Willow Valley Computer Club

Member of apcug

An International Association of Technology & Computer User Groups

Scammers

and

Other Invasive Species

Recognize Them

Deal With Them

Al Williams

Part 2 – June 1, 2023

Part 2
Dealing With Scammers – Protecting Our Online Accounts

Static Websites
and
Dynamic Websites

Static Websites – Years Ago

All visitors saw the same information – read only

Static websites were not interactive

Typical static website: resume, portfolio, brochure, etc.

Source: https://blog.hubspot.com/website/static-vs-dynamic-website

Static Websites - Today

All visitors still see the same information – read only

Static websites can be interactive –

- links
- buttons
- animations

Typical static website: resume, portfolio, brochure, etc.

Source: https://blog.hubspot.com/website/static-vs-dynamic-website

The Apple.com website as of July 1997

The site is static and interactive.

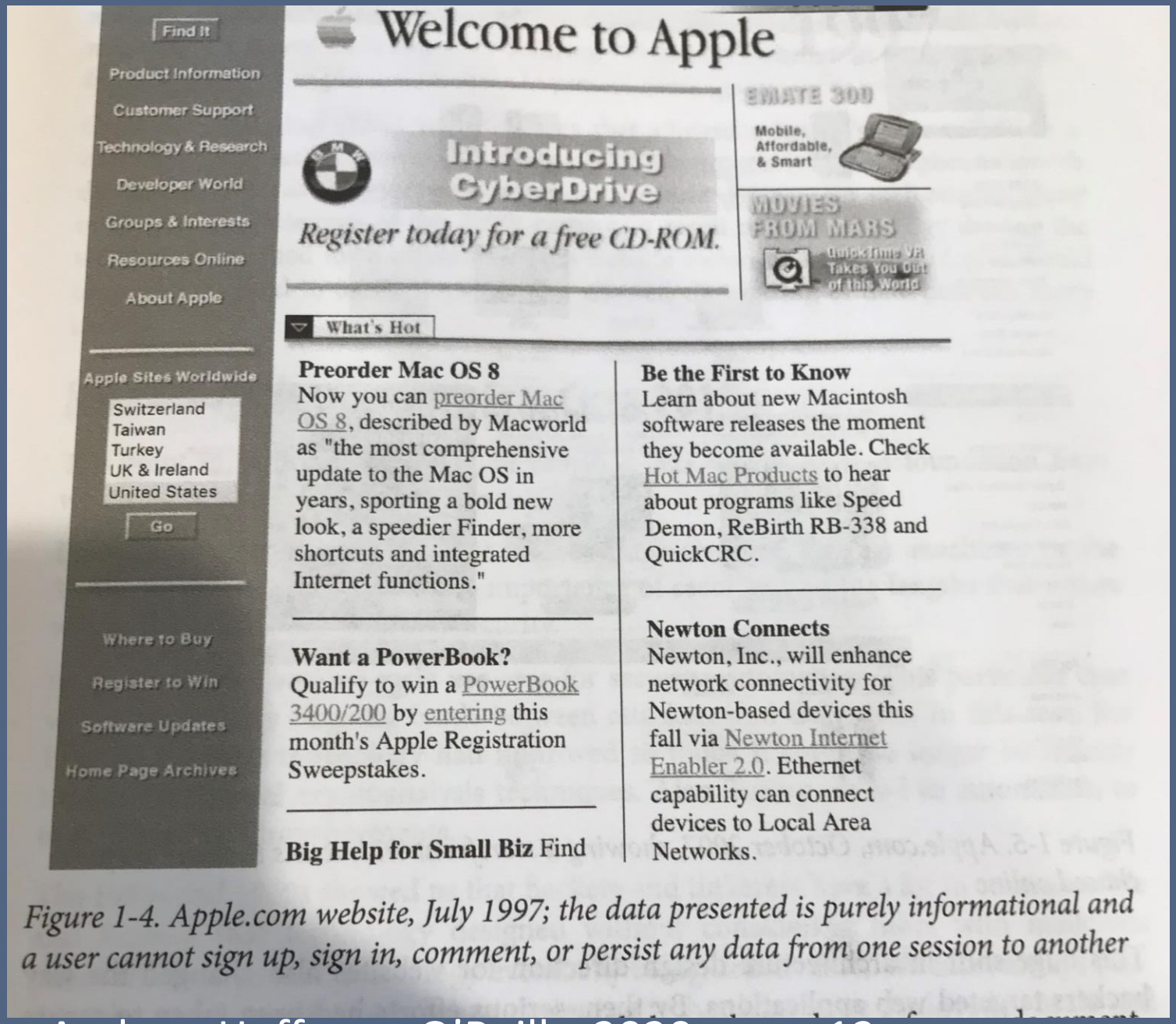


Figure 1-4. Apple.com website, July 1997; the data presented is purely informational and a user cannot sign up, sign in, comment, or persist any data from one session to another

Source: *Web Application Security*, Andrew Hoffman, O'Reilly, 2020, page 12

Static Websites – Protecting Our Accounts

You cannot put personal information on a static website

Most static websites will not ask you to protect your account

Dynamic Websites

Dynamic Websites - Today

Visitors see information selected for them by the website – visitors can read and write

Dynamic websites are interactive –

- links
- buttons
- animations

Typical: stores, financial, news, membership, blogs, social media…

Source: https://blog.hubspot.com/website/static-vs-dynamic-website

Dynamic Websites – Protecting Our Accounts

Typically, we put personal information on dynamic websites

We need to protect our accounts which in turn protects our personal information

Personal Information

Personal preferences –

- styles
- colors

Personal attributes –

- clothing sizes
- shoe size

Personally identifying information (PII)

Dealing With Scammers – Protecting Our Personal Information In Our Online Accounts

Many Websites Give Us Login Options

When we log into a website, we are proving to the website that we are authentic and not an imposter

We're accustomed to using username and password

Authentication options make it more difficult for an imposter to log into our account

We may be able to choose an authentication option that better meets our needs

Authentication Factors That We May Use

Something you know

Something you have

Something you are

If two factors are used, it is called 2FA (Two-Factor Authentication)

If three factors are used, it is called MFA (Multi-Factor Authentication)

Source: https://dojowithrenan.medium.com/the-5-factors-of-authentication-bcb79d354c13

Something That We Know

Answer to a Security Question
Password
Passphrase
PIN

Source: https://dojowithrenan.medium.com/the-5-factors-of-authentication-bcb79d354c13

Something That We Have

Cell phone
Software Authenticator
Security key

Source: https://dojowithrenan.medium.com/the-5-factors-of-authentication-bcb79d354c13

Something That We Are

fingerprint
retina
face
voice

Source: https://dojowithrenan.medium.com/the-5-factors-of-authentication-bcb79d354c13

Using
Something We Know

Websites Typically Require – Passwords

Attacking Passwords – Part 1

Google: at least 65% of people reuse passwords across multiple sites, if not all sites

Another survey: 91% of respondents claim to understand the risk of reusing passwords but 59% admitted to doing it anyway

The average person reuses each password as many as 14 times

Source: https://www.enzoic.com/blog/8-stats-on-password-reuse/

Attacking Passwords – Part 2

Compromised passwords are responsible for 81% of hacking-related breaches

Source: https://www.enzoic.com/blog/8-stats-on-password-reuse/

Preventing Successful Password Attacks

Create passwords using a password generator or roll dice

Passwords should be at least 18 characters with upper and lower case letters, numbers, and symbols

Passwords should be unique for every account

Record each password and username

- on paper
- in a password manager (preferred)

Some Websites Require – Security Questions

Security Questions

When you create the account, you provide answers to their questions

You answer one of those question when you log into the website

Attacking Security Questions

If your personal information is available on the Internet, the attacker can answer the security questions and log in

Source: https://www.bitdefender.com/blog/hotforsecurity/how-sim-swapping-attacks-work-and-how-to-protect-yourself/

Preventing Security Questions Attacks

To prevent security question attacks, do not provide accurate answers to security questions.

Source: https://www.bitdefender.com/blog/hotforsecurity/how-sim-swapping-attacks-work-and-how-to-protect-yourself/

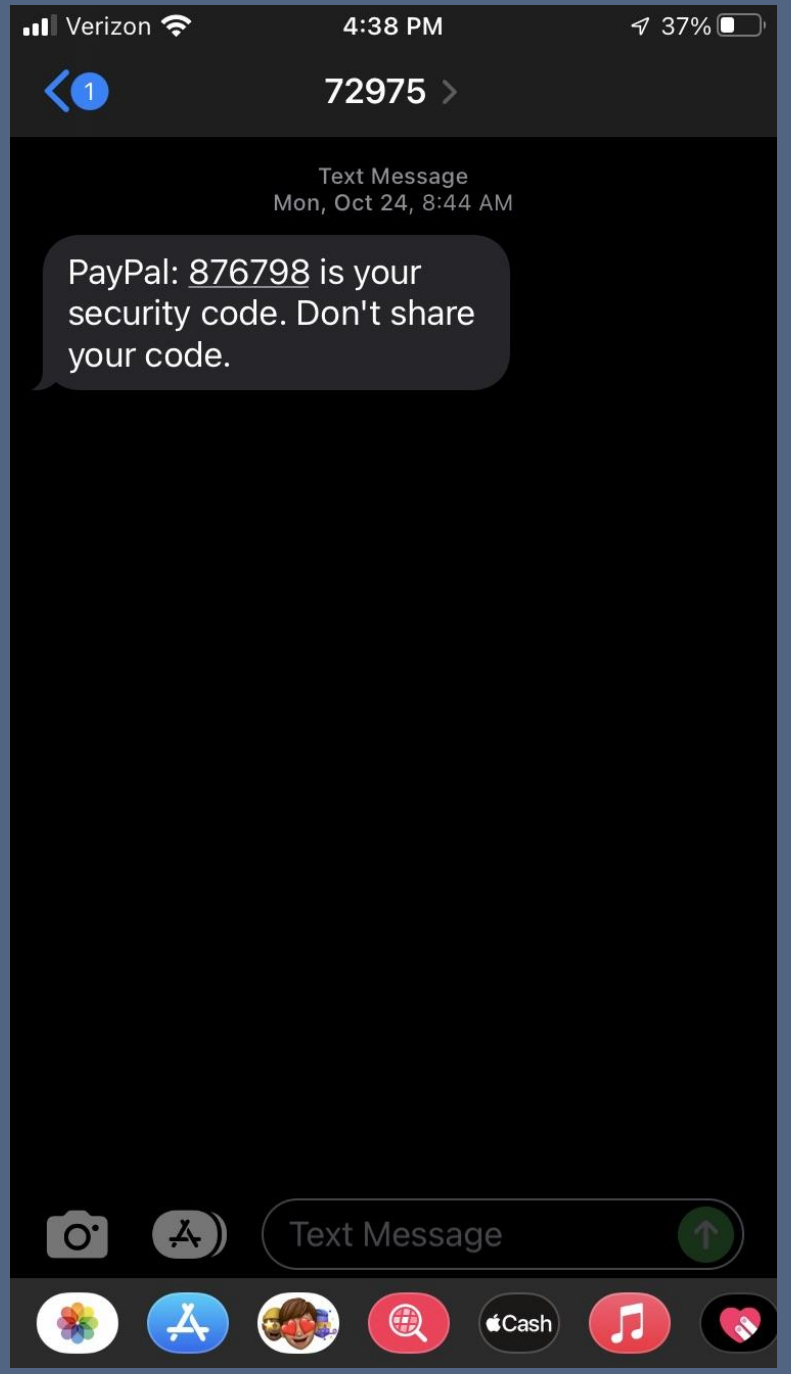
Using
Something We Have

Some Websites Offer This Option – Time-based One Time Passwords (TOTPs)

Using Text Messages

Time-based One Time Password via Text Message (SMS)

- Most TOTPs are six digits while some are 4, 5, or 7 digits
- TOTPs are typically valid for 30 seconds
- Simple Message Service (SMS) is the official name for text messages



Attacking SMS TOTP - SIM Swap

The attacker convinces your phone carrier to move your phone number to a new SIM card which the scammer owns.

Result: All phone calls and SMS messages now go to the attacker's phone which is using your phone number

Source: https://www.bitdefender.com/blog/hotforsecurity/how-sim-swapping-attacks-work-and-how-to-protect-yourself/

SIM Swap Attacks – How Successful Are They?

1,600 complaints in 2021 in USA

Loss of $68 million

Source: https://www.bitdefender.com/blog/hotforsecurity/how-sim-swapping-attacks-work-and-how-to-protect-yourself/

SIM Swapping isn’t likely but it can be costly

Preventing SIM Swap Attacks – Part 1

How to protect yourself from a phone number attack:

- Ask your phone company to add a password or PIN to your account
- Use a free Google Voice or a paid third party VoIP provider phone number for the TOTP website
- Do not forward Google Voice or third party VoIP text messages to your cell phone number

Preventing SIM Swap Attacks – Part 2

Reduce the likelihood of attack:

- Don’t talk about your financials on the web or social media
- Don’t post your phone number or any Personally Identifying Information (PII)

Preventing SIM Swap Attacks – Part 3

Additional steps to protect yourself from a SIM Swap attack:

Avoid this Time-based One-Time-Passwords via SMS option – if a stronger option is available from the website

Some Websites Offer This Option – Time-based One Time Passwords (TOTPs)

Using Phone Number (Not Text Messages)

Time-based One Time Password (TOTP) Using A Phone Number

You provide a phone number to the website. The website may require that you use a cell phone.

When you log in to the website, it will call your phone and read the TOTP digits to you

Attacking Phone TOTP Passwords

Cell phone calls are not encrypted

Intercepting cell phone calls has been done

It has to be done at the cell phone tower near you

It is difficult to do. This attack is unlikely.

Preventing Phone TOTP Attacks

You can prevent TOTP phone number attacks by using a third-party VoIP

- free Google Voice
- paid third-party VoIP

High Risk Situations

This presentation is intended to show you how to protect your online accounts against even unlikely attacks

This presentation does not address high risk situations

If your physical safety is in jeopardy and making any privacy mistake is life or death for you, this presentation is not for you.

See: Extreme Privacy, 4th Edition, Michael Bazzell – Chapter 2, Mobile Devices

Some Websites Offer This Option – Time-based One Time Passwords (TOTPs)

Using Email

Time-based One Time Password via Email

The six digits are sent to you by email

This not a good option because scammers are so successful with phishing attacks

Select a different option, unless this is the only option you can use

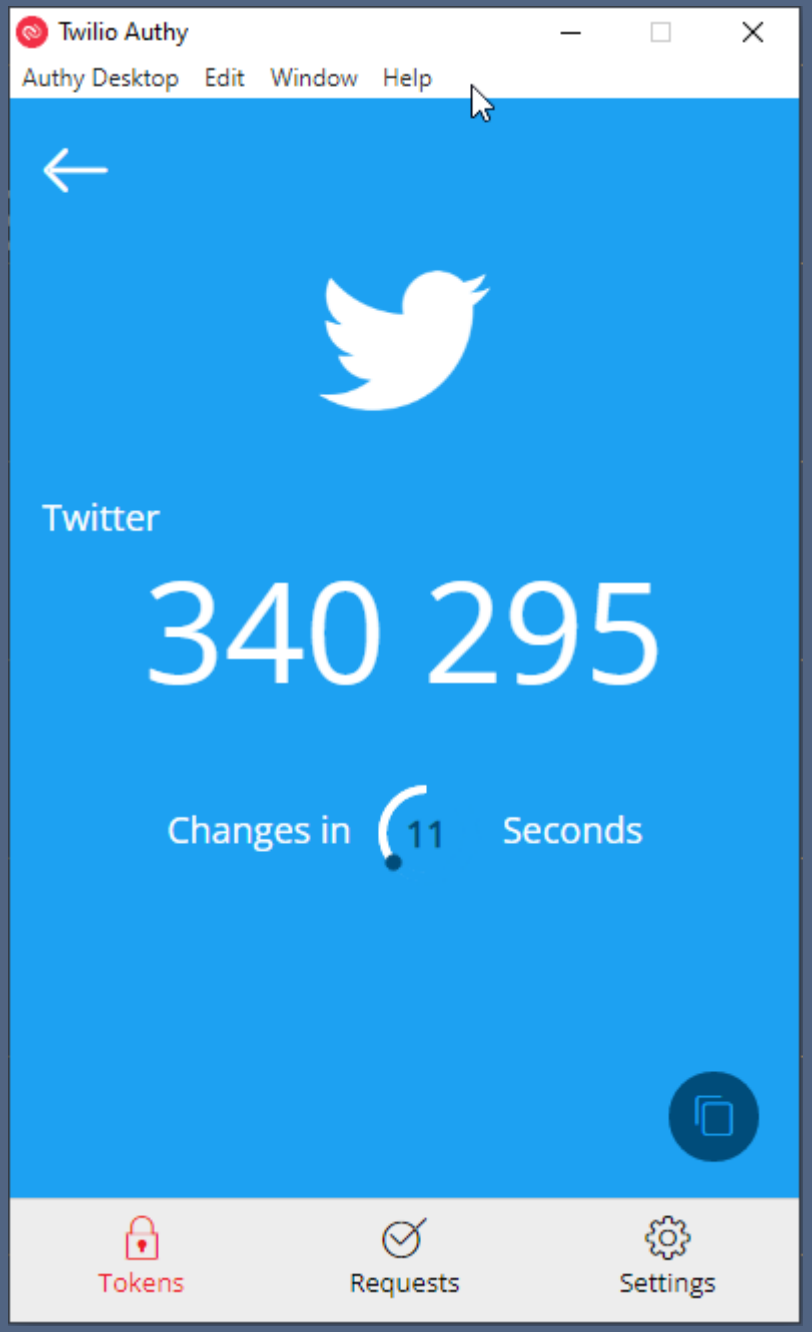
Some Websites Offer This Option – Time-based One Time Passwords (TOTPs)

Using A Software Authenticator

Time-based One Time Password Using A Software Authenticator

What does it look like?

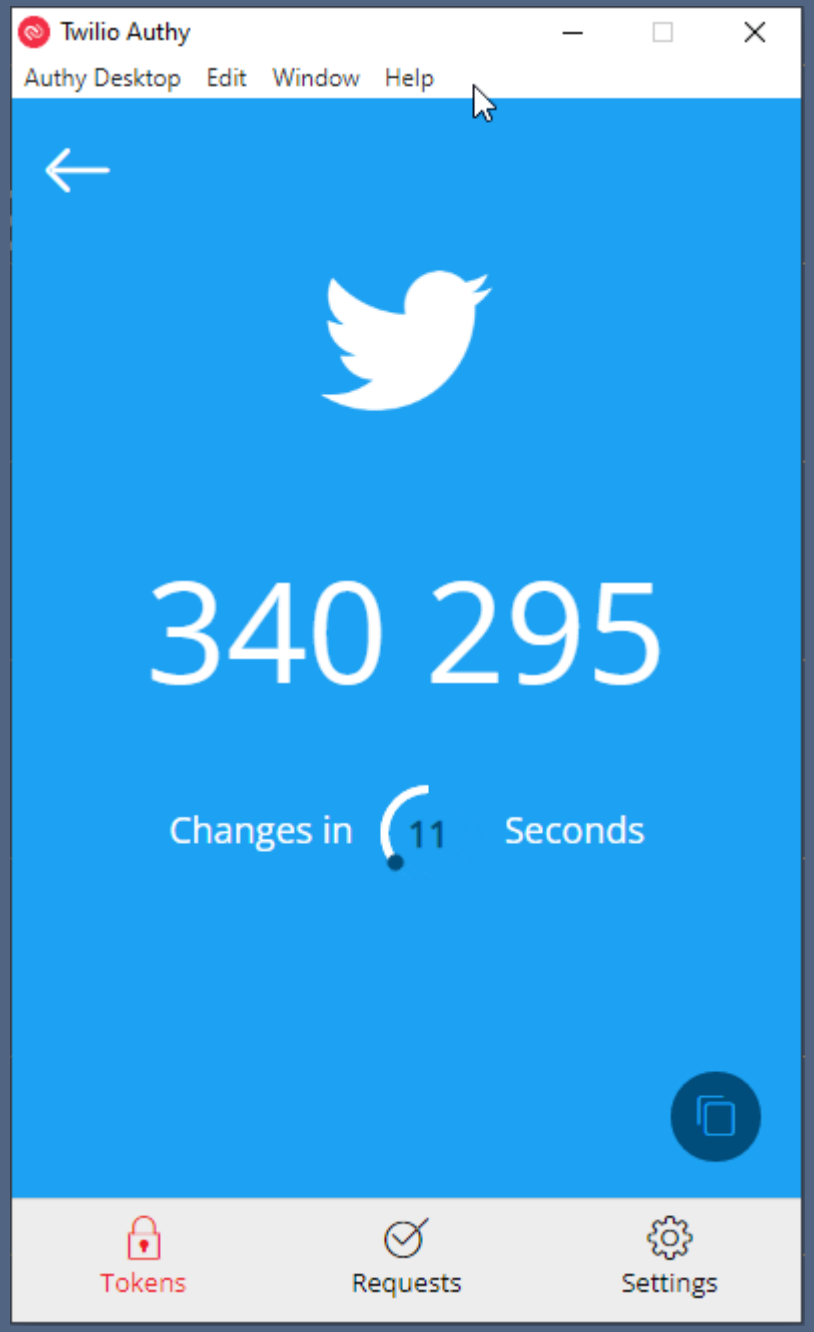
It looks the same on a cell phone, laptop, or desktop



Time-based One Time Passwords (TOTP) Using Software Authenticator

You install the software authenticator on your cell phone, iPad, laptop, or desktop

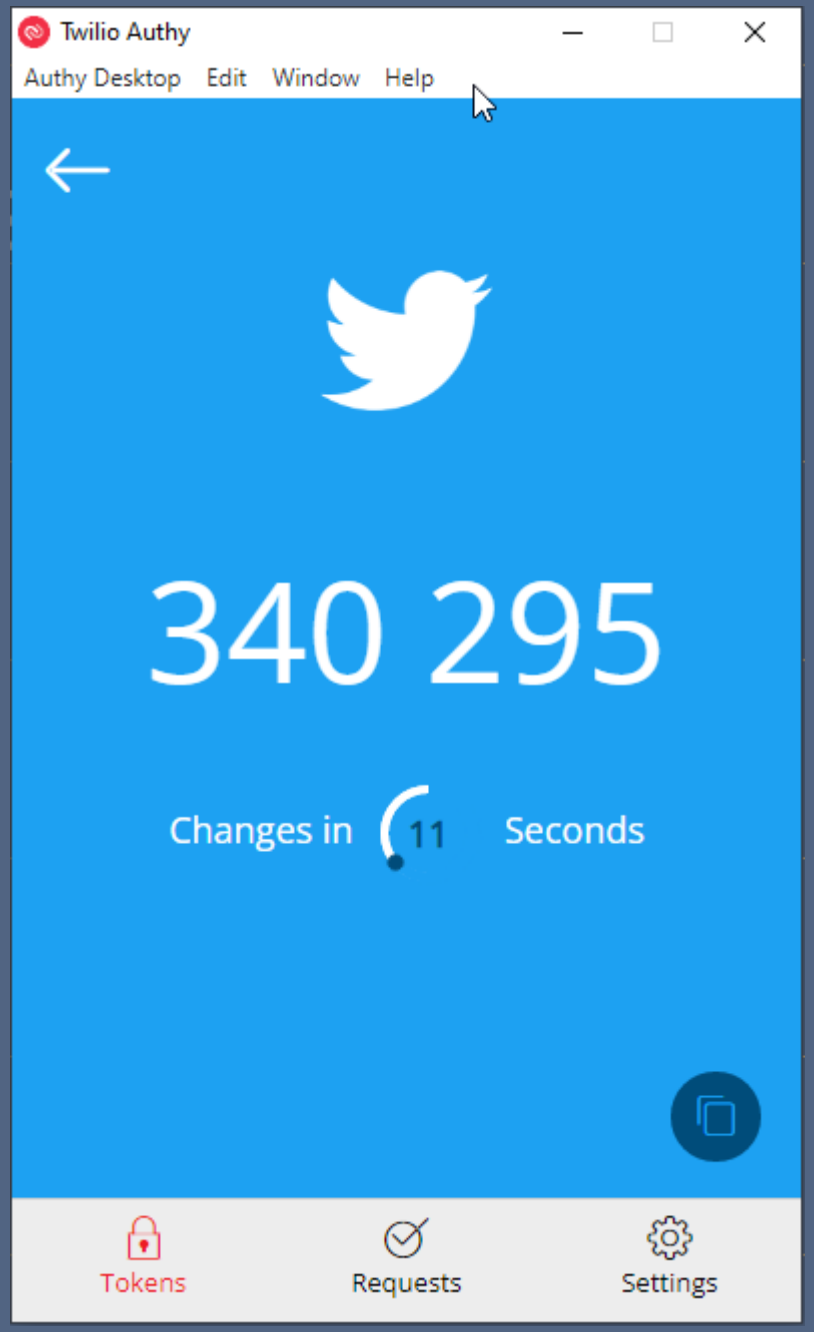
On each website that you want to use your software authenticator you follow their instructions to set it up



Time-based One Time Passwords (TOTP) Using Software Authenticator

You enter the six digits shown on the authenticator into the web site log in page

Popular authenticators: Authy (preferred), Google Authenticator, Microsoft Authenticator



Attacks on Authy

In August, 2022, an Authy data breach impacted 93 Authy users out of 75 million users

Authy recommends that once you have installed Authy on all the devices that you wish, that you disable “all Multi-device” in the app – this stops attackers

Source: Twilio breach let hackers gain access to Authy 2FA accounts
https://www.bleepingcomputer.com/news/security/twilio-breach-let-hackers-gain-access-to-authy-2fa-accounts/

Authy –
the likelihood of a breach is very low

Authy

Runs on

Android	Windows desktop	Apple Watch
iOS	Browser extension	

Has encrypted recovery backups

You must enable the backups – and keep the password safe

Source: Authy vs. Google Authenticator https://authy.com/blog/authy-vs-google-authenticator/

Authy

Offers three types of authentication including Push Authentication

Push Authentication is the most secure and is the default

Push Authentication’s six digit codes come from Authy’s server

Source: Authy vs. Google Authenticator https://authy.com/blog/authy-vs-google-authenticator/

Attacking Any Software Authenticators

Scammers will try to deceive you so that you log into their website instead of the real website that you want.

As you log into their website, they log into the real website.

They send a request for the six digit code to you and you enter the six digit code from the authenticator

They use that six digit code to log into the real website.

They now control your account on that website.

Preventing Software Authenticator Attacks

Use a password manager

Use a hardware security key

Use passwordless authentication

Use passwordless authentication and a hardware security key

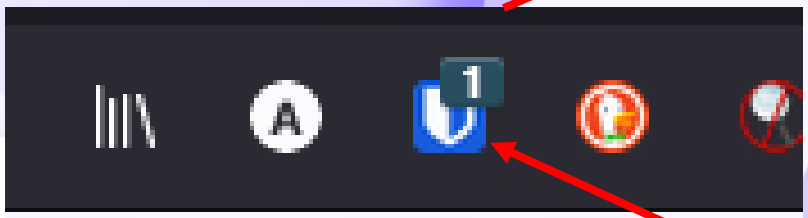
We Always Have This Option – Password Manager

https://account.proton.me/login

2

1

I have logged into the Bitwarden browser extension



3

The Bitwarden icon shows that Bitwarden has login information for one account for this website.

Proton

English

Sign in

Enter your Proton Account details.

Email or username

Password

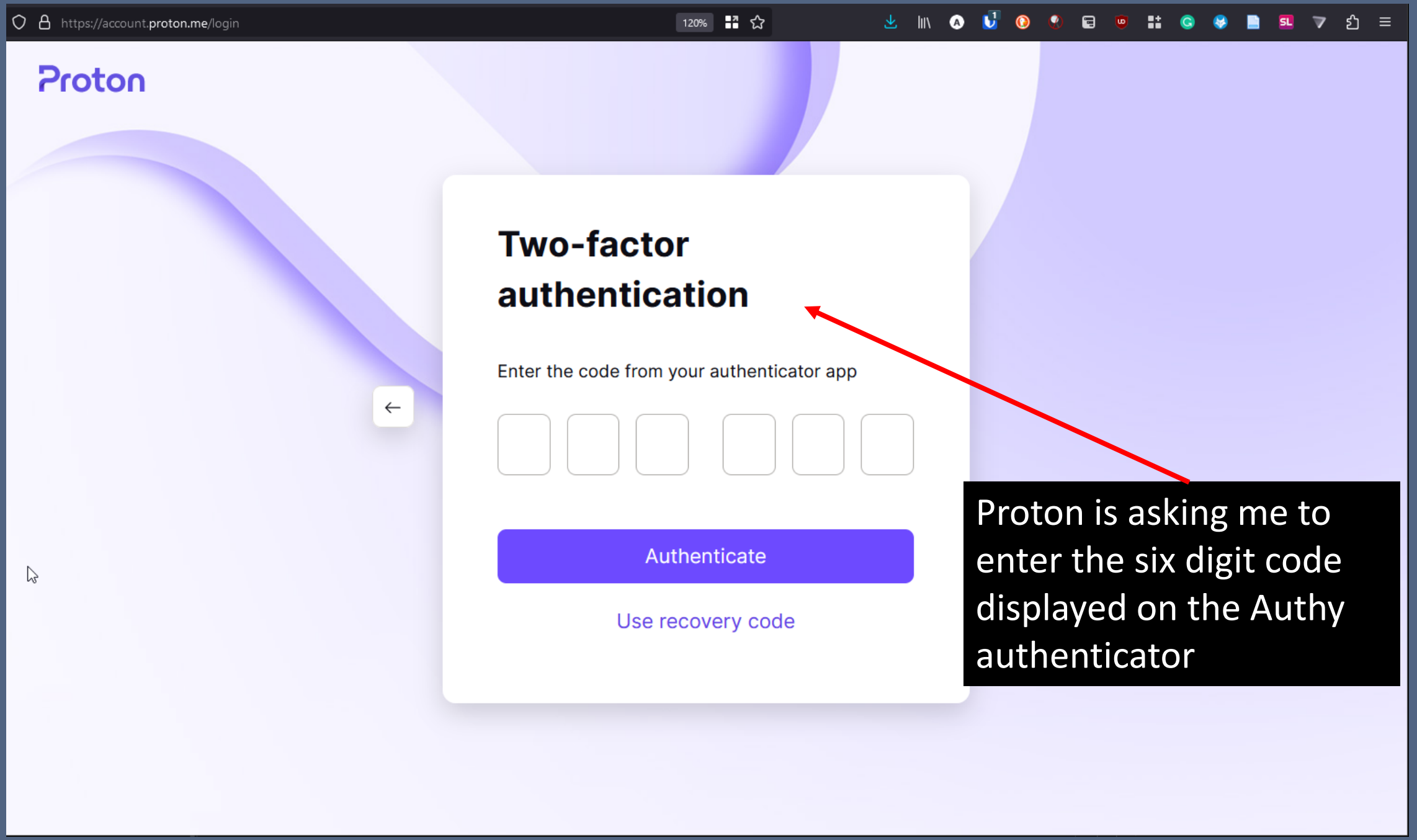
Keep me signed in

Not your device? Use a private browsing window to sign in and close it when done.
Learn more

Sign in

New to Proton? Create account

Need help?


https://account.proton.me/login
120%
Proton
Two-factor authentication
Enter the code from your authenticator app
Authenticate
Use recovery code
Proton is asking me to enter the six digit code displayed on the Authy authenticator

Some Websites Offer This Option – Hardware Security Keys

Hardware Keys

The hardware key sends a secure unique encrypted code, which verifies you, to the website

Plug the key into a USB port. When requested, tap the key

or

Hold the key next to your phone. When requested, tap the key

The dominant hardware security key provider is Yubico

Hardware Keys

No software is needed on your cell phone, iPad, laptop or desktop

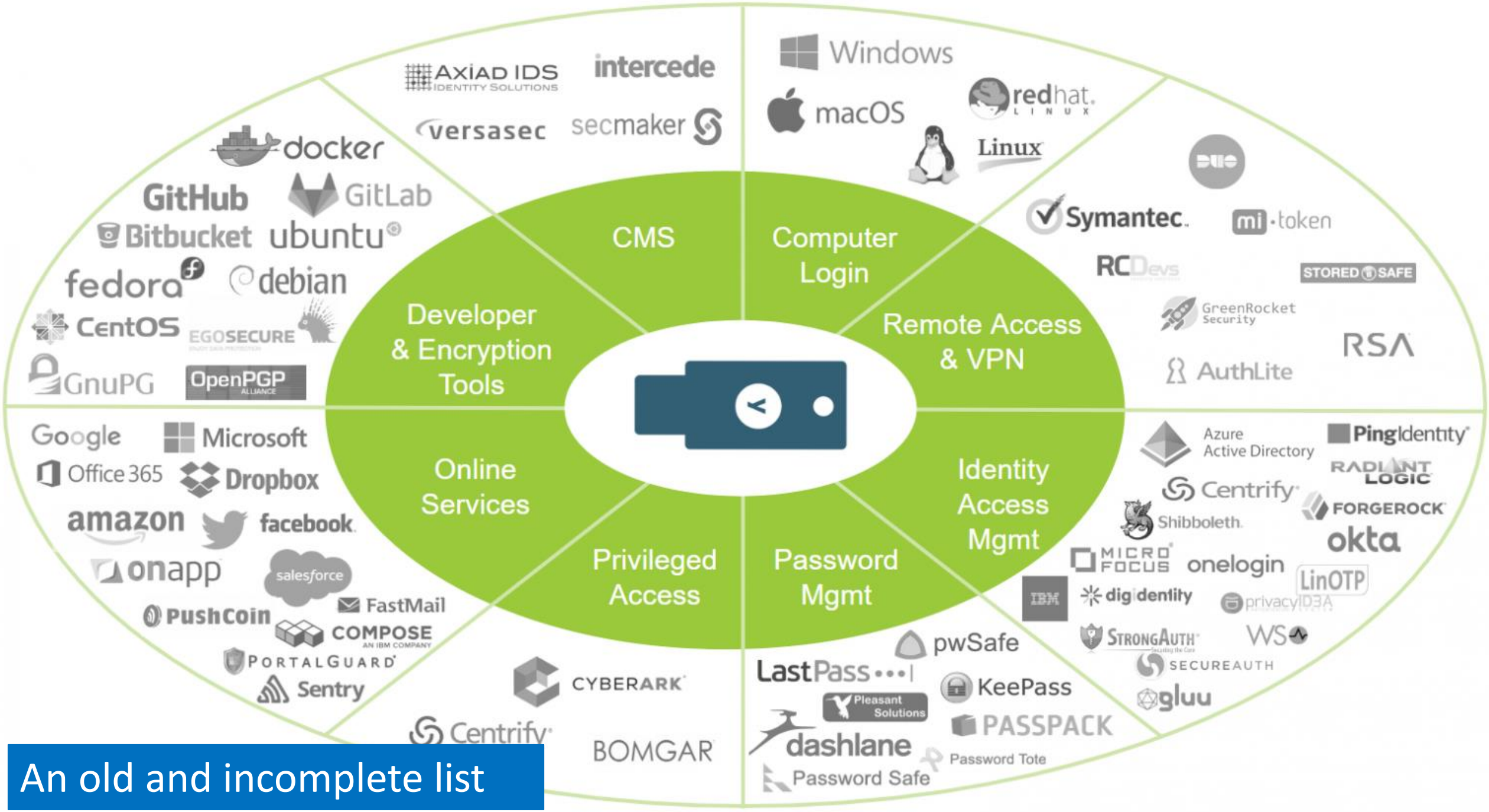
The keys do not need a battery

The keys come with different connectors to meet the needs of your device and different sizes to meet your desire

The YubiKey 5 Series

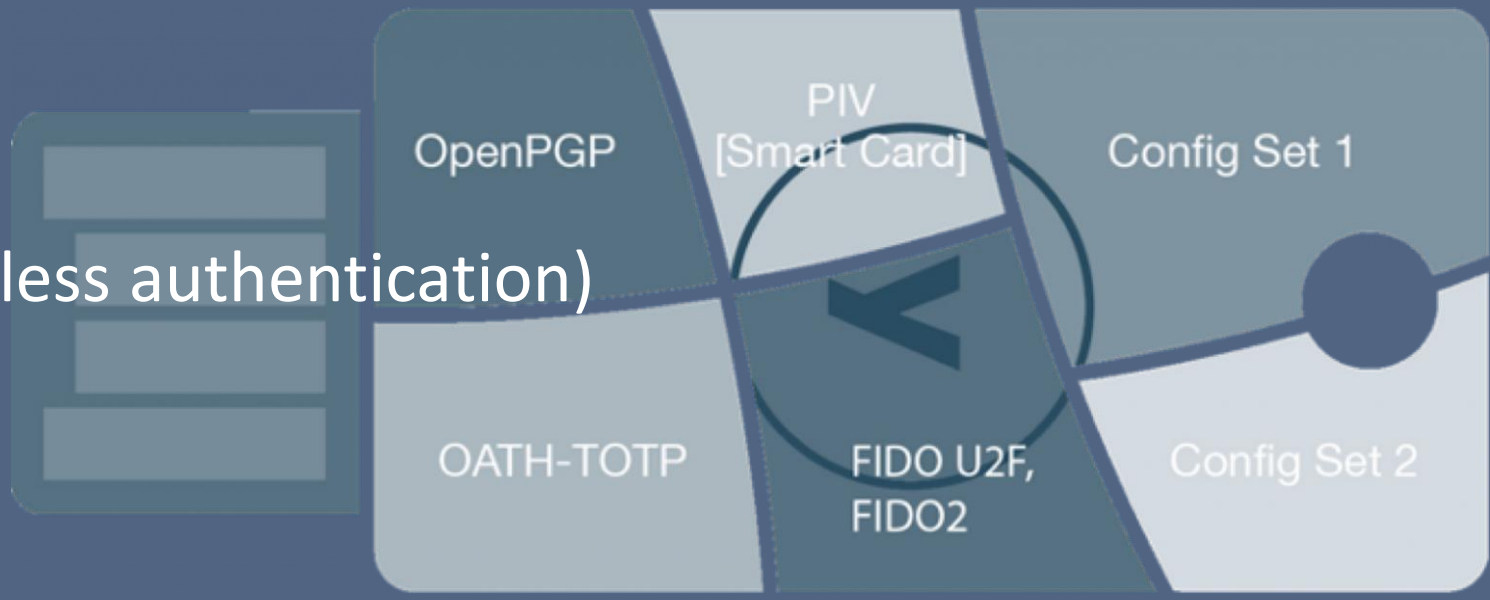
The key on the far left is 1.75 inches long

Source: https://www.yubico.com/why-yubico/how-the-yubikey-works/



An old and incomplete list

YubiKey 5 Series



Modern Systems

- WebAuthn/FIDO2 (passwordless authentication)

Legacy Systems

- FIDO U2F
- One-time password (OTP)
- OpenPGP 3
- Smart card authentication

WebAuthn/FIDO2 replaces username and password.
The YubiKey 5 key can use a PIN or biometric gesture to unlock the key.

Using Hardware Security Keys

Use Google to search for your website's support for hardware security keys.

Examples:

- Vanguard security key
- Wells Fargo security key

Attacking Hardware Keys

There are no known successful attacks on hardware keys, according to Yubico

Source: https://www.yubico.com/solutions/multi-factor-authentication/

Attacking Hardware Keys

"Google has not had any of its 85,000+ employees successfully phished on their work-related accounts since early 2017, when it began requiring all employees to use physical Security Keys in place of passwords and one-time codes, the company told KrebsOnSecurity."

Source: https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/

Some Websites Offer This Option – Prioritized Authentication

Prioritized Authentication

The website asks you to use your hardware security key

If you do not have your key, a TOTP six digit code is sent via SMS to the phone number you provided

Example: Vanguard

Using
Something We Are

Some Websites Offer This Option – Passwordless Authentication

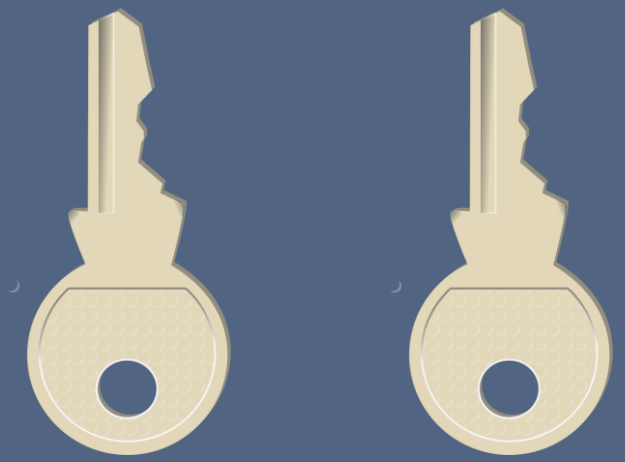
Typically, Passwordless Authentication Uses FaceID, TouchID, or Passcode

Hardware Security Keys May Also Be Used

Passwordless Authentication Is Also Called PassKeys

Why Use Passkeys?

Passwordless authentication cannot be phished



Private Public

What Are Passkeys?

A passkey is a digital key

Each key is a string of characters

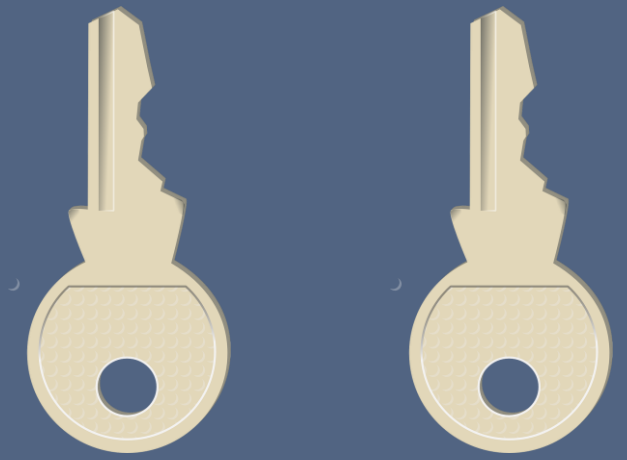
Passkeys

Passwordless authentication uses two keys – private and public

The public key is derived from the private key

An analogy

- The private key is the parent
- The public key is the child

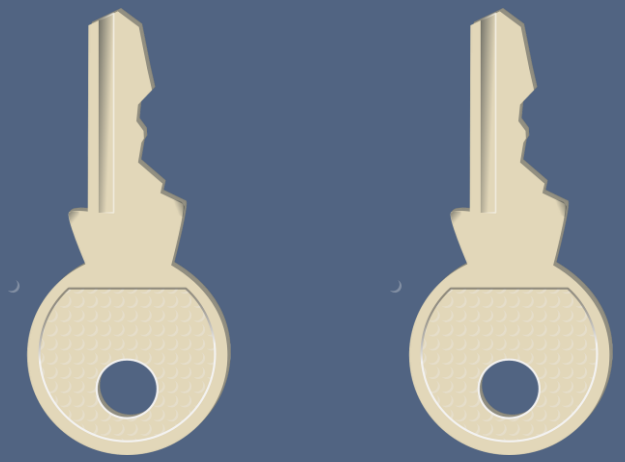


Private Public

Passkeys

The private key is stored on your cell phone, iPad, desktop, or other device

The public key is stored on the service: email, website, etc.

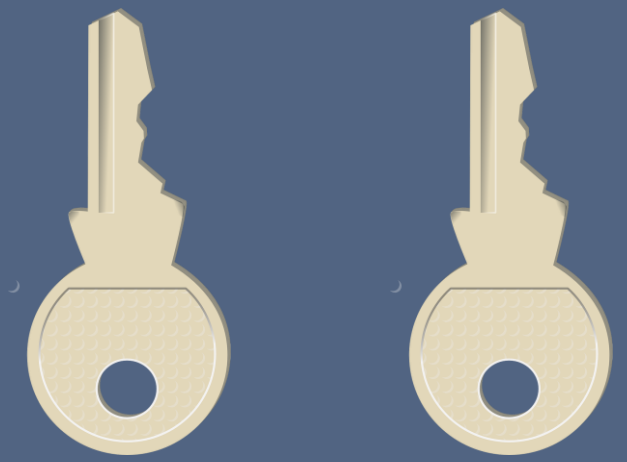


Private Public

Passkeys

When you log into a service, the service's public key verifies that you have the necessary private key on your device

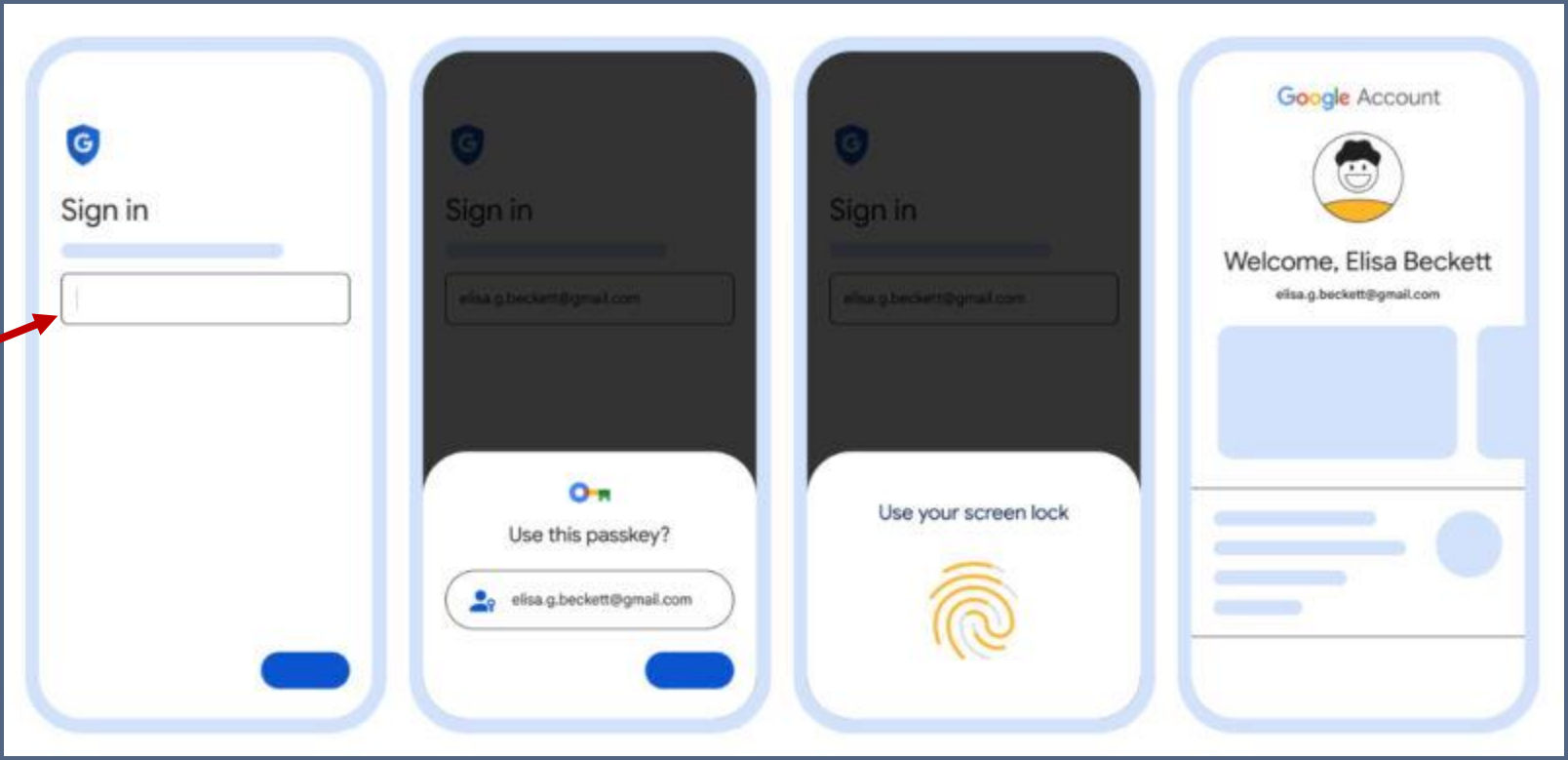
An analogy – the child knows the parent



Private Public

Using Passkeys – According To Google

Username



Source: https://arstechnica.com/gadgets/2023/05/passwordless-google-accounts-are-here-you-can-now-switch-to-passkey-only/

Passkeys and Bitwarden

Bitwarden supports passkeys

You may have up to 5 YubiKeys on a Bitwarden account

Passkeys Availability on Websites

- Support continues to be rolled out
- The number of websites supporting passkeys are few but increasing rapidly

Passkeys Availability On Devices

- Android
- Apple products
- Google
- Windows

The capability to sync our private keys across operating systems is not available - yet

Passkeys Training

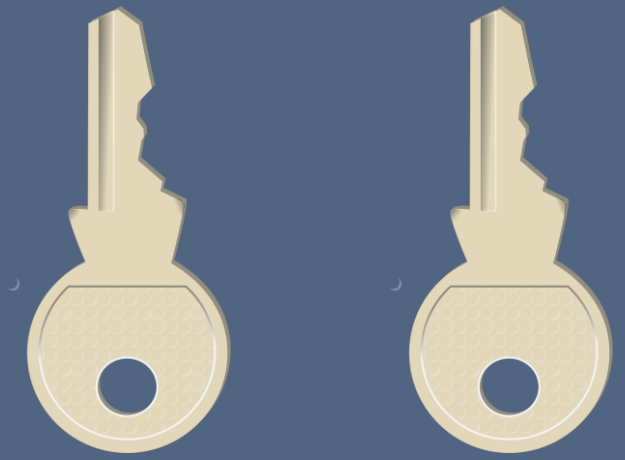
Apple products

Susan Culbertson has provided training on Apple’s implementation of passkeys: culbertson.susan@gmail.com

Some Websites May Offer This Option – Passkeys and Hardware Security Key

Passkeys and Hardware Security Key

You may also use a hardware security key with passkeys to increase the security on a high risk account



Private Public

Passkeys and Hardware Security Keys

- The YubiKey Series 5 supports Passkeys
- iPhone 7 and newer iPhones support YubiKey 5/NFC
- Android phones that have NFC enabled support YubiKey 5/NFC
- A YubiKey Series 5 key supports up to 25 separate accounts

Passkeys – Drilling Deeper

Entry level: https://www.howtogeek.com/763503/why-the-future-is-passwordless-how-to-get-started/

Intermediate level: https://duo.com/blog/webauthn-passwordless-fido2-explained-componens-passwordless-architecture

Detailed level: https://duo.com/blog/tags/administrators-guide

Summary

Weak and reused passwords encourage criminals

Security questions can be attacked unless you use untruthful answers

Time-based One Time Passwords can be attacked unless you take steps to prevent the attacker’s access to the TOTP

Hardware Security Keys have not been successfully attacked

Passwordless authentication cannot be successfully phished

Part 3 –
Invasive Species –
Collecting Our Personal Information

July 6, 10:30am, Cultural Center Theater

Questions?