Willow Valley Computer Club

Special Security Edition

January 27, 2023

Is Your Data in LastPass at Risk?

Do you use the LastPass password manager? If so, we recommend that you switch from LastPass to the Bitwarden password manager. Here's why.

In December of 2022, LastPass revealed that all of the approximately 25 million LastPass data vaults were copied by a hacker. The copies are not protected by features that LastPass implemented on their website: limited login attempts or two-factor authentication that a customer may have set up. Instead, the hacker may choose to use as many fast computers to crack the account passwords as he can afford.

Any LastPass account that does not use long, complex, and random passwords may be successfully hacked. Any LastPass account that *reuses* passwords may also be successfully hacked. However, it is impossible to predict when the hacker will hack any of the approximately 25 million LastPass accounts.

Because LastPass did not consistently keep up with best encryption practices, some LastPass accounts were protected by a high iteration count of 100,100 while some were protected by a very low iteration count of 1. You can check your iteration count by logging into your online LastPass account, select Account Settings, click Show Advanced Settings, and inspect the Password Iterations field.

The first table at the end of this article shows how long it would take to crack a password if the iteration count is 1. This table also shows how long it would take to crack a password if the password is *not* long, complex, or random.

The third table at the end of this article shows how long it takes to crack a long, complex, and random password if the iteration count is 100,100.

Bitwarden provides a tool that makes moving from LastPass to Bitwarden convenient. Ensure that your Bitwarden password is long, complex, and random. If your LastPass password was not long, complex, and random or if the LastPass iteration count was low, you should change the passwords for all your accounts after moving to Bitwarden. Ensure that the information in Bitwarden is always up to date.

For additional insight into the LastPass data breach, please see the **Drilling Deeper** on page 2.

Drilling Deeper

What Happened?
In August 2022, LastPass reported a breach by a threat actor who gained access to portions of the password manager's development environment. Although concerning, there was no indication that user data was at risk.

LastPass reported in December 2022 that the August 2022 breach was more serious than initially thought. An Ars Technica article has detail.[i]

Why Is This Breach Concerning?
There are three reasons for concern:

1. The threat actor copied every user's data vault
2. LastPass did not keep up with best encryption practices
3. A user's LastPass master password may not be strong enough to protect the user's data

Each of these concerns is addressed below. In addition, two-factor authentication, which provides additional protection, is addressed.

The Threat Actor Copied Every User's Data Vault
Normally, a user's data vault is protected from multiple log in attempts by LastPass. After eight login attempts, LastPass will not allow another login attempt for five minutes. This forced pause significantly slows down attempts to crack passwords. However, this login attempt protection does not exist for the vaults the threat actor copied. The threat actor may attempt to break the account password as frequently as they wish.

Also, if a LastPass user enabled two-factor authentication, the threat actor would need access to this authentication while attempting to crack the password. However, by copying the LastPass users' data vaults, two-factor authentication is bypassed and the threat actor has unlimited opportunity to try to crack the account (master) password. This means that the user's master password must be strong to resist cracking attempts.

LastPass Did Not Keep Up with Best Practices
LastPass' software is proprietary which means that no one may see how the software works unless they work for LastPass or are invited to view the software. In 2010, LastPass invited Steve Gibson, an information security professional, to review the inner workings of LastPass. After the review, Steve reported that the LastPass encryption practices were current and began promoting and advocating for LastPass.

No users knew that LastPass was not keeping all users up to date with best encryption practices until the details of the breach were released in December, 2022.

Your Password May Not Protect Your Data

There are three reasons why a user's master password may not protect their LastPass data vault. They are:

- The master password is used to protect other accounts as well
- The master password may not protect the user's data
  - The master password's length may be too short and may not have the necessary complexity
  - The master password may not be a randomly generated password

Using two-factor authentication on any account significantly increases account protection because the attacker must not only crack the password but must also find a way to crack the two-factor authentication.

The master password is used to protect other accounts as well

The threat actor can see any unencrypted website address information inside a user's LastPass data vault because LastPass did not encrypt that information. If one of those websites suffered a data breach and the user's password was leaked and that password was also used as the LastPass account password, the threat actor may easily open the user's LastPass data vault. To repeat, this can occur if a password is used for more than one account.

The master password may not protect the user's data

Intuitively, we know that a longer password provides better protection because it is harder to guess the password. A password also needs to be complex. If a password is all numbers, its complexity will increase as lower-case letters are added and increase further as upper-case letters are added. Adding symbols will increase the complexity even further. Intuitively, a long and complex password is more difficult to crack.

However, passwords also need to be random. Studies have shown that humans do not create random passwords. Instead, they tend to choose passwords that other people choose as well. Hackers collect passwords from data breaches and put them into long lists called dictionary lists.

Hackers assume that the password they are attacking will be found in a dictionary list. Only if the password was randomly generated will the hacker need to brute force the password. The longer and more complex a randomly generated password is, the longer it will take for a hacker to brute force the password.

How long does it take to brute force attack a password?

The three tables on pages 6-8 show how long it would take to brute force attack passwords with different lengths and complexities, assuming that the passwords are random and that an RTX 3090 GPU is used to brute force attack the password. The RTX 3090 GPU costs $1,903.54 on Amazon and is installed in a personal computer.

The third table shows the time to crack a password if the PBKDF2 hash method is used. This is the hash method used by LastPass – but the table assumes that 100,100 iterations are used while LastPass used only 1 iteration for some users. For 100,100 iterations, that table shows that a 10-character lower-case letters password would require 1 year to crack if an RTX 3090 GPU were used. Amazon Web Services offers a machine which is significantly faster. For the same password, the AWS machine would require 33 days. For an iteration of 1, the password would be cracked almost instantly. Faster machines are available.

If an attacker knows the hash of the password, the type of hash, and the number of hash iterations, then the time required to crack the password is determined by how much the attacker is willing to spend to do so. It does not mean that the attacker can successfully attack any password in a reasonable amount of time but this is why a short LastPass account password can be serious.

How do I generate a random password?
Here are three ways to generate a random password:

- Roll dice – see https://theworld.com/~reinhold/diceware.html for an explanation and https://diceware.dmuth.org/ for a practical way to roll the dice
- Use a password manager to generate a random password – see the user guide for the manager
- Use the password generator at https://generatepasswords.org/ to generate a password or a passphrase

The passwords will be random. It is important that you select long passwords. It is also important that you include lower-case letters, upper-case letters, numbers, and symbols when generating a password.

What is two-factor authentication and how do I use it?
Two-factor authentication means that you use two factors - something that you know (a password) and something you have (see below) – to log into an account. It is very difficult for an attacker to know your password and also have access to something you have. The something you have factor is typically implemented in one of three ways:

1. You receive a multiple digit code either by text message or email and enter it into an online form
2. You read a multiple digit code on a software authenticator (Authy, Google Authenticator, etc.) and enter the code into an online form
3. You use a hardware key which contains information that proves that you are authorized to log in

The best way to use two-factor authentication is to consult with the support team for the website account you want to protect.

What are information security professionals doing?
Because LastPass did not continue to use best encryption practices, many information security professionals are leaving LastPass and switching to different password managers. Steve Gibson is one of the professionals leaving LastPass.

What should I do?

Many Computer Club members are uncertain about what products they should use to protect their data. Some want a recommendation; some want advice and some want a suggestion. For them, we identify products that we assess to be the best of the currently available products. We also offer training to use those products.

We recommended LastPass approximately 12 years ago. We think it is best to leave LastPass, even if your LastPass account had 100,100 iterations and a strong password, because LastPass has not kept up with best encryption practices for all their customers. This is the first time in 12 years we have changed a recommendation.

If you are currently using a password management system such as NordPass, iCloud Keychain, Keeper, Dashlane, or others, you should continue to do so. We are not aware of any reports of problems with those managers.

There are two password managers that many information security professionals have chosen while leaving LastPass: 1Password and Bitwarden. These password managers are very similar technically. Bitwarden offers a free account as well as paid accounts while 1Password offers only paid accounts.

Bitwarden is open-source while 1Password is not. This means that anyone can review the Bitwarden software while only employees and invitees can review the 1Password software.

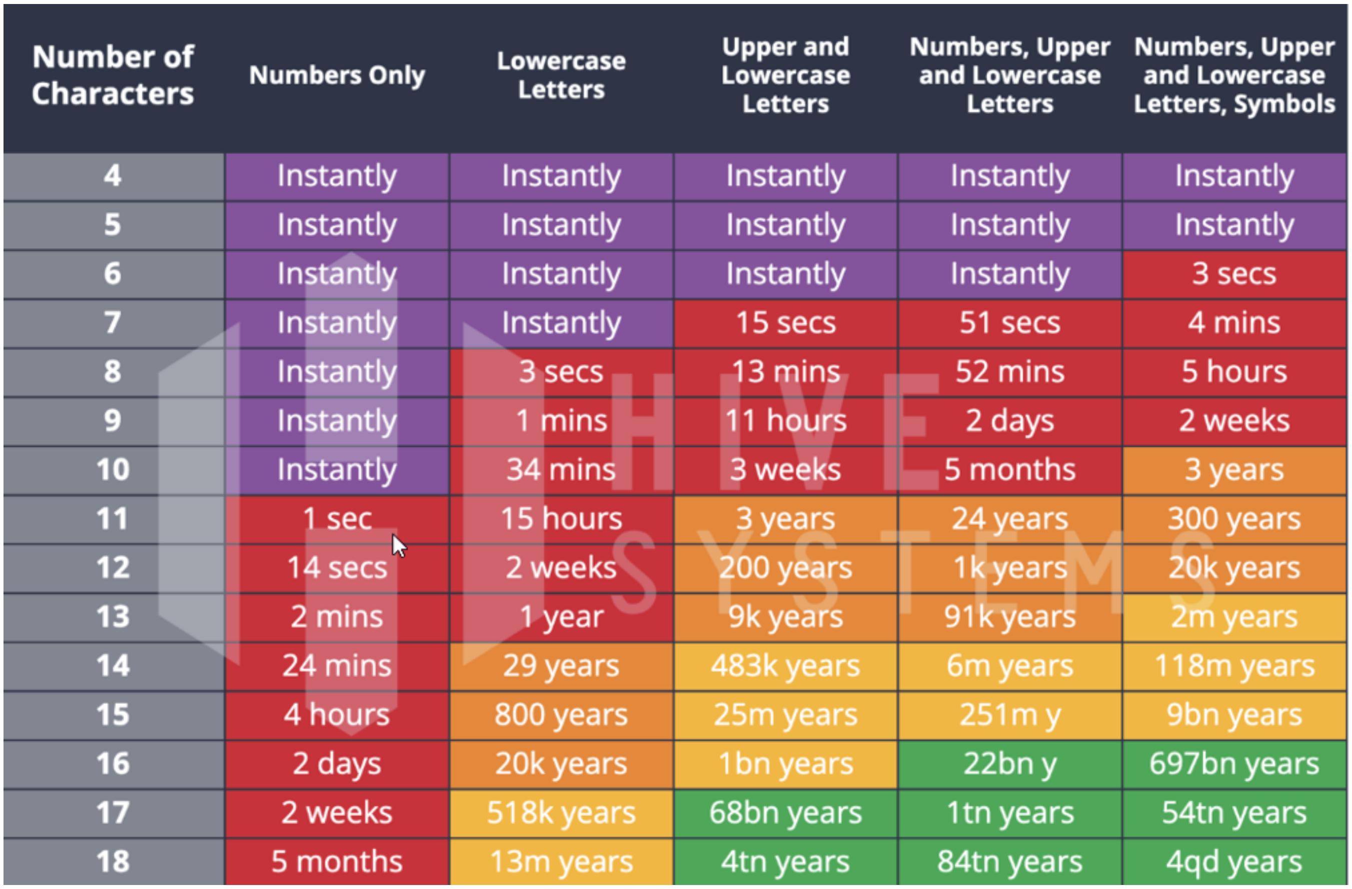
Because Bitwarden is open-source, it is our choice for a password manager.

It may seem daunting to move from one password manager to another but today’s password managers have tools to move existing password vaults to their vaults. Those tools greatly simplify the process.

Below are three tables that show how long it takes to crack a password.

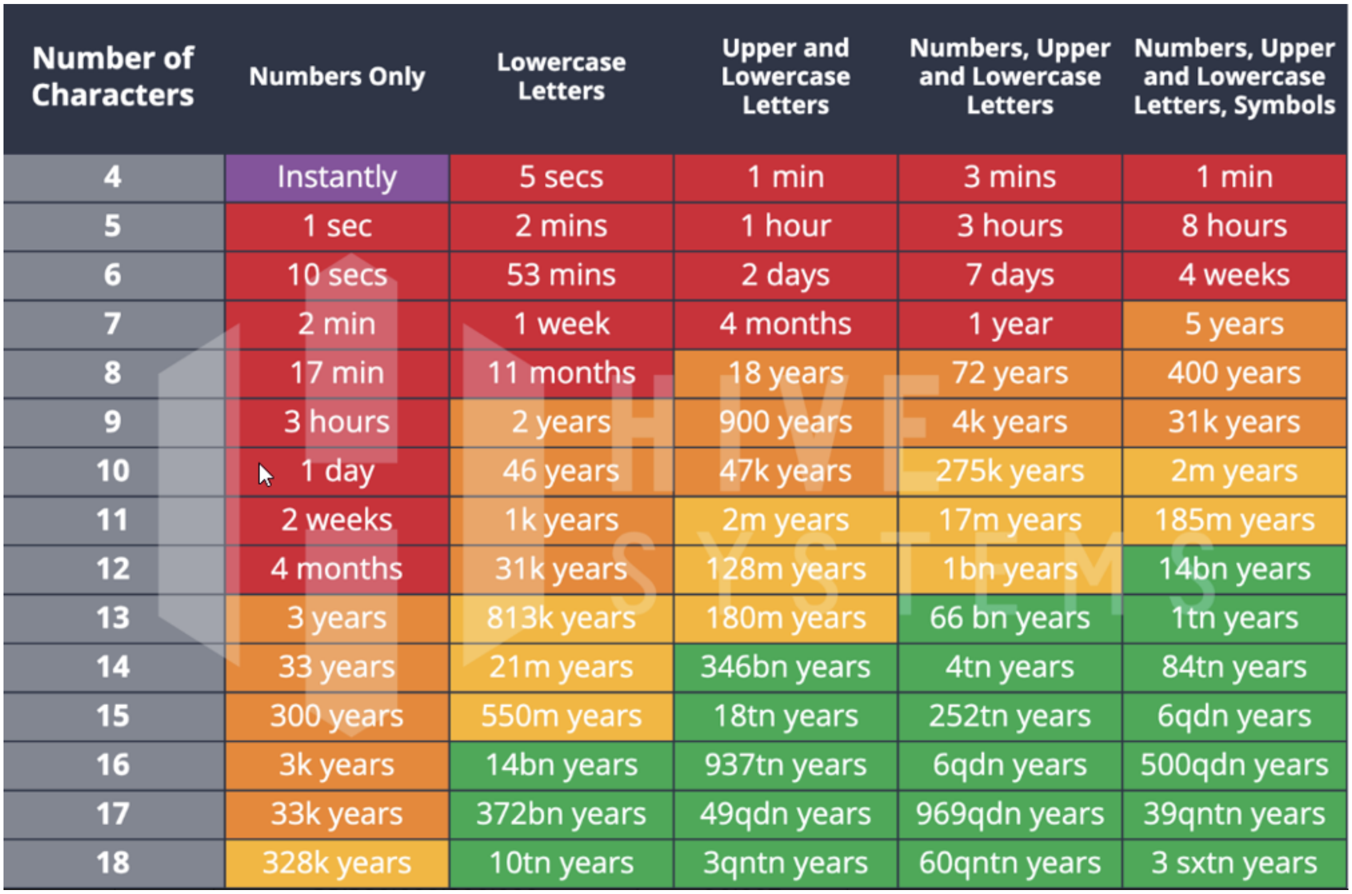
Times to crack a password that uses different hash methods while using an RTX 3090 GPU

The below figure shows the time required to crack a password using an RTX 3090 GPU if the website uses the MD5 hash method. This is the simplest method. Source: hivesystems.io



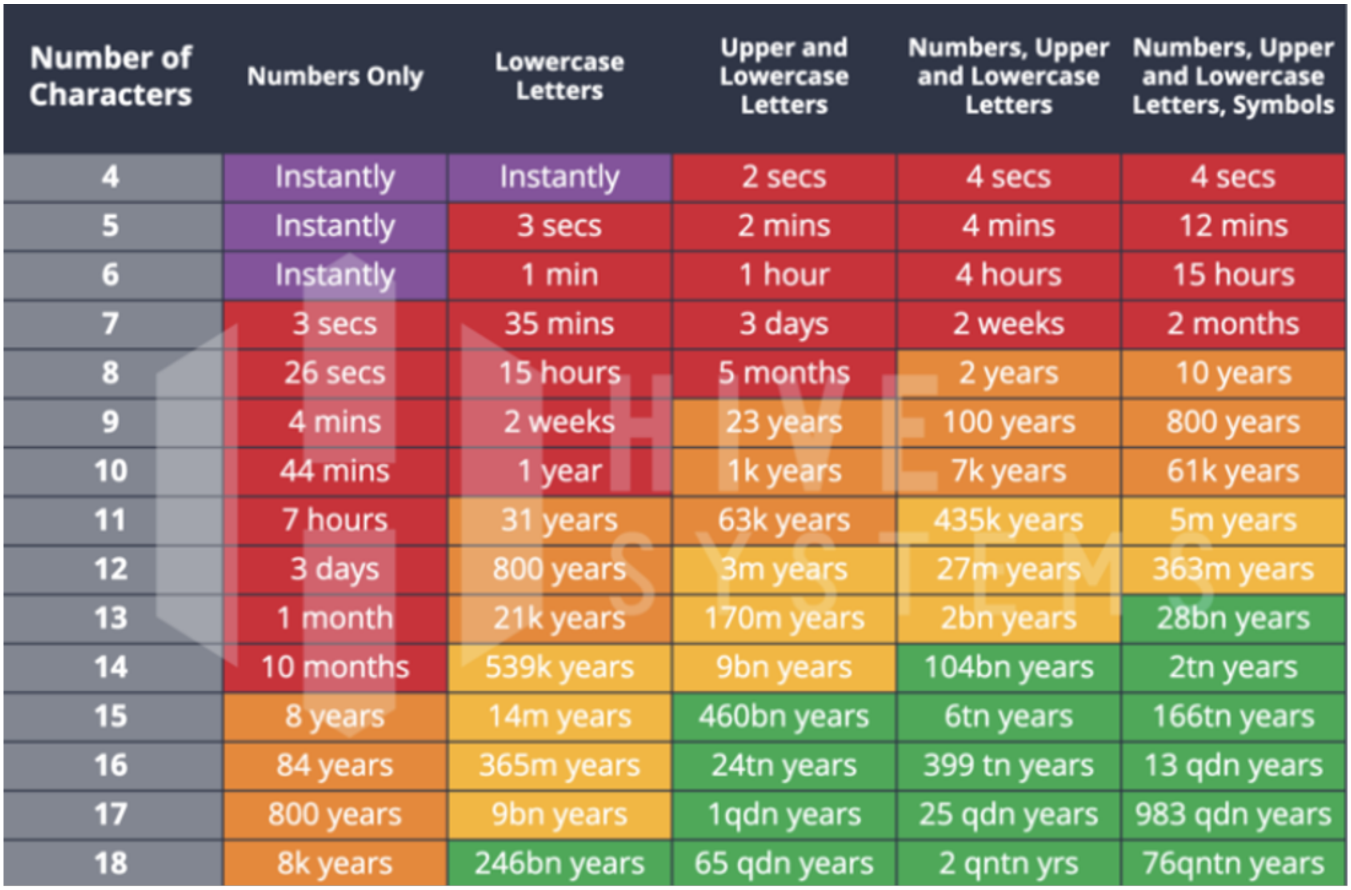
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	3 secs
7	Instantly	Instantly	15 secs	51 secs	4 mins
8	Instantly	3 secs	13 mins	52 mins	5 hours
9	Instantly	1 mins	11 hours	2 days	2 weeks
10	Instantly	34 mins	3 weeks	5 months	3 years
11	1 sec	15 hours	3 years	24 years	300 years
12	14 secs	2 weeks	200 years	1k years	20k years
13	2 mins	1 year	9k years	91k years	2m years
14	24 mins	29 years	483k years	6m years	118m years
15	4 hours	800 years	25m years	251m y	9bn years
16	2 days	20k years	1bn years	22bn y	697bn years
17	2 weeks	518k years	68bn years	1tn years	54tn years
18	5 months	13m years	4tn years	84tn years	4qd years

The below figure shows the time required to crack a password using an RTX 3090 GPU if the website uses the bcrypt hash method. This is an intermediate method. Source: hivesystems.io



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	5 secs	1 min	3 mins	1 min
5	1 sec	2 mins	1 hour	3 hours	8 hours
6	10 secs	53 mins	2 days	7 days	4 weeks
7	2 min	1 week	4 months	1 year	5 years
8	17 min	11 months	18 years	72 years	400 years
9	3 hours	2 years	900 years	4k years	31k years
10	1 day	46 years	47k years	275k years	2m years
11	2 weeks	1k years	2m years	17m years	185m years
12	4 months	31k years	128m years	1bn years	14bn years
13	3 years	813k years	180m years	66 bn years	1tn years
14	33 years	21m years	346bn years	4tn years	84tn years
15	300 years	550m years	18tn years	252tn years	6qdn years
16	3k years	14bn years	937tn years	6qdn years	500qdn years
17	33k years	372bn years	49qdn years	969qdn years	39qntn years
18	328k years	10tn years	3qntn years	60qntn years	3 sxtn years

The below figure shows the time required to crack a password using an RTX 3090 GPU if the website uses the PBKDF2 hash method. This is the current best practice method. Source: hivesystems.io



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	2 secs	4 secs	4 secs
5	Instantly	3 secs	2 mins	4 mins	12 mins
6	Instantly	1 min	1 hour	4 hours	15 hours
7	3 secs	35 mins	3 days	2 weeks	2 months
8	26 secs	15 hours	5 months	2 years	10 years
9	4 mins	2 weeks	23 years	100 years	800 years
10	44 mins	1 year	1k years	7k years	61k years
11	7 hours	31 years	63k years	435k years	5m years
12	3 days	800 years	3m years	27m years	363m years
13	1 month	21k years	170m years	2bn years	28bn years
14	10 months	539k years	9bn years	104bn years	2tn years
15	8 years	14m years	460bn years	6tn years	166tn years
16	84 years	365m years	24tn years	399 tn years	13 qdn years
17	800 years	9bn years	1qdn years	25 qdn years	983 qdn years
18	8k years	246bn years	65 qdn years	2 qntn yrs	76qntn years

[1] *LastPass users: Your info and password vault data are now in hackers' hands*, Ars Technica, 12/22,2022, https://arstechnica.com/information-technology/2022/12/lastpass-says-hackers-have-obtained-vault-data-and-a-wealth-of-customer-info/