Passkeys vs. Passwords

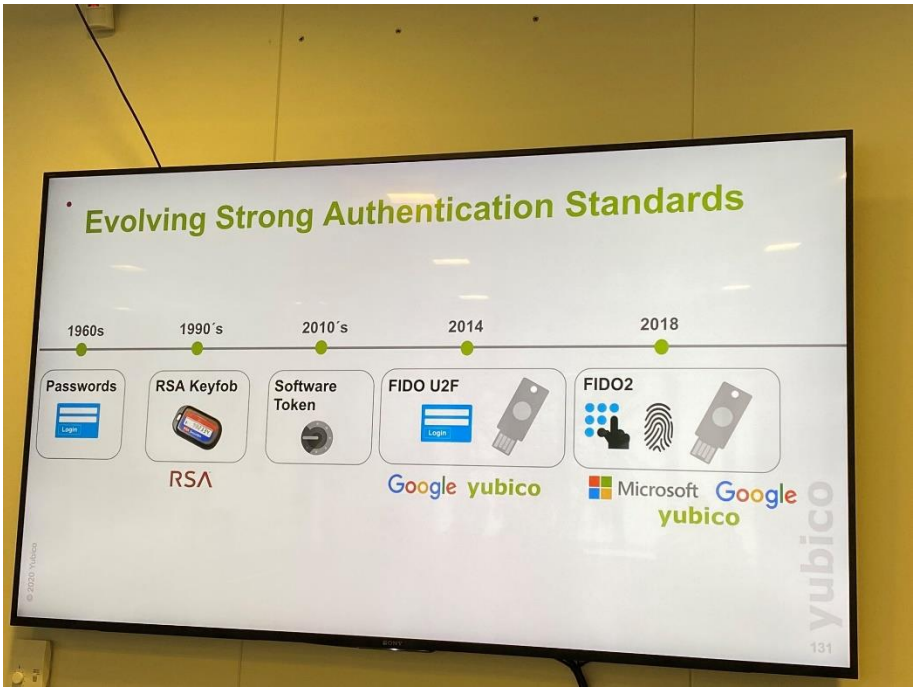
Passwords are no longer considered to be a trustworthy means to protect cloud-based account information. Leaders in the industry like Google, Apple, and Microsoft are trying to reduce our dependence on passwords, and hope to create a future without them.

Authentication refers to the ways that a web site allows users to access their account information. There are 3 types of authentications:

- Password — Something you know
- Security token — Something you have
- Biometric — Fingerprint, facial recognition, voice recognition

2-factor authentication (2FA) uses a combination of identification methods.

The evolution of the authentication methods looks like this:



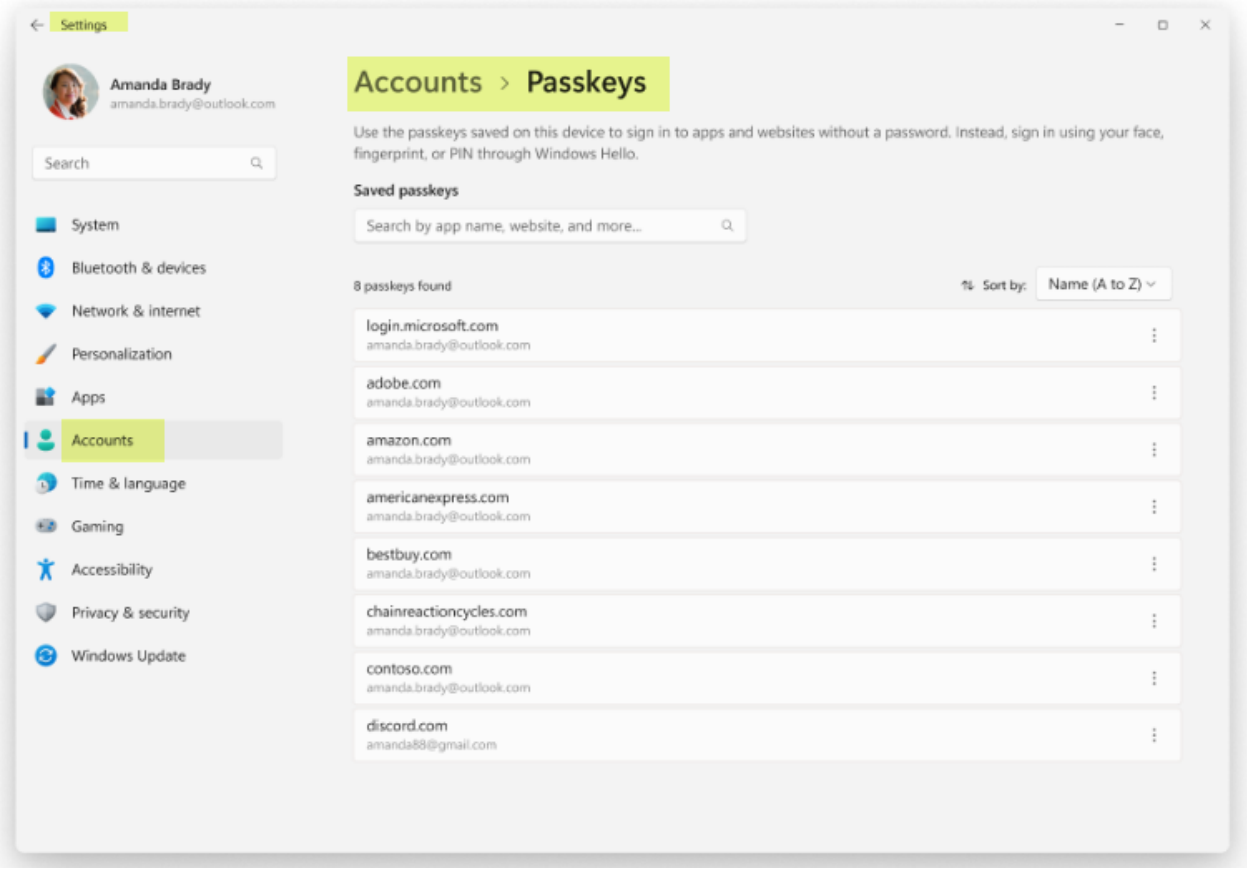
Smartphone leaders encourage us to use biometrics due to its convenience, but, in reality, they are quietly helping us to secure our private information better.

So how do passkeys work? Let's Talk About Passkeys [Dashlane YouTube]

The FIDO Alliance [FIDO] has been working since 2013 to come up with a replacement for passwords.

FIDO supports a full range of authentication technologies, including biometrics such as fingerprint and iris scanners, voice and facial recognition, as well as existing solutions and communications standards, such as Trusted Platform Modules (TPM), USB security tokens, smart cards, and near-field communication (NFC). The USB security token device may be used to authenticate using a simple password (e.g. four-digit PIN) or by pressing a button. The specifications emphasize a device-centric model.

Passkey support in Windows



By default, Windows offers to save the passkey locally if you're using Windows Hello. If you select the option **Use another device**, you can choose to save the passkey in one of the following locations:

- **This Windows device**: the passkey is saved locally on your Windows device, and protected by Windows Hello (biometrics and PIN)
- **iPhone, iPad or Android device**: the passkey is saved on a phone or tablet, protected by the device's biometrics, if offered by the device. This option requires you to scan a QR code with your phone or tablet, which must be in proximity of the Windows device
- **Linked device**: the passkey is saved on a phone or tablet, protected by the device's biometrics, if offered by the device. This option requires the linked device to be in proximity of the Windows device, and it's only supported for Android devices
- **Security key**: the passkey is saved to a FIDO2 security key, protected by the key's unlock mechanism (for example, biometrics or PIN)

If you login to your Windows computer with a Microsoft Account, you will have at least one Passkey in your list.

The newest versions of all password managers now allow you to store passkeys in your password vault, and that gives them the ability to go with you to whatever device you want to use.

Want to know which web sites support passkeys?
Look here: Passkeys.directory [1Password]

Want to implement passkeys on a web site?
Look here: Passkeys Implementation - step by step guide [Passkeys.com]