

2024 Europe Community Meeting

# Safeguarding Your Boat So You Don't Get Hooked



# Andrew Jamieson

Vice President, Standards  
PCI Security Standards Council



# Who has heard of the FIDO Alliance?



# Who has heard of passkeys?



# Who knows what phishing is?



# 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.

# 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






*"On the Internet, nobody knows you're a dog."*



GARAGE  
NO  
ENTRY

 Username

 \*\*\*\*\*

Remember Me

[Forgot Password?](#)

**LOGIN**

**REGISTER**



# The Foundation of Authentication is Fundamentally Flawed

When our primary factor is passwords → and 2FA & MFA are no longer secure...

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)

50%

Rise in MFA-related security events in Q1 2024, with 25% involving unauthorized push notifications.  
(Thales)

64%

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

Easily phished or socially engineered ▲ Difficult to use and maintain ▲ MFA can be hacked

# Generative AI adds fuel to the phishing fire

**967%**

Rise in credential phishing  
in particular since Q4 2022

(Slashnext)

**1265%**

Rise in malicious phishing  
emails since Q4 2022

(Slashnext)

**54%**

Of consumers have noticed  
phishing messages become more  
sophisticated in last 60 days

(FIDO Alliance)

# Multi-Factor Authentication Example



Password / OTP

# Attacking Authentication

**Non-Complex Password**



Guessing, credential stuffing, bruteforce, phishing  
Session / token hijack, technology bypass, enrollment attacks

# Attacking Authentication

**Non-Complex Password**



Guessing, credential stuffing, bruteforce, phishing  
Session / token hijack, technology bypass, enrollment attacks

**Complex Password**



Credential stuffing, bruteforce, phishing  
Session / token hijack, technology bypass, enrollment attacks

# Attacking Authentication

**Non-Complex Password**



Guessing, credential stuffing, bruteforce, phishing  
Session / token hijack, technology bypass, enrollment attacks

**Complex Password**



Credential stuffing, bruteforce, phishing  
Session / token hijack, technology bypass, enrollment attacks

**Complex Unique  
Password**



Bruteforce, phishing  
Session / token hijack, technology bypass, enrollment attacks

# Attacking Authentication

**Non-Complex Password**

Guessing, credential stuffing, bruteforce, phishing  
Session / token hijack, technology bypass, enrollment attacks

**Complex Password**

Credential stuffing, bruteforce, phishing  
Session / token hijack, technology bypass, enrollment attacks

**Complex Unique Password**

Bruteforce, phishing  
Session / token hijack, technology bypass, enrollment attacks

**Complex Unique Password + OTP**

Phishing, SIM hijack/swapping  
Session / token hijack, technology bypass, enrollment attacks

**Phishing Resistant Authentication**

Session / token hijack\*, technology bypass, enrollment attacks

\*Note: Device / session binding, ZTA can help with this

# What is a Passkey?

## Passkey

/ˈpas, kē/ noun

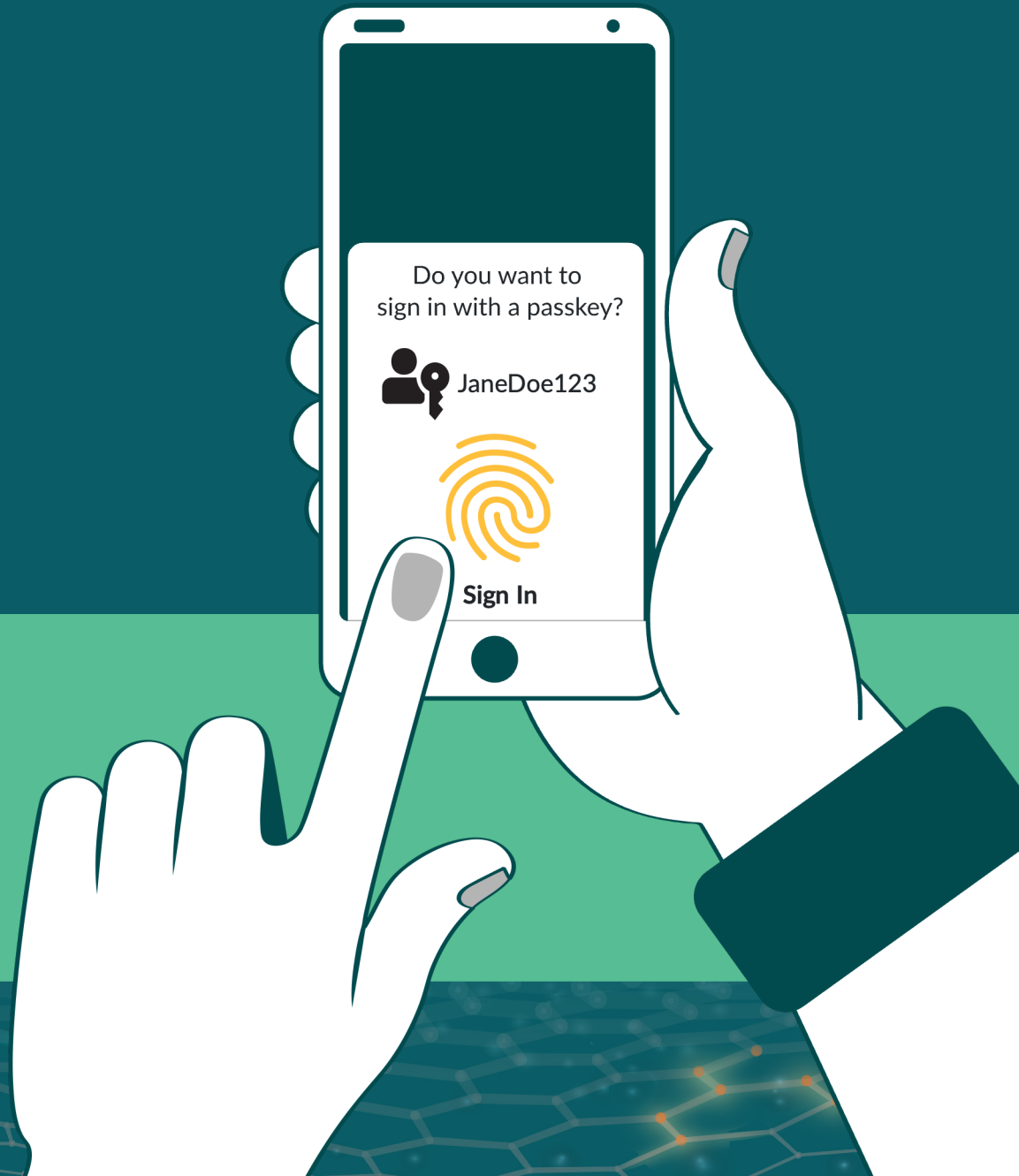
Passkeys are a password replacement based on FIDO protocols that provide faster, easier, more secure sign-ins to online services.

A passkey may be synced across a secure cloud so that it's readily available on all of a user's devices, or it can be bound to a dedicated device such as a FIDO security key.

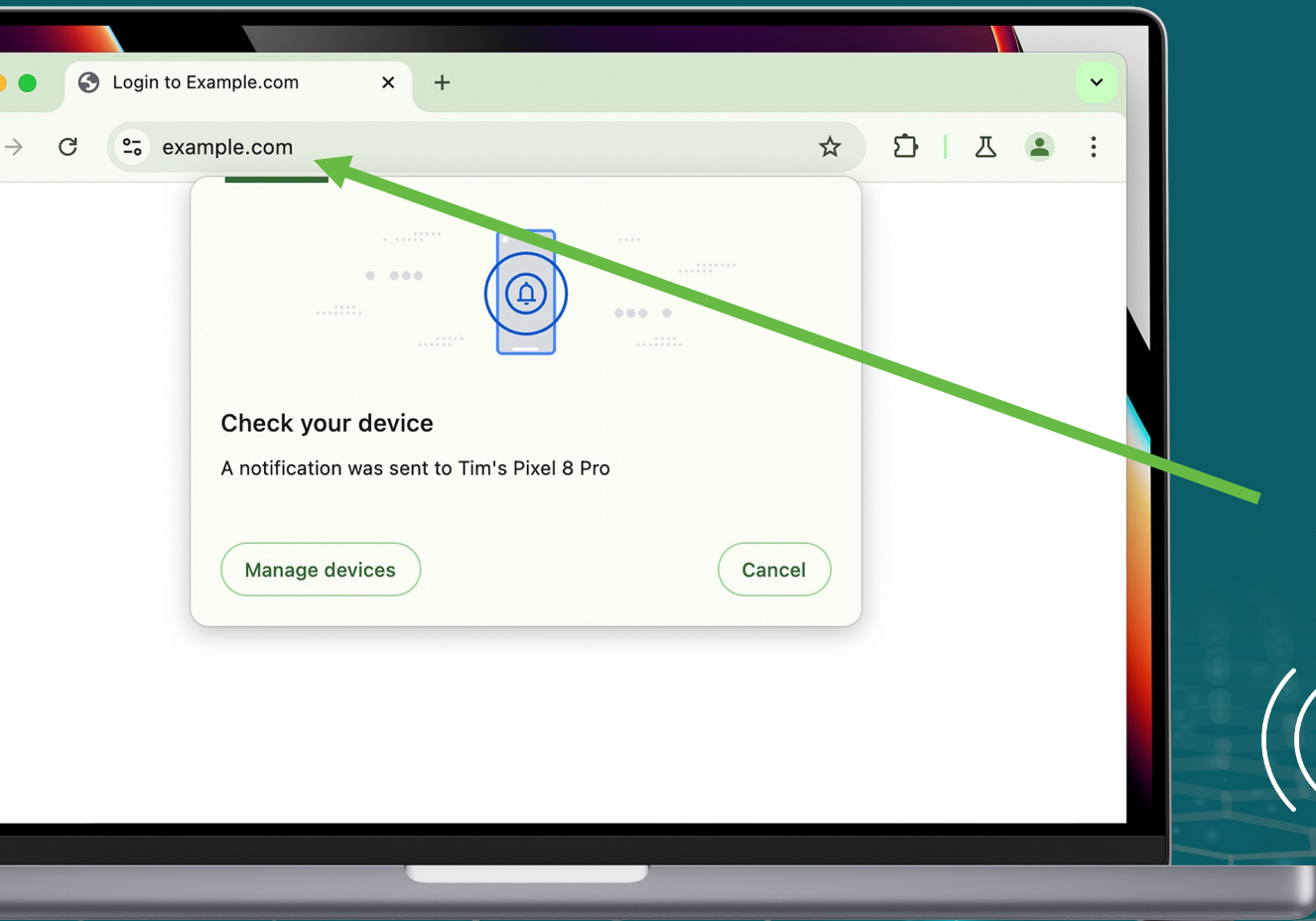
## 4x simpler

Passkeys are 4x simpler to use since they don't need to be remembered or typed. You just use your fingerprint, face scan, or screen lock to sign in across all your devices and platforms.

Source: Google



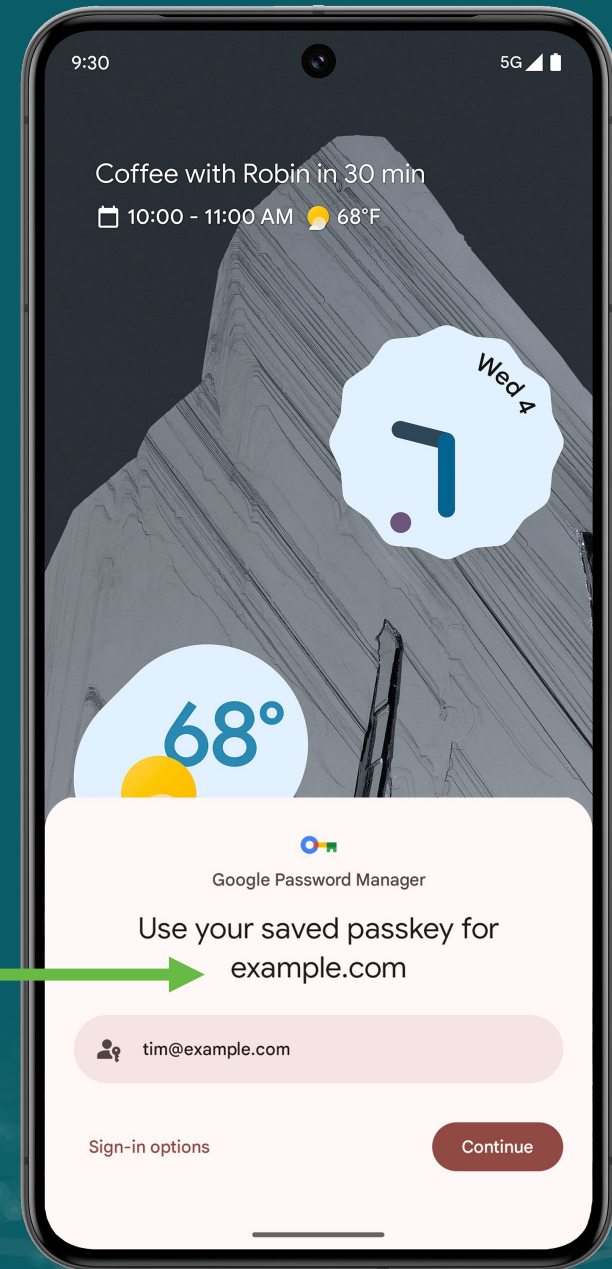
# How Does Phishing Resistant Authentication Work?



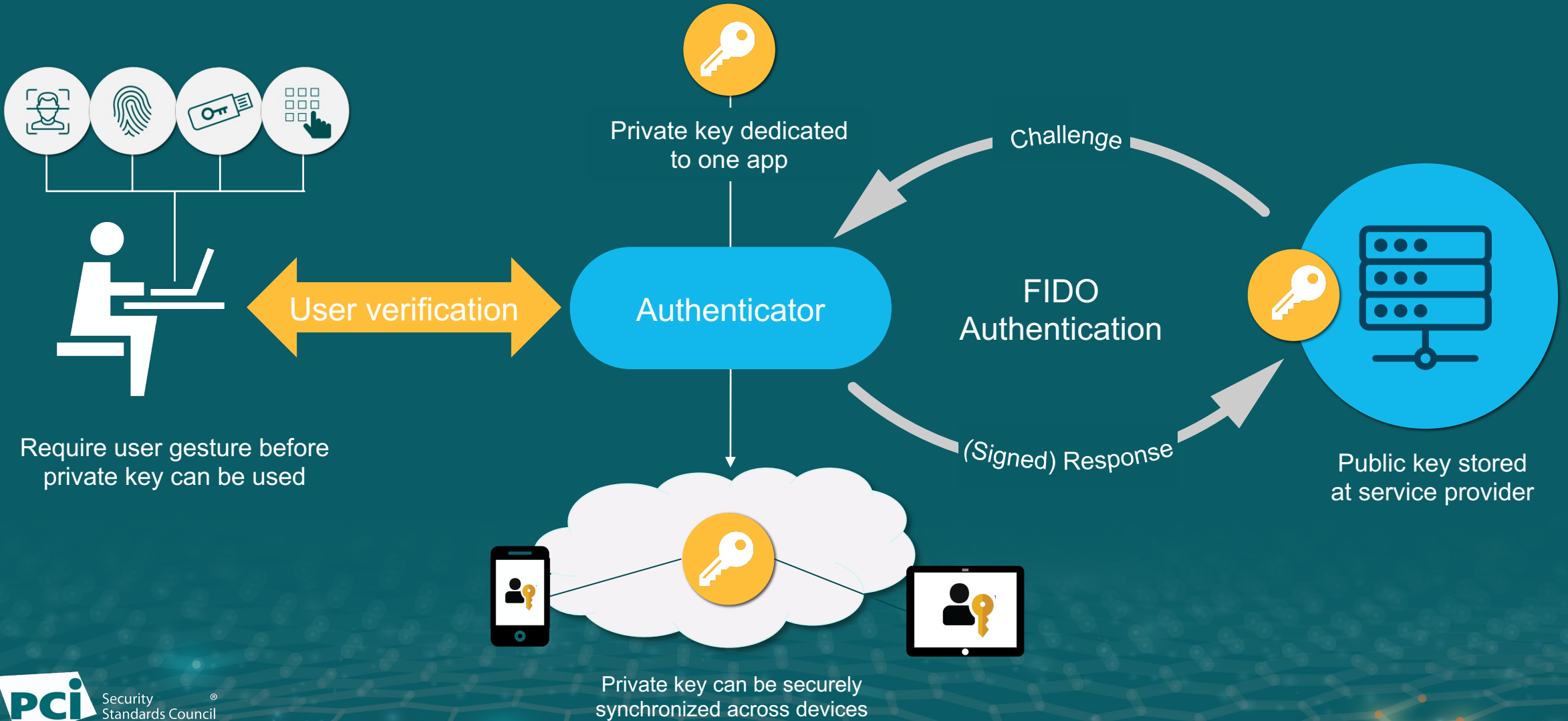
*public key  
cryptography*

*name binding*

*(( ( proximity ) ) )*

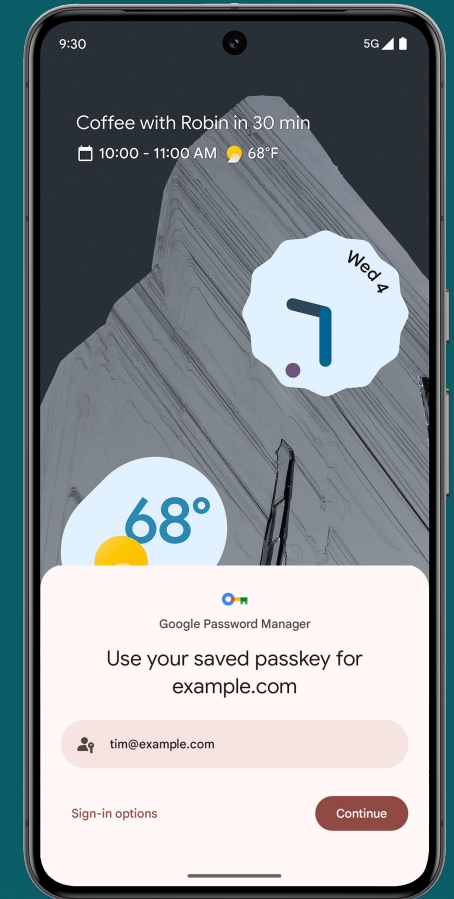
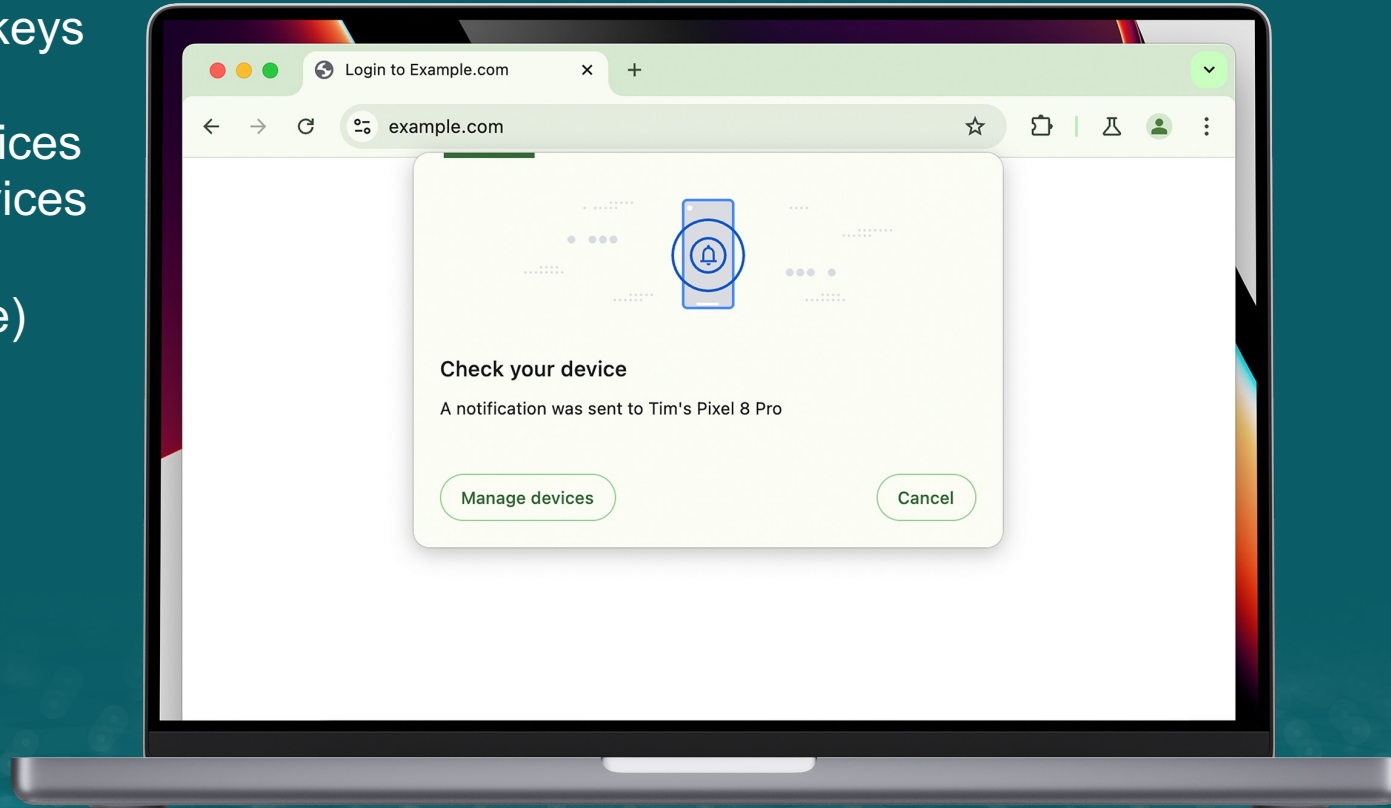


# Same Approach – With New Syncing Capabilities



# Cross-Device Authentication

Enables passkeys to be used to sign-in to services on nearby devices (as well as on primary device)



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



Chrome on iOS

Edge on Ubuntu

Edge on iOS



**Today!**



Apps on Mac

Apps on Android

Chrome on Ubuntu

Safari on Mac



Edge on Windows

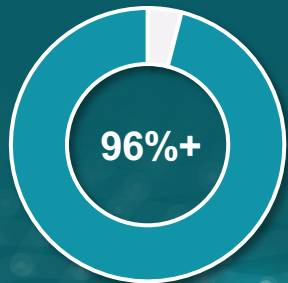


# Passkey Adoption by the Numbers

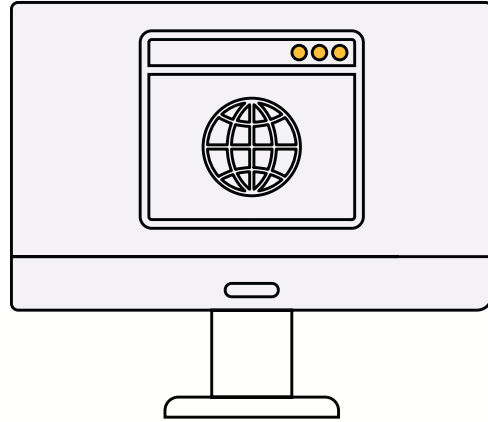
(Since October 2022)



of the world's top 100 websites and services

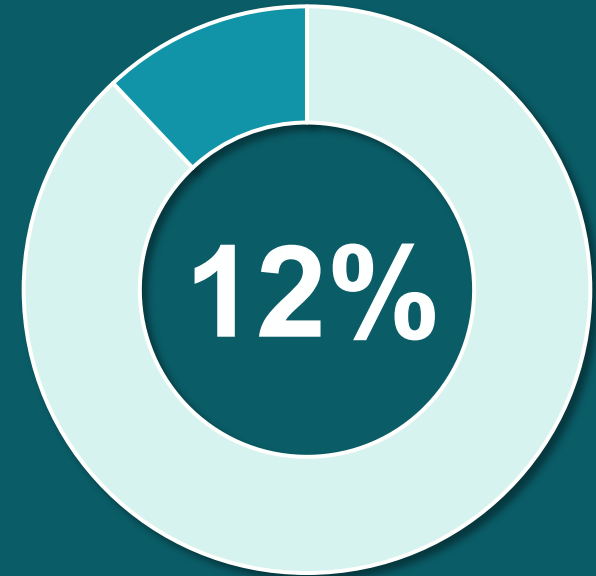


of active browsers

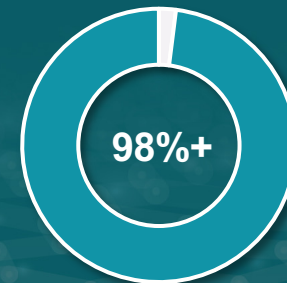


More than **13B**

accounts can now leverage passkeys for sign in



of the world's top 250 websites and services



of mobile devices

# Proven Success



Within the first few months...

- 97% login success rate
- 14% eligible user adoption rate
- 2% reduction in SMS OTP login

## 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



- 4x improvement in sign-in success rate (vs passwords)
- ½ the sign-in time
- 400M+ accounts have used passkeys
- 1B+ sign-ins with passkeys

## 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

# PCI DSS and Phishing-Resistant Authentication

## PCI DSS Requirement

8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.

## Interpretation

Phishing-resistant authentication can be used, but must be coupled with some other authentication factor

# PCI DSS and Phishing-Resistant Authentication

## PCI DSS Requirement

## Interpretation

**8.4.1** MFA is implemented for all non-console access into the CDE for personnel with administrative access.

Phishing-resistant authentication can be used, but must be coupled with some other authentication factor

**8.4.2** MFA is implemented for all non-console access into the CDE.

### **8.4.2** Guidance

This requirement does not apply to:

User accounts that are only authenticated with phishing-resistant authentication factors.

Phishing-resistant authentication can be used without another authentication factor

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

# PCI DSS and Phishing-Resistant Authentication

## PCI DSS Requirement

## Interpretation

**8.4.1** MFA is implemented for all non-console access into the CDE for personnel with administrative access.

Phishing-resistant authentication can be used, but must be coupled with some other authentication factor

**8.4.2** MFA is implemented for all non-console access into the CDE.

### **8.4.2** Guidance

This requirement does not apply to:

User accounts that are only authenticated with phishing-resistant authentication factors.

Phishing-resistant authentication can be used without another authentication factor

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Console access refers to a system with a direct physical connection to another system component, where that connection does not rely on a networked connection ...

Console access does not include situations where the system is used to access other system components over a networked connection. For example, access via a laptop or workstation using a physically connected keyboard is not considered “console access” if that system requires a networked connection to access any other system component. (from FAQ 1577)

# PCI DSS and Phishing-Resistant Authentication

## PCI DSS Requirement

## Interpretation

**8.4.1** MFA is implemented for all non-console access into the CDE for personnel with administrative access.

Phishing-resistant authentication can be used, but must be coupled with some other authentication factor

**8.4.2** MFA is implemented for all non-console access into the CDE.

### **8.4.2** Guidance

This requirement does not apply to:

User accounts that are only authenticated with phishing-resistant authentication factors.

Phishing-resistant authentication can be used without another authentication factor

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Console access refers to a system with a direct physical connection to another system component, where that connection does not rely on a networked connection ...

Console access does not include situations where the system is used to access other system components over a networked connection. For example, access via a laptop or workstation using a physically connected keyboard is not considered “console access” if that system requires a networked connection to access any other system component. (from FAQ 1577)

It is NOT a requirement of PCI DSS that all factors are authenticated prior to indication of success of any one factor

# Recommendations

- 12-character password requirements are coming (April 2025)
- MFA for all non-console access is coming (April 2025)
- Ideally, replace passwords with phishing-resistant authentication where you can (then no need to worry about 12-character passwords or MFA for non-admin access!)
- Secure your enrollment and authentication reset processes
- Consider the security around your authentication – enrollment, reset, auth tokens, OTP delivery
- Most auth uses cryptography, so keep PCI DSS 12.3.3 in mind!

# Where Do I Find Out More?



[fidoalliance.org/passkeys](https://fidoalliance.org/passkeys)

# Hands Up If You Still Don't Know What FIDO, Passkeys, or Phishing Are?



# Thank you!

