

Forum:[Hack Forums](#)

Thread: [2FA is an added LAYER of security](#)

minimalist - February 19, 2016, 8:45 pm

This is a problem that's all too common on Hack Forums: members treating the 2FA account protection feature as surefire way to protect their accounts from theft and unwanted misuse. With the events from a month back and some recent occurrences, I thought that everybody should remember that 2FA is just an added layer of security. It does not protect your account against hijackers, and there are probably some things that are wrong with the system.

Your passwords on every site should be different (in an ideal situation), and your usernames should be as well. Either can be generated by yourself or a machine, but god damn...don't make it simple. These steps of caution will aid in protecting against brute force and data leaks, the most common points of failure that I've observed.

So...once again, don't treat 2FA like a system that'll defend your account every time. Because it's not.

Armada - February 19, 2016, 9:00 pm

Agreed.

2FA is added security, but CAN be defeated.

Its not a fail safe 100%, however one of the best tools we got.

Cryptic™ - February 19, 2016, 9:05 pm

Quote:Your passwords on every site should be different (in an ideal situation), and your usernames should be as well. Either can be generated by yourself or a machine, but god damn...don't make it simple. These steps of caution will aid in protecting against brute force and data leaks, the most common points of failure that I've observed.

A lot of ppl tend to use the same or similar passwords for each site because they don't wanna use remember tons of different passwords.

It's best to use software like 1Password or LastPass that store your logins for every site, encrypt it, and you can protect your 1Password/LastPass with 2FA.

<https://lastpass.com/> They have a chrome extension/desktop client/android/iphone client.

If anyone wants a free month of premium PM me. Premium lets you use it on your mobile device.

Light - February 19, 2016, 9:15 pm

(Feb 19, 2016 10:05 PM)Cryptic™ Wrote: [\[CITE\]](#) A lot of ppl tend to use the same or similar passwords for each site because they don't wanna use remember tons of different passwords.

It's best to use software like 1Password or LastPass that store your logins for every site, encrypt it, and you can protect your 1Password/LastPass with 2FA.

<https://lastpass.com/> They have a chrome extension/desktop client/android/iphone client.

If anyone wants a free month of premium PM me. Premium lets you use it on your mobile device. I'm actually paying yearly for their premium service, love it.

Omniscient - February 19, 2016, 9:17 pm

The best security is very very simple.

1. Don't download.
2. Don't visit untrusted links.
3. Use unique passwords on each site that are at least 12 characters with numeric/upper+lower alpha and special characters if the site allows it.

2FA adds to that very simple formula.

Armada - February 19, 2016, 9:18 pm

(Feb 19, 2016 10:05 PM)Cryptic™ Wrote: [\[CITE\]](#) A lot of ppl tend to use the same or similar passwords for each site because they don't wanna use remember tons of different passwords.

It's best to use software like 1Password or LastPass that store your logins for every site, encrypt it, and you can protect your 1Password/LastPass with 2FA.

<https://lastpass.com/> They have a chrome extension/desktop client/andriod/iphone client.

If anyone wants a free month of premium PM me. Premium lets you use it on your mobile device. That is actually a fantastic idea.

Also many AVs offer a Pw safe option. Kaspersky does for sure.

Cryptic™ - February 19, 2016, 9:19 pm

(Feb 19, 2016 10:15 PM)Productivity Wrote: [\[CITE\]](#) I'm actually paying yearly for their premium service, love it.

I've been using LastPass for years. Awesome product.

It's \$12/year. Or if you refer someone, you both get a month free.

For the past 2 years I just post in the small rewards/favors section and pay ppl like \$0.25-\$0.50 cents to use my referral and pretty much get the year for \$6 or less.

Thanks to lastpass my passwords on every site are randomly generated (example '@0mp42O0fNHRg\$ePbWl0') or longer.

Mr Kewl - February 19, 2016, 9:41 pm

(Feb 19, 2016 10:05 PM)Cryptic™ Wrote: [\[CITE\]](#) A lot of ppl tend to use the same or similar passwords for each site because they don't wanna use remember tons of different passwords.

It's best to use software like 1Password or LastPass that store your logins for every site, encrypt it, and you can protect your 1Password/LastPass with 2FA.

<https://lastpass.com/> They have a chrome extension/desktop client/andriod/iphone client.

If anyone wants a free month of premium PM me. Premium lets you use it on your mobile device. There have been cases such sites getting hacked and their Db getting leaked. I'm very skeptical using online tools and resources.

Retribute - February 19, 2016, 10:10 pm

(Feb 19, 2016 10:41 PM)Mr Kewl Wrote: [\[CITE\]](#) There have been cases such sites getting hacked and their Db getting leaked. I'm very skeptical using online tools and resources.I agree. I would never trust sites like that.

Port 22 - February 19, 2016, 10:26 pm

I'd recommend KeePass over LastPass, since KP doesn't connect to the internet at all. They also have a portable version. Also it's free.

\$lick - February 19, 2016, 11:26 pm

(Feb 19, 2016 10:17 PM)Omniscient Wrote: [\[CITE\]](#) The best security is very very simple.

1. Don't download.
2. Don't visit untrusted links.
3. Use unique passwords on each site that are at least 12 characters with numeric/upper+lower alpha and special characters if the site allows it.

2FA adds to that very simple formula.

1. Things can be downloaded without you knowing. (Drivebys/bloatware)
2. Ads and many other things can inject harmful code into websites that are legit.
3. Passwords can be recovered any number of ways. (Most malware tells you which website matches what password)

Any security can be defeated, there is no magic formula to keeping yourself safe.

The real answer is to do everything you can do and then just hope for the best, the harder you make it the less likely it will happen but... it will happen, maybe not to your HF account but to one of your accounts.

Vicellus Drum - February 20, 2016, 12:07 am

(Feb 19, 2016 10:17 PM)Omniscient Wrote: [\[CITE\]](#) The best security is very very simple.

1. Don't download.
2. Don't visit untrusted links.
3. Use unique passwords on each site that are at least 12 characters with numeric/upper+lower alpha and special characters if the site allows it.

2FA adds to that very simple formula.

My dad always said the best firewall/anti-virus was the human brain. Just a bit of logic, and you've got yourself a bulletproof setup.

Armada - February 20, 2016, 4:09 am

(Feb 20, 2016 01:07 AM)Vicellus Drum Wrote: [\[CITE\]](#) My dad always said the best firewall/anti-virus was the human brain. Just a bit of logic, and you've got yourself a bulletproof setup.

My dad claimed the said BS until I gave him a virus to teach him the truth.

Common sense goes a LONG way, but software defensive help greatly.

Even I make mistakes, I can execute a viral binary just as easily as anyone. Id be absolutely fucked without my AV and malwarebytes.

minimalist - February 20, 2016, 4:20 am

Do people really use a third party service to generate passwords for their online accounts? That's a concept that has never really made sense to me - I'll continue with storing passwords in my head.

King Cin - February 20, 2016, 4:26 am

If you're not comfortable with storing passwords on a third-party program, write them down and put them somewhere safe.

Stupid - February 20, 2016, 9:44 am

(Feb 20, 2016 05:20 AM)Minimalist Wrote: [\[CITE\]](#) Do people really use a third party service to generate passwords for their online accounts? That's a concept that has never really made sense to me - I'll continue with storing passwords in my head.

Password Managers also protect you from phishing. They can store passwords you wouldn't be able to remember, protecting you from phishing.

Lastpass may have had a leak, however keep in mind that all user passwords are fully encrypted, just as KeePass. Which one you prefer doesn't really matter, however Lastpass features some very nice apps/programs and automatically syncs your devices. To use your passwords in KeePass you would need to manually sync the password file.

Vicellus Drum - February 20, 2016, 1:33 pm

(Feb 20, 2016 05:09 AM)Armada Wrote: [\[CITE\]](#) My dad claimed the said BS until I gave him a virus to teach him the truth.

Common sense goes a LONG way, but software defensive help greatly.

Even I make mistakes, I can execute a viral binary just as easily as anyone. I'd be absolutely fucked without my AV and malwarebytes.

Logic isn't the only defense mechanism. It's like a shield.

I wouldn't go to war with only a shield.

minimalist - March 13, 2016, 10:22 am

A little more relevant now that email logins are enabled.

Doctor Blue - March 14, 2016, 9:59 am

I know this is an old bump, but I'd like to add to this:

(Feb 19, 2016 10:17 PM)Omniscient Wrote: [\[CITE\]](#) 3. Use unique passwords on each site that are at least 12 characters with numeric/upper+lower alpha and special characters if the site allows it.

If the site doesn't allow it, it's usually because they don't hash your password. Otherwise there's no reason to disallow any of the special characters.

crazyycast13 - March 14, 2016, 11:27 am

(Mar 14, 2016 09:59 AM)Doctor Blue Wrote: [\[CITE\]](#) I know this is an old bump, but I'd like to add to this:

If the site doesn't allow it, it's usually because they don't hash your password. Otherwise there's no reason to disallow any of the special characters.

And I'll add a tip from something that I've learned while talking with my friends in the crypto section.

When you first make a password for a site, randomly generate it based on the rules of the site. Register, log in, log out, and then click on a "forgot your password" link. If for some reason the site sends you back the password you entered, congratz, the site isn't hashing your password. That means if anyone access the login tables or whatever, your password is up for grabs. I made that mistake once, and I never did again.

When you enter a password, it should be hashed server side. The fastest way to figure out if it is not is the above. Also, do not, I repeat, do not, reuse password rules. Once a cracking algorithm finds one, it might find two, and if it finds two, it will find all hashes that followed whatever rule set you made.

Always assume that at some point in time someone will be attempting to crack your hash, and plan

accordingly.

minimalist - April 14, 2016, 3:48 pm

Hey, this has just become relevant once again!

Caliban - April 14, 2016, 4:14 pm

My security tips:

- >Have a good AV (like Avast!) and regularly do Malwarebytes Scans.
- >Must have Plugins: NoScript or Flashcontrol, uBlockOrigin (that Plugin is gold! blocks malicious websites aswell as ads) and optionally Disconnect or something similar.
- >Keep everything updated (JRE etc.)
- >Use complex passwords (except for really useless accounts) and use 2FA on your really important accs.(hf acc, main e-mail, facebook)
- >Dont be friends with shady people
- >Use your brain lol

Thats all i can think of atm.

SwimmingPool - April 14, 2016, 4:19 pm

If people didn't use the same password on every website they signup for and didn't download all of the shitty programs they find online everyone would be a lot more secure.

kevs - April 14, 2016, 4:35 pm

I use KeePassX and have never had any problems with it. Just wrote my master key on a piece of paper.

Yoshikage Kira - April 14, 2016, 4:40 pm

It does not protect your account against hijackers

You're not entirely wrong, but you're not right either.

If a HF member gets their password stolen(ex: through a database dump), and not their 2fa device, the attacker will not be able to login unless they're infected(if that's the case then they can grab the OTP/browser cookies to access the account).