

Forum:[Hack Forums](#)

Thread: [Using Authy Desktop - is it a bad idea?](#)

James Burnham - April 20, 2019, 9:02 pm

I switched to Authy Desktop because it is more convenient than using the mobile app, but I am not sure whether this is a good idea securitywise. What Authy do you use? Mobile or Desktop?

SIM-3257834 - April 20, 2019, 9:24 pm

Mobile because I'd rather have my two devices stay separated. Just in case of unauthorized entry.

PerfectStorm - April 20, 2019, 9:24 pm

I currently use it for my 2FA never had a problem with it. Suggest you use it on phone and desktop incase you lose one.

Dorrance - April 20, 2019, 9:36 pm

I feel if you use desktop you are more vulnerable

PerfectStorm - April 20, 2019, 9:37 pm

(Apr 20, 2019 09:36 PM)Dorrance Wrote: [\[CITE\]](#) I feel if you use desktop you are more vulnerable Why would you assume that? they are both the same concepts.

Dorrance - April 20, 2019, 9:54 pm

(Apr 20, 2019 09:37 PM)PerfectStorm Wrote: [\[CITE\]](#) Why would you assume that? they are both the same concepts.

Both concepts but I have heard stories and almost been one of those victims who had there BTC stoke

PerfectStorm - April 20, 2019, 9:55 pm

(Apr 20, 2019 09:54 PM)Dorrance Wrote: [\[CITE\]](#) Both concepts but I have heard stories and almost been one of those victims who had there BTC stoke

Had your BTC stolen because of authy not working? how do you mean

Dorrance - April 20, 2019, 10:01 pm

(Apr 20, 2019 09:55 PM)PerfectStorm Wrote: [\[CITE\]](#) Had your BTC stolen because of authy not working? how do you mean

Someone almost got into it, is what I'm saying.

PerfectStorm - April 20, 2019, 10:02 pm

(Apr 20, 2019 10:01 PM)Dorrance Wrote: [\[CITE\]](#) Someone almost got into it, is what I'm saying. Hmm close call. I never had that sort of thing happen.

I did have one of those clipboard switchers infected once.

Prince™ - April 20, 2019, 10:03 pm

Mobile imho is the better device in terms of security concerns.

Banana - April 20, 2019, 10:30 pm

use mobile if u want to be more secure otherwise just use desktop

Mr. Robot - April 20, 2019, 10:45 pm

Don't use it on desktop 100% - new windows exploits daily and all it takes is for them to watch.

James Burnham - April 20, 2019, 10:58 pm

Yeah, but I can use a master password to encrypt Authy. Plus, if I were to get ratted, the hacker could just steal the cookies and login anyway.

"If there is local malware on your computer it doesn't really matter whether you are using 2 separate devices to log in with two-factor authentication. To illustrate the threat, let's take a look at the following authentication scenario where the user uses a RSA Hardware Token and see why even in this scenario, two-factor authentication cannot prevent the attacker from gaining access to your account.

Once you successfully log in to a site, your browser locally stores a unique identifier for your session, called a session cookie. This cookie is then used to inform the site on subsequent requests that you have already authenticated, so that the site doesn't ask you to log in again. What this basically means is that there's no point for the malware to steal your credentials or two-factor token when it can simply steal your authenticated sessions."

<https://authy.com/blog/introducing-authy-for-your-personal-computer/>

?Apocalypse - April 20, 2019, 11:04 pm

Just create a virtual machine and use it for the desktop app, if you are concerned about security.

Keep in mind the idea of using authy, you get both mobile and desktop as a backup option.

Bossk - April 21, 2019, 5:51 am

You save maximum 20 seconds doing this, stick to mobile.

int - April 21, 2019, 5:59 am

(Apr 20, 2019 09:24 PM)YouTube Wrote: [CITE](#) Mobile because I'd rather have my two devices stay separated. Just in case of unauthorized entry.

this, someone rdp's into your computer and everything is gg

Disease - April 21, 2019, 3:45 pm

I'm in the mobile-only camp on this one. Separation of concerns.

On all of my devices (desktops, laptops, and phones), I use LastPass to manage my passwords. No two accounts of mine use the same password- ever. And all passwords are 20+ random alphanumerical and special characters, unless a website restricts maximum length (in which case, it'll be maximum length). Because the password manager creates and stores these passwords, and facilitates filling them in (or at least copying them to clipboard upon request), I never need to fill out a password. Thus someone logging everything I type will never see even a username, let alone a password.

LastPass, and many other accounts, are also set up with Multi-Factor Authentication. Run off of my phone, never off of my desktop. Compromise my PC, fine. I'll recover that. But unless you can also compromise my mobile device (because you're never going to get me to fall for providing you an authentication code), you're SOL.

At best, you'll get my LastPass password, as I do have to type that in. But again, I have MFA

enabled, so good luck getting anything out of that. And, as it's a unique password, it's useless for any other accounts I may have.

Unexplained - April 21, 2019, 6:02 pm

(Apr 20, 2019 09:24 PM)YouTube Wrote: [\[CITE\]](#) Mobile because I'd rather have my two devices stay separated. Just in case of unauthorized entry.

This.

I feel if your system has any unauthorized access, the shit is sitting right. All your "keys" to your personal stuff is too easily accessible.

Keep that shit separate and on your mobile device.

(Apr 21, 2019 03:45 PM)Disease Wrote: [\[CITE\]](#) I'm in the mobile-only camp on this one. Separation of concerns.

On all of my devices (desktops, laptops, and phones), I use LastPass to manage my passwords. No two accounts of mine use the same password- ever. And all passwords are 20+ random alphanumerical and special characters, unless a website restricts maximum length (in which case, it'll be maximum length). Because the password manager creates and stores these passwords, and facilitates filling them in (or at least copying them to clipboard upon request), I never need to fill out a password. Thus someone logging everything I type will never see even a username, let alone a password.

LastPass, and many other accounts, are also set up with Multi-Factor Authentication. Run off of my phone, never off of my desktop. Compromise my PC, fine. I'll recover that. But unless you can also compromise my mobile device (because you're never going to get me to fall for providing you an authentication code), you're SOL.

At best, you'll get my LastPass password, as I do have to type that in. But again, I have MFA enabled, so good luck getting anything out of that. And, as it's a unique password, it's useless for any other accounts I may have.

I have yet to dive into something like LastPass. Do you feel its security is good?

I've had people I talked with that have had their shit compromised through one of those password vault services.

Disease - April 21, 2019, 7:01 pm

(Apr 21, 2019 06:02 PM)TheBanker Wrote: [\[CITE\]](#) This.

I feel if your system has any unauthorized access, the shit is sitting right. All your "keys" to your personal stuff is too easily accessible.

Keep that shit separate and on your mobile device.

I have yet to dive into something like LastPass. Do you feel its security is good?

I've had people I talked with that have had their shit compromised through one of those password vault services.

LastPass is very open about the fact that they did, once, experience a security breach. It was fairly well contained, though. In fact, no password data was compromised. And their response to it has only instilled, in me, more confidence in them than ever. They are also very transparent (well, as transparent as can be) with their security model. You can [read it about it yourself](#), and make a judgement call. In short, with their model, your data is (relatively) safe, even if their database was

exposed and dumped. That's due to attackers requiring more than just the data... they need account-level authentication and encryption keys to have a hope's chance at working with the data.

In my opinion- LastPass is exponentially more secure than the common alternatives: storing passwords locally, or only using a small set of passwords across all of your accounts. In fact, I'd go as far as to say it is infinitely more secure than the latter, as that's simply the utter absence of security (and 1 is infinitely more than 0). Unfortunately, the latter is what most people will do. Even here on HF... I did a thread not that long ago, asking about this. And the number of individuals here, at HackForums, that embody the utmost deplorable security practices is astonishing. I'd have thought more people here would be wise to such elementary issues. But alas, ignorance knows no bounds!

Unexplained - April 21, 2019, 7:05 pm

(Apr 21, 2019 07:01 PM)Disease Wrote: [\[CITE\]](#) LastPass is very open about the fact that they did, once, experience a security breach. It was fairly well contained, though. In fact, no password data was compromised. And their response to it has only instilled, in me, more confidence in them than ever. They are also very transparent (well, as transparent as can be) with their security model. You can [read it about it yourself](#), and make a judgement call. In short, with their model, your data is (relatively) safe, even if their database was exposed and dumped. That's due to attackers requiring more than just the data... they need account-level authentication and encryption keys to have a hope's chance at working with the data.

In my opinion- LastPass is exponentially more secure than the common alternatives: storing passwords locally, or only using a small set of passwords across all of your accounts. In fact, I'd go as far as to say it is infinitely more secure than the latter, as that's simply the utter absence of security (and 1 is infinitely more than 0). Unfortunately, the latter is what most people will do. Even here on HF... I did a thread not that long ago, asking about this. And the number of individuals here, at HackForums, that embody the utmost deplorable security practices is astonishing. I'd have thought more people here would be wise to such elementary issues. But alas, ignorance knows no bounds!

Ignorance is bliss, lol...

I appreciate the feedback. I was checking out their services and they have premium stuff, like \$3/mo. Are you using the free version and happy with it?

Disease - April 22, 2019, 2:00 pm

(Apr 21, 2019 07:05 PM)TheBanker Wrote: [\[CITE\]](#) Ignorance is bliss, lol...

I appreciate the feedback. I was checking out their services and they have premium stuff, like \$3/mo. Are you using the free version and happy with it?

You'll be fine with their free platform. I generally upgrade everything I use. But I actually use the free tier of LastPass. Even with it being one of my most valued tools. The premium tier just doesn't provide anything that is a must-have in my opinion. The free tier is full-featured.

ShinyThings - April 22, 2019, 2:09 pm

If you're going to run it on a VM sure... Desktop would probably be easy to use but your phone is probably the safest way.