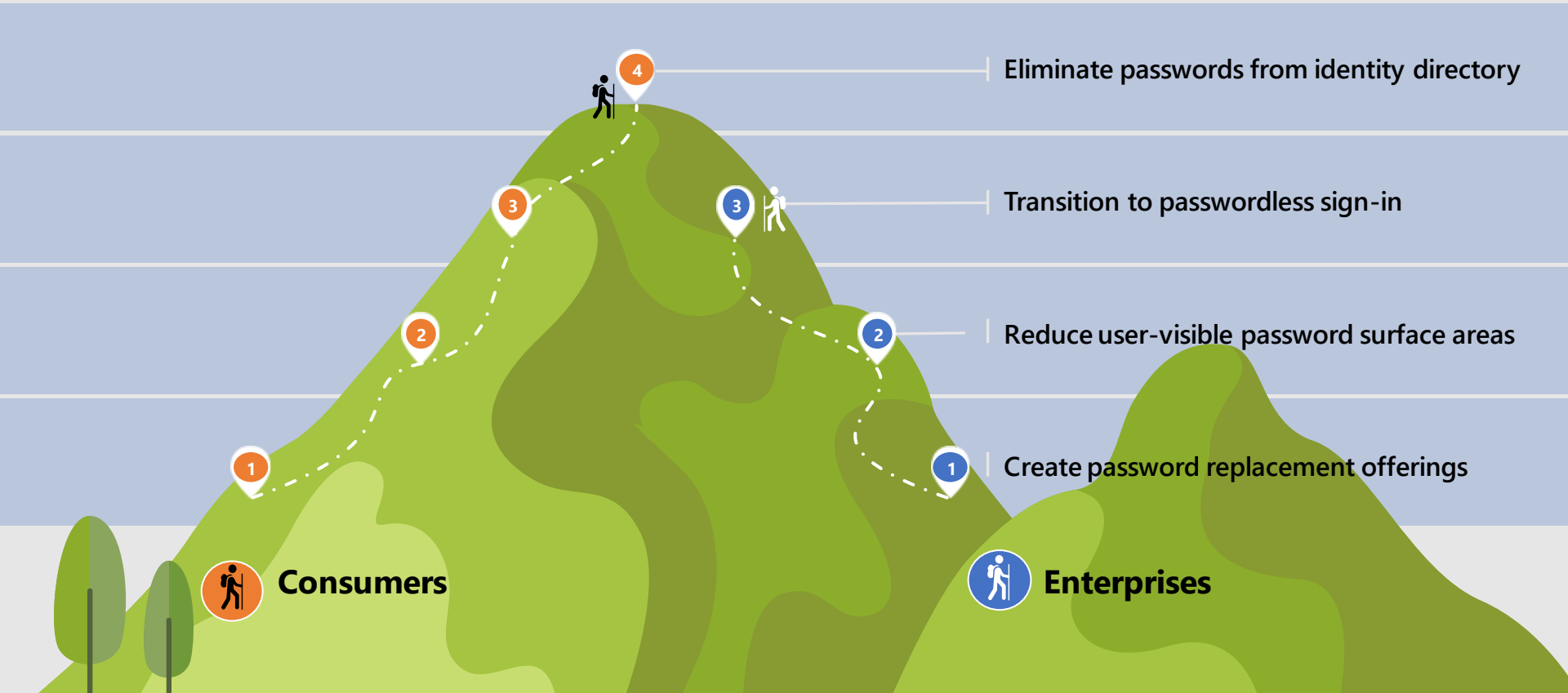
Maturity Level 1	Maturity Level 2	Maturity Level 3 Phishing resistant
Password + Voice	Microsoft Authenticator Passwordless	Certificate based authentication
Password + SMS	Password + Hardware Tokens OTP	FIDO2 security key
	Password + Microsoft Authenticator Number match	Windows Hello for Business
	Password + Software Tokens OTP	Passkey
+ Any method in Maturity Levels 2 & 3	+ Any method in Maturity Level 3	

What does your Passwordless journey look like?

Passwordless Journey



Passwordless Journey



Steps to take when you #GoPasswordless

- Presence in IdP (Eg Microsoft Entra ID, Okta, Ping)
- Update apps to support modern authentication
- Device readiness
- Credential registration and bootstrapping
- Drive usage of Passwordless creds

Planning your passwordless journey

Strengthen Your Credentials Tasks	Step 1 (days)	Step 2 (weeks)	Step 3 (within year)	Step 4
Enable MFA	Enroll your users in converged registration	Require Azure MFA with conditional access on sensitive apps	Add device-based factors like hybrid-join or Intune management	Require MFA on all apps (satisfied with Passwordless)
Passwordless gives you SSO to valuable apps	M365 + Move SaaS apps to Azure AD	Integrate WAM/Kerb apps with App Proxy/ Secure Hybrid Access	Modernize custom apps to use Azure AD	Sunset your LDAP and WAM apps
Deploy Windows Hello for Business	Plan/work to get AAD join or Hybrid AAD join with Windows 10 1909 or greater	Enable an MFA Solution for your end users with Azure AD.	Roll out WHFB to users, even with only PIN.	HW refresh to get more friendly WHFB form factors.
Enable Passwordless Credentials	Enable FIDO2 & Phone Sign in for all users (Grassroots discovery)	Drive Authenticator across Mobile Users. (https://aka.ms/nudge)	Launch a Phone Sign in registration campaign	Explore new FIDO2 form factors; Phone as FIDO2 key
Improve Password Management – Use Passwords less	Roll out Azure AD Password Protection	Change your password policy to our guidelines.	Deploy Azure AD Self-Service Password Reset if not deployed	Scramble passwords for users who do not need them.
Privileged Users	Deploy FIDO2 keys for privileged users, helpdesk and breakglass accounts	Implement SAWs using Device Filters	Move scripts to Service Principals and Managed Identities	Remove/scramble passwords of privileged users

Where are you today? (Example from a well-deployed customer)

Strengthen Your Credentials Tasks	Step 1 (days)	Step 2 (weeks)	Step 3 (within year)	Step 4
Enable MFA	Enroll your users in converged registration	Require Azure MFA with conditional access on sensitive apps	Add device-based factors like hybrid-join or Intune management	Require MFA on all apps (satisfied with Passwordless)
Passwordless gives you SSO to valuable apps	M365 + Move SaaS apps to Azure AD	Integrate WAM/Kerb apps with App Proxy/ Secure Hybrid Access	Modernize custom apps to use Azure AD	Sunset your LDAP and WAM apps
Deploy Windows Hello for Business	Plan/work to get AAD join or Hybrid AAD join with Windows 10 1909 or greater	Enable an MFA Solution for your end users with Azure AD.	Roll out WHFB to users, even with only PIN.	HW refresh to get more friendly WHFB form factors.
Enable Passwordless Credentials	Enable FIDO2 & Phone Sign in for all users (Grassroots discovery)	Drive Authenticator across Mobile Users. (https://aka.ms/nudge)	Launch a Phone Sign in registration campaign	Explore new FIDO2 form factors; Phone as FIDO2 key
Improve Password Management – Use Passwords less	Roll out Azure AD Password Protection	Change your password policy to our guidelines.	Deploy Azure AD Self-Service Password Reset if not deployed	Scramble passwords for users who do not need them.
Privileged Users	Deploy FIDO2 keys for privileged users, helpdesk and breakglass accounts	Implement SAWs using Device Filters	Move scripts to Service Principals and Managed Identities	Remove/scramble passwords of privileged users

Passkeys

Passkeys are the future

Terminology

- **Platform authenticator** – the device that stores multiple credentials, for authentication on that device, native to the operating system (e.g. Windows Hello for Business)
- **Roaming authenticator** – a device that stores credentials, separate from where authentication is happening (e.g. FIDO2 security keys)
- **CDA – cross-device authentication** (formerly referred to as “Cloud-assisted Bluetooth, aka CaBLE)

Challenges today

- Roaming authenticators are required to bootstrap the platform
- Roaming authenticators cost money
- Consumers (and enterprises) are not interested in buying security keys
- Consumers are not interested in putting a new item on their keychain
- Device loss is also an issue with roaming authenticators
- "WebAuthn" and "security key" are confusing for users

The Vision

- As easy to use as a password
- Easy for users to understand and recognize
- Leverages a user's existing investments
- Durable across device loss
- Geo-aware and inclusive

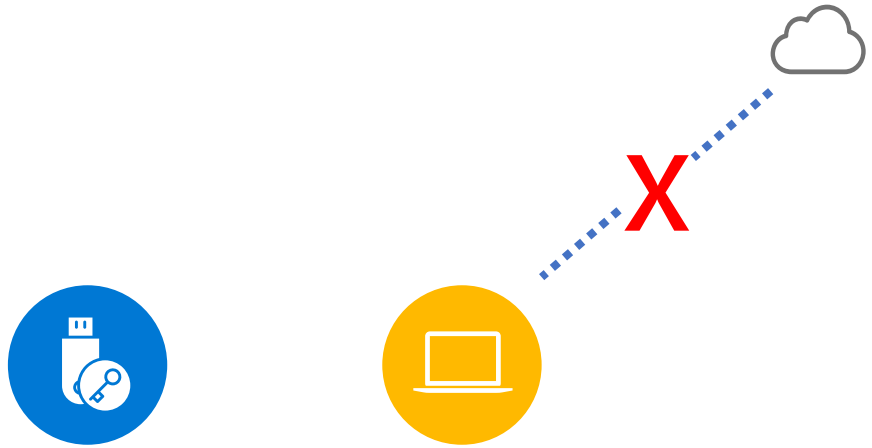
passkey

(n.) a password replacement that is safer, easier, and faster to use.

Single Device vs. Multi-Device Passkeys

Single-Device Passkey

A webAuthn credential where the private key is stored on one, and only one authenticator and cannot leave the device.



Security Keys

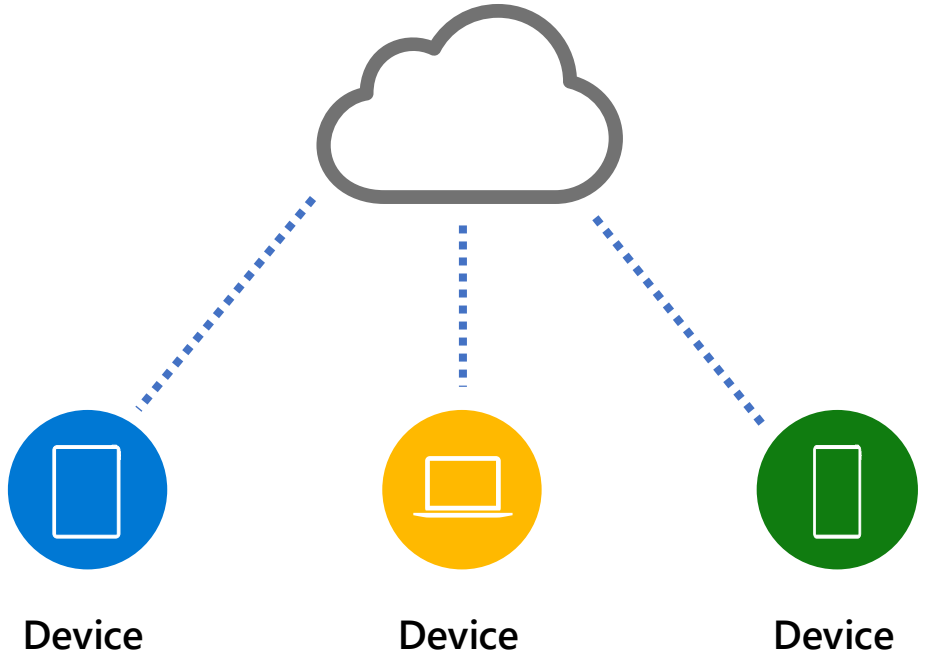
USB, NFC, Bluetooth, etc.

Smart Device

Windows Hello, Touch ID, FaceID, etc.

Multi-Device Passkey

A webAuthn credential where the private key is available on one or more devices and is synced through a platform cloud.



Phishing resistant MFA

"Authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system"

Learn more:
https://aka.ms/PhishResistantExplained From Strong to Stronger: Phishing Resistant authentication methods
Memo 22-09 multifactor authentication requirements overview - Microsoft Entra | Microsoft Learn

Implementing passwordless

Applications

- Use an identity service that supports passwordless
- Use modern authentication
- Implement using standard SDKs in your apps.

Challenges

- Legacy support
- User resistance
- Technical challenges

Dos

01

Get an enthusiastic exec support

- Make sure they don't get locked out.

02

Identify the important scenarios

- It's not all or nothing, password scramble is not needed from day 1.

03

Choose the authentication methods and start with registration

- These methods have additional considerations.

04

Move to enforcement

Don’ts

01

Don’t get in your users’ way. Enable creds.

- let security-minded people help you

02

Don't plan on flipping a switch

- It's a journey

03

Don’t let perfect be the enemy of progress

- using less passwords is always a win

THANK YOU

@merill | merill.net | entra.news