
UNLOCKING IDENTITY: IMPLEMENTING PASSWORDLESS AUTHENTICATION AT HARVARD

Presented by

Nathan Hall & ~~Erin Courville~~

Ingrid Skoog



**A REAL INCIDENT
IN UNDER A MINUTE**



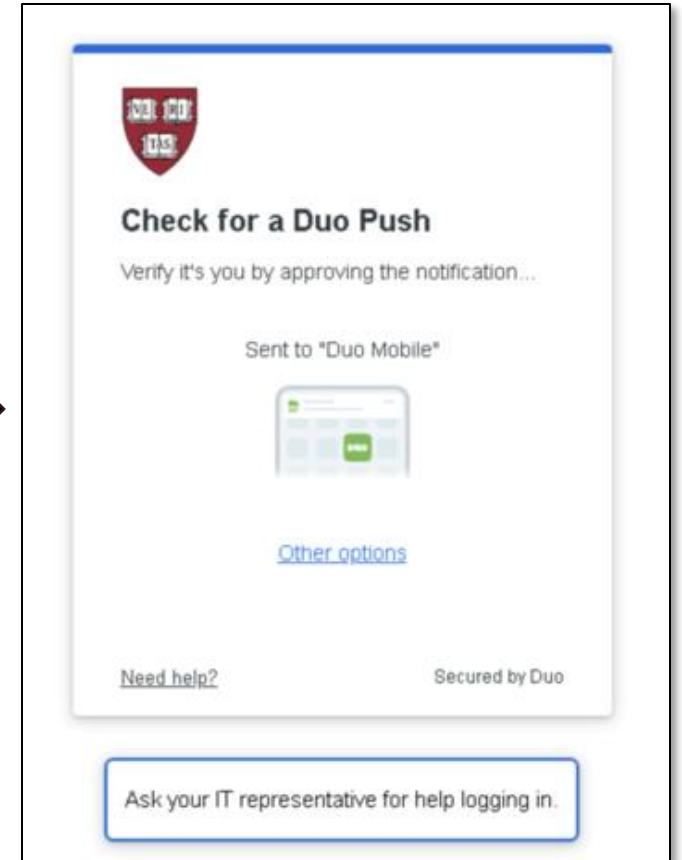
IT STARTED WITH A PHONE CALL...



IT STARTED WITH A PHONE CALL...

A web browser window showing a sign-in page for "HARVARDKEY". The page has a white background with a light gray border. At the top, the text "HARVARDKEY" is displayed in a sans-serif font, with "KEY" in red. Below it, the heading "Sign In" is in a larger, bold, black font. There are two input fields: the first is labeled "Email Address" and contains a cursor; the second is labeled "Password" and has a toggle icon (an eye) to its right. Below the password field is a blue button with the text "SIGN IN" in white. At the bottom of the page, there is a link that says "FORGOT YOUR PASSWORD?".

IT STARTED WITH A PHONE CALL...

A web page titled "HARVARDKEY Sign In". It features a "Email Address" input field with a cursor, a "Password" input field with a toggle eye icon, and a blue "SIGN IN" button. At the bottom, there is a link that says "FORGOT YOUR PASSWORD?".

... AND RESULTED IN THIS



HARVARD UNIVERSITY
Information Technology

Browse resources 

About 

Get help

[Home](#) > [News](#) > Recent cybersecurity incident information and FAQ

Recent cybersecurity incident information and FAQ

November 22, 2025

On Tuesday, November 18, 2025, Harvard University discovered that information systems used by Alumni Affairs and Development were accessed by an unauthorized party as a result of a phone-based phishing attack. The University acted immediately to remove the attacker's access to our systems and prevent further unauthorized access.

We continue to work with law enforcement and third-party cybersecurity experts to investigate this incident. This website will be updated.

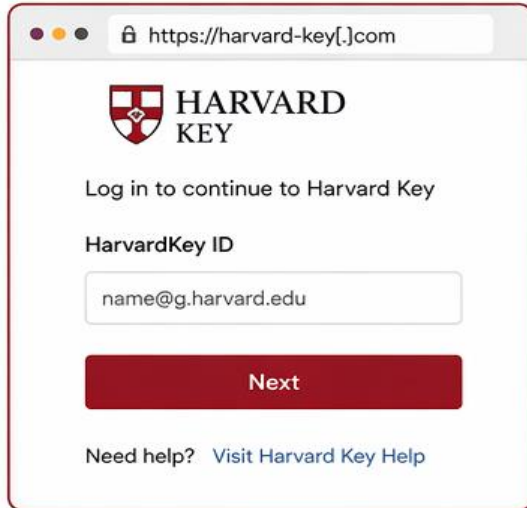
Last updated: December 19, 2025

Browser in the Middle (BitM) Phishing Attacks that Defeat MFA

Attackers act as a real-time proxy between the victim and the legitimate site, stealing the session after MFA is completed.

1 ATTACKER

Creates a fake login page that proxies all traffic to the real site



2 VICTIM (BROWSER)

Thinks they are logging in normally, completes MFA

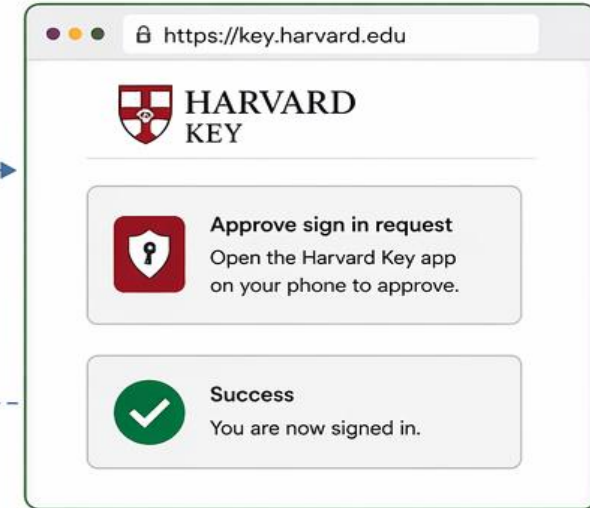


What the victim sees:

- ✓ Real Harvard Key login flow
- ✓ Real MFA prompt
- ✓ Access to their account

3 LEGITIMATE WEBSITE

Performs real authentication and MFA



What the website sees:

- ✓ Valid login
- ✓ MFA approved
- ✓ Legitimate session

Normal Login Flow (Safe)



You connect directly to Harvard Key.
The session cookie is only between you and Harvard.

Browser in the Middle (Phishing)



The attacker proxies everything in real time and steals the session cookie after MFA, giving them full access — even with MFA enabled.

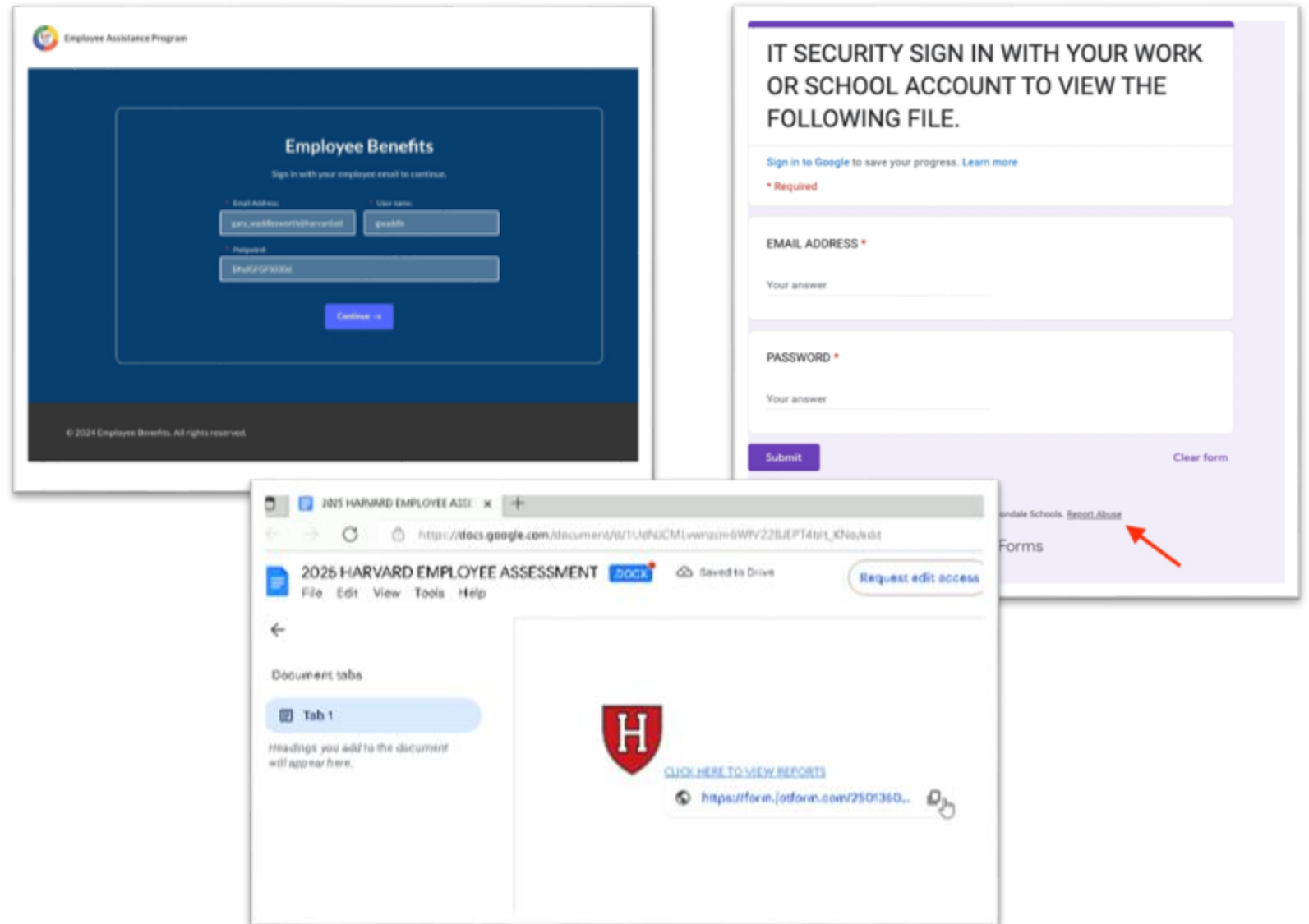
Why It Defeats MFA

- MFA is real and completed by the victim.
- The attacker never sees the password or code.
- The attacker steals the session cookie after MFA and reuses it.
- Works in real time.

Key Takeaway: MFA protects credentials, not sessions. If an attacker can sit in the browser, they can steal the authenticated session.

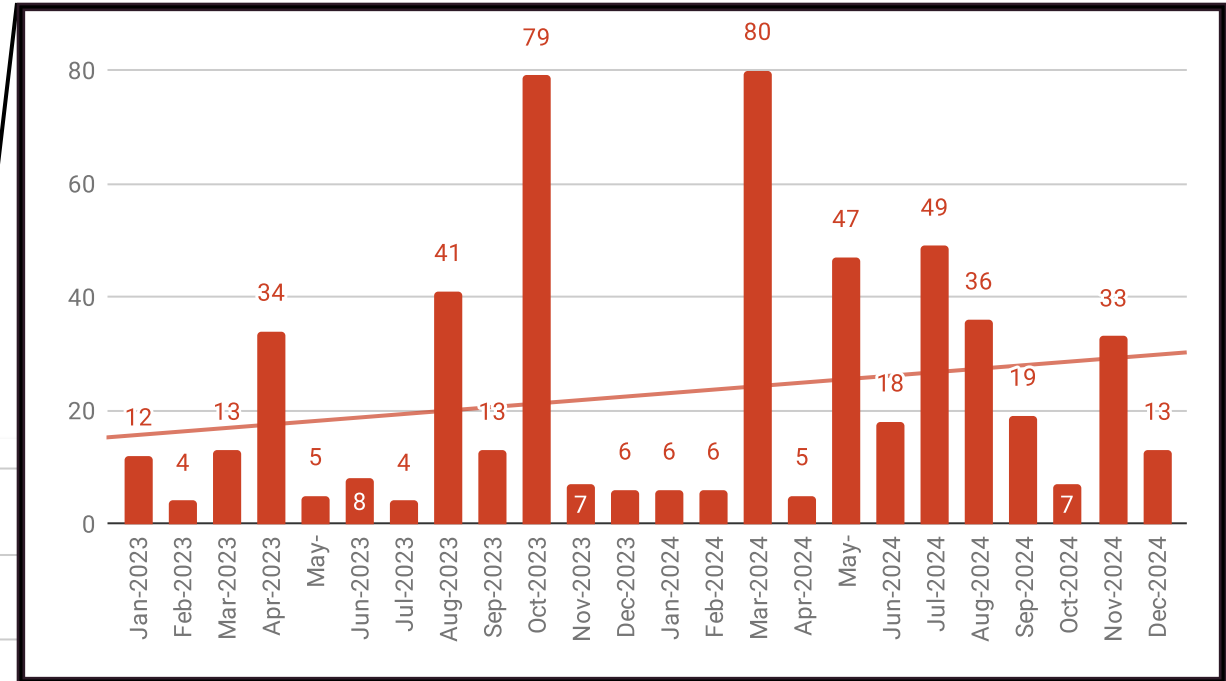
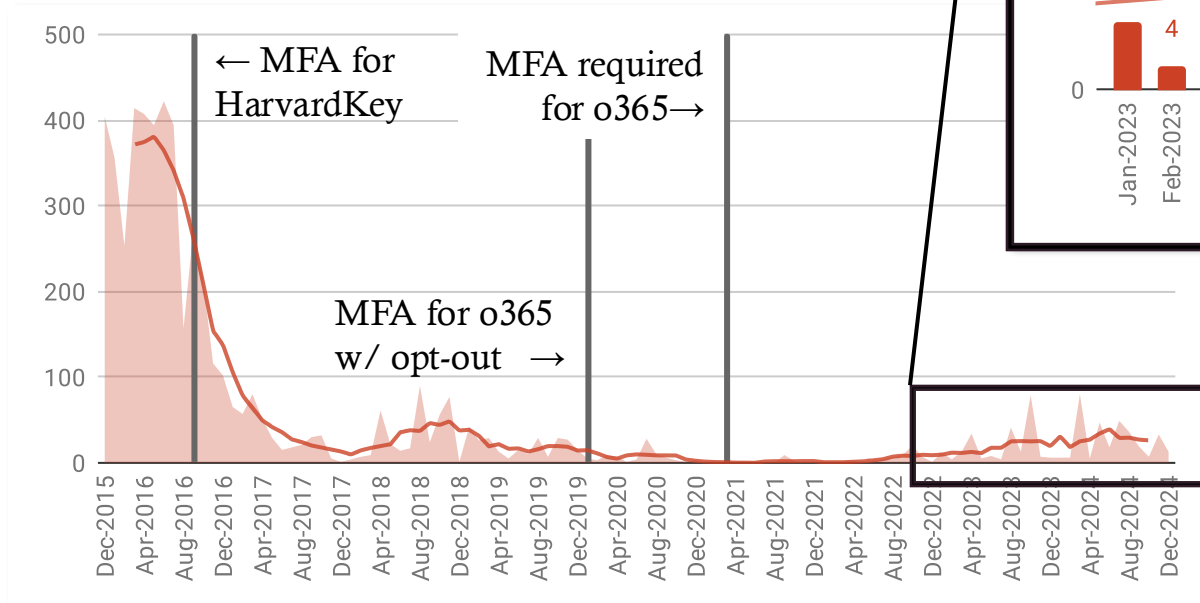
NOT AN EDGE CASE

- Prompt-bombing
- HOTP collection
- Simultaneous login triggering MFA prompt
- Attacker in the Middle phishing kits
- SIM swap attacks

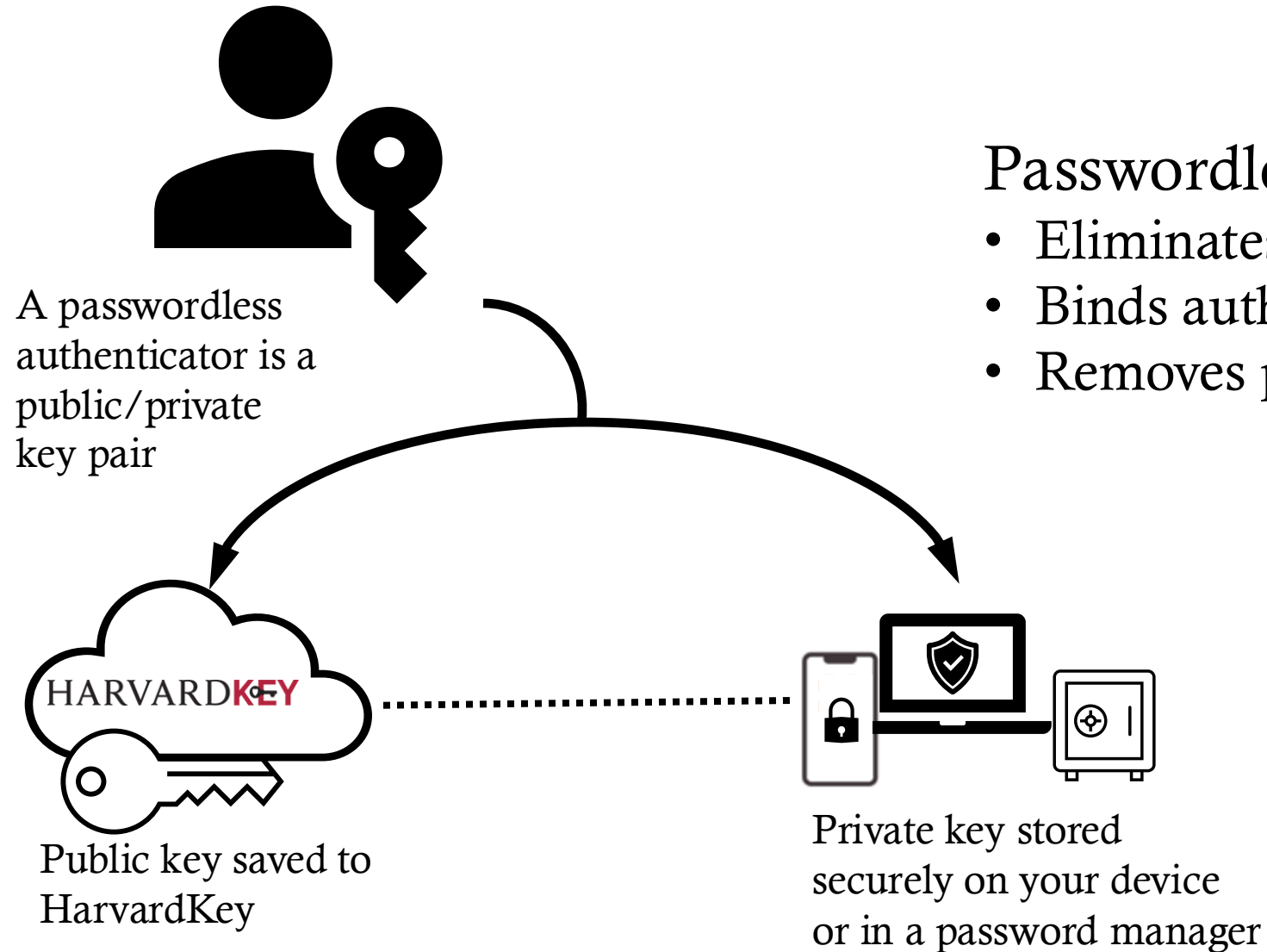


COMPROMISED ACCOUNT TREND

- HarvardKey is our SSO implementation
 - 500,000+ accounts, 110,000+ monthly active users
 - 200,000 authentications/day
 - 1,000 application integrations



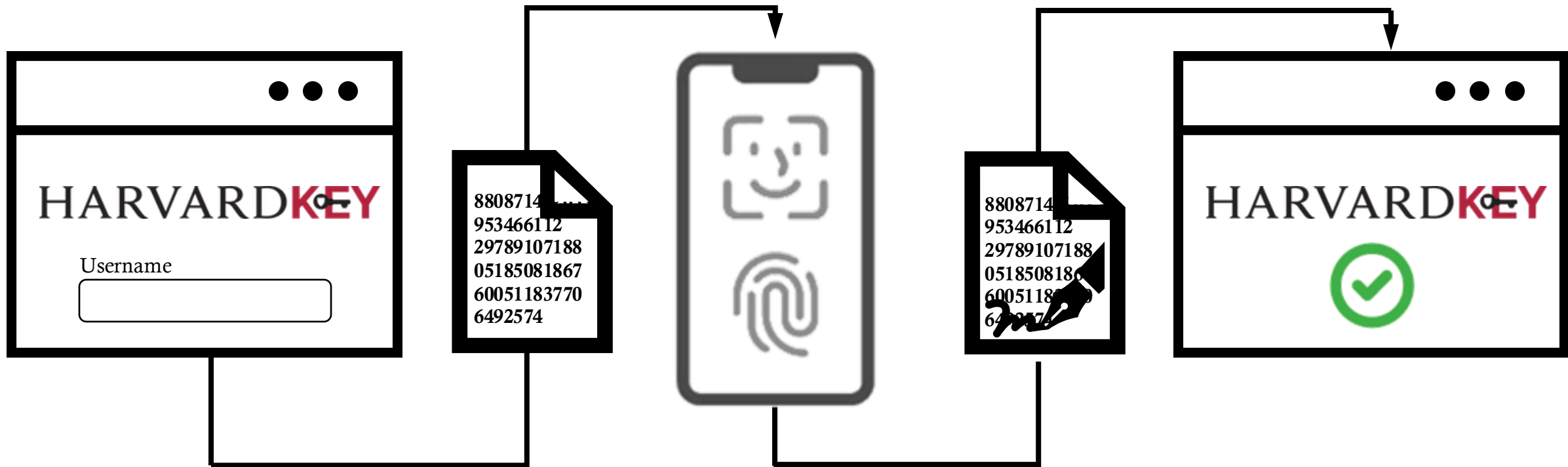
PASSWORDLESS CHANGES THE GAME



Passwordless:

- Eliminates shared secrets (passwords)
- Binds authentication to the site
- Removes push prompts and SMS

PASSWORDLESS AUTHENTICATION



Server sends a login challenge

You unlock your private key using your device's security mechanism.

Your device signs the challenge with your private key.

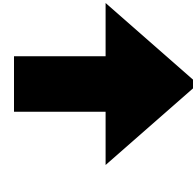
Server verifies the signature with the public key

FROM IDEA TO IMPLEMENTATION

HOW IT STARTED



HOW IT'S GOING



SaaS



Locally
Managed



WORKSTREAMS

Workstream

Scope

Approach

Okta to power HarvardKey

Lay the foundation

- Architect and implement an enterprise-wide identity platform using Okta
- **Launch a new HarvardKey sign-in screen**

- Single cutover day
- Minimize user impact

Okta MFA for users

Improve security; reduce complexity and operating costs

- **Migrate 100K+ MFA-required users to Okta security methods**
- **Encourage enhanced authentication options for all HarvardKey users**

- Enable Okta for everyone
- Passwordless as default option
- Pilot with IT and early adopters
- Migration in waves over 12 months
- Continuous refinement with each wave

Migrate apps to Okta

Improve security, stability, & resiliency; reduce complexity and operating costs

- Delegate authentication to Okta
- Migrate all to Okta to improve security, stability, and resiliency

- Delegate on one day
- Migrate over 18 months
- Regular reporting on migration progress

Enhanced security capabilities

Improve security through passwordless auth and endpoint posture assurance

- **Require passwordless authentication for some populations**
- **Require endpoint posture assurance when accessing high-risk applications**

- Require passwordless in waves by risk
- Passwordless readiness prior to cutover

OKTA CUTOVER DAY

Impacted Population:

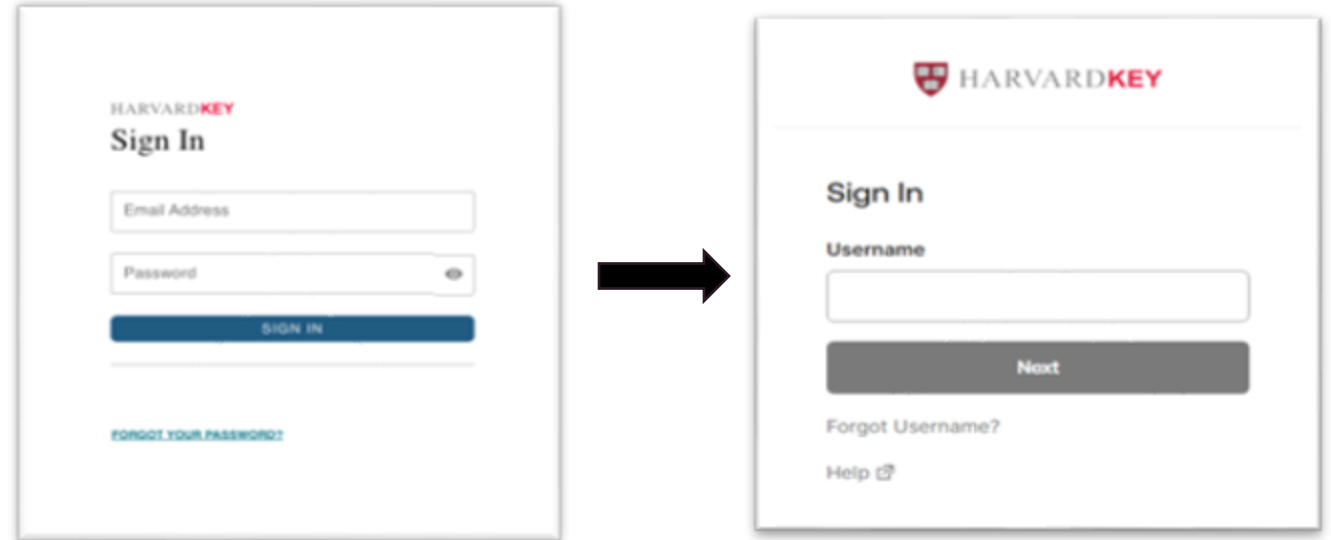
- 500,000 HarvardKey account holders
- ~120,000 MFA users

Changes:

- New login screen
- Link Duo to Okta on next login

User Communications:

- Banner on login screen
- Emails
 - New login coming soon (month before)
 - Changes are here (day before)
- Announcement on IT support phone lines



IT Communications and Coordination:

- Monthly stakeholder meetings
- Dedicated Slack channels
- Interactive demos
- Surge staffing on support lines

OKTA FOR MFA

Change: Okta replaces Duo for MFA

Impacted Population:

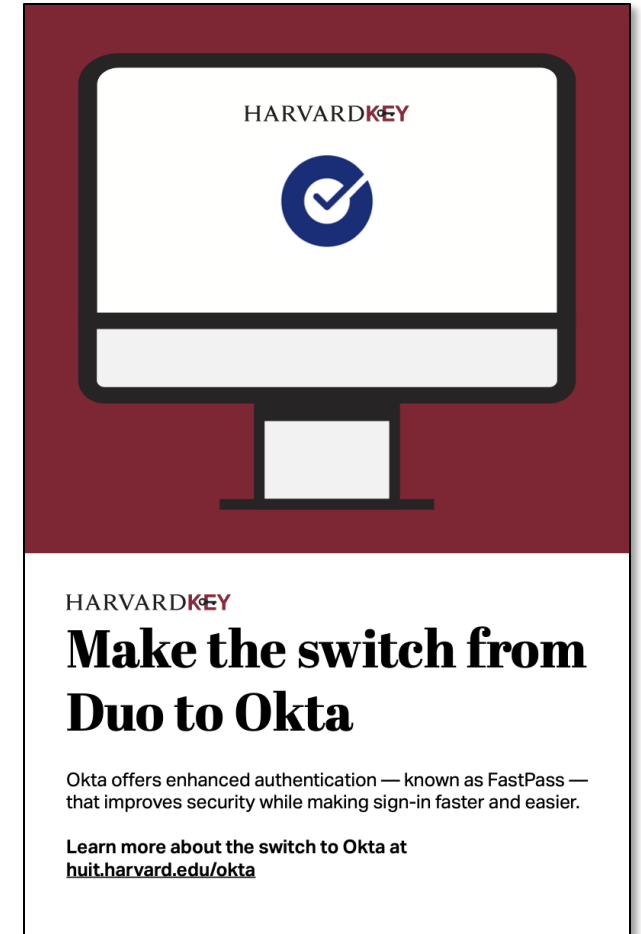
- ~120,000 users university wide
- spread across 17 waves over 12 months

User comms:

- Three emails
 - Enroll now (month before)
 - Reminder (two weeks before)
 - Deadline (day before)
- Posters

IT comms and coordination:

- Monthly stakeholder meetings
- Dedicated Slack channels
- Okta adoption reporting
- Template language



GOING PASSWORDLESS

Change: Passwordless required

Impacted Population:

- ~50,000 users university wide
- multiple waves over 12 months

User comms:

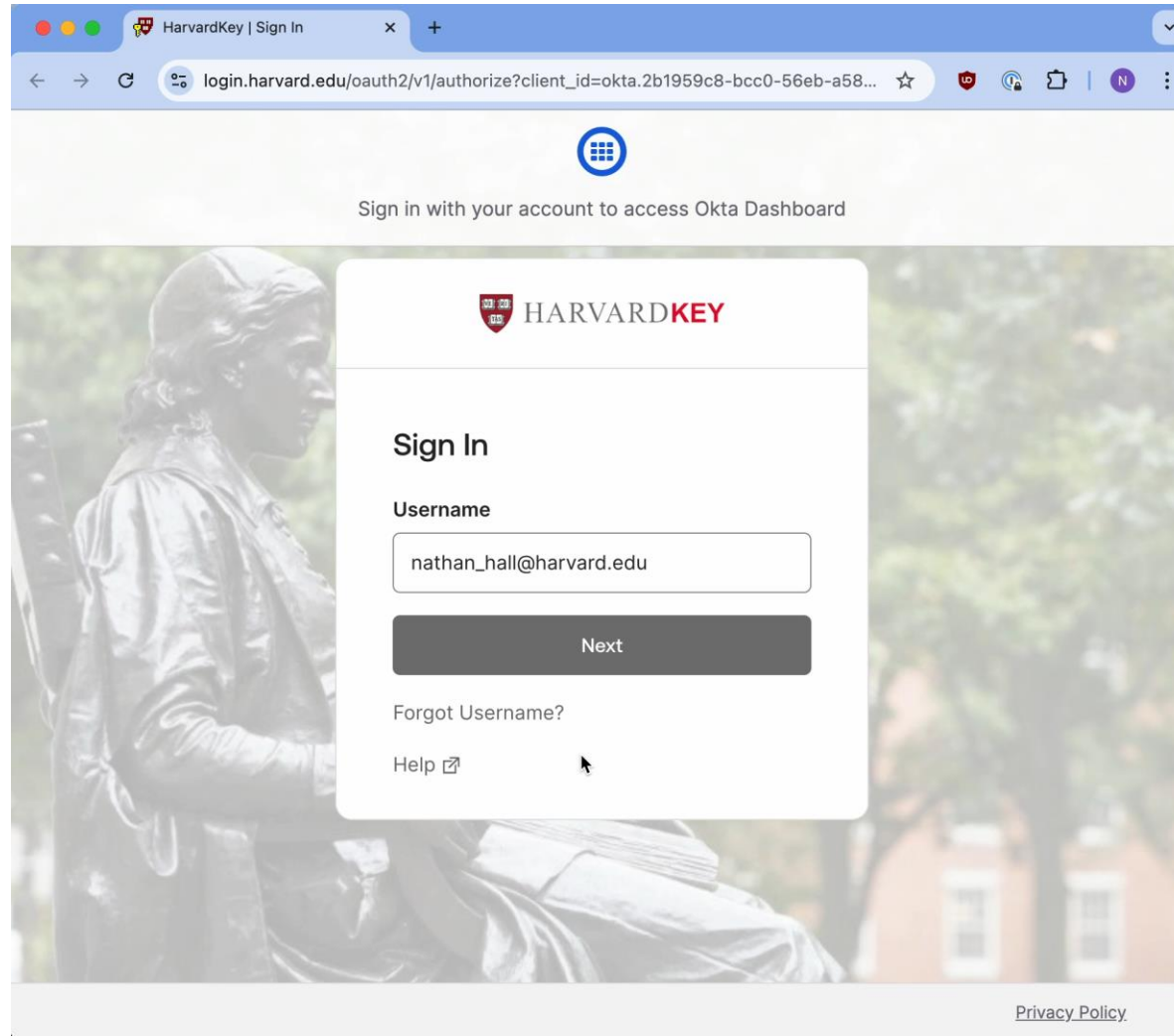
- Three emails
 - Go passwordless now (month before)
 - Reminder (two weeks before)
 - Deadline (day before)
- Posters

IT comms and coordination:

- Monthly stakeholder meetings
- Dedicated Slack channels
- Passwordless readiness reporting

RESULTS

PASSWORDLESS IN ACTION



The screenshot shows a web browser window with the HarvardKey Sign In page. The browser's address bar displays the URL `login.harvard.edu/oauth2/v1/authorize?client_id=okta.2b1959c8-bcc0-56eb-a58...`. The page features a blue grid icon at the top center, followed by the text "Sign in with your account to access Okta Dashboard". Below this is a large background image of a statue. Overlaid on the image is a white sign-in form with the HarvardKey logo at the top. The form includes a "Sign In" heading, a "Username" label, a text input field containing `nathan_hall@harvard.edu`, a dark "Next" button, a "Forgot Username?" link, and a "Help" link with an external icon. A mouse cursor is positioned over the "Help" link. At the bottom right of the page, there is a "Privacy Policy" link.

HarvardKey | Sign In

login.harvard.edu/oauth2/v1/authorize?client_id=okta.2b1959c8-bcc0-56eb-a58...

Sign in with your account to access Okta Dashboard

HARVARDKEY

Sign In

Username

nathan_hall@harvard.edu

Next

[Forgot Username?](#)

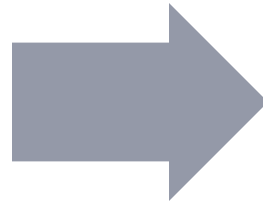
[Help](#)

[Privacy Policy](#)

I AM NOT GIVING HARVARD MY FINGERPRINT

Challenges:

- Belief Harvard was collecting biometric information
- Community member distrust of biometric authentication



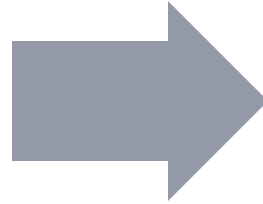
What worked: Non-biometric options

- Device-based PIN
- Passkey in a password manager
- Yubikeys

MY DEVICE DOESN'T SUPPORT PASSWORDLESS

Challenges:

- Computers without biometric hardware
- Computers unsupported by Okta Verify
- “I don’t have a smart phone”



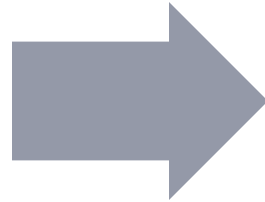
What worked: Options

- Windows Hello with PIN unlock
- Passkey in a password manager
- Passkey cross platform authentication
- Yubikeys

I LOG IN FROM A VIRTUAL DESKTOP

Challenges:

- IT supported Virtual Desktop Infrastructure (VDI)
- Individuals connecting via Remote Desktop and then authenticating



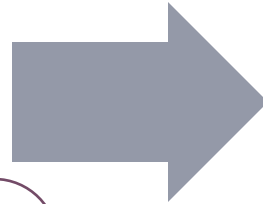
What worked: Exceptions and Options

- Allow fallback to push MFA from vetted instances
- Passkey in a password manager

I USE SHARED/PUBLIC COMPUTERS

Challenges:

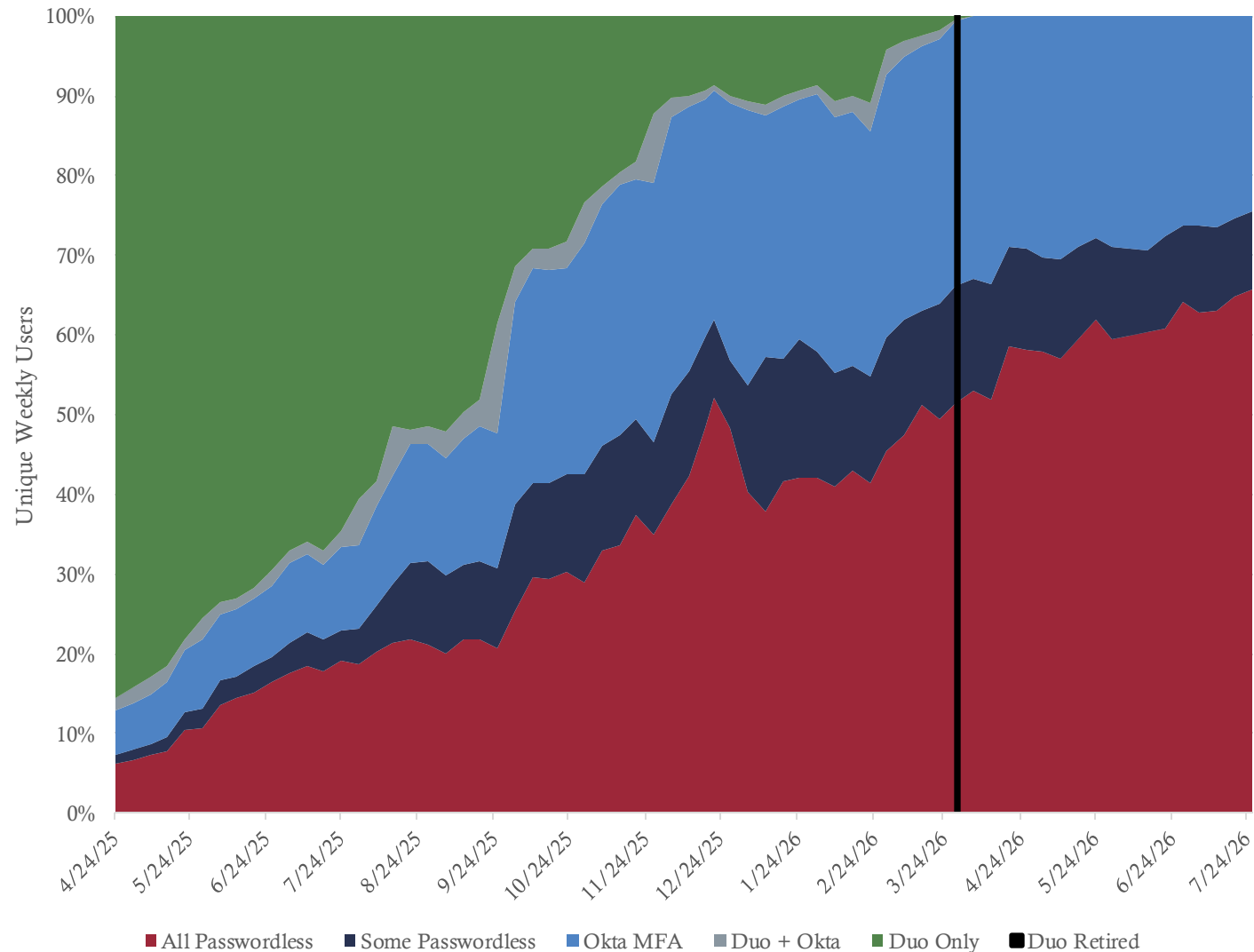
- Computer labs/library kiosks
- Classroom instructor computers



What we're testing:

- Passkey cross platform authentication
- Yubikeys
- Allowing traditional MFA from some Harvard networks

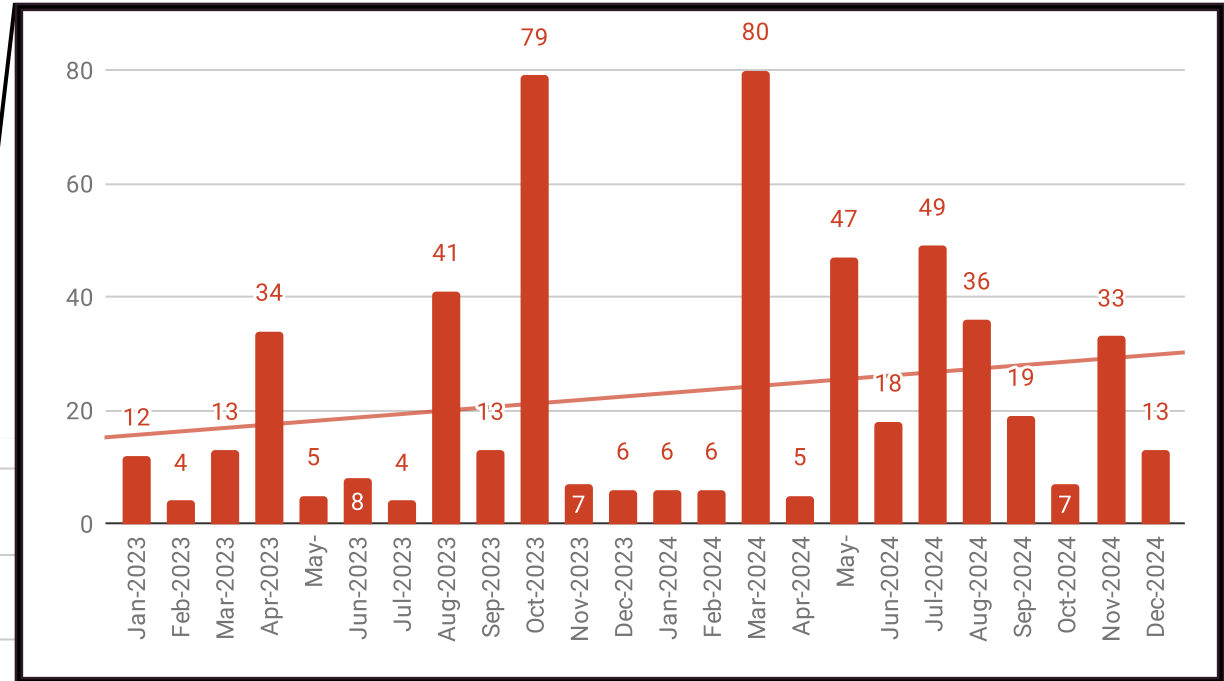
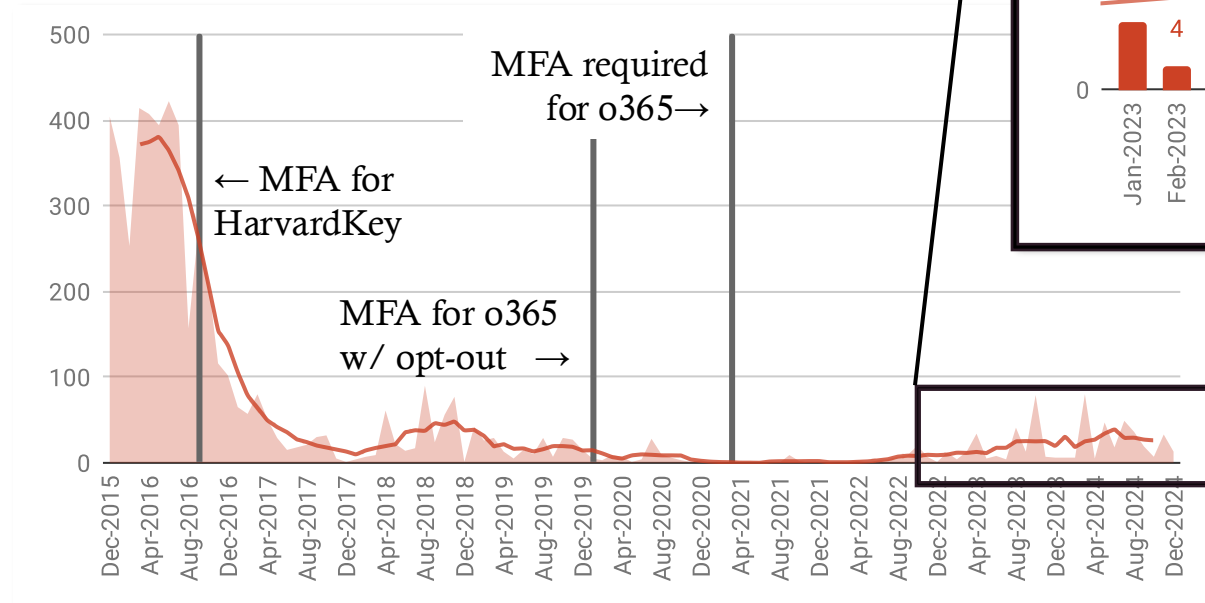
OKTA AND PASSWORDLESS ADOPTION



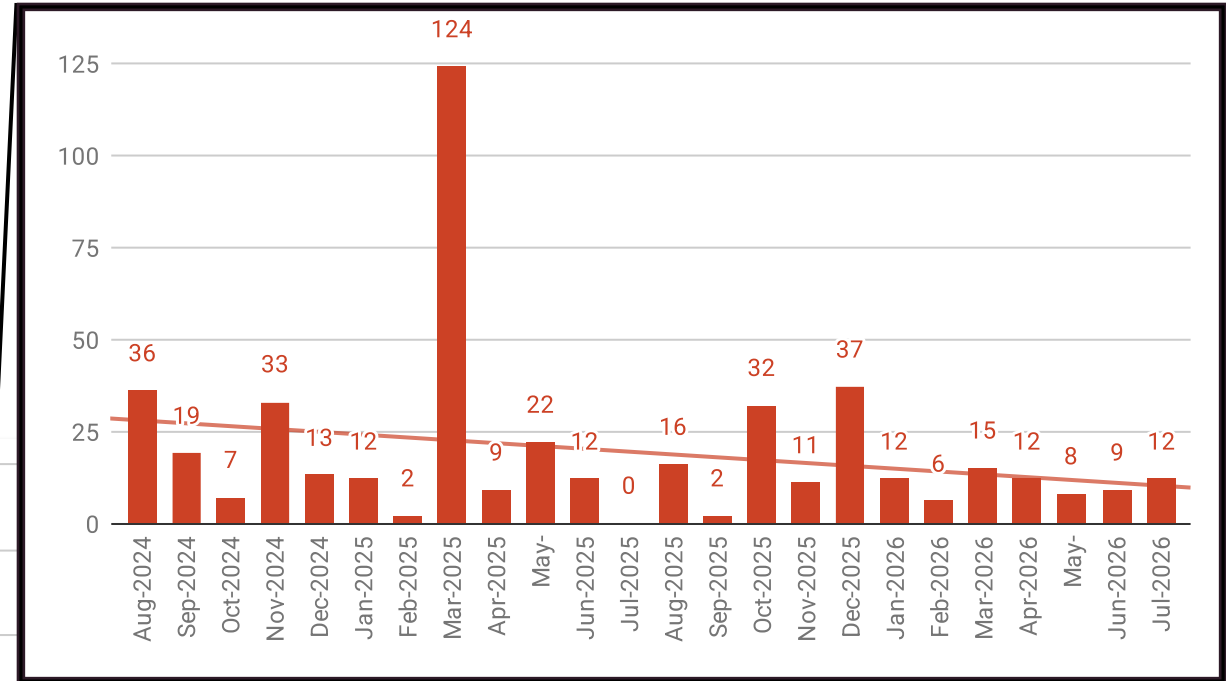
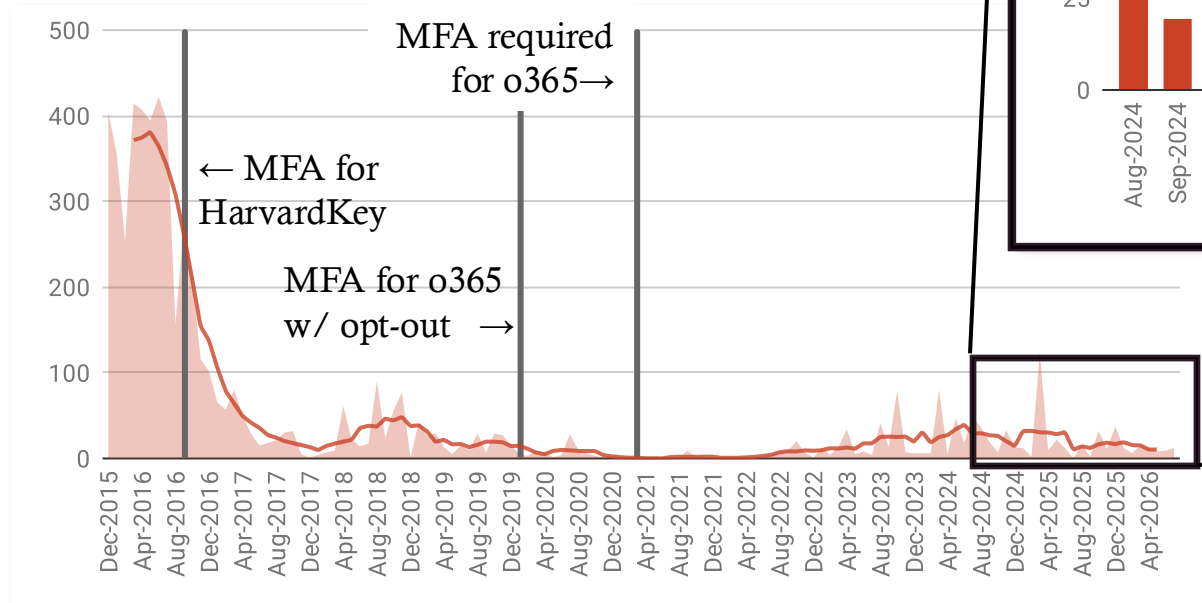
Making passwordless the easy default drove high adoption:

- 2/3 of users are all passwordless
 - Only 10% are passwordless required
- 75% use passwordless at least sometimes

WHERE WE STARTED



WHERE WE ARE NOW



WHAT'S NEXT

Completing
Passwordless
Required Rollout

All staff by end of summer 2026
Faculty by end of December 2026

Staying
ahead of
attackers

Device enrollment phishing – We have restricting self-service device enrollment to limit this attack surface.
Compromised devices – We plan to implement device posture checks to restrict access from unhealthy devices.

Q & A