UNIVERSITY OF OSLO

Identity Day

Device-Bound vs. Synced Credentials

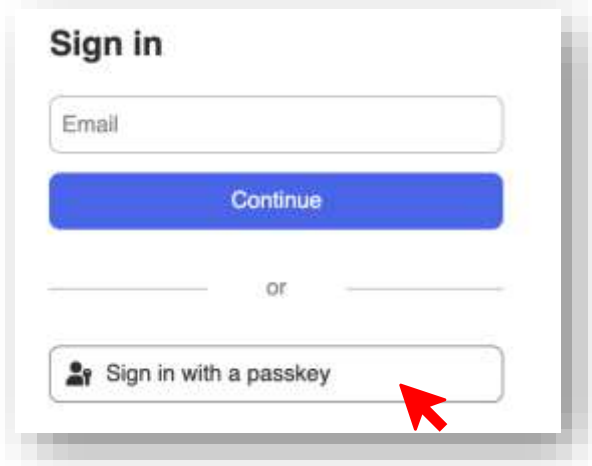
A Comparative Evaluation of Passkey Authentication

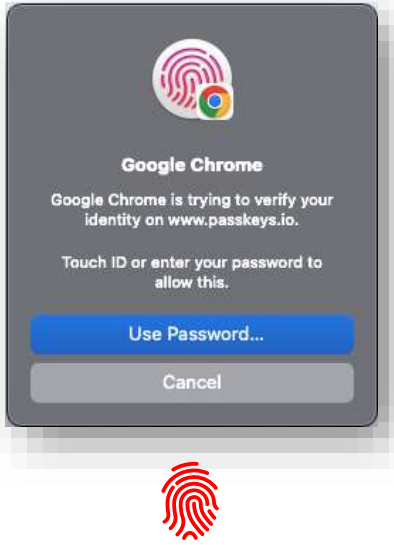
Andre Büttner

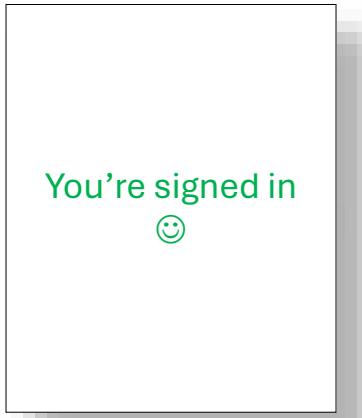
Oslo, 10th April 2025

Digital Security Research Group

Passkeys in action







Intro to Passkeys

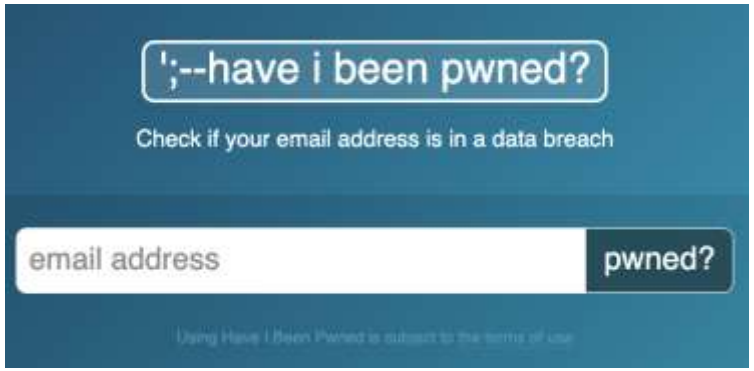
- End-user term for passwordless authentication
- Developed by the FIDO Alliance
- “Phishing-resistant”
- FIDO2 standard
  - WebAuthn (W3C WebAuthn WG)
  - CTAP2 (FIDO Alliance)

Source: https://www.yubico.com/no/product/security-key-series/security-key-nfc-by-yubico-black/

Source: https://fidoalliance.org/passkeys/

Passwords are not secure

- Used insecurely (even with Password Managers)
- Leaked databases
- Vulnerable to phishing

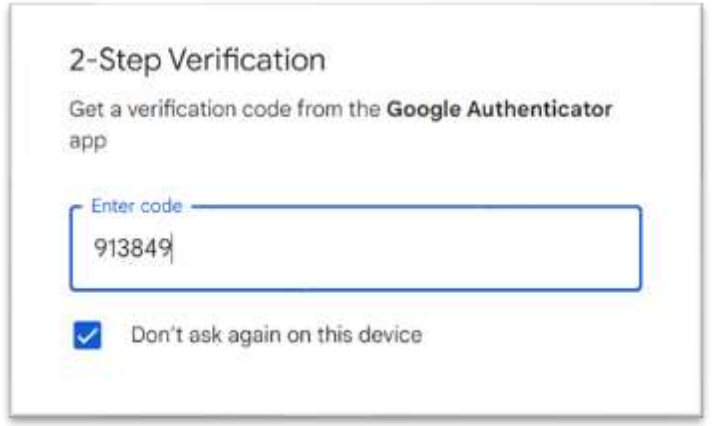


Source: https://haveibeenpwned.com/

Source: https://pixabay.com/vectors/phishing-credentials-data-login-6573326/

MFA also has flaws

- Perceived as inconvenient
- Takes longer
- Often requires additional device
- May be vulnerable to real-time phishing



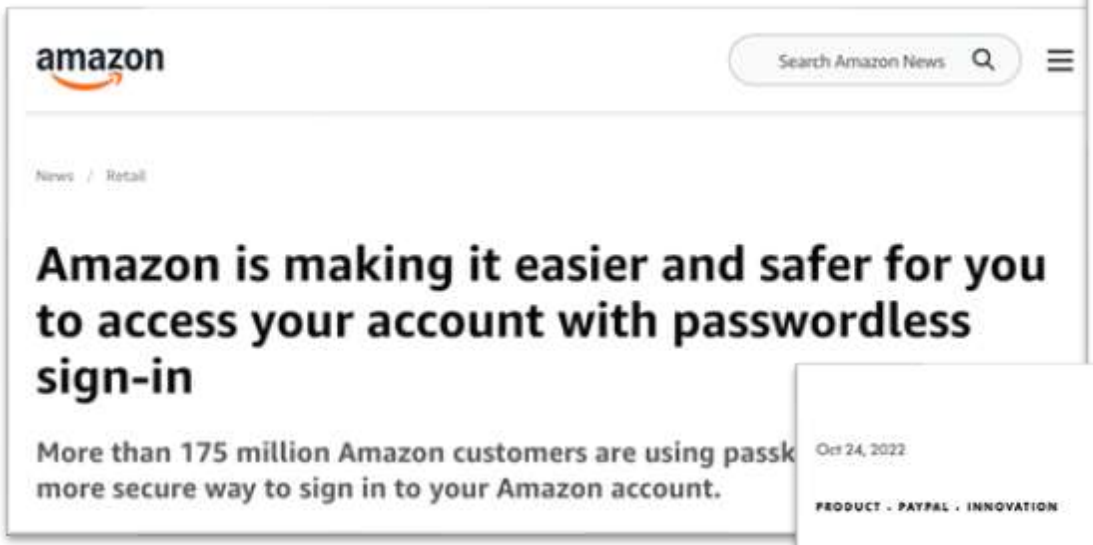
Source: Screenshot of Google 2FA Login

MFA Code Interception at scale: Phishing-as-a-Service

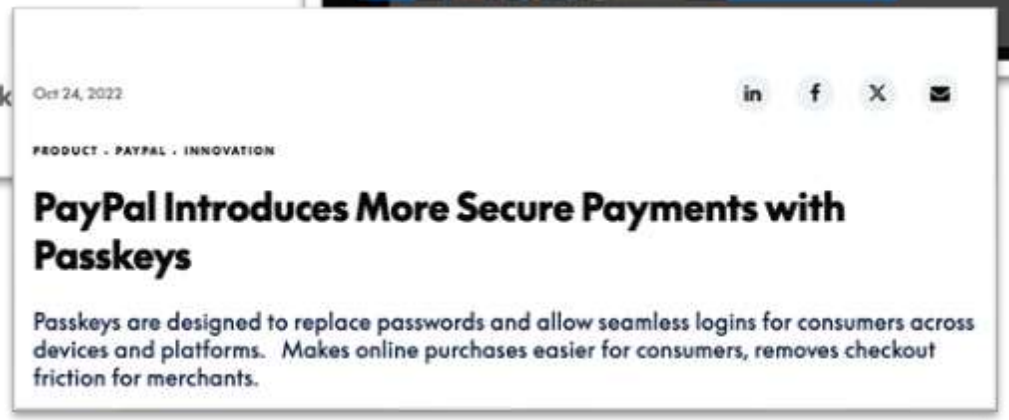
Phishing-as-a-Service (PhaaS) platforms have lowered the barrier for attackers to automate MFA bypass. These platforms enable attackers to set up phishing campaigns that intercept credentials and MFA tokens in real time. Services like Evilginx2 and Modlishka automate the phishing process, allowing attackers to log in as the victim effortlessly.

Source: https://www.keystrike.com/blogs/hacking-humans---an-mfa-challenge

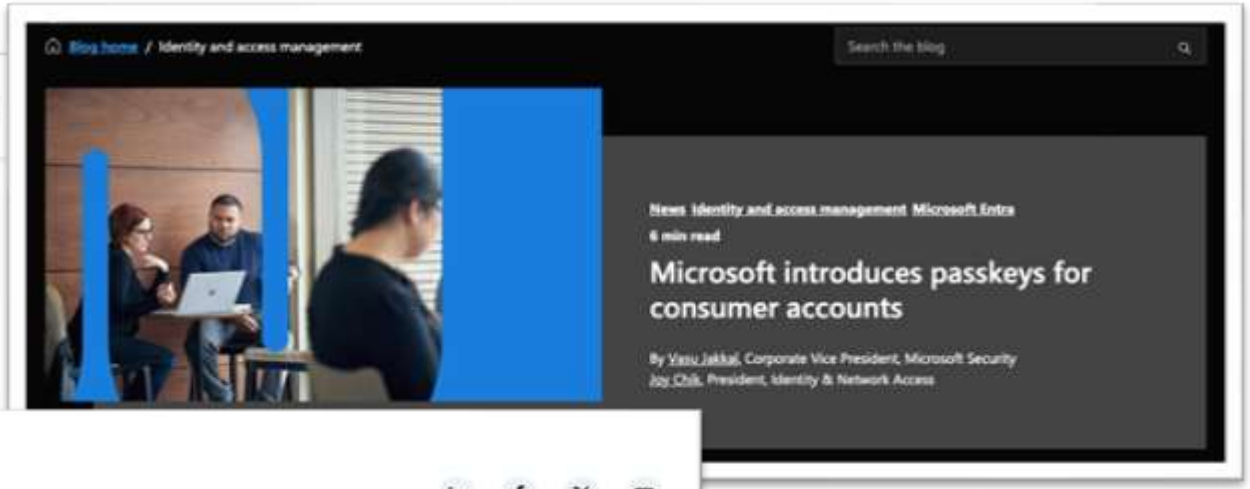
Passkeys are already widely supported



Source: https://www.aboutamazon.com/news/retail/amazon-passwordless-sign-in-passkey



Source: https://newsroom.paypal-corp.com/2022-10-24-PayPal-Introduces-More-Secure-Payments-with-Passkeys



Source: https://www.microsoft.com/en-us/security/blog/2024/05/02/microsoft-introduces-passkeys-for-consumer-accounts/

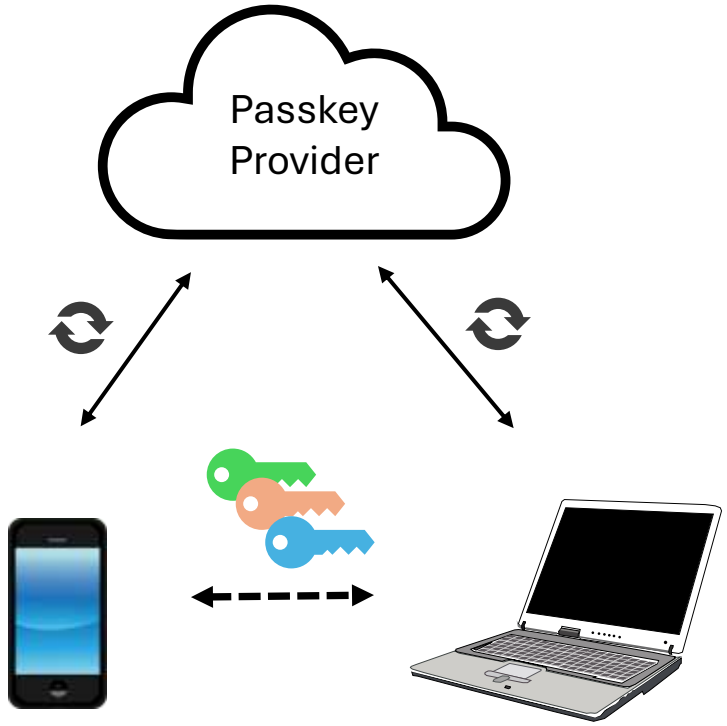
Public authorities recommend it

Source: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/241001_Nutzung_Passkeys.html

Source: https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/nsm-anbefaler-overgang-til-phishingresistent-autentisering

Device-Bound Passkeys

Synced Passkeys



Passkey types

Device-Bound Passkeys

- Credentials never leave the devices
- Authenticator device attestation
- Controlled by the user
- Device loss → credential loss
- NIST AAL3 compliant*

Synced Passkeys

- Credentials synced across devices
- No device attestation
- Involve a Passkey Provider
- Credentials may be backed up
- NIST AAL2 compliant†

* NIST Special Publication 800-63B. **Digital Identity Guidelines - Authentication and Lifecycle Management**. DOI: https://doi.org/10.6028/NIST.SP.800-63b.
† NIST SP 800-63Bsup1. **Incorporating Syncable Authenticators Into NIST SP 800-63B**. DOI: https://doi.org/10.6028/NIST.SP.800-63Bsup1.

Passkey Provider

First-Party Provider

- Device or browser built-in
- Examples: Google Password Manager, Apple Passwords, ...
- Credential access requires unlocking device
- Limited compatibility across different ecosystems

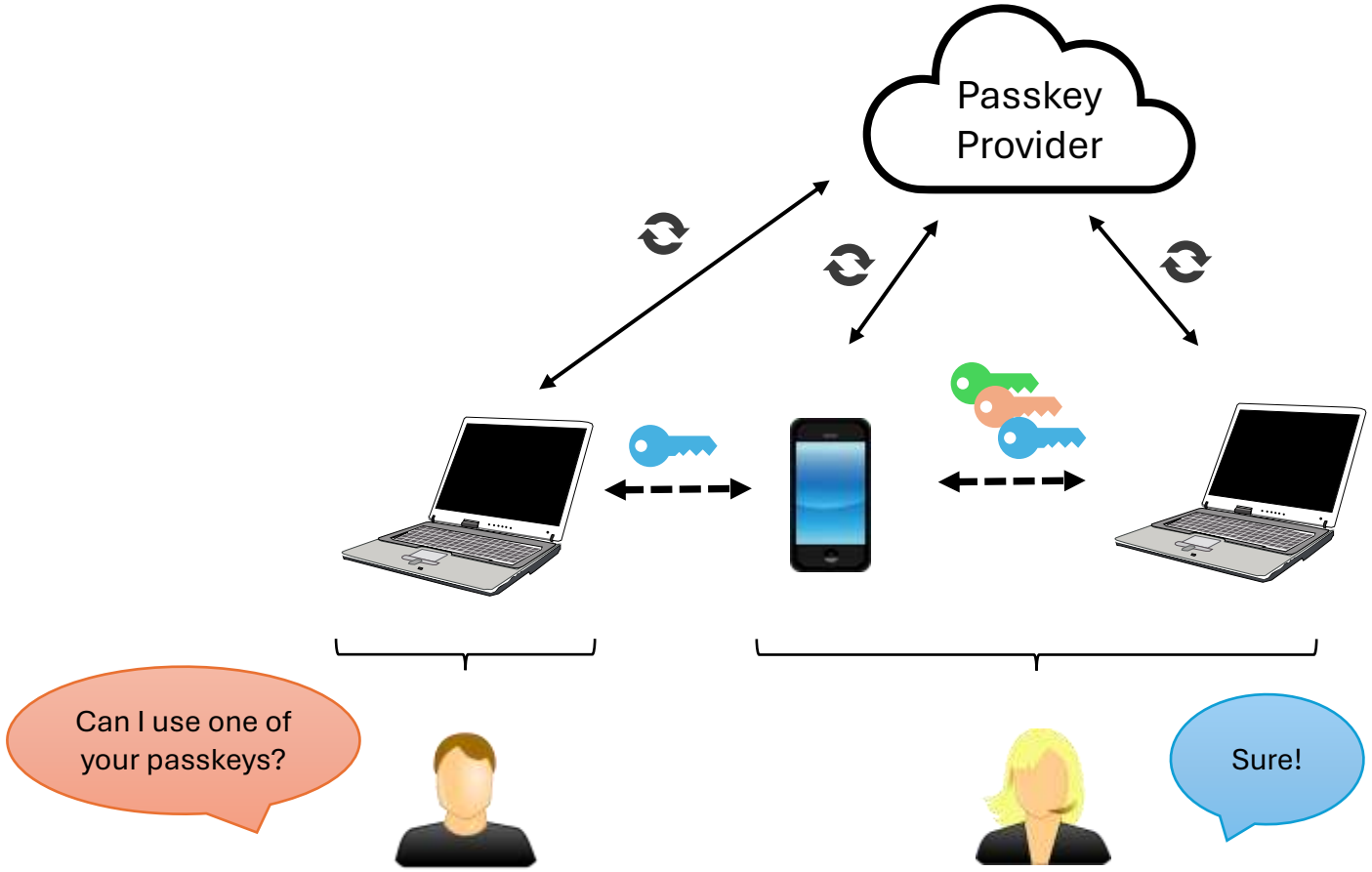
Source: Screenshot of Apple Passwords

Third-Party Provider

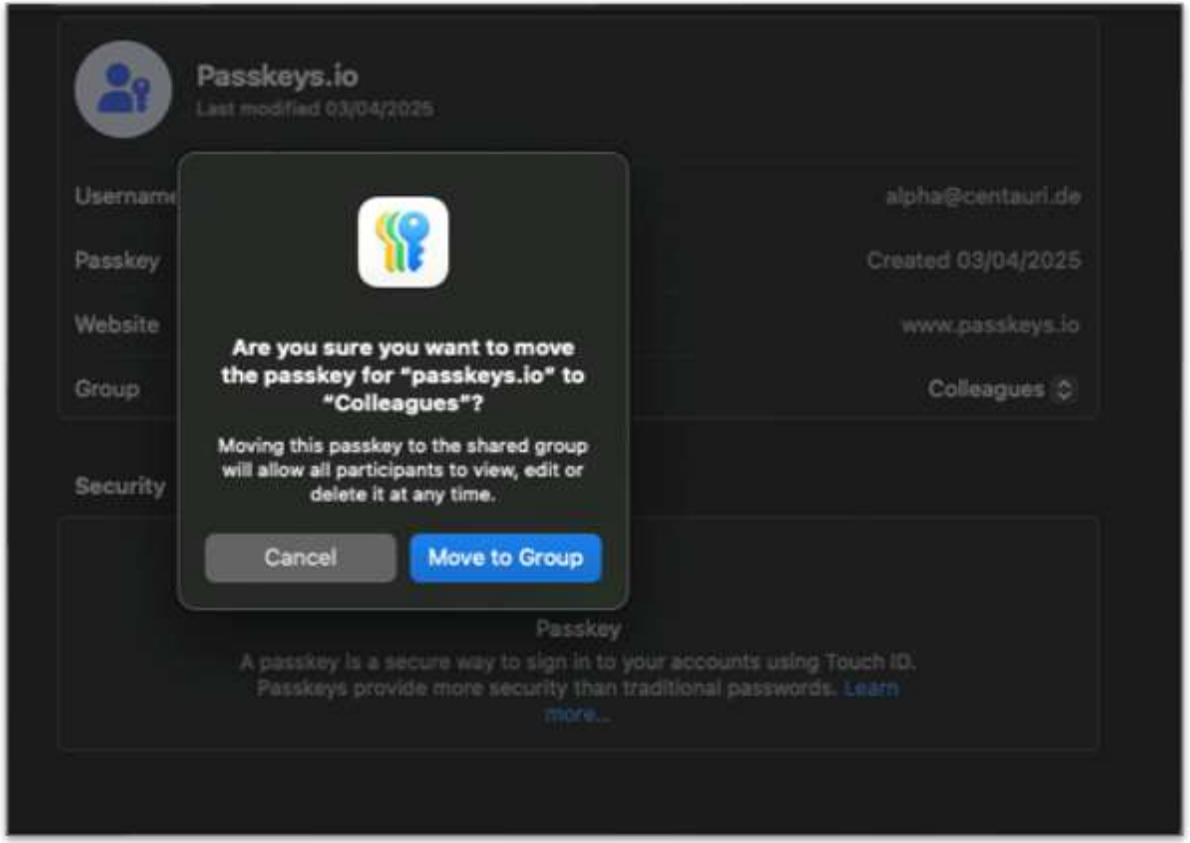
- Installed through additional app or browser extension
- Examples: LastPass, Bitwarden, ProtonPass, ...
- Usually lower access restrictions
- High compatibility across different ecosystems

Source: Screenshot of Bitwarden

Shared Passkeys

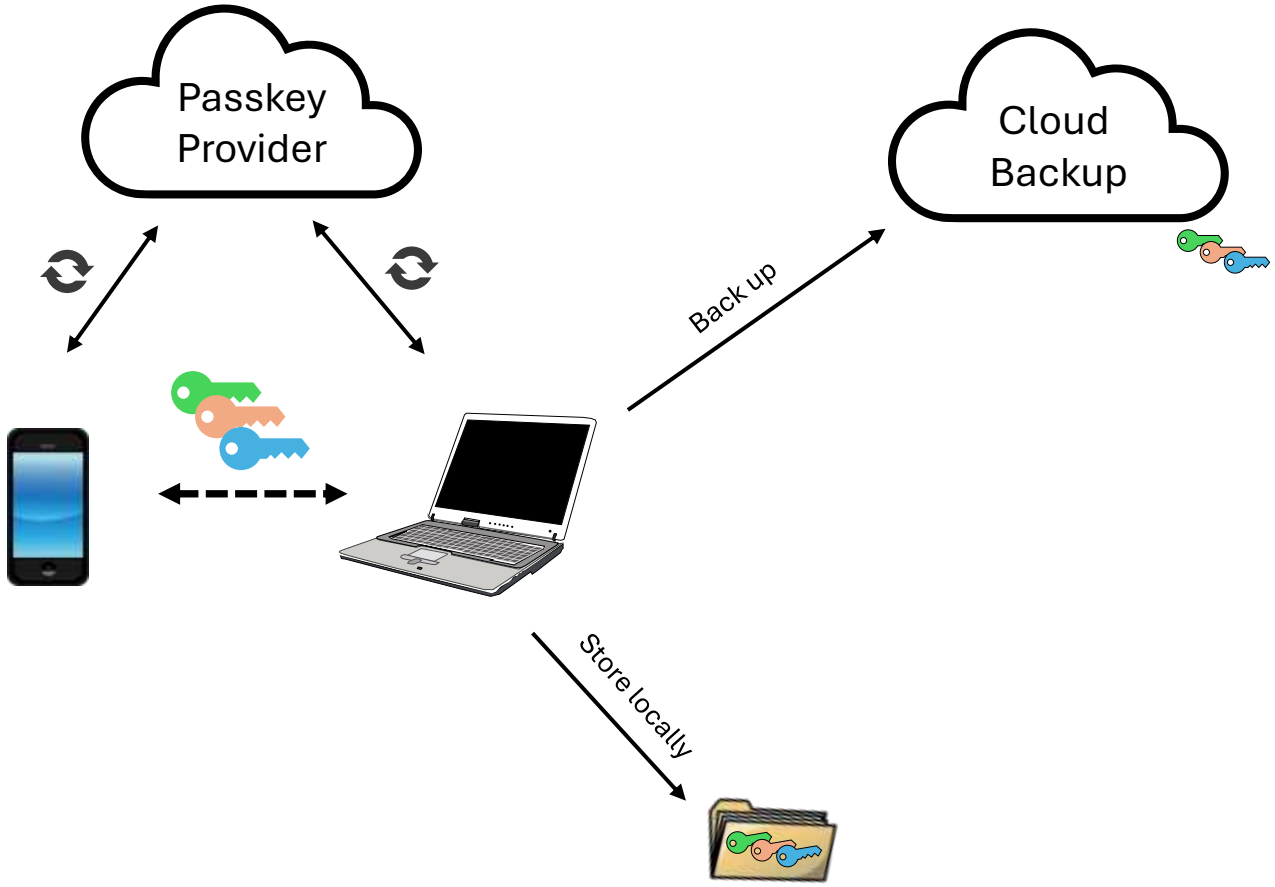


Shared Passkeys



Source: Screenshot of Apple Passwords

Exported Passkeys



Evaluation of Passkeys

- We compared*
    1. Password
    2. Device-Bound Passkeys
        - Platform Authenticator
        - Roaming Authenticator
    3. Synced Passkeys
        - 1st-Party Provider
        - 3rd-Party Provider

- Method
    - Qualitative evaluation framework† to compare authentication methods
    - Comparison of 25 different usability, deployability, and security benefits

*A. Büttner and N. Gruschka. **Device-Bound vs. Synced Credentials: A Comparative Evaluation of Passkey Authentication**. ICISSP 2025. DOI: https://doi.org/10.5220/0013380600003899.

† J. Bonneau, C. Herley, P. C. v. Oorschot and F. Stajano. **The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes**. 2012 IEEE Symposium on Security and Privacy. DOI: https://doi.org/10.1109/SP.2012.44.

Evaluation - Security

		Device-Bound Passkeys		Synced Passkeys	
SECURITY	**Password**	**Platf. Auth.**	**Roam. Auth.**	**1st-Prty Prov.**	**3rd-Prty Prov.**
Resil.-to-Physical-Observation	✗	✓	✓	✓	✓
Resil.-to-Targeted-Impersonation	?	✓	✓	✓	✓
Resil.-to-Throttled-Guessing	✗	✓	✓	✓	✓
Resil.-to-Unthrottled-Guessing	✗	✓	✓	✓	✓
Resil.-to-Internal-Observation	✗	✓	✓	?	?
Resil.-to-Leaks-from-Other-Verifiers	✗	✓	✓	✓	✓
Resil.-to-Phishing	✗	✓	✓	✓	✓
Resil.-to-Theft	✓	✓	✓	✓	✓
No-Trusted-Third-Party	✓	✓	✓	✗	✗
Requiring-Explicit-Consent	✓	✓	✓	✓	✓
Unlinkable	✓	✓	✓	✓	✓

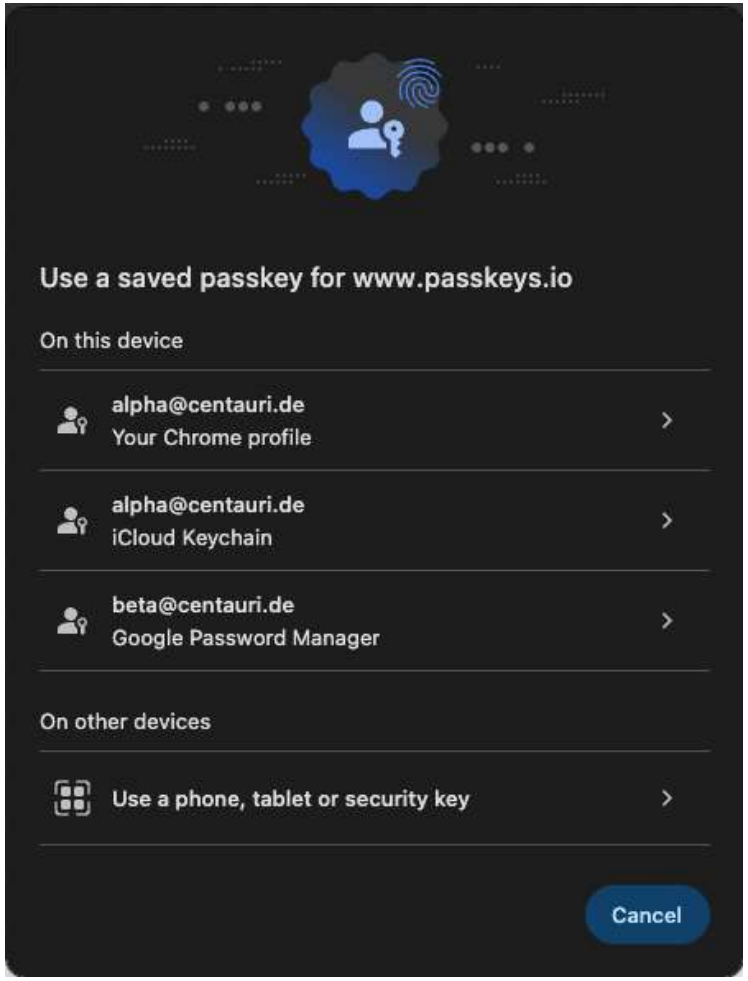
✓ offered ? partially offered ✗ not offered

Evaluation - Usability

		Device-Bound Passkeys		Synced Passkeys	
USABILITY	**Password**	**Platf. Auth.**	**Roam. Auth.**	**1st-Prty Prov.**	**3rd-Prty Prov.**
Memorywise-Effortless	✗	✓	✓	✓	✓
Scalable-for-Users	✗	✓	✓	✓	✓
Nothing-to-Carry	✓	✓	✗	✓	✓
Physically-Effortless	✗	✓	✗	✓	✓
Easy-to-Learn	✓	✓	✓	?	✗
Efficient-to-Use	✓	✓	?	✓	✓
Infrequent-Errors	?	✓	?	✓	✓
Easy-Recovery-from-Loss	✓	✗	✗	?	?

✓ offered ? partially offered ✗ not offered

Where are my Passkeys stored?



Only accessible on one device

Accessible on my Apple devices

Accessible from all my devices with Google account signed in

Where are my Passkeys stored?

Chrome Profile

Apple Passwords

Google PWM

Bitwarden

iPad

iPhone

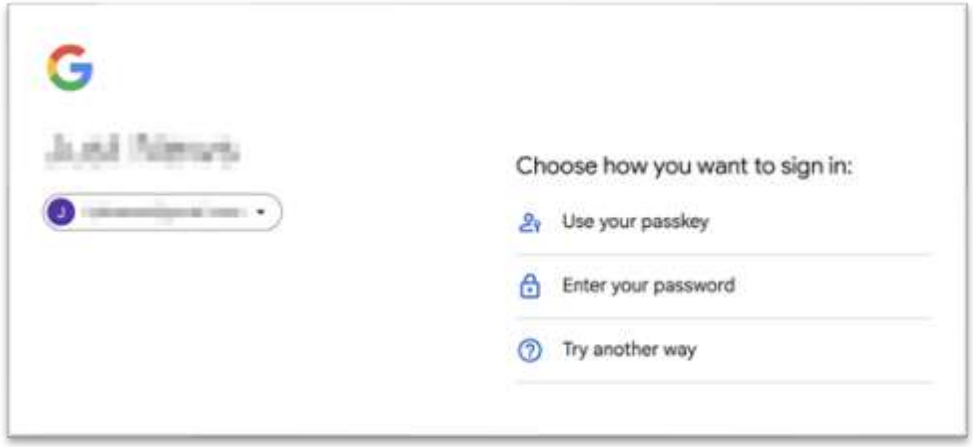
MacBook

Windows

Android Phone

How are Passkeys implemented by online services

- Usually only an **alternative** to password / MFA authentication
- Few online services allow to disable the password entirely
- Many online services strongly encourage their users to set up a passkey
  - Observed on, e.g., Amazon and PayPal
  - See also Microsoft research for increasing Passkey adoption of users*

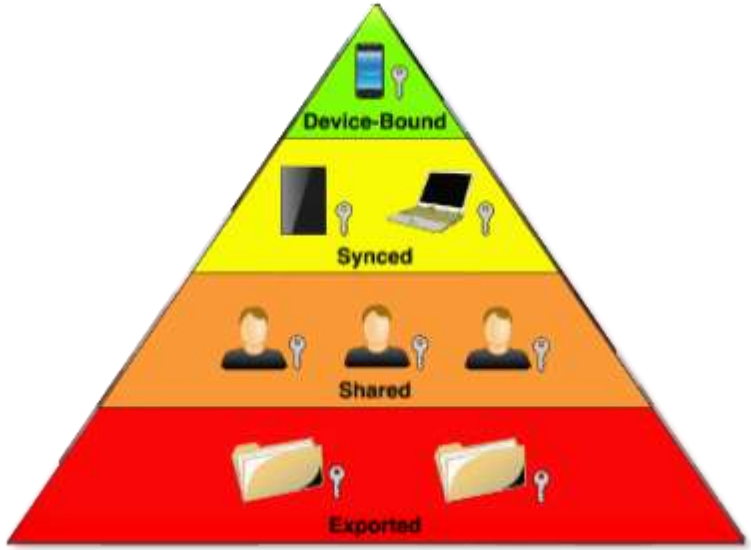


Source: Screenshot of Google Login

Source: Screenshot of Amazon after Login

* https://www.microsoft.com/en-us/security/blog/2024/12/12/convincing-a-billion-users-to-love-passkeys-ux-design-insights-from-microsoft-to-boost-adoption-and-security/

Key takeaways



1) Passkeys != Passkeys

→ Security of Passkeys depends on
- the type of Passkey
- the implementation of Passkey Providers
- their usage and access restrictions

2) Synced Passkeys <u>can</u> mitigate credential loss

→ Increase awareness about storage location

3) Passkeys need improvements regarding <u>usability</u> and <u>synchronization</u>

Recommended reads

- Andre Büttner and Nils Gruschka. **Device-Bound vs. Synced Credentials: A Comparative Evaluation of Passkey Authentication**. ICISSP 2025. DOI: https://doi.org/10.5220/0013380600003899.

- FIDO Alliance. **Passkey Central.** https://www.passkeycentral.org/.

- Microsoft. **Convincing a billion users to love passkeys: UX design insights from Microsoft to boost adoption and security**. https://www.microsoft.com/en-us/security/blog/2024/12/12/convincing-a-billion-users-to-love-passkeys-ux-design-insights-from-microsoft-to-boost-adoption-and-security/.

- W3C WebAuthn WG. **Web Authentication: An API for accessing Public Key Credentials Level 2**. https://www.w3.org/TR/webauthn/.

- FIDO Alliance. **Client to Authenticator Protocol (CTAP)**. https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html.

UNIVERSITY OF OSLO

Identity Day

Thank you!

Contact
Andre Büttner
University of Oslo
Email: andrbut@ifi.uio.no

Also on

Digital Security Research Group