

Forum:[Hack Forums](#)

Thread: [Passkeys](#)

Omniscient - July 17, 2026, 10:55 am

Should I add them to HF?

Do you use them on websites regularly?

Give me your feedback on this. I'm contemplating it. Probably fairly easy to vibe code the feature into HF.

m0hx - July 17, 2026, 11:04 am

I recently just started setting them up on some of my accounts, and ngl they make life easier (not having to open authenticator and waiting for code etc), but I have love-hate thing for passkeys and I don't know why. Sometimes I just don't want them, sometimes I prefer them.

tbh I don't know much about passkeys and how they work, or how secure are they compared to OTP/2FA codes, but I'd say yea add them to HF cuz most modern sites have them.

Charlie Sheen - July 17, 2026, 11:17 am

I use them anywhere that I can. It's nice being able to quickly login as I use a different password for each site.

Jamika - July 17, 2026, 11:47 am

I've never used it, and I never will. I think some members here might prefer it and use it, but it's not for me.

Charlie Sheen - July 17, 2026, 12:34 pm

(Jul 17, 2026 11:47 AM)Jamika Wrote: [\[CITE\]](#) I've never used it, and I never will. I think some members here might prefer it and use it, but it's not for me.

Just curious your reasoning behind that? They are great to combat phishing. They protect against data breaches. Much more convenient. Most sites are adopting and getting rid of passwords.

jcole - July 17, 2026, 12:36 pm

I would use it if implemented.

SoulZeh - July 17, 2026, 1:01 pm

I also use where I can and when, I find it 100% easier and just less hassle.

I'd 100% use it .

Omniscient - July 17, 2026, 2:15 pm

Why Passkeys Are Better Security

Passkeys offer stronger account protection than using a password alone and are often easier to use than traditional two-factor authentication.

Password Only

A password can be guessed, reused, leaked in a data breach, or stolen through phishing. Even a

strong password is still something you must type and something an attacker may be able to capture.

Password + 2FA

Two-factor authentication adds an important extra layer of protection. An attacker usually needs both your password and your temporary 2FA code.

However, some forms of 2FA can still be targeted through phishing, SIM swapping, malware, or convincing a user to enter a code on a fake website.

Passkeys

Passkeys use cryptographic authentication stored on your device or password manager. There is no password to type, remember, or accidentally give to a phishing website. Resistant to phishing

- Cannot be guessed or reused

- No temporary codes to enter

- Can use your fingerprint, face, device PIN, or security key

Security Comparison

Password only: Basic protection

Password with 2FA: Strong protection

Passkey: Strong and phishing-resistant protection

Passkeys are not magic, and you should still secure your devices and recovery methods. However, for most members, a passkey provides better protection than a password alone and a smoother login experience than entering a password and 2FA code every time.

Raijin - July 17, 2026, 2:19 pm

No I don't use passkeys. I don't like any kind of stored credentials.

Omniscient - July 17, 2026, 2:51 pm

(Jul 17, 2026 02:19 PM) Raijin Wrote: [\[CITE\]](#) No I don't use passkeys. I don't like any kind of stored credentials.

All credentials are stored somewhere. Just reality. Hardware passkeys probably the most secure you can get nowadays. But imho overly inconvenient to use them constantly for mundane online activity.

I'm still iffy on passkeys myself but I do recognize their convenience and all my research seems to conclude they are more secure than 2FA.

AI Quote: Generally, yes—passkeys are more secure than a password combined with ordinary 2FA, especially when that 2FA uses SMS, email codes, authenticator-app codes, or push notifications.

The main advantage is phishing resistance. A passkey is cryptographically tied to the legitimate website, so it cannot be entered into a convincing fake HF login page. Passwords and most 2FA codes can still be stolen or relayed through phishing. CISA identifies FIDO/WebAuthn—the technology behind passkeys—as the widely available phishing-resistant authentication method. ([CISA][1])

A useful ranking would be:

1. Password only — weakest
2. Password + SMS/email 2FA — significantly better
3. Password + authenticator-app 2FA — strong, but still phishable
4. Passkey — strong and phishing-resistant
5. Hardware-bound passkey/security key with secure recovery — strongest practical option

The important caveat is recovery. A secure passkey login can be undermined if HF lets someone bypass it through a weak email-reset or account-recovery process. Also, synchronized passkeys depend partly on the security of the user's Apple, Google, Microsoft, or password-manager account.

So I would revise the post's comparison to say:

> Passkeys generally provide stronger protection than passwords with traditional 2FA, particularly against phishing, credential theft, and reused passwords.

FIDO specifically states that passkeys can replace older password-plus-OTP flows while providing phishing- and replay-resistant authentication. ([fidoalliance.org][2])

[1]: https://www.cisa.gov/more-password?utm_source=chatgpt.com "More than a Password | CISA"

[2]: https://fidoalliance.org/passkeys-2/?utm_source=chatgpt.com "Passkeys | FIDO Alliance"

Tha Sneak - July 17, 2026, 3:54 pm

Passkeys are a minimum requirement for most highly sensitive areas such as government, military, law enforcement, company computers, and such it would make sense to utilize it where available especially in this day and age where AI is bringing a host of side effects to include helping to aid those that are well versed to target websites and leak large data tables of credentials, exploits like never before seen, and malware that is more complex than ever.

I would gladly use it and it is better to have and not need that need and not have.

Omniscient - July 17, 2026, 4:06 pm

(Jul 17, 2026 03:54 PM)Tha Sneak Wrote: [\[CITE\]](#) Passkeys are a minimum requirement for most highly sensitive areas such as government, military, law enforcement, company computers, and such it would make sense to utilize it where available especially in this day and age where AI is bringing a host of side effects to include helping to aid those that are well versed to target websites and leak large data tables of credentials, exploits like never before seen, and malware that is more complex than ever.

I would gladly use it and it is better to have and not need that need and not have.

But HF is nowhere near that sensitivity level for security. And we honestly rarely have stolen accounts now that there is 2FA across the internet.

If anything, I am hoping it adds a level of convenience. Lost 2FA's because of device changes is the biggest obstacle currently.

Scrub - July 17, 2026, 4:12 pm

I wouldn't mind either way, anytime I visit I'm already pre logged in, I had enough issues with Authy

when I had got a new phone on my old account lmao

Omniscient - July 17, 2026, 4:16 pm

(Jul 17, 2026 04:12 PM)Scrub Wrote: [\[CITE\]](#) I wouldn't mind either way, anytime I visit I'm already pre logged in, I had enough issues with Authy when I had got a new phone on my old account lmao I like 2FAS, Authy imho is garbage now.

Scrub - July 17, 2026, 4:16 pm

(Jul 17, 2026 04:16 PM)Omniscient Wrote: [\[CITE\]](#) I like 2FAS, Authy imho is garbage now. I don't have much feedback other then if it is implements I'd use it likely.

Jamika - July 17, 2026, 11:53 pm

(Jul 17, 2026 12:34 PM)Charlie Sheen Wrote: [\[CITE\]](#) Just curious your reasoning behind that? They are great to combat phishing. They protect against data breaches. Much more convenient. Most sites are adopting and getting rid of passwords.

As far as I know, it requires a place to store the key. On my phone? There's no way I'd remember where I put it. It would be great on a computer—or for someone who's more organized than I am.

CL1B - July 18, 2026, 3:23 am

I think it's unnecessary right now, perhaps when the user base grows and demand naturally grows it makes sense. I think all time HF's devs have should be going towards making engaging things on HF like the talked about hack games and ddos wars etc.

Basically if it's anything but working on new ways to directly get engagement up I don't think it's worth it in any way.. 2FA holds it place quite nicely.

Omniscient - July 19, 2026, 5:42 pm

(Jul 18, 2026 03:23 AM)MarlboroMan Wrote: [\[CITE\]](#) I think it's unnecessary right now, perhaps when the user base grows and demand naturally grows it makes sense. I think all time HF's devs have should be going towards making engaging things on HF like the talked about hack games and ddos wars etc.

Basically if it's anything but working on new ways to directly get engagement up I don't think it's worth it in any way.. 2FA holds it place quite nicely.

I like that thinking. Focus on engagement.

Will take that to heart.

TB12 - July 19, 2026, 8:32 pm

Would be nice, I use passkeys everywhere I can. 2FA works fine for me though

Snowwy - July 19, 2026, 8:57 pm

I've been using passkeys a lot more recently, basically wherever I can, so if HF makes it available, I'll surely use it.

sweetkins21xx - July 19, 2026, 9:01 pm

I recently just started setting them up on some of my accounts, and ngl they make life easier (not having to open authenticator and waiting for code etc), but I have love-hate thing for passkeys and I don't know why. Sometimes I just don't want them, sometimes I prefer them.

tbh I don't know much about passkeys and how they work, or how secure are they compared to OTP/2FA codes, but I'd say yea add them to HF cuz most modern sites have them.

Omniscient - July 20, 2026, 11:52 am

(Jul 19, 2026 09:01 PM)sweetkins21xx Wrote: [\[CITE\]](#) I recently just started setting them up on some of my accounts, and ngl they make life easier (not having to open authenticator and waiting for code etc), but I have love-hate thing for passkeys and I don't know why. Sometimes I just don't want them, sometimes I prefer them.

tbh I don't know much about passkeys and how they work, or how secure are they compared to OTP/2FA codes, but I'd say yea add them to HF cuz most modern sites have them.

My guess is that we all feel an "ick" from the centralized feeling of passkeys. Windows for example seems to want you to have them in their system. Android devices want them on theirs (Google).

Doing some checking it seems that BitWarden is a decent 3rd party password manager that does support Passkeys.

Skorp - July 20, 2026, 1:22 pm

From a convenience perspective? Yes. From a security perspective? No.

Not for Hackforums at its initial stage (setup) right now. I would understand if 2FA was not doing its purpose on securing accounts, but it is. Maybe after the server move? Especially if you introduce some cool AI features, it would be pretty awesome to have :)

Omniscient - July 20, 2026, 1:44 pm

(Jul 20, 2026 01:22 PM)Skorp Wrote: [\[CITE\]](#) From a convenience perspective? Yes. From a security perspective? No.

Not for Hackforums at its initial stage (setup) right now. I would understand if 2FA was not doing its purpose on securing accounts, but it is. Maybe after the server move? Especially if you introduce some cool AI features, it would be pretty awesome to have :)

I'm in the middle of setting up a Vaultwarden private server (uses BitWarden services). I thought more about it today how many of us don't trust the passwordless passkeys and I believe it's because of 3rd parties like Google and Microsoft are at the center of all your PW's. They appear to be trying to get rid of the possibility of self-custody of passwords with passkeys. You can't write down your passkey on a piece of paper. It's stored digitally in the cloud by Big Tech. I personally consider that untrustworthy.

I'm hoping I can advance my own personal security with Vaultwarden but then also guide others on the process and why it's a good solution.

Skorp - July 20, 2026, 2:07 pm

(Jul 20, 2026 01:44 PM)Omniscient Wrote: [\[CITE\]](#) I'm in the middle of setting up a Vaultwarden private server (uses BitWarden services). I thought more about it today how many of us don't trust the passwordless passkeys and I believe it's because of 3rd parties like Google and Microsoft are at the center of all your PW's. They appear to be trying to get rid of the possibility of self-custody of passwords with passkeys. You can't write down your passkey on a piece of paper. It's stored digitally in the cloud by Big Tech. I personally consider that untrustworthy.

This is exactly the reason why I choose to stay with 2FA on alot of my accounts. It is scary on what the future might be when they have all of our Passkeys and who knows, do whatever they want with them? Yuck. 2FA I have my device right here hehe.

Hopefully you find a solution with Vaultwarden ?

Omniscient - July 20, 2026, 2:42 pm

(Jul 20, 2026 02:07 PM)Skorp Wrote: [\[CITE\]](#) This is exactly the reason why I choose to stay with 2FA

on alot of my accounts. It is scary on what the future might be when they have all of our Passkeys and who knows, do whatever they want with them? Yuck. 2FA I have my device right here hehe.

Hopefully you find a solution with Vaultwarden ?

It's certainly troubling to go from what is a password and 2nd authorization device (2FA) to a single sign-on held by a 3rd party. It's imho a convenience thing more than better security.

Monero-chan - July 20, 2026, 4:07 pm

(Jul 17, 2026 10:55 AM)Omniscient Wrote: [\[CITE\]](#) Should I add them to HF?

Do you use them on websites regularly?

Give me your feedback on this. I'm contemplating it. Probably fairly easy to vibe code the feature into HF.

I've been using 2FA via a YubiKey 5C NFC, I sort of forgot that they support passkeys as well. I should probably should start using passkeys now given that they are better than 2FA. I'm most likely going to hold off on doing that until I get a backup key, since I nearly lost mine numerous times (and Apple accounts actually require 2 separate keys to set up which I didn't know until recently). Probably going to go for the 5C Bio, for the increased security in the off chance someone gets a hold of mine.

(Jul 20, 2026 01:44 PM)Omniscient Wrote: [\[CITE\]](#) I'm in the middle of setting up a Vaultwarden private server (uses BitWarden services). I though more about it today how many of us don't trust the passwordless passkeys and I believe it's because of 3rd parties like Google and Microsoft are at the center of all your PW's. They appear to be trying to get rid of the possibility of self-custody of passwords with passkeys. You can't write down your passkey on a piece of paper. It's stored digitally in the cloud by Big Tech. I personally consider that untrustworthy.

I'm hoping I can advance my own personal security with Vaultwarden but then also guide others on the process and why it's a good solution.

I been using Bitwarden as my password manager for years. Given what they have been going through with the ownership change back in May, It wouldn't be a bad idea to jump ship and switch over to a self-hosted Vaultwarden instance. I was considering switching to KeePassXC but considering the 3rd party clients (especially on iOS) require subscriptions or \$50+ lifetime licenses, I'm probably just going to set up Vaultwarden since I've been already using Bitwarden. Lets hope that they don't touch Vaultwarden if they start Bitwarden behind a paywall.

Mix - July 20, 2026, 4:17 pm

I would use this over 2fa, Much better than messing around with a another device to get into places. Plus IMO its easier to use.

Headspace - July 20, 2026, 5:36 pm

+1 for the option of adding a passkey.

It protects account access and isn't a cumbersome process.

Eran - July 24, 2026, 6:51 am

I don't really use them, but I don't see any reason why not to add them to HF. Perhaps I should start using them generally.