Passwords

How to manage them.

How we may get rid of them completely with Passkeys.

You need a way to identify yourself to computer programs and remote sites.

The traditional method is a username and password.

Cartoon removed

Password Managers

Password managers will remember your password and fill it in for you.

- automatically log you into websites, services, accounts
- provide security reports such as weak passwords, leaked password and information on unsafe websites
- allow you to carry your passwords with you.

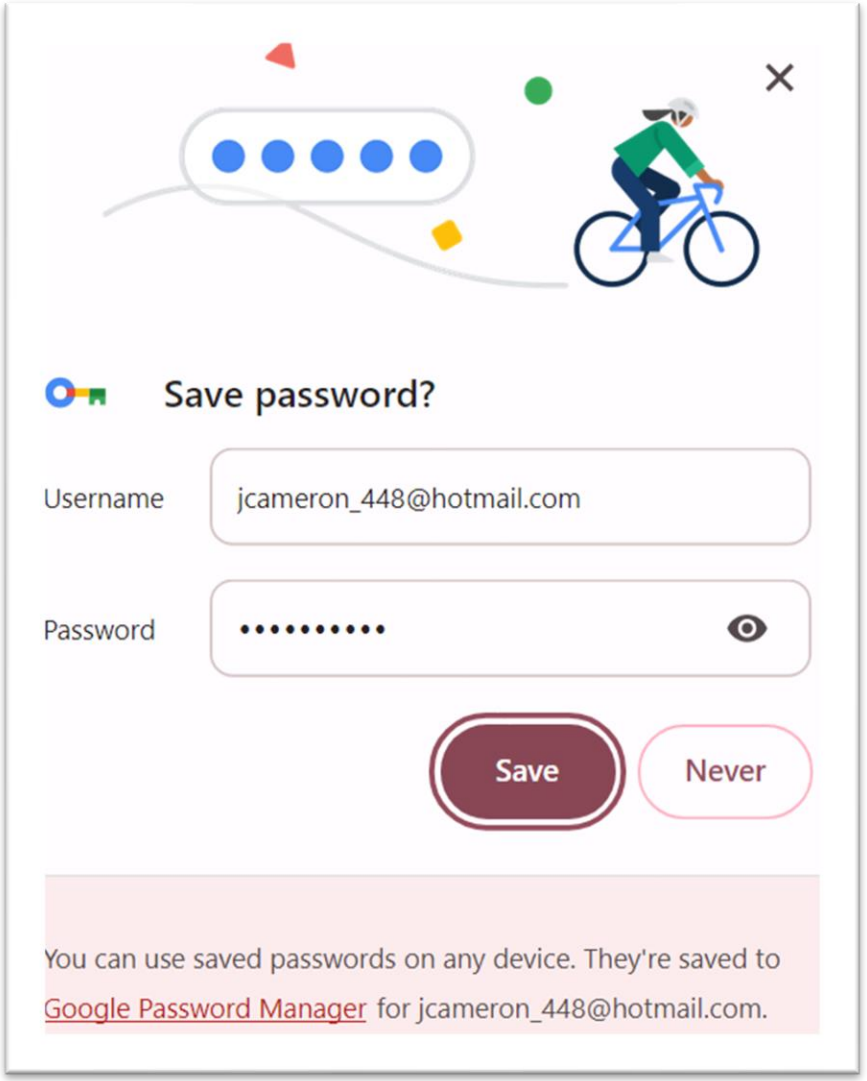
Web Browsers

Web Browsers include easy to use Password Managers (Chrome, Safari, Edge, Firefox, Brave ...).

Web browsers will ask if you want to save the password the first time you enter a new site.

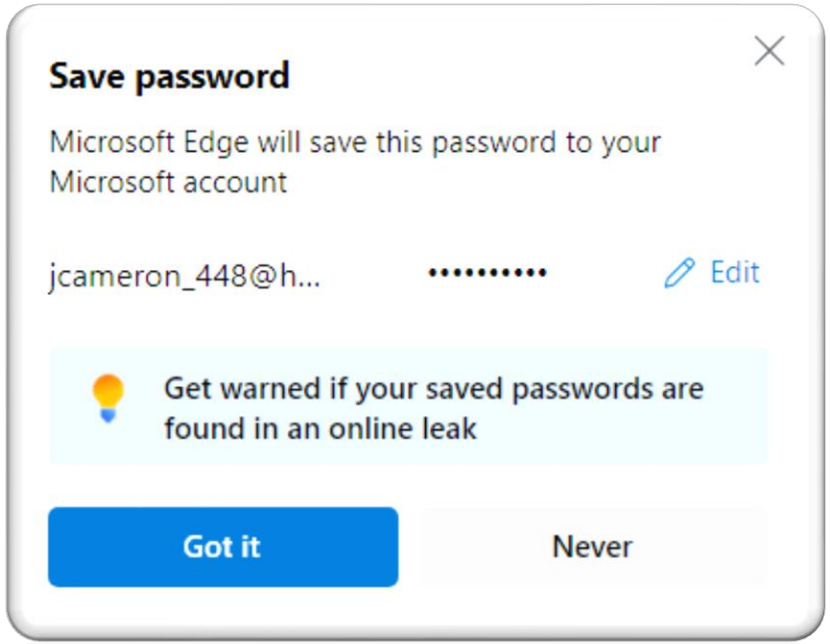
If you say yes, your password is saved by the browser and automatically inserted when you next go to the site.

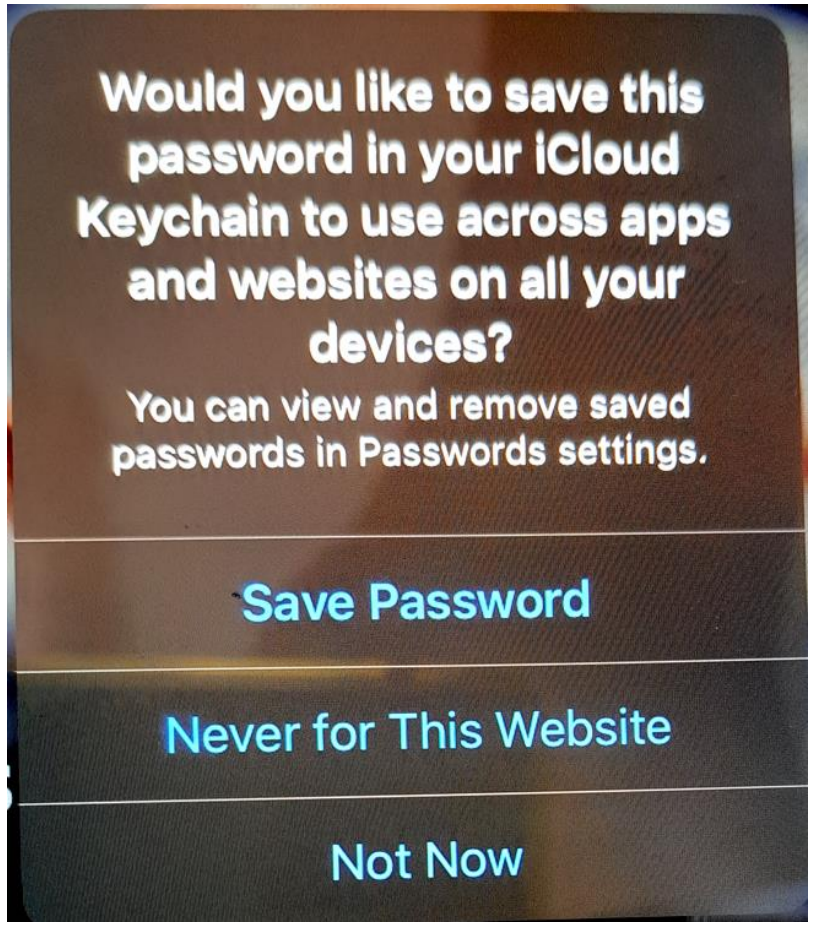
Your passwords will be available across devices. For example a password saved on a PC using Google Chrome will also be available on your mobile phone and even on your iPad/iPhone if you use Chrome.



Chrome

Edge





Safari

Stand alone Password Managers

1Password, LastPass, Keeper and others. These work across all hardware platforms. They require a browser extension to be loaded. Can import passwords from browsers.

Some have a limited free version, for example Lastpass. Full version require payment. Prices range from about $50 to $120 per year.

They usually have more options than the browser based versions. For example, shared passwords with other people, and digital inheritance where the password manager also stores your documents.

Cartoon removed

Passkeys – a new access method

Passkeys are a new way to log in to a remote site. They replace passwords.

Passkeys depend on you having a computer device that you control.

To set up a new Passkey to a remote site a secure connection is made between your device and the remote web site. Both ends store cryptography keys allowing for future secure connections between **your device** and the remote site.

Then whenever you log in, your device checks it really is you. It then sends your authorization over the secure link. ID methods for the device are typically:

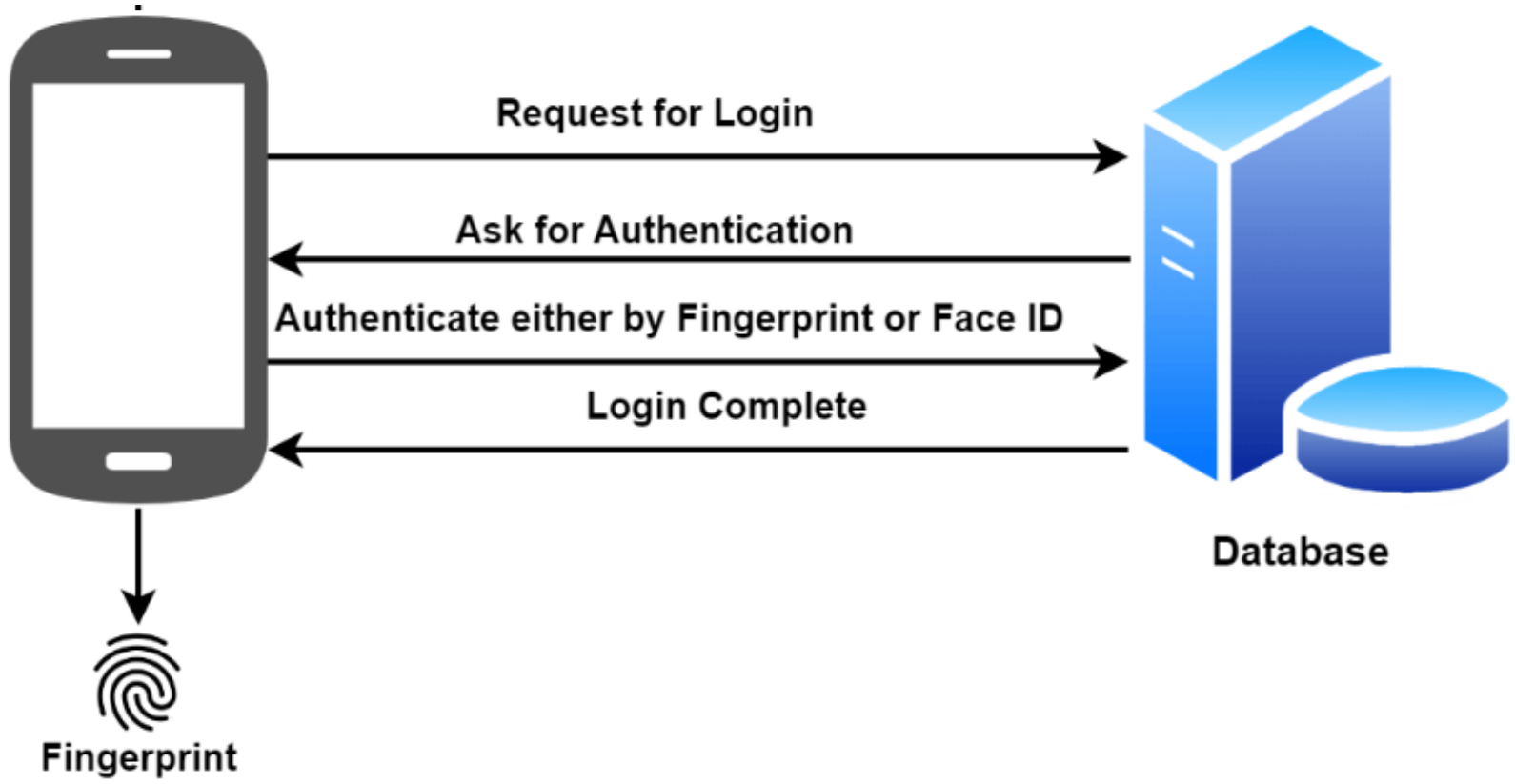
- Face Identification
- Fingerprint
- PIN code – 4 or more letters or numbers

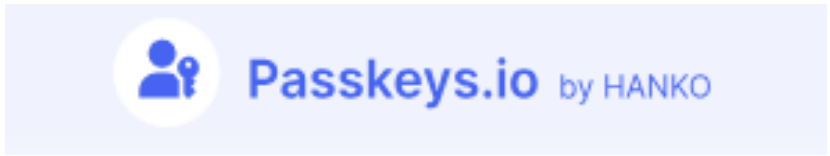
Passkeys

The Passkey securely links your device to the remote site using public key cryptography.

The remote site can then trust that if your device says it is you, it really is you.

There is no phishing, guessing of passwords, or hacking of the remote site.




Passkeys.io by HANKO


WebAuthn.io
A demo of the WebAuthn specification
johnwic
Success! Now try to authenticate...
Register
Authenticate
Advanced Settings

Where are Passkeys stored

By default, when Passkeys are created they are stored as follows:

- On Apple devices on iCloud Keychain.
- On Android devices in Google Password Manager.
- On Windows in Windows Hello.

Third party Password Managers, 1Password, Keeper etc manage their own Passkeys.

There is currently no easy way to move Passkeys between storage types.

What Web sites support Passkeys

Currently limited, About 150 sites. Sites include Apple, Adobe, Amazon, eBay, Google, GitHub, LinkedIn, PayPal, TikTok, Microsoft, Nintendo, WhatsApp, Shop by Shopify and Uber. There appears to be no Australian .au sites.
(https://passkeys.directory/)

Google Account

Passkeys

Start using your passkeys

With passkeys you can now use your fingerprint, face, or screen lock to verify it's really you

Use passkeys

Passkeys enable you to securely sign in to your Google Account using your fingerprint, face, screen lock, or hardware security key. Only set up passkeys on devices you own. Learn more

Automatically created passkeys

Android devices automatically create passkeys for you when you sign in to your Google Account. Manage devices

Galaxy A53 5G
Last used: Not yet used

+ Create a passkey

Q&A Passkeys

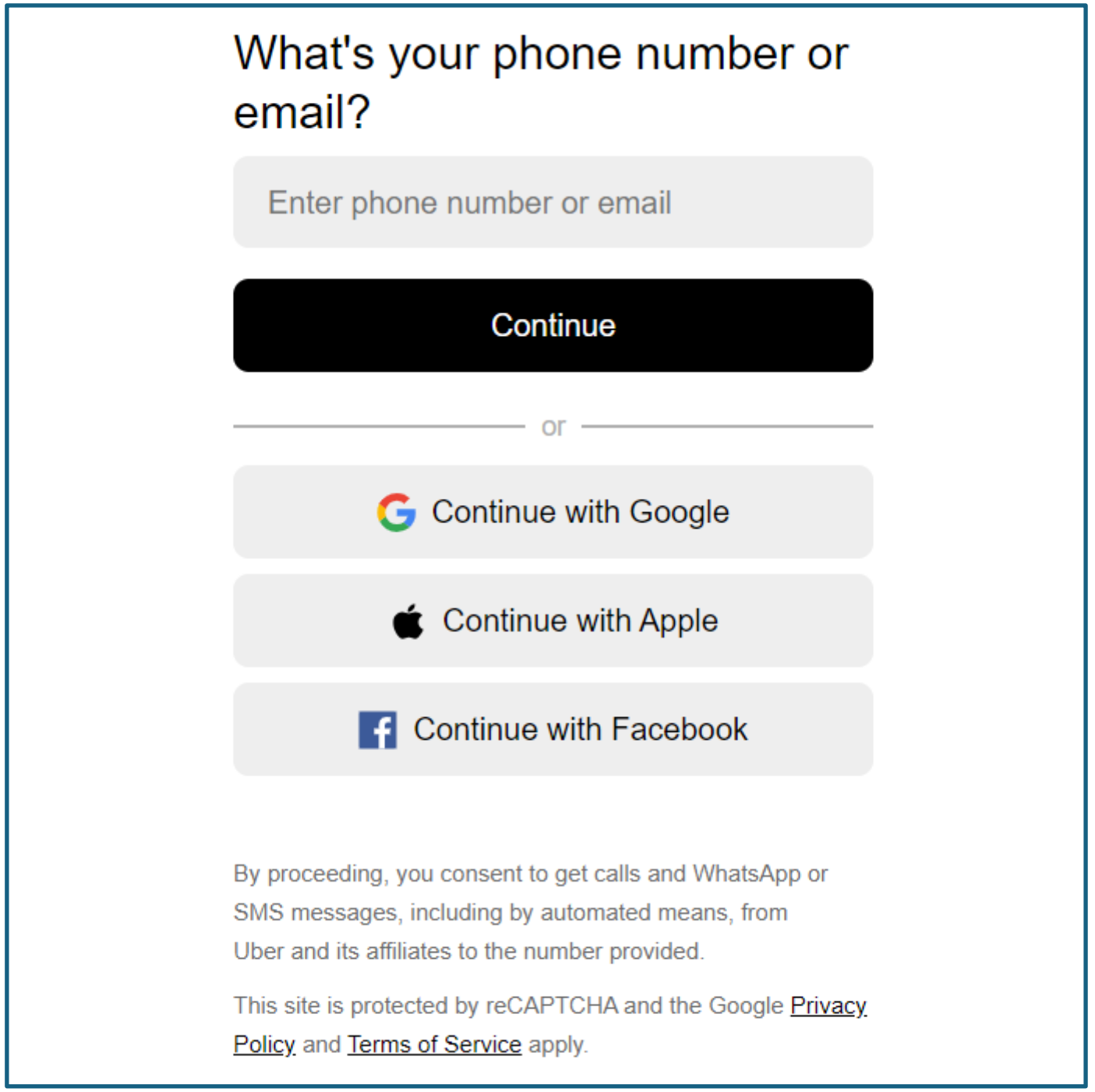
- **Will passkeys completely replace passwords?** – No, you can use both. It will be a very long time (if ever) before all sites accept Passkeys.
- **Is opting-into passkey mandatory?** – No, you can keep using your password.
- **Do I need to set up passkeys on all my devices individually?** – You will need separate passkeys on each device type unless the devices are synchronised. If you need to go across multiple device types use 1Password or Keeper.
- **Can I have multiple Passkeys for the same remote site.** Yes, you can create more than 1 passkey to the same remote site.
- **What is the account recovery process if I lose my device?** In worst case you will need to use email account recovery with a one time password (Magic Link Login).

Questions

OpenID Connect

If you are already be logged into your Google/Apple/Facebook account this account can act as your “Identity Provider”. Security on these core accounts is critical.

The remote site gets sent your email address or phone number and possibly other information.



Good sites Feb 2024

Passwords vs. Passkeys - FIDO Bites Back! (youtube.com) – OK 10m

1Password Passkey Tutorial | How to Use Passkeys in 1Password (youtube.com) 1:15 onwards

Google Passkeys Have Arrived (here's how to use them) (youtube.com)

Goodbye Passwords! Hello Passkeys (youtube.com) (0:30 onwards)

What Are Passkeys? - Are Passwords Going EOL?! (youtube.com)

White Paper: Multi-Device FIDO Credentials - FIDO Alliance

Passkeys explained! My take on Google’s password killer... (youtube.com)