



Our opening graphic was created using the ChatGPT prompt: Create a humorous image of Passkeys vs Passwords and the byline "Which is right for you?"

I've known about passkeys for a few years but was always a bit nervous about messing things up and losing access to my accounts. If it ain't broke don't fix it. But we figured now is a good time to revisit.

# Intro

- Importance of creating strong and unique passwords - most folks do
- Better to use a password manager that creates more complex strings
- Even the most complex passwords are still vulnerable to phishing
- Tricked into entering your password at a fraudulent “look-alike” website

For years, security experts have emphasized the importance of creating strong and unique passwords. In a recent survey, 85 percent of adults in North America do. But only 34 percent of respondents use a password manager to create those passwords, which typically creates more complex strings than many people would manually.

But even the most complex passwords are vulnerable to phishing, where unsuspecting users are tricked into disclosing their passwords or entering them at a fraudulent look-alike website controlled by the attackers. Even using an authentication app isn't foolproof—you could still be tricked into entering your one-time password on a fake log-in page.



# What is Authentication?

- Determining whether someone or something is who or what they say they are
- Provides access control by checking if user credentials match those in a database
- Ensures that systems, processes and enterprise information are secure

Let's remind ourselves of some basic terms.

Online authentication is the process of determining whether someone or something is who or what they say they are. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or a data authentication server. In doing this, authentication ensures that systems, processes and enterprise information are secure.

# What is Phishing?

- Scam where attackers deceive people into revealing sensitive info or installing malware
- Refers to the use of lures to “fish” for sensitive info
- Attacks have become increasingly sophisticated
- Most common type of Cybercrime

Phishing is a form of social engineering and a scam where attackers deceive people into revealing sensitive information or installing malware such as viruses, worms, adware, or ransomware.

It is a variation of the word “fishing” and refers to the use of lures to “fish” for sensitive information.

Phishing attacks have become increasingly sophisticated and often mirror the site being targeted, allowing the attacker to observe everything while the victim navigates the site. Attacks now include email spam, voice calls, sms texts, QR codes, page hijacking and Man-in-the-Middle techniques. This could be an entire topic in itself for a future MUGOO meeting.



# Authentication Evolution

- Simple passwords - “my dog’s name”
- More complex passwords - S\$&vJ@P1!
- Multi-Factor Authentication - a text code
- Public Key Authentication
- Passkeys, which typically use both Multi-Factor and Public Key techniques

We can look back over our own years of online experience and reflect on how things have evolved.

# Why Passkeys?

- Tech industry has been keen to create a more secure, password-free future
- You don't need to worry about putting your password into a shady website
- Passkeys are “free” and you don't need to carry them around
- Can be used on phones, tablets, computers and across your devices

Because of the risks with passwords, the tech industry has been eager to create a password-free future. Passkeys — jointly developed by Apple, Google, Microsoft, and others — are an alternative to passwords, providing robust protection against phishing attacks and website breaches. The authentication standards are maintained by FIDO Alliance (Fast IDentity Online) and the World Wide Web Consortium.

Passkeys separate and compartmentalize every aspect of the authentication process. Thus, you can't be a victim of a phishing attack since you don't need to worry about putting your password into shady websites, and they make data breaches less damaging as your account credentials are useless to an attacker if they don't have the other piece of the log-in puzzle.

Physical security keys, which can distinguish between legitimate websites and look-alikes, are another technology that many security pros recommend. However, passkeys appeal to more people, because they are free and you don't need to carry them around.

Passkeys can be used on phones, tablets, or computers, and implemented across devices. The technology still isn't as widespread and convenient to use as it could be. However, it's not too early to consider using it for at least some of your accounts as passkeys continue to be integrated and standardized across more services.



# Multi-factor Authentication

- Requires multiple secure elements
- *Something you know*, usually a password or PIN
- *Something you have*, a security key or authenticator embedded in your device
- *Something you are*, a unique biometric
- Most passkey authenticators include at least two of these factors

Multi-factor authentication refers to authentication that requires multiple secure elements to get you into an application.

The three primary authentication factors include: Something you know, Something you have and/or Something you are.

Something you know is usually a password used to prove your identity. Something you know could also come in the form of a 4 or 6 digit PIN used to unlock the device.

Something you have is a unique item in your possession. Within the concept of passkeys, this will refer to the authenticator; whether that be a security key, or an authenticator embedded in a personal device such as your iPhone.

Something you are refers to an element unique to your person, in the space of biometrics. This could include a fingerprint, facial scan, optic id, voice detection, or could even go as far as a DNA test.

Most passkey authenticators will include at least two of the factors mentioned above. A user will present something they have (the authenticator), and something they either know (PIN) or are (biometric), to complete any registration or authentication process.

# Public Key Authentication

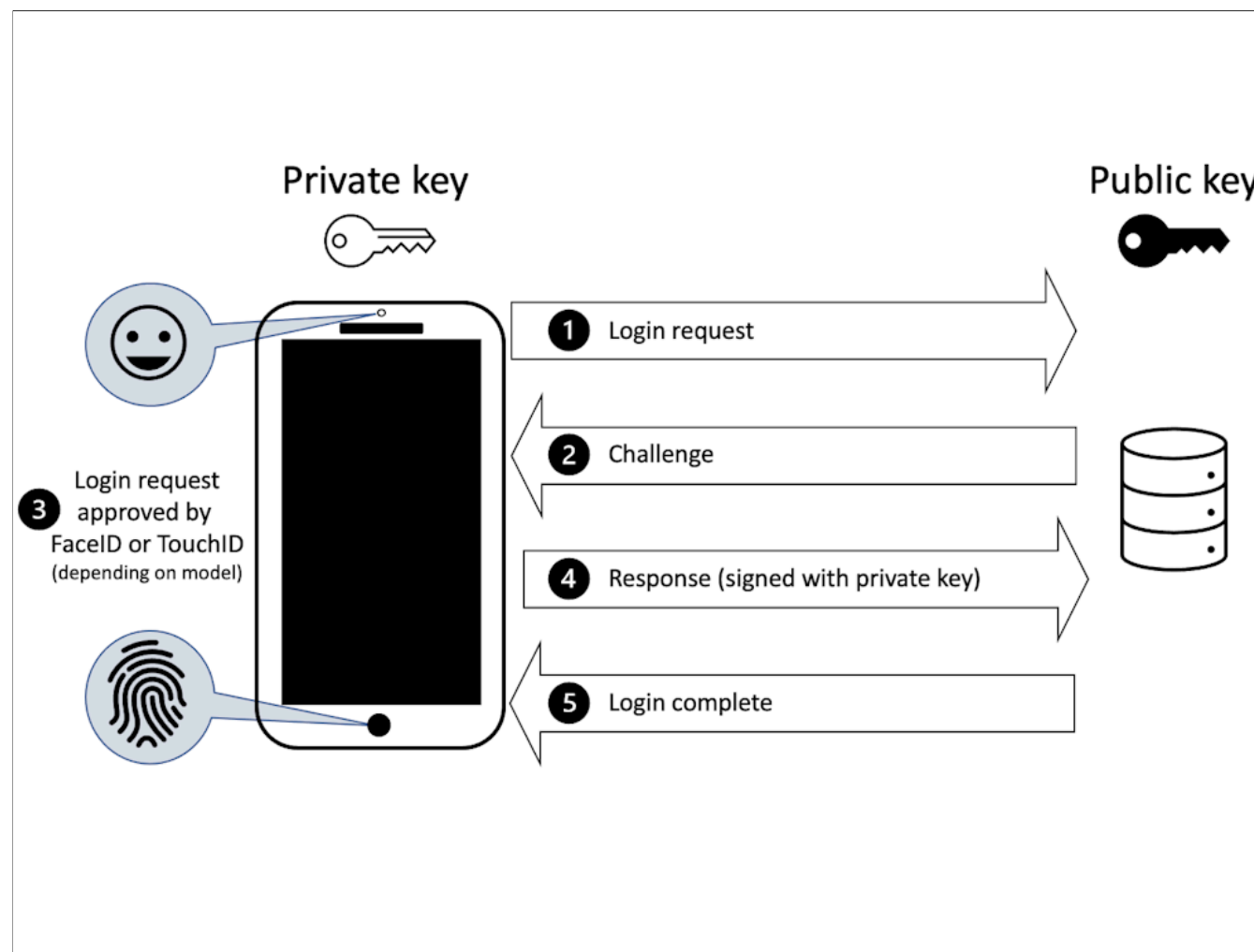
- Passkeys rely on a public key system
- Authenticator provides a public key to an app that has a corresponding private key on the authenticator
- Application can issue challenges, encrypted by the public key to a user
- If user can successfully decrypt the challenge with their private key, they will be authenticated

Passkeys use public-key encryption for security, which means authentication requires two separate keys: one that is stored on your device, and the other on the service where your account is held. Passkeys can also be synced with Apple's iCloud, and your key can be copied from one device, such as your iPhone or Macbook, to another.

Passkeys require some form of authentication before they can be used. That might be the passcode you use to unlock your screen, or a form of biometric authentication such as a face scan or a fingerprint. That biometric data stays local on your own device.

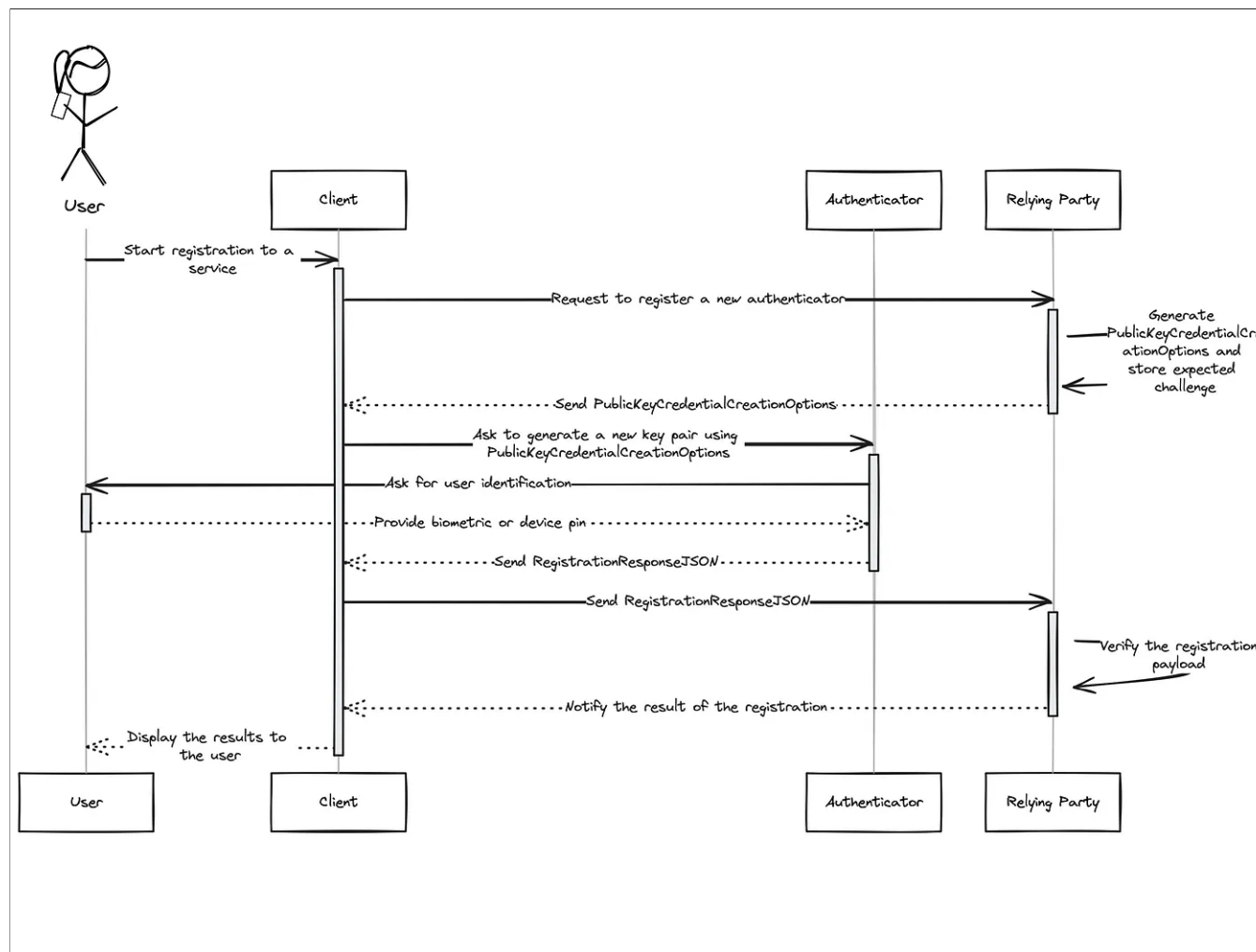
During a registration ceremony, your authenticator will provide a public key to an application that will have a corresponding private key that exists on the authenticator. An application can then issue challenges, encrypted by the public key to a user. If the user is successfully able to use their private key to decrypt the challenge, then they will be authenticated into your application.





PKI, Public Key Infrastructure systems have been around for a long while ... if you remember the old Nortel Entrust. This schematic outlines the login exchange.

Rather than having to remember or find all those passwords, the idea is that you are authenticated by your biometric login on that device.



The actual dialogue exchange is a bit more involved and happens in a fraction of a second.



# Benefits of Passkeys

- Cannot be guessed or shared
- Resist phishing attempts because they are unique to sites they are created for
- Won't work on fraudulent look-alikes
- Cannot be stolen by hacking into a company's server
- Possible to recover or revoke a lost passkey

Passkeys keep your accounts more secure than passwords. They use powerful cryptography, which makes every passkey strong.

Passkeys have other benefits; for example, they cannot be guessed or shared. Also, passkeys resist most phishing attempts because they're unique to the sites they're created for, so they won't work on fraudulent look-alikes. Most importantly, in the age of near-constant data breaches, your passkeys cannot be stolen by hacking into a company's server or database, making any stolen data far less valuable to criminals.

What happens if you lose your phone — do you also lose access to your online accounts? This should not be a problem, as long as you've connected your passkey across multiple devices. And you can later revoke a passkey from your iCloud keychain.

# Getting Started

- You are typically prompted to create a passkey at the time of login
- Apple has made the setup of passkeys quite easy
- Android devices automatically create a passkey when you log in to Google
- Dozens of services support passkeys
- I chose to start with [Amazon.ca](https://www.amazon.ca)

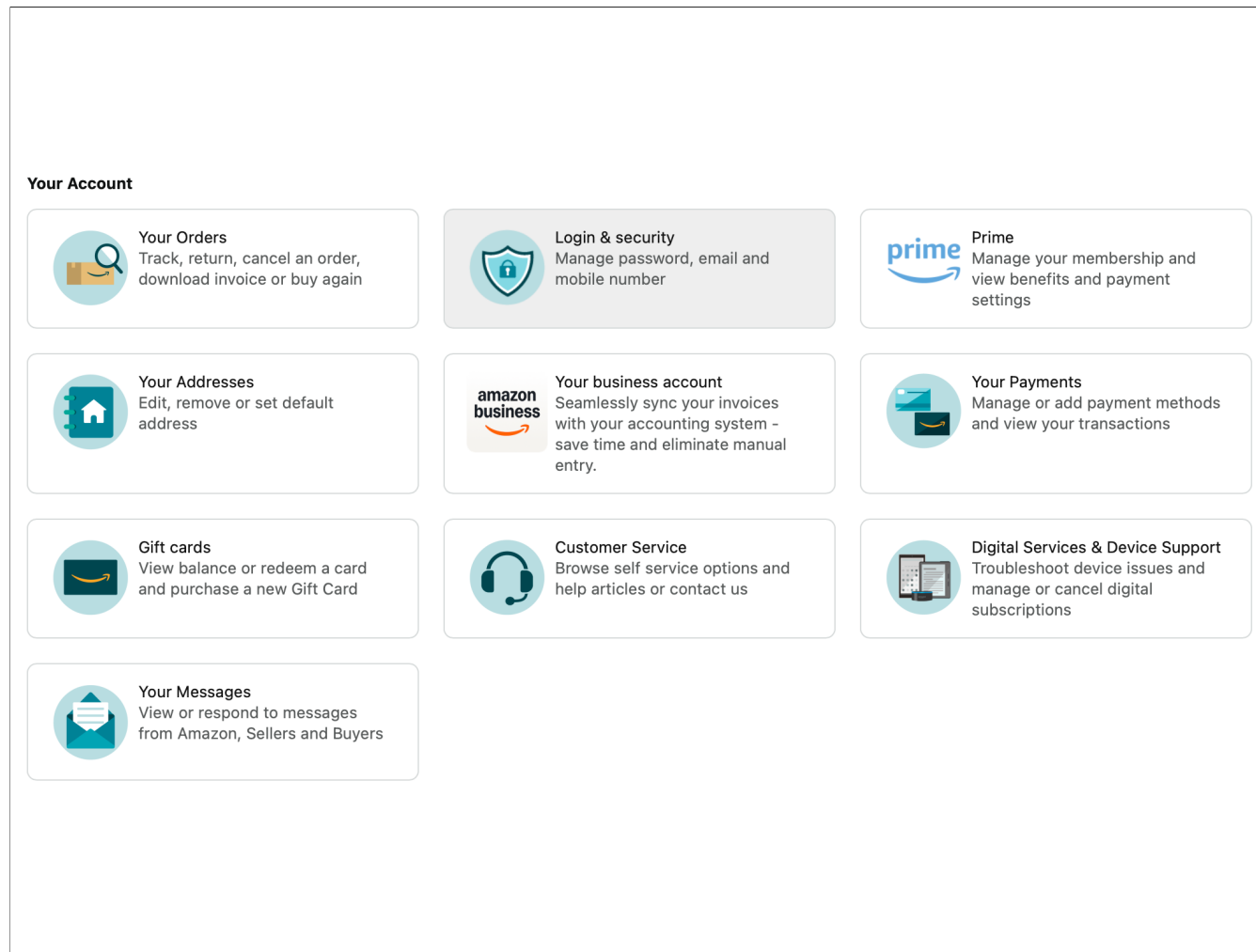
Websites and services will typically prompt you to create and use a passkey at the same step that you'd normally log in with a traditional password.

Apple requires you to use a traditional password to log in to your Apple ID, but creating a passkey on an Apple device will let you sign in with that passkey on any Apple device, as long as your device runs iOS 16 or macOS Ventura or newer, and you are using iCloud Keychain.

Android devices may automatically create passkeys when you log in to your Google account. You can start using passkeys for personal Google accounts by going to the setup page and selecting "start using passkeys." You need Windows 10 or up to use passkeys on a PC, and Windows 11, version 22H2 or newer to access features such as synchronization. Some browsers might not support passkeys, so you may need to switch to a supported browser to set up a passkey for your Google account.

You can already use passkeys with dozens of companies such as Amazon, Best Buy, Hyatt, and PayPal.






My [amazon.ca](https://amazon.ca) account was a good place for me to start. It's a service that I use fairly often, but there would be no extreme hardship if it stopped working.

Here is a sequence of screens on [amazon.ca](https://amazon.ca) that allowed me set up the passkey.

I have logged in using my email address user name and Safari generated password. I then click on "Your Account" followed by a click on "Login & security."

[Your account](#) > [Login & Security](#)

## Login & Security

<b>Name</b> David J Rhynas	Edit
<b>Email</b> djrhy[REDACTED].com	Edit
<b>Primary mobile number</b> +1613 [REDACTED] Quickly sign in, easily recover passwords and receive security notifications with this mobile number.	Edit
<b>Passkey</b>  Sign in the same way you unlock your device by using face, fingerprint or PIN.	Set up
<b>Password</b> *****	Edit
<b>2-step verification</b> +1613 [REDACTED] Enter a code sent to your verification method, in addition to your password, to sign in securely.	Manage
<b>Compromised account?</b> Take steps such as changing your password and signing out everywhere.	Start

In this example, I’m adding a passkey to an account that had been previously set up with a password and “2–step verification” which I find to be quite convenient now that Apple delivers the text or email code right to the login screen.

At this point, I click on “Set up” on the Passkey line.

It also possible to set up a brand new account with a passkey only, but at this time I’m more comfortable having the password backup.



# Passkey

Passkeys are an easier and safer way to sign in than passwords. It works with the same face, fingerprint or PIN you already use to unlock your device. We don't store your face, fingerprint or PIN data.

Set up

## More about passkeys

Use passkey on different devices, including a computer



Sharing passkeys with friends and family



Use passkeys with 2-step verification.



Privacy considerations



The next screen I see has a yellow “Set up” button.

✓ Set-up is complete. Next time you can sign in with your passkey instead of a password.

## Passkey

Sharing this account with someone who wants to sign in with a passkey? They'll need to set up their own.

**1 passkey on amazon.ca**



iCloud Keychain

Set up: Apr. 17, 2025



Add a passkey



If you want to add a passkey, use a different cloud service account (for example, an Apple ID or Google account).

### More about passkeys

Use passkey on different devices, including a computer



Sharing passkeys with friends and family



Use passkeys with 2-step verification.

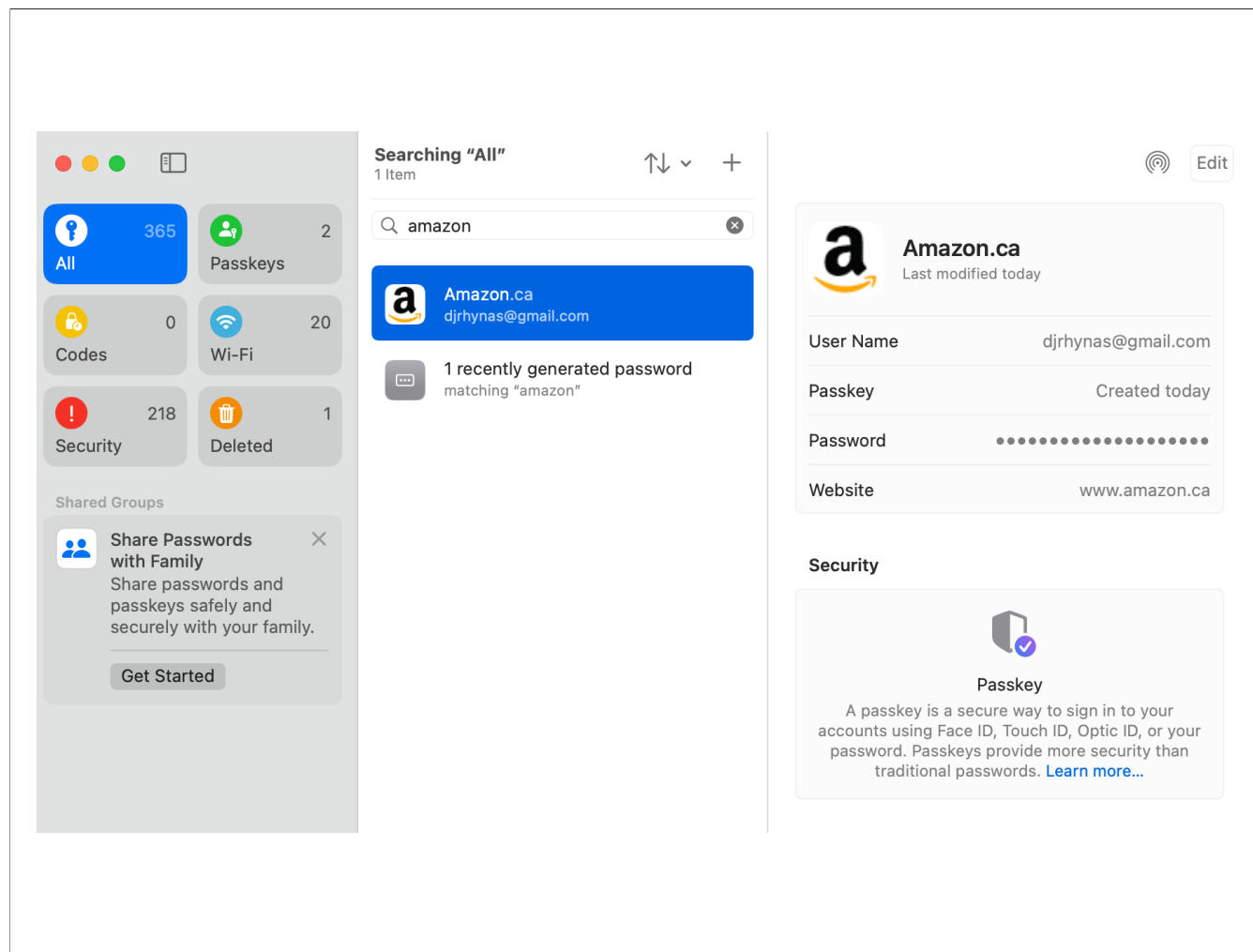


Privacy considerations



I click on that and this is the confirmation that comes back. The Set-up is complete.

There is also the ability to set up another passkey if you have more than one cloud service, i.e. Google in addition to Apple.

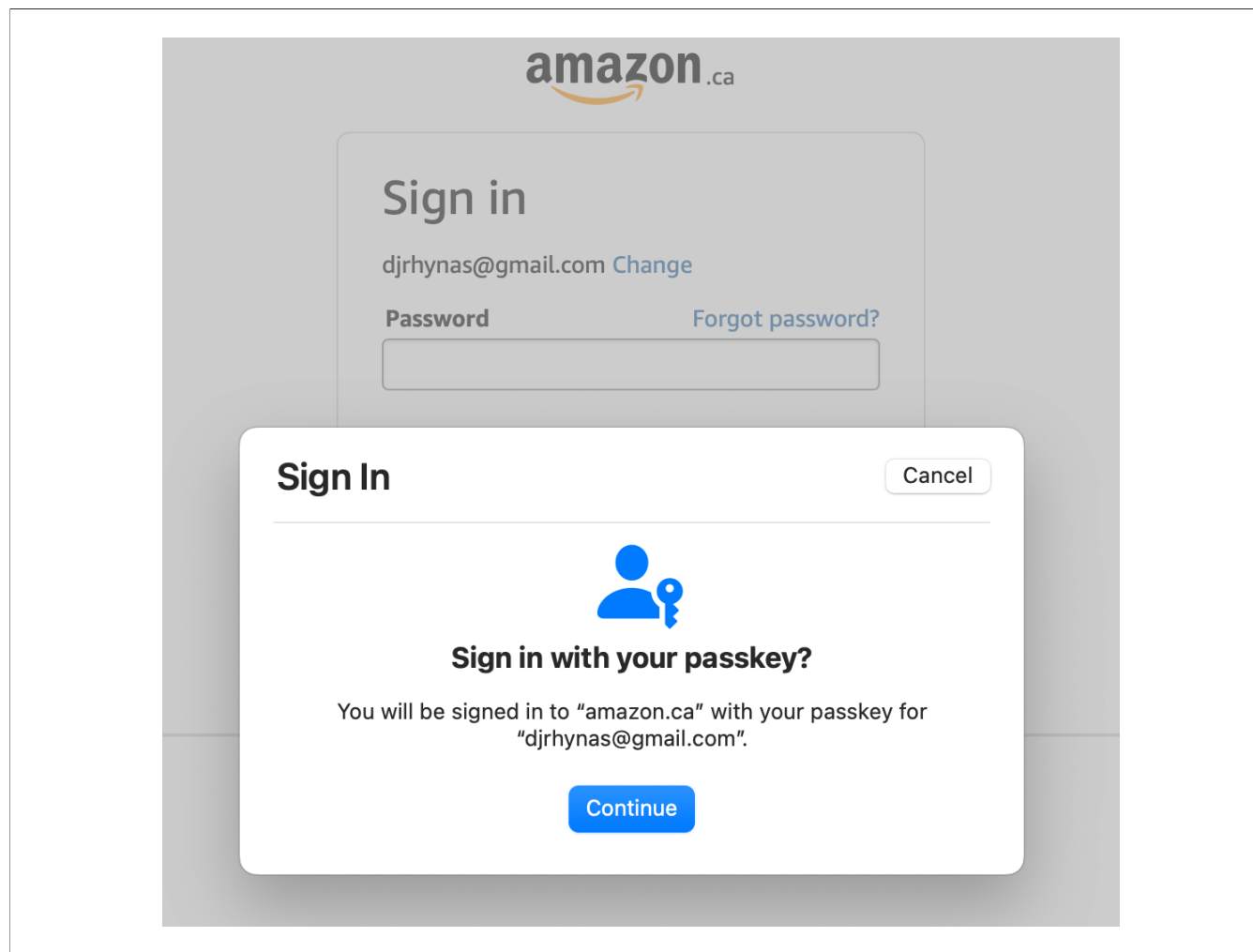


If I then go to my Apple Passwords entry which is linked to my iCloud Keychain, this is what appears.

Note that I still have my older password plus the new passkey. This would allow me to still use a device that is not passkey compatible. When I hover my curser over the password, I can see the character string. There is nothing visible for passkey other than when it was created.

Also on the left, you can see that it is possible to share passwords and passkeys with other family members.





With passkey, you continue to sign in to your device exactly as you already do today ... either either with facial or fingerprint recognition or a numeric PIN (Personal Identification Number).

When I next go to [amazon.ca](https://amazon.ca) it now gives me the option to sign in with my passkey so I no longer need to enter the password character string.



## Two-Step Verification

For added security, please enter the One Time Password (OTP) that has been sent to a phone number ending in 221

Enter OTP:



Fill code 566991 in this browser  
From Messages

Sign in

- [Didn't receive the OTP?](#)

It still proceeds with two factor authentication and otherwise seems pretty much the same as what I have been doing all along. By clicking on the Fill code I am now back into my account.

# With Apple

- First log in to your Apple ID with your traditional password
- Create your Apple Passkey and you are then able to login with *any* of your Apple devices
- Devices must be at iOS/iPadOS 16 or macOS Ventura or later and you must enable iCloud Keychain

If we consider Apple to be another wide-reaching service, we may choose to use passkey authentication here as well.

As mentioned earlier, Apple requires you to use a traditional password to log in to your Apple ID, but creating a passkey on an Apple device will let you sign in with that passkey on any Apple device, as long as your device runs iOS 16 or macOS Ventura or later, and you are using iCloud Keychain.

This allows you to sign in to apps and websites on iPhone, iPad, Mac, Apple TV, Vision Pro, and web browsers on other platforms. It's quite broad and flexible.



# Passkey Limitations

- Only available on select websites, apps so keeping track can be a challenge
- May be tricky to set up, not seamless
- You can share passkeys across Apple devices using *iCloud Keychain*
- But it's not always easy across iOS, Android and Windows devices
- User experience could be improved

Keeping track of where you can use passkeys may be challenging. For example, if you use a passkey to log in to an app on your phone, you could still need a password on your laptop if you want to use a browser that doesn't yet work with passkeys.

There is not yet a seamless and easy way to share passkeys across Apple and Android devices or natively across Windows devices.

The technology has other quirks, too. You can use passkeys with Apple's Safari browser, but if you are on a MacBook, you may have to use the Chrome browser to set up a Google passkey.

For these reasons, until we see further maturation, it perhaps only makes sense to go all-in on passkeys if your primary devices are part of the same ecosystem — like most of us who are firmly in the Apple camp with an iPhone, Mac and iPad.

# What's Next For You?

- Too soon to switch from passwords for *all* your accounts
- Continue using a Password Manager
- Continue using 2-factor authentication
- Start experimenting with Passkeys for specific accounts
- Make sure you have a backup when using a Security Key

Passkeys are still in their early stages. Given that they're not yet available for all services, operating systems, and devices, it's too soon to switch away from using passwords for all your online security. But you can start experimenting with passkeys for specific accounts.

Either way, you'll still want to use a password manager to keep your passwords safe. Since passkeys aren't intended to completely replace passwords, this will ensure you can always fall back to traditional methods if you decide using them isn't for you. And at least two factor authentication is always recommended.

Apple's Passwords allow you to store passkeys, and other password managers are working on this feature. As passkeys continue to propagate, more service providers, password managers, and operating system vendors are creating better ways to easily port them from one platform to another.

You can also store passkeys on a "Security Key". This is a physical device that you can use as a second form of authentication when logging in to an account. Such passkeys can't be copied which can make them more secure, but it's important to register these passkeys on multiple Security Keys kept in different locations. If the passkey only exists on that Security Key and isn't backed up to the cloud, you could permanently lose access to your account if you don't have it stored elsewhere.