

German/US Expert Meeting

IT Security Association Germany (TeleTrust) in cooperation with FIDO Alliance

San Francisco, 30.04.2025

Passkeys: Foundations and State of Adoption

Andrew Shikiar

CEO and Executive Director

FIDO Alliance

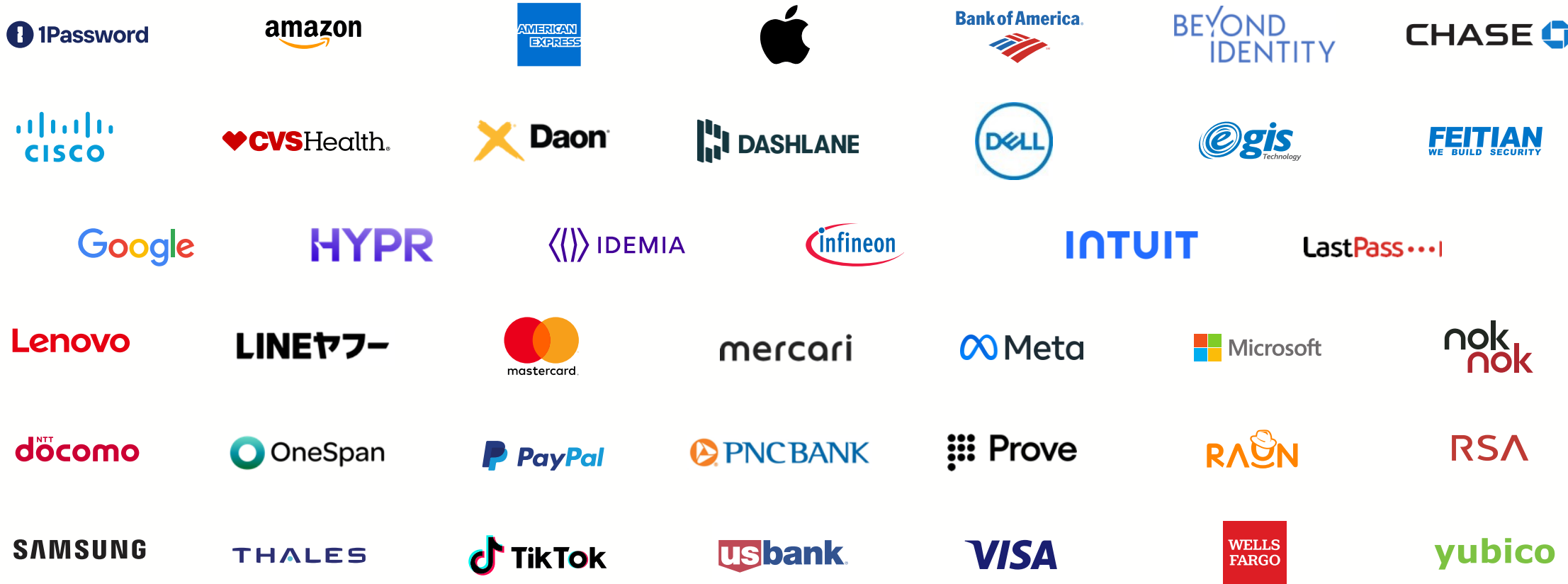
What is the FIDO Alliance?



The FIDO Alliance is an open industry association with a focused mission: **reduce the world's reliance on passwords.**

To accomplish this, the FIDO Alliance promotes the development, use and compliance with standards for authentication and device attestation.

Backed by 300+ global tech leaders



- + Sponsor members
- + Associate members
- + Liaison members
- + Government members

The FIDO Alliance works to fulfill its mission through...



Technical Specifications

Define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords



Industry Certification Programs

Ensure interoperability, security and usability of products, services and components

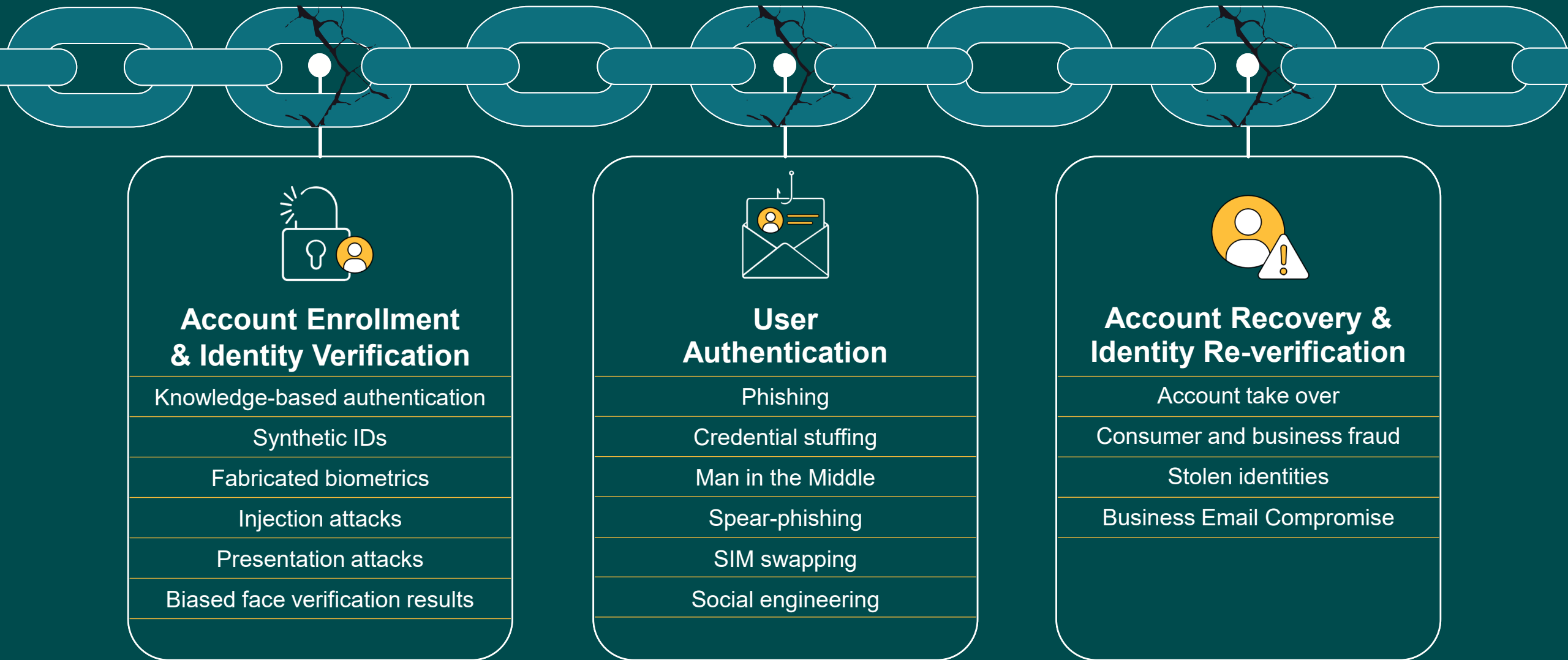


Market Adoption Programs

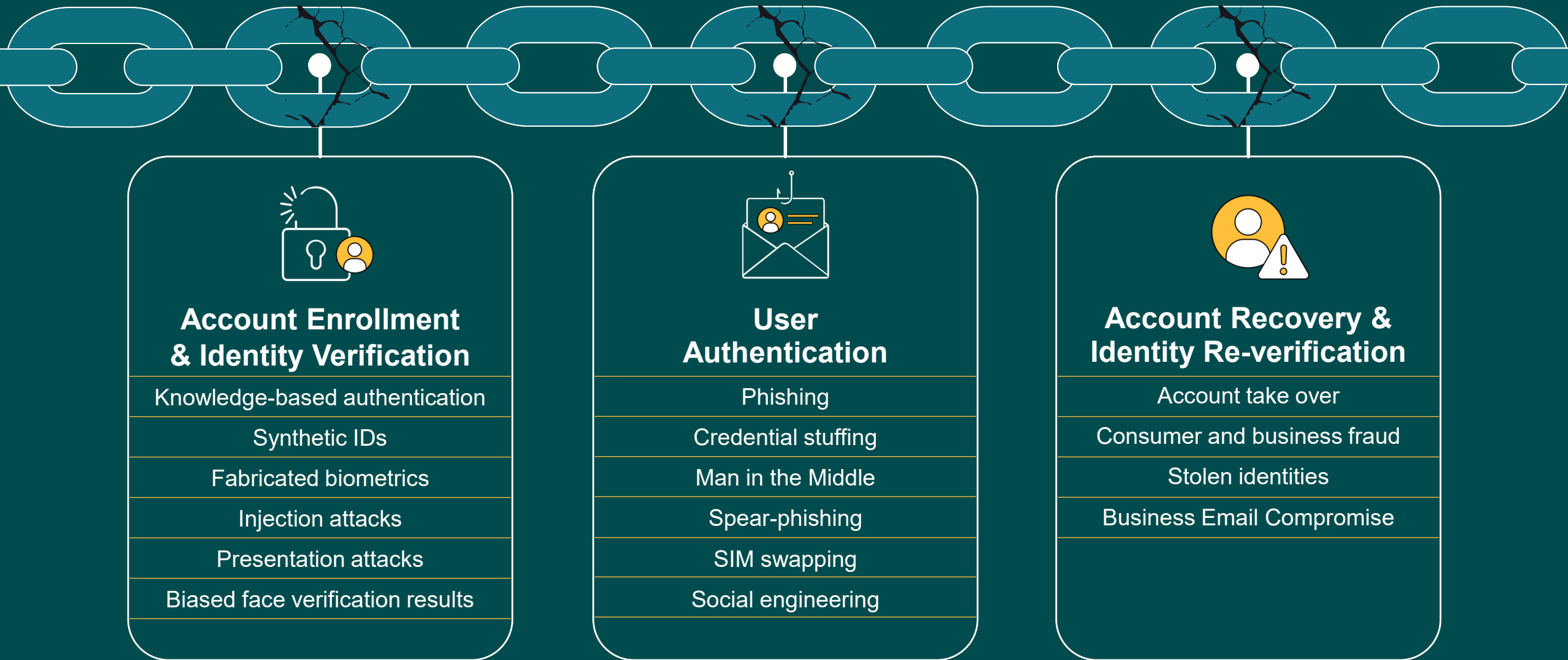
Promote the use of FIDO globally to drive adoption and education

FIDO's role in the account lifecycle

Today's Risks Span the Identity Lifecycle



Today's Risks Span the Identity Lifecycle



The foundation of authentication is fundamentally flawed

When our primary factor is passwords...

81%

of hacking-related breaches
are caused by weak or stolen
passwords
(Ping Identity)

43%

Gave up on a purchase
because they forgot their
password
(FIDO Alliance)

76%

Rise in direct financial loss
from successful phishing
attacks from 2022-2023
(Proofpoint)

64%

either use weak passwords or
repeat variations of passwords
(Keeper)

Easily phished or socially engineered, difficult to use and maintain

Layering on does not work

...then our additional layers – while well-intended and necessary
– are there to cover up password problems

4 Ways Hackers use Social Engineering
to Bypass MFA

The Hacker News

Multifactor Authentication Bypass: Attackers Refine
Tactics: During the first quarter of 2024, nearly half
of all security incidents involved MFA.



The art of MFA Bypass: How attackers regularly
beat two-factor authentication



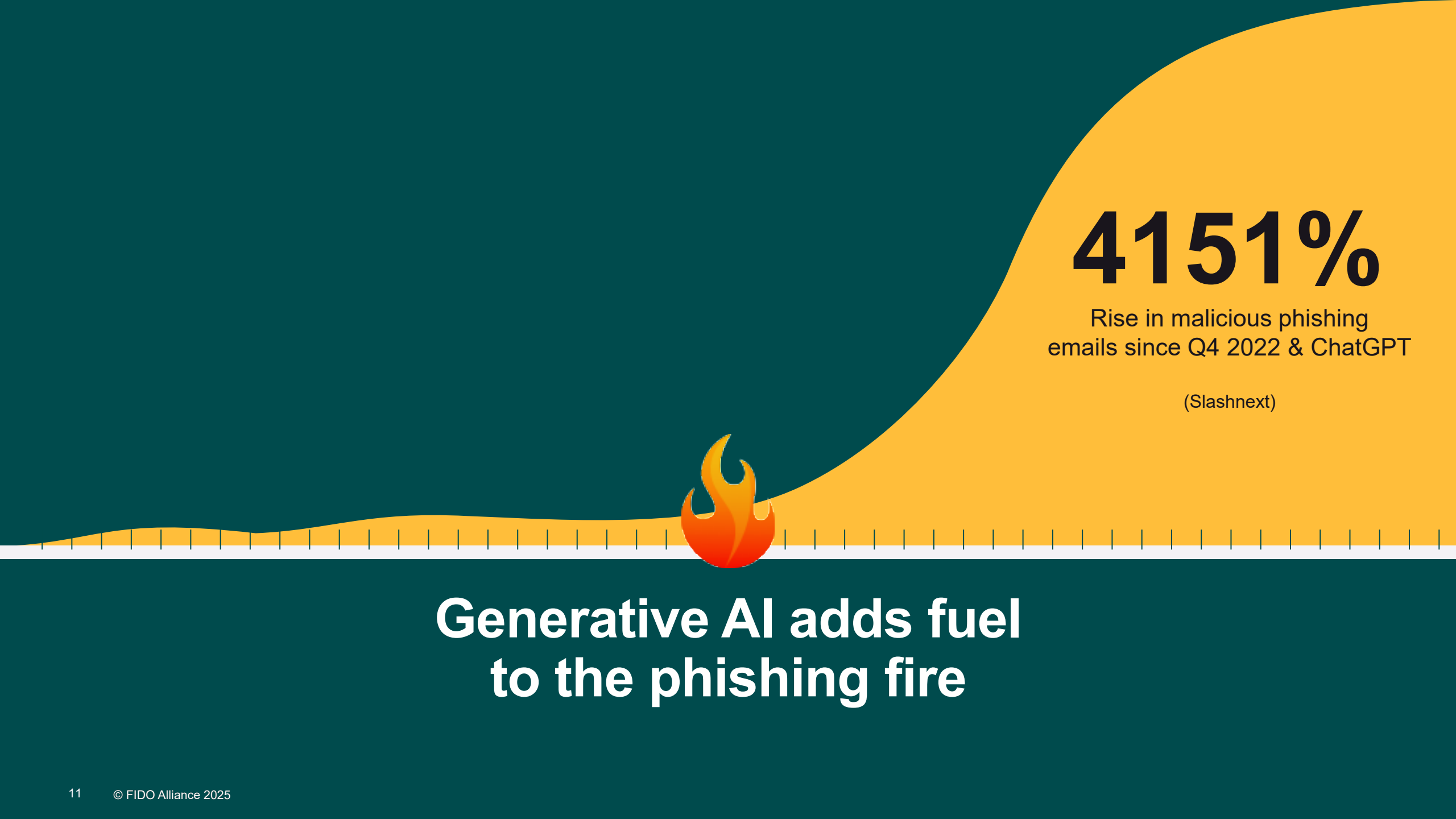
New MFA-bypassing phishing kit targets
Microsoft 365, Gmail accounts

BLEEPINGCOMPUTER

Often still phishable, socially engineered, difficult to use and maintain



Generative AI adds fuel to the phishing fire



4151%

Rise in malicious phishing
emails since Q4 2022 & ChatGPT

(Slashnext)

**Generative AI adds fuel
to the phishing fire**

4151%

Rise in malicious phishing emails since Q4 2022 & ChatGPT

(Slashnext)

30x

More affordable and equally efficient compared to humans

(Harvard Kennedy School)

53%

of consumers reported more suspicious messages and online scams in 2024

(FIDO Alliance)

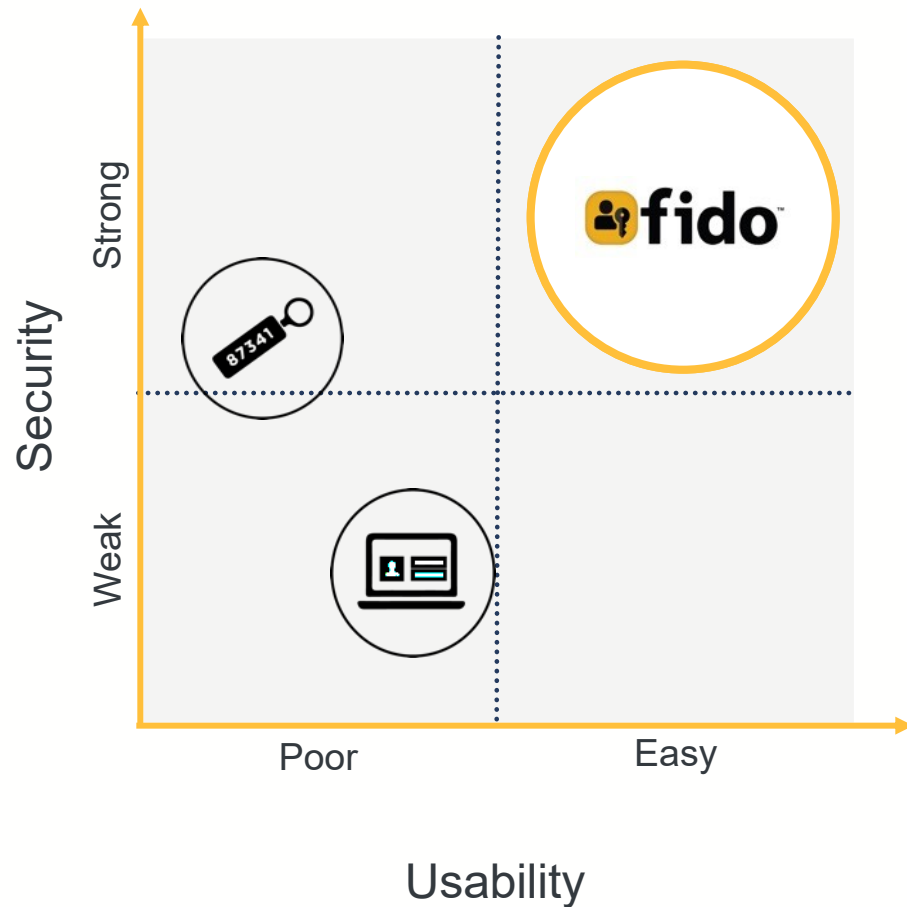


Generative AI adds fuel to the phishing fire

Passkeys represent a fundamental pivot

If phishing is now the primary threat, a single phishing-resistant authenticator is more valuable (in most cases) than two factors which are both easily phished.

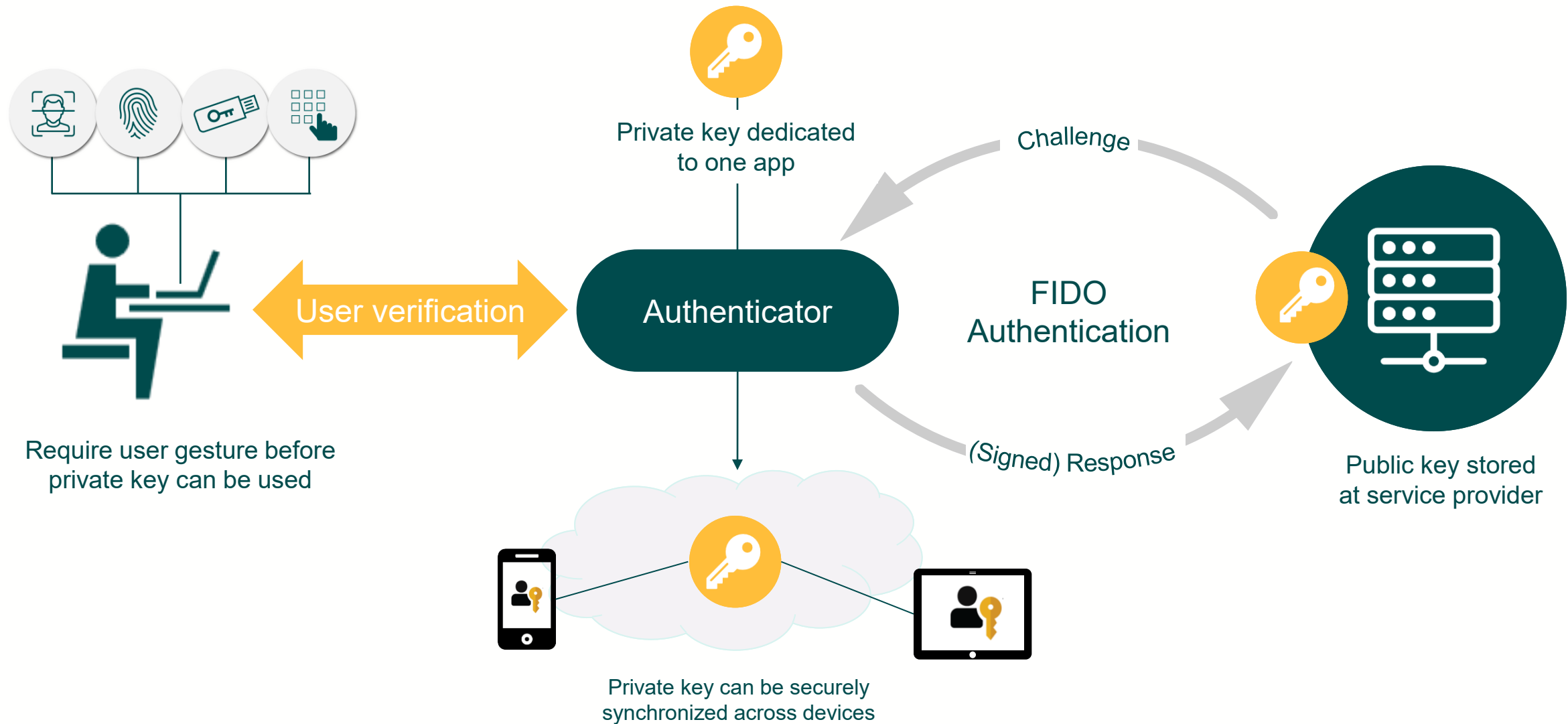
FIDO since 2013: Simpler and stronger



Open standards for simpler, stronger authentication using **public key cryptography**

- Single Gesture –
- Possession-based –
- Phishing-resistant –

Phishing-resistant authentication with passkeys



The state of adoption

Chrome on Windows

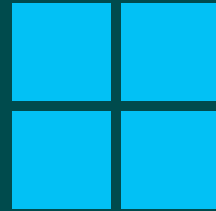


Firefox on Windows

Chrome on Android

Edge on Android

Apps on iOS



Available



Safari on iOS

Chrome on Mac

Edge on Mac

Edge on Ubuntu



Chrome on iOS

Edge on iOS

Apps on Mac



Apps on Android

Chrome on Ubuntu



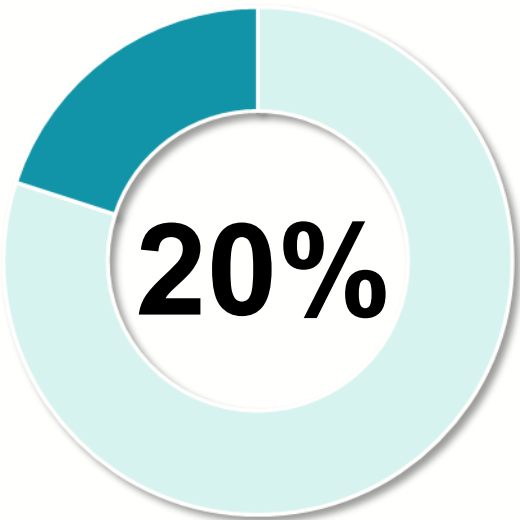
Edge on Windows

Safari on Mac

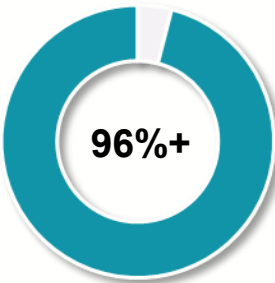
Today!

Passkey adoption by the numbers

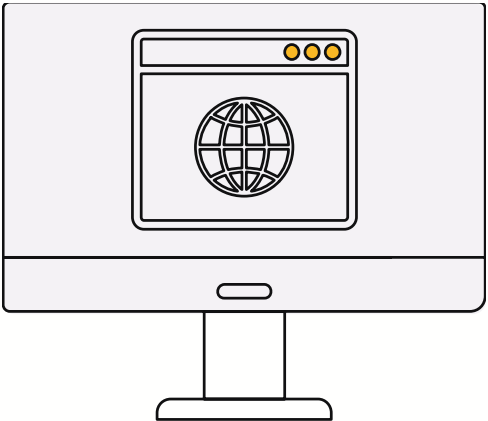
(Since October 2022)



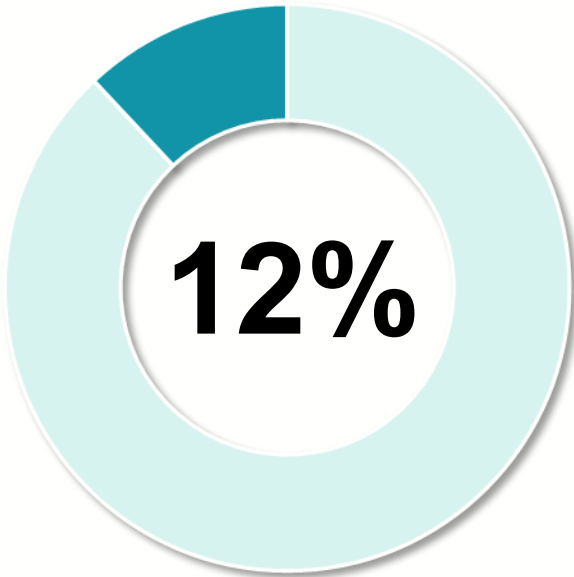
of the world's top
100 websites and services



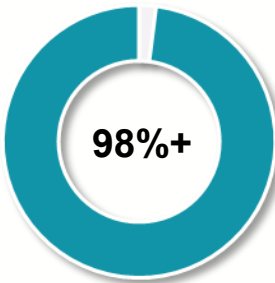
of active
browsers



More than **15B**
accounts can now leverage
passkeys for sign in



of the world's top
250 websites and services



of mobile
devices

Consumer adoption snapshots

Microsoft

- 99% completion rate for passkey enrollment
- 98% sign-in success rate
- 3x faster sign-ins over passwords
- 9x faster sign-ins over password + MFA



PlayStation

- 24% reduction in sign-in time on web
- 29% of password resets resulted in passkey conversion, removing passwords completely
- 88% of users engaging with passkey content completed the transition and eliminated their passwords



Mercari

- Sign-in success rate grew from 67.7% (SMS 2FA) to 82.5% – over a 21% improvement
- Authentication time decreased from 17s (SMS 2FA) to 4.4s – nearly 4x faster
- ZERO phishing incidents



Air New Zealand

- 30% opt-in in first 24 hours
- 4.7x improvement time to complete & improvement in success rate
- 50% reduction in abandonment rates
- Reduced account recovery calls and call center attacks



Passkey awareness and adoption is increasing

57%

of consumers
are aware of
passkeys – up from
39% in 2022



87%

of organizations
have deployed
passkeys for
workforce sign-ins

Enterprise / workforce adoption snapshots

IBM

- Conditional MFA approach, introduced synced passkeys June 2022 in addition to pre-existing device-bound passkeys
- Prioritizing user education and adoption with education and manager incentives
- Determines use of synced vs device-bound passkey via appropriate assurance level



Alibaba

- 19k employees actively using passkeys (10% increase from 2023)
- 50,000 passkey requests weekly
- 1,000,000 fewer 2FA texts in past year
- User-reported issues have significantly decreased



T-Mobile

- 200,000+ YubiKeys deployed for employees, vendors and partners
- Replaced passwords and OTPs with device-bound security keys for passwordless authentication
- Deployment completed in under three months
- Reduced phishing incidents, improved cybersecurity efficiency

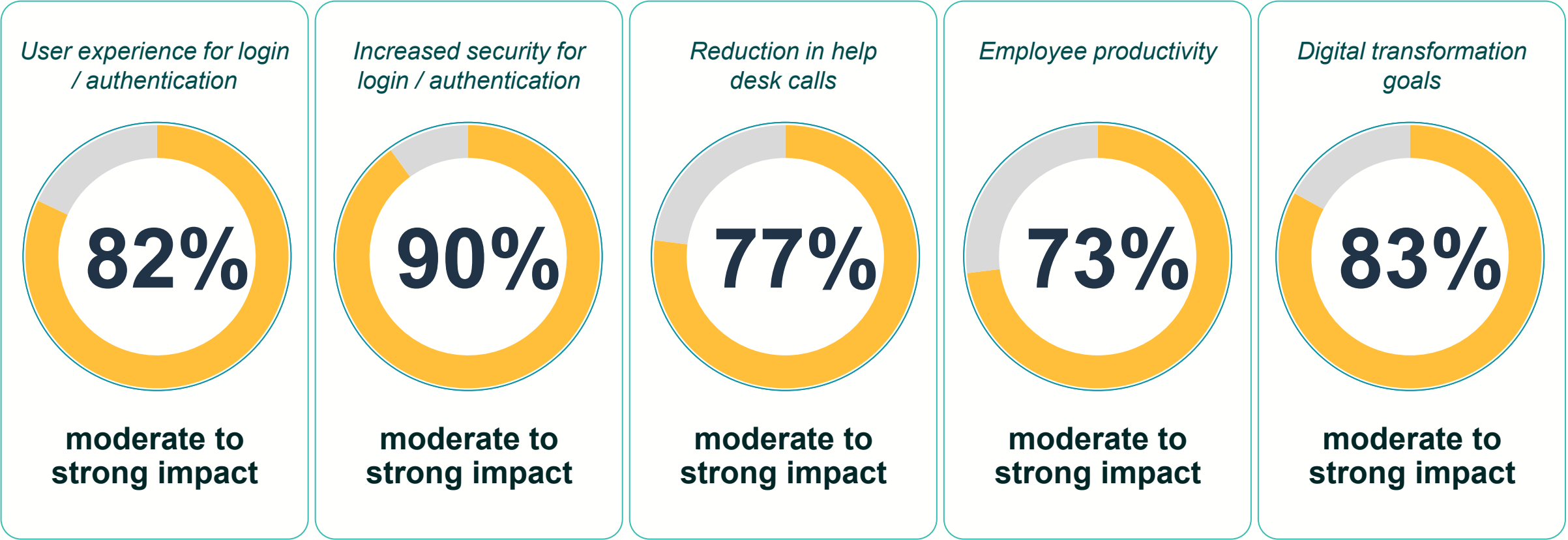


DocuSign

- 20% reduction in password reset costs just 3-4 months post-rollout
- Resulted in increases in Net Promoter Scores
- Reduced documented customer complaints about login flows



Enterprises report significant benefits due to passkey implementations



Government Adoption

myGov

- Deployed in June 2024
- Adoption increased by 750% in first 8 weeks
- 500,000 users by end of 2024; 40% of which (200K) had disabled their password.
- Adoption continues to rise as user education improves and more government agencies integrate passkeys into their systems



UK NHS

- 20+ services with sign-in integrated
- 250,000 FIDO authorization requests a week
- 25,000 new users per week with FIDO UAF biometric authentication
- Reduced SMS OTPs by two-thirds, yielding significant cost savings



USDA

- Workforce device-bound passkey rollout in 2024
- Two device-bound FIDO options were piloted
- 600+ applications protected from advanced MFA bypass techniques by using FIDO authentication in SSO system

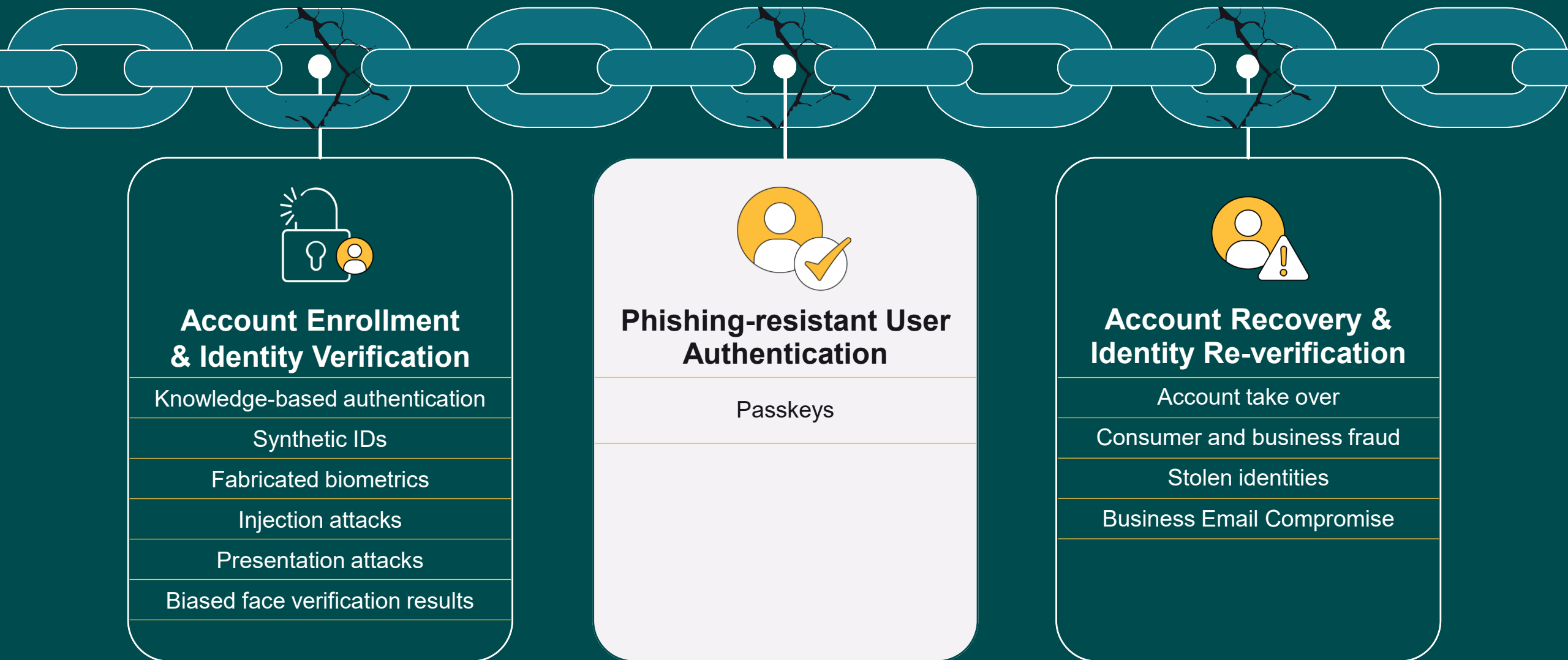


Taiwan Ministry of the Interior

- TW FidO launched with UAF in 2019, and updated with FIDO2 to integrate with Mobile Citizen Digital Certificate in 2022
- Free PKI for Taiwanese businesses and agencies to accelerate adoption
- 200+ apps from central & local governments, telecom and financial service providers as of June 2024



Account lifecycle: Addressing today's risks



Deepfakes and bias are problems today

...strong IDV can detect deepfakes and improve IDV accuracy...

– liveness and bias testing are needed to assure security, usability, and equity

Security Firm Accidentally Hires North Korean Hacker, Did Not KnowBe4

DARKREADING

'I was misidentified as shoplifter by facial recognition tech'

B B C

MGM Resorts Hackers Broke In After Tricking IT Service Desk

Bloomberg

How Wrongful Arrests Based on AI Derailed 3 Men's Lives

W I R E D

1 out of 4 reported feeling discrimination when using biometric face verification technologies.

– FIDO Alliance Remote IDV Report, 2024

FIDO IDV and Biometric Authentication Certification Programs



Document Authenticity

- Tests for authenticity of government-issued ID documents
- Verifies the authenticity of government-issued documents during initial account set up and account recovery (i.e., employees, citizens)
- Complements the FIDO IDV Face Verification program



Face Verification

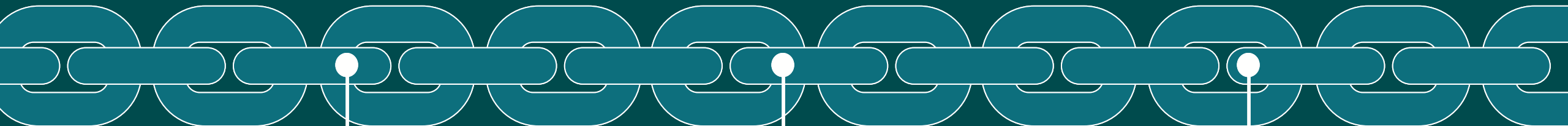
- Tests for security, bias, accuracy, and liveness of facial biometrics
- Verifies identities using “selfie-match” technology matched to the user’s government-issued ID (i.e., employee onboarding with I-9 and passport)
- Complements the IDV Document Authenticity program



Biometric Components

- Tests for security, bias, and accuracy of biometric performance during FIDO authentication
- Assures performance, interoperability, and security of biometric components used in FIDO authentication
- Complements the FIDO Certified Authenticator program

Securing the Account Lifecycle: **The FIDO Approach**



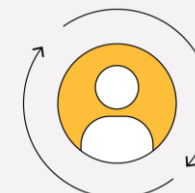
Secure Account Enrollment

Certified Remote Identity Verification



Phishing-resistant User Authentication

Passkeys



Secure Account Recovery



In summary

In summary

- ✓ Phishing, deepfakes and other generative AI-driven attacks are targeting each part of the account lifecycle with no signs of slowing down
- ✓ Awareness and adoption of passkeys is increasingly steadily – with adopters seeing real business benefits on top of increased security
- ✓ FIDO technologies and certifications are ready and available today to help you keep attackers out at every step

Get involved

- ✓ Get started with passkeys: visit passkeycentral.org
- ✓ Require and Use FIDO Certified products
- ✓ Get FIDO Certified
- ✓ Join the FIDO Alliance to drive passkey adoption and future identity initiatives



USE PASSKEYS!

THANK YOU