10 Bad Password Habits You Need to Break

We've all got dozens of accounts spread around the web that require a username and password. You probably understand the importance of a solid password, but everyone's definition of "secure" is a little different. Let's make sure you haven't fallen victim to some common bad password habits.

Insecure Password Storage

A password is something you likely need to use often, so it's natural to make it something that will be easy to remember. That's why many people use birthdays and other personal information in their passwords. However, this is one of the worst things you can do.

The truth is a lot of this "personal" information is not so personal. It wouldn't be hard for someone who *really* wants to hack your account to find your birthday, middle name, child's name, or home address. This even applies to the names of famous people. Any password that is a real word, name, or

anything else that exists in the world is inherently easier to crack with software.

Using a "Keyboard Walking" Password

WPEngine

Even seemingly "random" strings of letters and text can be easily figured out if you're not careful. "Keyboard Walking" is one form of creating passwords that is much more common than you might think. This is when people use letters, numbers, and symbols that are next to each other on a keyboard.

The idea is if you use a string of keys that are next to each other on the keyboard, you'll create a random password that is still easy to remember. The problem is a lot of people have this same idea, and it's very easy for cracking software to go through all possible keyboard walking combinations.

Reusing the Same Passwords Everywhere

The previous habits get even worse if you use those same insecure passwords in multiple places. Again, you probably need passwords in a dozen or more places, so it's perfectly natural to want only one password to remember. But that's a very bad idea.

If someone cracks your password in one place, the logical next step would be to try that very same password in other places. You're making it very easy for someone to get inside all of your accounts with minimal effort.

Insecure Password Storage

Maybe the previous habits are old news, and you've already been creating strong passwords for each individual website. But that brings up a new problem—how do you keep track of passwords that are explicitly designed to be hard to remember?

What you *shouldn't* do is put them in a spreadsheet, email them to yourself, or keep them in a text file. It's a similar situation to using the same password everywhere. If someone were to ever get into these "safe" storage places, they'd essentially have the keys to your kingdom.

Not Using a Password Generator or Manager

Justin Duino / How-To Geek

There are two readily available things you may not be using that can drastically improve your passwords. First, a password generator, which is exactly what it sounds like—a tool that creates passwords. These passwords are much, much more secure than anything you can think up.

The problem with generated passwords is they're impossible to remember, and we already talked about why it's a bad idea to store passwords in a spreadsheet or text file. The solution is a password manager, which securely keeps track of your passwords for you. Some password managers even work as password generators themselves.

Now, you may be thinking a password manager is no different than a spreadsheet. If someone gains access to your password manager, they'd have all your passwords. Password managers require one "Master Password" to access the passwords. That means you only have one password to remember, and it should be stored in a safe offline place.

Skipping Multi-Factor Authentication

More and more services are supporting various forms of multi-factor authentication—commonly "two-factor authentication." A simple username and password combo is the first layer of defense; adding an extra layer (or two) is considered "multi-factor authentication," and you should stop avoiding it.

A common example of multi-factor authentication is using a phone number for confirmation after signing into a website. After you successfully enter your username and password, an automated text is sent to your phone with a PIN. You have to enter that PIN to fully sign in. The idea is if someone were to get your password, they'd also need your phone number to gain access—which is more difficult.

Phone numbers aren't actually the best method for two-factor authentication, though. Apps like Google Authenticator and Authy are much harder to crack than phone numbers.

Never Updating Old Passwords

Using insecure passwords is bad enough, but sticking with them for years on end is even worse. Sadly, data breaches have become a common thing. When it happens to a website that you have an account with, your username and password are out there for anyone to grab.

Changing your passwords regularly makes that leaked information outdated. If a website tells you a data breach has happened, you should absolutely take the time to change your password. You can also use "Have I Been Pwned?" to see if your information has been leaked.

Using Passwords Instead of Passkeys

The thing about passwords is most of the problems are due to the people who create them. Using a password in the first place might be the biggest mistake you're making. Passkeys are the future of passwords, and you should use them whenever you can.

A passkey is more like unlocking your phone than entering a username and password. For example, your Facebook password is used anywhere you can access the Facebook website or app. A passkey, on the other hand, is tied to the device it was created on.

So, let's say you were using a passkey for Facebook, and you wanted to sign into the website on your computer. Instead of entering your username and password, you'd scan a QR code from your phone and then unlock your phone to sign into Facebook. Your phone is the "password," and no one can get in without it.

The good news is there are solutions for every bad password habit out there. The bad news is it's up to you to use them. Thankfully, tools like password managers and passkeys make the process much simpler and more secure than trying to do things on your own.