# How Secure Is My Password?


## *7 Keys to Effective Passwords*

by FrameWork IT Services

**PRINT THIS PAGE AND KEEP IT CLOSE TO YOUR COMPUTER**



# The Shocking Truth Behind Password Security

**90%**

of employee passwords are crackable within 6 hours.

**65%**

of people use the same password everywhere.

**47%**

of corporate knowledge workers report a productivity drain due to password management.

**7%**

of users use password managers, while 57% memorize their passwords, 11% write them down, and 25% allow their browsers to save them.

**38%**

of knowledge workers share access to web apps and services.

**30%**

of adults have more than 10 passwords to keep track of.

**51%**

of users change their password only when they forget it. 20% only reset when they hear about a hack in the news.

**49%**

of ex-employees actually logged into ex-employer accounts after leaving the company.

# How Secure Is My Password?

## 1. Begin By Using A Password Manager

Making use of a password management platform will provide a number of benefits, including:

- auto-generating strong passwords for you,
- storing them in an encrypted central location,
- syncing passwords across multiple devices and
- the ability to create links to the services you use with a quick copy/paste tool so you don't even have to type the password out (or remember it).

The best part? You only need to remember the one master password…just don't lose it!

There are several good Password Manager services available. Some store your data in the cloud and others offer an "offline" version if your concerned about the safety of your data in the cloud. At the end of this list you'll find some of the password managers you will want to check out. They're effective and you won't be disappointed - check them out!

| | |
|---|---|
| "abcdefg" (7 characters) | Less Than One Second |
| "abcdefgh" (8 characters) | 31 Minutes, 52 Seconds |
| "abcdefghi" (9 characters) | 31 Minutes, 52 Seconds |
| "abcdefghij" (10 characters) | 13 Hours, 48 Minutes |
| "abcdefghijk" (11 characters) | 14 Days, 23 Hours |
| "abcdefghijK" (11 characters, 1 capital) | 85 Years, 1 Month |
| "La7tuh23!" (9 characters, mixed) | 6 Years, 5 Months |

*Amount Of Time to Crack A Password*

## 2. Make Your Password Long

Make sure you password is 8 characters as a minimum (recommend 12 as a minimum). Every character you add after the first "8" increases the time it takes to crack the password **exponentially**.

Mix things up with upper/lower case, a number or symbol and your results will be drastically improved. The table below does a great job of illustrating just how impactful simple changes can be to your password security against the average brute force attack.

The examples in the table above are sequential (bad idea), but as you can see a random mixture of characters in a 9-character password is significantly stronger than the simple sequential 9-character example. Simply changing the last character to a capital in the 11 character example had an enormous impact on the password strength.

## 3. Nonsense Is Your Friend

Long passwords are good, but not good enough on their own.

Two of the most popular methods of cracking a password are commonly called "Brute Force" and "Dictionary" attacks, and they work pretty much as you would expect given their names.

A brute force attack continuously tries different credentials using essentially every character combination possible. It does this until it lands on the correct password, the attacker decides to change tactics, or they move onto the next target.

A dictionary attack is similar in that it attempts to discover the password by using common dictionary words, along with words that have been added to the "dictionary" list such as common passwords used by others (e.g. password1234, princess, iloveyou, etc.).

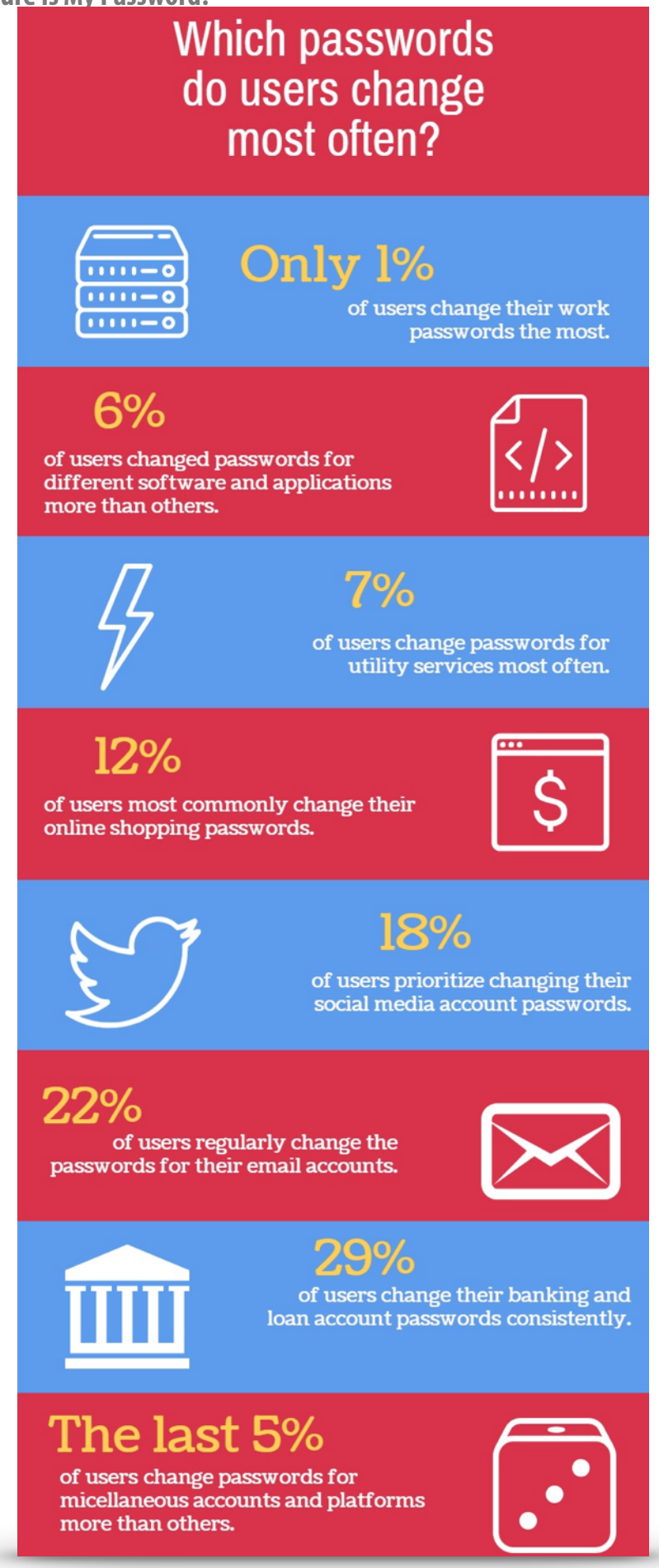
As technology has improved, attackers haven't missed an opportunity to include that new technology in their arsenal. Through AI and machine learning, some attacks are smart enough to recognize a potential phrase because the algorithms have picked up on a pattern. Don't give them what they're expecting!

The phrase "Wall purple curb" wouldn’t be great because those are all easily recognized words, but the random nature of the phrase makes it more difficult to crack as opposed to "That purple house".

Substituting number or symbols will help boost the strength, but the same rule applies here - don't give them what they expect. To

explain, don't boost the strength of your random phrase "Wall purple curb" by changing the "a" in Wall to an "@", or the 'e' in purple to a 3...that's expected.

Find a way that makes sense to you (and that you can easily remember) to shift things slightly, that one little change could have exponential benefit to your password security. So, DO use numbers and symbols, just try to AVOID the familiar/expected and STAY AWAY from anything sequential on your keyboard (H@use1234 isn't great simply because of the sequential numbers at the end).



## 4. Do Not Reuse Passwords


Changing a number or symbol variation on an otherwise identical password isn't an ideal approach to security due to the fact that many people do that exact same thing.

When you take a trip to the beach, do you put your wallet and other valuables in your shoes to conceal them? That behavior is so common that most common thieves might think to look first. Security is all about doing things that most criminals would NOT expect you to do.

This is one instance where the value of a password manager really becomes apparent, since it'll securely store and remember all of your various credentials. There are circumstances where using the same password in multiple places may not really have much of an impact, particularly when your personal information isn't stored on those platforms, but the danger is still present even then. Your password to something like the "Kite Flying Club" may not seem critical, but if an attacker leveraged that information to attack somebody that you associate yourself with... you get the idea.

Finally, it seems that you hear about a major company or website experiencing a data breach that exposed not only sensitive personal

information, but usernames, emails, and passwords as well. If your information is a part of one of those breaches, you can count on the bad guys trying those credentials against all of the most common and most popular platforms out there. A majority of phishing attacks are conducted using information that is publicly available or has been leaked in a data breach!

## 5. Do Not Use Personal Information

We know it makes it easier to remember if you use your dog's name, relatives birthdate, old street number, favorite car, etc., but it only serves to make you an easy target. Unless you've managed to stay off the "grid" all these years, much of that information is already floating around in cyberspace and may have even been shared by you on social media.

## 6. Keep Them Fresh

At the minimum, change them at least every 180 days or every 6 months. The higher the frequency, the safer you will be!

Most people avoid changing their passwords on a regular basis because they already feel overloaded with the sheer number of passwords they have to juggle, and changing them would make it completely impossible to remember them for any significant length of time. Again, this is another instance in which a password manager comes in handy!

Regularly changing passwords can also help mitigate the risk you face in

the scenario described above where your logon information is leaked at the source when those companies experience a breach.

## 7. Keep Them Secret, Keep Them Safe

Avoid sharing your passwords with others, even someone you know that you can trust, such as family members. What if they have trouble remembering it and write it down somewhere without letting you know? Or they share it with another trusted individual who then writes it down? Once it is out of your "hands", it is out of your control.

You can see where this relates to some other items in this list, such as reusing the same password across multiple sites/ services. If you used the same password everywhere you would be sharing the key to your whole digital life, not just that one place. If you find yourself in a situation where you must share a password for any reason, make sure to get it changed immediately after they no longer need access.

Also, you should avoid writing your username and passwords down. Like the wallet in your shoe, those looking for your

information already know the usual places - sticky notes on your monitor, under your mousepad or keyboard, etc. Not all bad actors are coming from the Internet.

If you've realized how valuable a password manager can be but are concerned you can't remember the master password without writing it down, at least make sure to keep the written note in a secure location such as your wallet, home fire safe or locked file cabinet.

***To view a list of recommended and trusted sources for managing your passwords and online security, please visit this page:***

ismypasswordajoke.com/tools

***Signup for our For Our FREE Secure My Business from Cyber Threats Webinar:***

*ismypasswordajoke.com/webinar*