South Bay Apple MUG
Macintosh

vol 22, issue 6 **June 2022**

A Monthly CUPFUL for South Bay Apple Mac User Group Members

Our next SBAMUG Meeting via Zoom: Wednesday, June 29 at 6:30 p.m.

The June 29 meeting will begin at 6:30 p.m. with a Q & A Session. Everyone is encouraged to participate and all questions are welcome, from basic to complex.

The main presentation will begin about 7:15 p.m. with club member George Wilde discussing Apple's significant new products announced during this month's Apple Worldwide Developers Conference. These products include two new MacBooks incorporating a brand new and faster M2 chip. Apple also announced updates to the system software on all current Apple devices. These updates include macOS 13 (named Ventura), iOS 16, iPadOS 16, tvOS 16, and watchOS 9 – all with many exciting new features and available free later this year. Join us!

IN THIS ISSUE

Page 1: June Meeting Topic; Will We See You at the SBAMUG Picnic?

Page 2: Basic Club Information; June Membership Report

Page 3: Shareware for June; How To Join Our Zoom Meetings; The iPhone Baby: How 15 Years Shaped a Generation

Page 4: SBAMUG Summer BBQ Picnic

Page 5-10: Why Passkeys Will Be Simpler and More Secure Than Passwords

Page 11: Membership Benefits & Form

Will we see you at the SBAMUG Picnic on Wed. July 27?

Instead of a July Zoom meeting, SBAMUG is hosting a BBQ picnic!

All food and drinks will be provided by the club *and we really hope you and your guest will come join in the festivities.*

It's been more than two years since we have met in person, so come join the fun. Zoom meetings are informative but nothing beats sharing a story or joke in person!

See page 4 for the flier. *Be sure to RSVP so we know how much food to buy. Thanks!*

Welcome to the SBAMUG!

(South Bay Apple Mac User Group)

Members, friends and colleagues are invited to attend our monthly meetings (usually the last Wednesday of the month). Annual membership entitles you to receive this online monthly newsletter, plus many more benefits (see page 8). **The $35 annual membership dues are waived for 2022.** Visit sbamug.com to become a member or to get more information. **Meetings will be held virtually via Zoom until further notice.**

SBAMUG Virtual Meeting Format:

6:30-7:15 p.m. Question & Answer Session
Everyone welcome, beginners encouraged!

7:15-8:00 p.m. Announcements & Presentation

Membership Report: 70 members (as of 6/9/22)

On A Sad Note…
Club member John Gebhard passed away in March 2022. We send condolences to his family.

Thank You, Member Renewals!
Michael Maiuri, Guillermo Martinez, Wayne Miyoshi, Russ Neglia, Dick Rath, Glenn Scoble, Arnold Silver, Pam Townsend, George Wilde, Arthur Yahiku

Membership-related Information & Questions:
Contact CW Mitchell at cwmitchell@sbamug.com

- for information about membership, dues and benefits
- if your name is misspelled or the expiration date is incorrect on your membership card

It's EASY To Renew!
Look for renewal letter in the mail. Sign and date the form and return it with payment* using the enclosed self-addressed envelope.

*No payment required for 2022 as club fees have been waived

Virtual Meetings: Online via Zoom
In-Person Meetings: Lomita VFW Hall
1865 Lomita Blvd., Lomita
Mailing Address: C.W. Mitchell
4861 W. 136th St., Hawthorne CA 90250-5631
Phone: (310) 644-3315
Email: info@sbamug.com
Website: http://www.sbamug.com

Officers & Volunteers:

President: Kent McDonald
Vice President: Jim Pernal
Secretary: Nancie Silver
Treasurer: C.W. Mitchell
Directors at Large: Dave Nathanson, Arnold Silver, George Wilde, Joan King
PD Disk Editor: Jim Pernal
Membership: C.W. Mitchell
Member Development: Nancie Silver (publicity). Jim Pernal (website updates)
Programming: Kent McDonald
Server Director: Dave Nathanson
Newsletter: Nancie Silver
USPS Liaison: C.W. Mitchell
Refreshments: Arnold Silver/Andy Paroczai

Other Meetings:

- Tuesday (6 days after last Wednesday) - SBAMUG Core Group, 7:30 p.m. on Zoom. Contact CW Mitchell at cwmitchell@sbamug.com or send email to info@sbamug.com for core group Zoom meeting invite.
- 3rd Thursday every other month - InDesign User Group, 7:00 p.m. at various locations in LA area, laidug.com
- Last Saturday each month - Northrop Grumman - Ham Radio & Computer Swap Meet, 7:00-11:30 a.m. Meet at SE corner of Marine/Aviation Blvd, Redondo Beach (visit w6trw.com to see if swap meet is cancelled due to Covid-19)
- Los Angeles Portable Users Group: Mac OS X, iPhone, iPod, MacBook, etc. at lapug.org/
- Find more: http://www.apple.com/usergroups/

THE SOUTH BAY MUG (ISSN 1058-7810) is published monthly for $35 per year by South Bay Apple Mac User Group, 28110 Ridgeforest Court, Rancho Palos Verdes, CA 90275. Periodicals postage paid at El Segundo, CA and at additional mailing offices.
POSTMASTER: Send address changes to THE SOUTH BAY MUG, c/o CW Mitchell, 4861 W. 136th Street, Hawthorne, CA 90250-5631.

The South Bay MUG is published by the non-profit South Bay Apple Mac User Group. Excerpts may be reprinted by user groups and other non-profit media. Credit must be given to SBAMUG and the author. In addition, a copy of all reprinted materials must be sent to us at the above address. The South Bay MUG is an independent publication not affiliated or otherwise associated with or sponsored or sanctioned by Apple® Computer, Inc. The opinions, statements, positions and views stated herein are those of the author(s) or publisher and are not intended to be the opinions, statements, positions or views of Apple® Computer, Inc.

SBAMUG June 2022 Shareware

Here's to the start of summer. Seven items this month.

A Better Finder Rename 11.48: File, photo, and MP3 batch renamer. Instant Preview. Usual bug fixes in this version OS 10.10+ $24.95 https://www.publicspace.net/ABetterFinderRename/index.html

Carbon Copy Cloner 6.1.2: Bootable backup program. Updates from previous version. Mac 10.15+ $39.99 https://bombich.com

Garden Planner 3.8.24: This program lets layout your garden and landscape. Drag and drop plants, trees, buildings, etc. Color image. Also creates a list MacOS 10.6+ $38.00
https://www.gardendesignerapp.com

MacFamilyTree 10.0.7: Latest update to this Genealogy program. Mac OS 10.15+ $34.95 https://www.syniumsoftware.com/macfamilytree

Parcel 7.4.3: Parcel tracking software information for 265 delivery services. Push notifications for other Apple devices. Mac 10.14.5+ Free up to 3 shipments at the same time, or $4.99 year for unlimited. https://parcelapp.net

StitchBuddy 2.19.1: With StitchBuddy you can organize, preview, modify, convert, and combine embroidery designs. Mac OS 10.12+ Free Mac App Store

UTM Coordinate Converter 2.0.2: Converts between various latitude/longitude systems and Universal Transverse Mercator system. Mac OS 10.14+ Free https://www.ewert-technologies.ca/home/products/utm-coordinate-converter-home.html

See you at the June meeting online.

Jim Pernal PD Editor

JOIN US FOR OUR MONTHLY MEETINGS!

WE MISS YOU!

Instructions on using Zoom…

1) A Zoom meeting invitation will be sent to everyone who is signed up on the club's email list (everybody@sbamug.com).

2) To be added to the mailing list, follow the instructions at https://www.sbamug.com/our-sbamug-email-group/

3) When you receive the Zoom invitation email, save the link to your calendar so that on the day of the meeting, you can find it more easily.

4) To join the Zoom meeting, click on the link provided in the invitation email. This will allow you to install the free Zoom app. The meeting invitation will also include a meeting ID and password, which you may need.

5) *DO YOU NEED HELP WITH ZOOM?* Anyone having trouble logging on to the Zoom meeting online should call CW Mitchell at 310-644-3315 before the next meeting and he will help you get logged on.

Yes, we know you can't schmooze over ZOOM meetings…but, the ***upside*** *of ZOOM is that other family members can also watch the meeting, you save money on gas (right now, that's really worth a lot!), you can have your pet(s) with you, and you can enjoy all the drinks and snacks you want!*

THE IPHONE BABY: HOW 15 YEARS SHAPED A GENERATION (Video)

Check out this link:

https://www.wsj.com/video/series/iphone-baby/the-iphone-at-15-an-inside-look-at-how-apple-transformed-a-generation/4E458113-42D7-4DC0-8DAE-1F66EB93AE99

Come to the SBAMUG Summer BBQ Picnic!

Wednesday, July 27
5:00 pm - ?

Polliwog Park
1601 Manhattan Beach Blvd.

(Street parking on MB Blvd. and
in parking lot off Redondo Avenue)

✳ **RSVP** so we know how much food and drink to buy!!!
✳ Bring a guest - the more, the merrier!
✳ Food and drinks provided by the SBAMUG Club:

- hotdogs (beef and veggie), buns & condiments
- potato salad, green salad, cookies, fruit
- bottled water & soft drinks

✳ We will reserve a few picnic tables and barbecue; feel free to bring an extra chair or blanket
✳ Alcoholic drinks are prohibited in the park, per the City of Manhattan Beach

RSVP to Nancie at piglet10@cox.net or by text at 310-941-4501

South Bay Apple Mac User Group
SBAMUG
www.sbamug.com

Why Passkeys Will Be Simpler and More Secure Than Passwords

Apple has unveiled its version of passkeys, an industry-standard replacement for passwords that offers more security and protection against hijacking while simultaneously being far simpler in nearly every respect.

You never type or manage the contents of a passkey, which is generated when you upgrade a particular website account from a password-only or password and two-factor authentication login. Passkeys overcome numerous notable weaknesses with passwords:

- Each passkey is unique—always.
- Every passkey is generated on your device, and the secret portion of it never leaves your device during a login. (You can securely sync your passkeys across devices or share them with others.)
- Because passkeys are created using a strong encryption algorithm, you don't have to worry about a "weak" password that could be guessed or cracked.
- A website can't leak your authentication credentials because sites store only the public component of the passkey that corresponds to your login, not the secret part that lets you validate your identity.
- An attacker can't phish a passkey from you because a passkey only presents itself at a legitimately associated website.
- Passkeys never need to change because they can't be stolen.
- Passkeys don't require two-factor authentication because they incorporate two different factors as part of their nature.

After a test run with developers over the last year, Apple has built passkey support into iOS 16, iPadOS 16, macOS 13 Ventura, and watchOS 9, slated for release in September or October of this year. These operating systems will store passkeys just as they do passwords and other entries in the user keychain, protected by a device password or passcode, Touch ID, or Face ID. Passkeys will also sync securely among your devices using iCloud Keychain, which employs end-to-end encryption—Apple never has access to passkeys or other iCloud Keychain data.

Best of all, perhaps, is that Apple built passkeys on top of a broadly supported industry standard, the W3C Web Authentication API or WebAuthn, created by the World Wide Web Consortium and the FIDO Alliance, a group that has spent years developing approaches to reduce the effectiveness of phishing, eliminate hijacking, and increase authentication simplicity for users. Apple, Amazon, Google, Meta (Facebook), and Microsoft are all FIDO board members, as are major financial institutions, credit card networks, and chip and hardware firms.

Many websites and operating systems already support WebAuthn via a hardware key like the popular ones made by Yubico. You visit a website, choose to log in using a security key, insert or tap a button on the hardware key, and the browser, operating system, and hardware key all talk together to complete the login. A passkey migrates the function of that hardware key directly into the operating system—no extra hardware required. Websites that already support hardware-based WebAuthn should be able to support passkeys with little to no effort, according to Apple.

Before we get started, note that Apple writes "passkey" in lowercase, an attempt to get us to use it alongside password, passcode, and passphrase as a common concept. Google, Microsoft, and other companies will offer compatible technology and may also opt for the generic passkey name. While new terminology can cause confusion, “passkey” is better than the more technically descriptive “multi-device FIDO credentials,” which doesn’t exactly roll off the tongue.

Let’s dig in to how passkeys work.

Passkeys Bring the Benefits of Public-Key Cryptography to Everyday Logins

Passkeys rely on public-key cryptography, something we’ve been writing about at TidBITS for nearly 30 years. With public-key cryptography, an encryption algorithm generates a secret that’s broken into two pieces: a private key, which you must never disclose, and a public key, which you can share in any fashion without risk of exposing the private key. Public-key cryptography underpins secure Web, email, and terminal connections; iMessage; and many other standards and services.

Anyone with a person’s public key can use it to encrypt a message that only the party who possesses the private key can decrypt. The party who has the private key can also perform a complementary operation: they can “sign” a message with the private key that effectively states, “I validate that I sent this message.” Crucially, anyone with the public key can confirm that *only* the private key’s possessor could have created that signature.

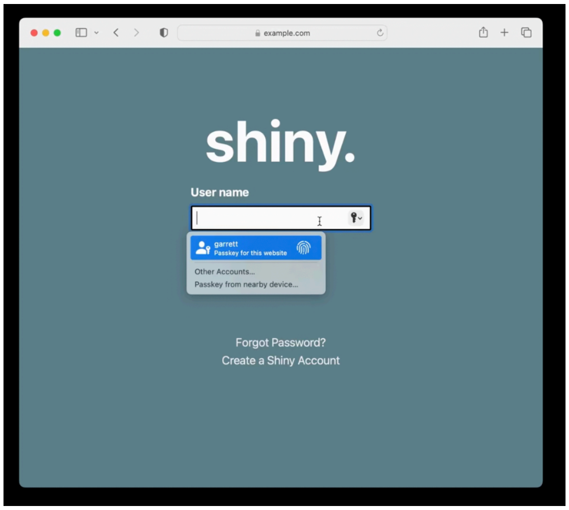
A passkey is a public/private key pair associated with some metadata, such as the website domain for which it was created.

With a passkey, the private key never leaves the device on which it was generated to validate a login, while a website holds only the corresponding public key, stored as part of the user’s account.

To use a passkey, the first step is to enroll at a website or in an app. You’re likely familiar with this process from any time you signed up for two-factor authentication at a site: you log in with existing credentials, enable 2FA, receive a text message or scan a QR code into an authentication app or your keychain (in iOS 15, iPadOS 15, and Safari 15 for macOS), and then verify your receipt.

With a passkey, the process is different. When you log in to a website offering passkey authentication, you will have an option to upgrade it to a passkey in your account’s security or password section. The website first generates a registration message that Apple’s operating systems will interpret—it happens at a layer you never see. In response, your device creates the public/private key pair, stores it securely and locally, and transmits the public key to the website. The site can then optionally issue a challenge for it and your device can present it to confirm the enrollment.

On subsequent visits, when you’re presented with a login, your iPhone or iPad will show the passkey entry in the QuickType bar and Safari in macOS will show it as a pop-up menu. In both cases, that’s just like passwords and verification codes today. As with those login aids, you’ll validate the use of your passkey with Touch ID, Face ID, or your device passcode, depending on your settings.



Source: Apple

Behind the scenes, your request to login via a passkey causes the site server to generate a "challenge" request using the stored public key. Your device then has to build a response using your stored private key. Because you initiate a passkey login by validating your identity, your device has access to your passkey's private key when the challenge request comes in and can respond to the challenge without another authentication step. The server validates your device's response against your stored public key, ensuring that you are authorized for access. If it all checks out, the website logs you in.

A passkey replaces two-factor authentication, and it's worth breaking down why, as it seems counter-intuitive: how can a single code held on a device provide distinct aspects of confirmation? The rubric for multiple security factors is usually stated as at least two of "something you know, something you have, or something you are." A passkey incorporates at least two of those:

- **Something you know:** While commonly thought of as a password, the "know" part is really any fixed piece of information you possess. Think of a 20-character randomly generated password stored in your password manager. Do you "know" that? Yes, in the sense that it's retrievable exactly as entered.
- **Something you have:** Because passkeys are locked to devices, you prove your possession of a device by unlocking the passkey: no device, no passkey.
- **Something you are:** Although passkeys don't require biometric authentication using Face ID or Touch ID, it's an option. Apple always lets you use a device passcode to backstop Face ID or Touch ID, so it's a blurred line with "something you know" compared to a dedicated biometric device with no fallback option.

Think for a moment about the advantages here. A passkey:

- **Resists phishing:** As with passwords and verification codes, your device will only present a passkey in QuickType or as a pop-up menu option when on a website's specific domain associated with the passkey. An attacker can't fool you into entering a passkey on a deceptive site, as can be done with a password.
- **Prevents reuse of a stolen key on other accounts:** Because each passkey is unique to its associated website, even if the site suffers a security breach, the only credential that can be stolen is your public key. That public key is useless to help a thief log in as you at another site as they lack your private key to answer the login challenge.
- **Blocks damage from malicious code injection on a website you visit:** A malicious party can often "inject" malicious JavaScript onto an otherwise benign page. It has happened at times even to major websites, usually due to poorly vetted malicious ads delivered automatically through self-service advertising networks. A website that falls prey to just a front-end attack on its HTML and scripts wouldn't allow the attacker to produce a valid challenge request for your device's passkey. The site would also have to suffer from a back-end compromise of its server code for account information to be at risk, at which point the site's data is probably fully compromised anyway.
- **Blocks guessing, identity searching, brute force:** Because every passkey has a super-complex secret, an attacker can't successfully

guess or brute force your access to a site.

- **Eliminates 2FA hijacking:** Because passkeys don't have a second factor, they aren't vulnerable to SMS hijacking and interception, site impersonation and phishing, and other techniques to acquire a second factor.

Apple stores each passkey as just another entry in your keychain. If you have iCloud Keychain enabled, the passkeys sync across all your devices. (iCloud Keychain requires two-factor authentication enabled on your Apple ID; Apple hasn't said if passkeys will replace its internal use of 2FA for its user accounts.)

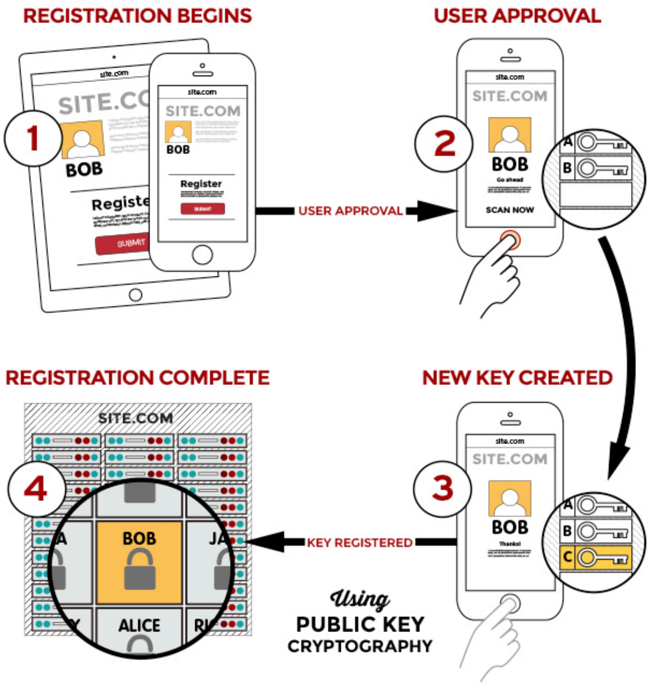
You can share a passkey with someone else using AirDrop. This means you have to be in proximity to the other person, another element in security. The details are shared through end-to-end encryption, allowing the private key and other data to be passed without risk of interception. Apple hasn't provided much more detail than that AirDrop sharing is an option, so there may be other provisos or security layers.

Because passkeys replace passwords and a second factor, you may be reasonably worried at this point about losing access to your passkeys if you're locked out of your Apple ID account or lose all your registered devices. Apple has several processes in place for recovering Apple ID account access and broad swaths of iCloud-synced data. For an Apple ID account, you can use Apple's account recovery process or an account Recovery Key. For iCloud data, if you've enabled the friends-and-family recovery system, iCloud Data Recovery Service, you can use that to re-enable access. After you recover account access, Apple has an additional set of steps that enable you to retrieve iCloud Keychain entries: it involves sending a code via SMS to a registered phone number and entering a device passcode for one of the devices in your iCloud-synced set.

This is all a fabulous reduction in the potential for successful attacks against your Internet-accessible accounts. But there's more: Apple isn't building yet another walled garden. Instead, passkeys are part of a broad industry effort with which Apple says its implementation will be compatible.

Passkeys Are an Industry Standard, Not a Proprietary Technology

Apple built its passkey support on top of the previously mentioned WebAuthn standard, which describes the server side of how to implement a Web-based login with public-key cryptography. FIDO created standards for the client side of that equation and calls the combination of its protocol and WebAuthn FIDO2. Apple developed its own client-side approach that's compatible with standard WebAuthn servers and should be interchangeable with other companies' rollouts of passkeys. Google, Microsoft, and Apple made a joint announcement in May 2022 committing to this approach, too.



FIDO's schematic for a generalized registration process. (Source: FIDO Alliance)

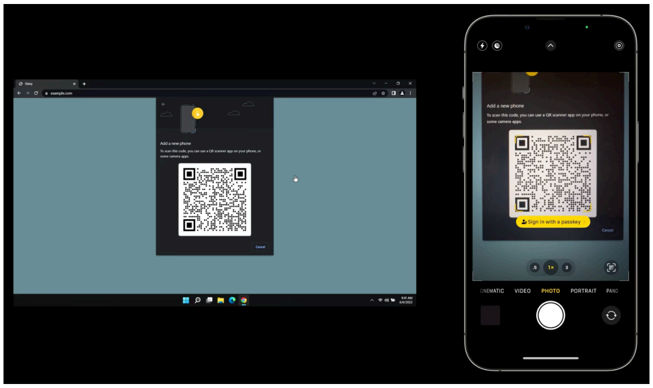
In Apple's passkey introduction video for developers, engineer Garrett Davidson emphasized Apple's commitment to compatibility, saying:

> *We've been working with other platform vendors within the FIDO Alliance to make sure that passkey implementations are compatible cross-platform and can work on as many devices as possible.*

He then demonstrated using a passkey on an Apple device to log in to a website on a PC, showing how a QR code could be used to enable a passkey login to one of your accounts on a device or browser that's not connected to your existing devices or ecosystem.

Here's how you might log in to a passkey-enabled account on someone else's PC using your iPhone with your passkey as the authenticator. During the login, you can opt to add a device instead of entering a passkey or other authentication in the browser. The website's server generates a QR code that includes a pair of single-use passwords—they're generated just for that login and used in the next step for additional validation. (Note that the device with the browser could be any passkey-supporting operating system and device. The authenticating devices might be limited by Apple or other companies to a smaller set, much like you can only use an iPhone to confirm Apple Pay in Safari on a Mac, not a Mac with Touch ID to confirm Apple Pay from an iPhone.)

The PC in our example also starts broadcasting a Bluetooth message that contains the information needed to connect and authenticate directly with the server. Scan that QR code on your iPhone, and the iPhone uses an end-to-end encrypted protocol to create a tunnel with the PC's Web browser using the keys shown in the QR code. (This encrypted connection isn't part of the Bluetooth protocol, by the way, but data tunneled over Bluetooth; Bluetooth doesn't incorporate the necessary encryption strength.)



Add a new phone

To scan this code, you can use a QR scanner app on your phone, or some camera apps.

Add a new phone

To scan this code, you can use a QR scanner app on your phone, or some camera apps.

Source: Apple

This Bluetooth connection provides additional security and verification by offering *out-of-band* elements, or details that the PC isn't presenting to the device that's providing authentication—here, your iPhone. Because Web pages can be spoofed for phishing attacks, the Bluetooth connection provides a device-to-device backchannel for key details:

- **Server addresses:** The QR code doesn't tell the iPhone what server (or list of servers) it can connect to for the actual passkey connection. That prevents a browser from providing malicious information.
- **Key validation:** The successful creation of an end-to-end encrypted two-way session over Bluetooth using the keys in the QR code enables the iPhone and PC to confirm that the QR code the browser delivered and the iPhone scanned are identical. (Apple hasn't yet provided full details on this stage. The operating system clearly generates the QR code based on a request from the browser, and the browser can't sniff the Bluetooth connection. So a front-end attack that displayed a malicious QR code wouldn't work, as the PC and iPhone communicate without the browser in the loop.)

- **Proximity:** Connecting over short-range Bluetooth demonstrates, with confidence, that the PC and iPhone are near each other.

This broad device and platform compatibility lets you maintain the same degree of passkey security and simplicity without downgrading to a weaker method for login when accessing your account using other people's devices. Whenever there's a way to force a weaker login method, malicious parties will exploit that via phishing, social engineering, or other interception techniques. (Providing a second factor via an SMS text message versus a verification code is a prime example of a weaker backup approach that has been exploited.) In fact, until passkeys can be used exclusively, password-based logins will have to remain available, and they'll remain vulnerable.

There might be some usability hiccups as passkeys roll out, but they shouldn't be widespread. It's possible, for instance, that some WebAuthn server components will need to be updated or that Apple will have to add more edge cases to its framework to encompass how things work in the wild.

But imagine a world in which you can securely log in to websites using any current browser on any device running any modern operating system, without having to create, remember, type, and protect passwords. It's relaxing just to think about.

The main question that remains unanswered is how portable passkeys will be among ecosystems: can I use iOS and Android and Windows and share a passkey generated on one among all three? Given that Apple has built an AirDrop-sharing method for passkeys, I hope FIDO's broad compatibility includes sharing passkeys among operating systems, too.

A Return to Security through Proximity

Passwords have provided an uneasy security compromise since their introduction decades ago when multi-user computing systems began to require protection. Passwords are patently imperfect, a relic of an age when physical proximity provided the first level of protection, something rendered moot by the Internet.

In an effort to answer some of the weaknesses in a password system, two-factor authentication was grafted on to require that you had something besides a password, something that required holding or being near an object to validate your right to log into a computer, service, or website. But because 2FA starts with an account password and uses a second method that can be subject to compromise or phishing, it remains a patch applied to a damaged wall.

The passkey is a modern replacement for passwords that rebuilds the security wall protecting standard account logins. Proximity—in the form of the device that stores your passkeys—is a powerful tool in reducing account hijacking and interception. Passkeys may seem scary and revolutionary, but they're actually safer and, in some ways, a bit old-fashioned: they're a bit of a throwback to a time when having access to a terminal provided proof you were authorized to use it.

Article written by Glenn Fleishman on June 27, 2022

SOUTH BAY APPLE MAC USER GROUP
c/o C.W. Mitchell
4861 136th Street
Hawthorne, CA 90254-5631

PERIODICALS

Join, Renew or Give a Gift of a SBAMUG Membership!

For only $35 per year*, you get:

- Monthly meeting presentations
- Get help from our experts via our Email Group
- Monthly newsletter (We publish 11 issues per year!)
- Use our Wiki
- Free web space & e-mail on our server
- Build your own website
- Create your own blog
- Special merchant discounts $$$
- Occasional swaps, free software, opportunity drawings

http://www.sbamug.com/join.html
or contact Membership Chair
CW Mitchell at
cwmitchell@sbamug.com
*($35 membership fee waived for 2022)

SBAMUG Membership Application

South Bay Apple Macintosh User Group provides you with a local source of shared knowledge & experience through monthly meetings, trainings and monthly newsletter.

Individual & Family Memberships: $35 per year*
(*membership fee is waived for 2022)

□ New Member(s)   □ Member Renewal

Name:____
Spouse/Partner Name:____________________________
Address:______________________________________
City:____
State:______________________ Zip:_____________
Home Phone: (_____)_____________________________
Member Cell: (_____)_____________________________
Spouse/Partner Cell: (_____)______________________
Member Email Address:___________________________
Spouse/Partner Email:____________________________
Member computer interests: ______________________
Spouse/Partner computer interests:_________________
Devices you use most:____________________________
Current level of Mac expertise:
Member: ___ Beginner ___ Intermediate ___Advanced
Spouse/Partner: ___ Beginner ___ Intermediate ___Adv.
How did you hear about SBAMUG?__________________
____
I would like to help with the club. Please contact me at:
____
Comments:____________________________________
____
Signature: ____________________________________
Date: ____

Mail your Application (no check needed for 2022) to our mailing address (see page 2), or bring to our monthly meeting at VFW Hall when in-person meetings resume.