Password Management Best Practices - Tips for Selecting and Managing Your Passwords

Reports of cybersecurity breaches have saturated the news and media. Every day, we wake up, shake our heads over reports of another data breach, and get on with our day. A quick analysis reveals that the common denominator across most data breaches is a compromised password.

This is why selecting and managing strong passwords is the cornerstone of modern-day cybersecurity. It could be the difference between keeping your account safe and a data breach. This isn't to say that your password is the only security measure you can optimize, but it is definitely a bigger piece of the puzzle.

Most people are sloppy with password selection, often picking passwords that are easy to remember and guess. We reuse them repeatedly across multiple applications. It's time to fine-tune our password management strategy.

Best Password Practices

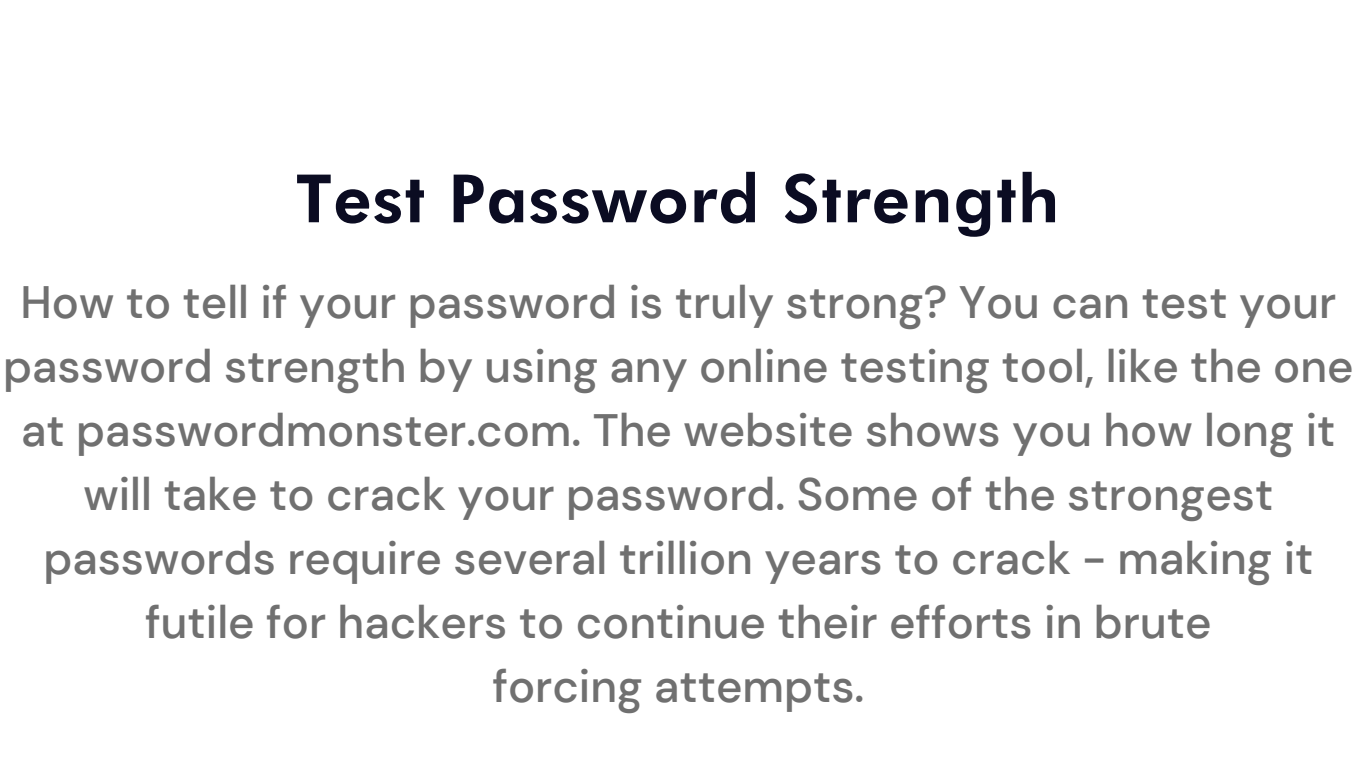
Create a Long Password

A longer password is more difficult for hackers to break into. These passwords are usually greater than eight characters and utilize a mixture of upper and lowercase letters, symbols, and numbers. For obvious reasons, the password should not be easy to guess. So, for example, the password shouldn't be based on your birthday, pet's name, mother's name, or the name of your first school.

And if you really want to give hackers a hard time cracking your password, then create a passphrase up to 64 characters long. You can do this with the help of a password generator.

Encrypt Your Passwords

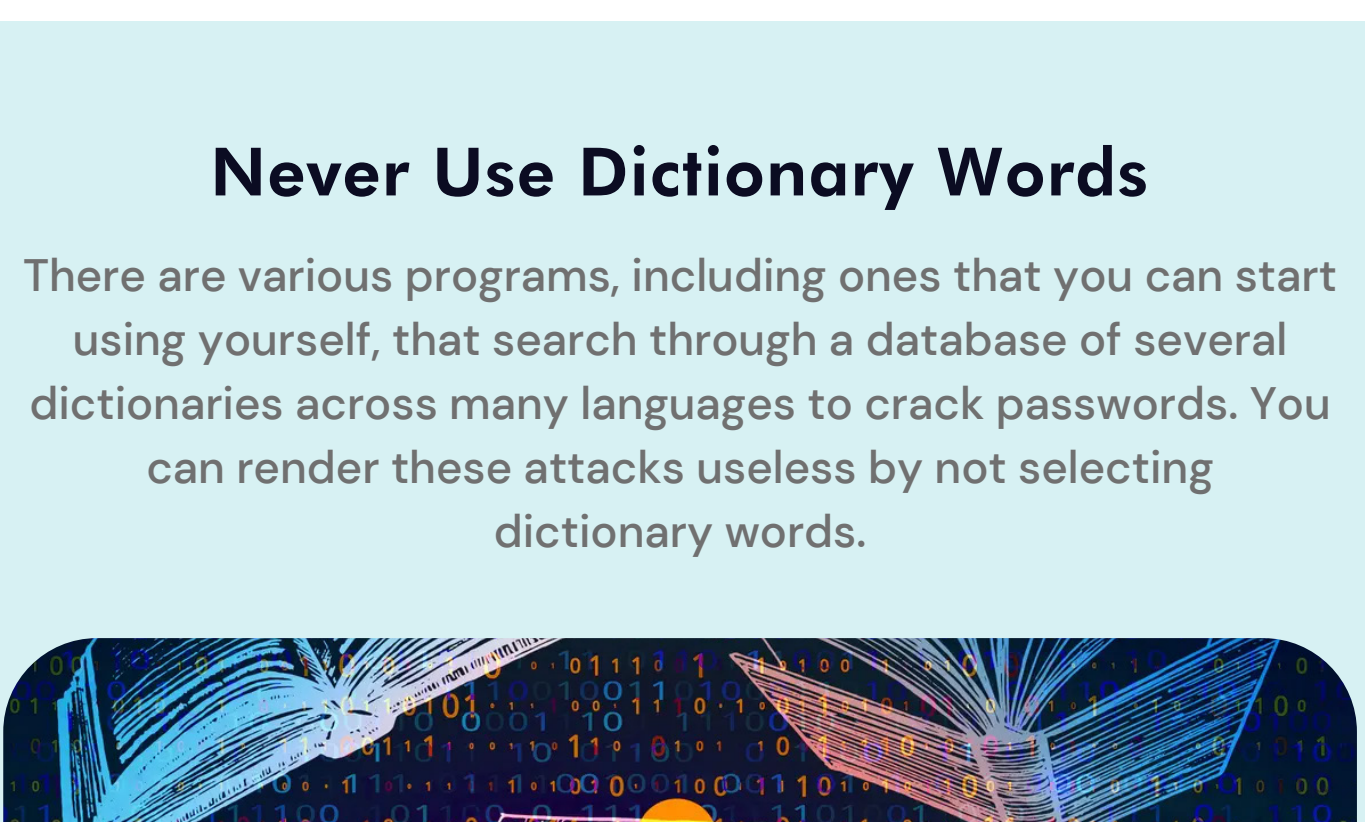
Hackers know that your account is protected by a strong password. Their goal may be to steal the password through MiTM attacks or social engineering attacks. This is why you should encrypt your passwords so that hackers cannot read them. Password encryption is especially important if you are sending them through emails or storing them in a USB drive for later retrieval.



Test Password Strength

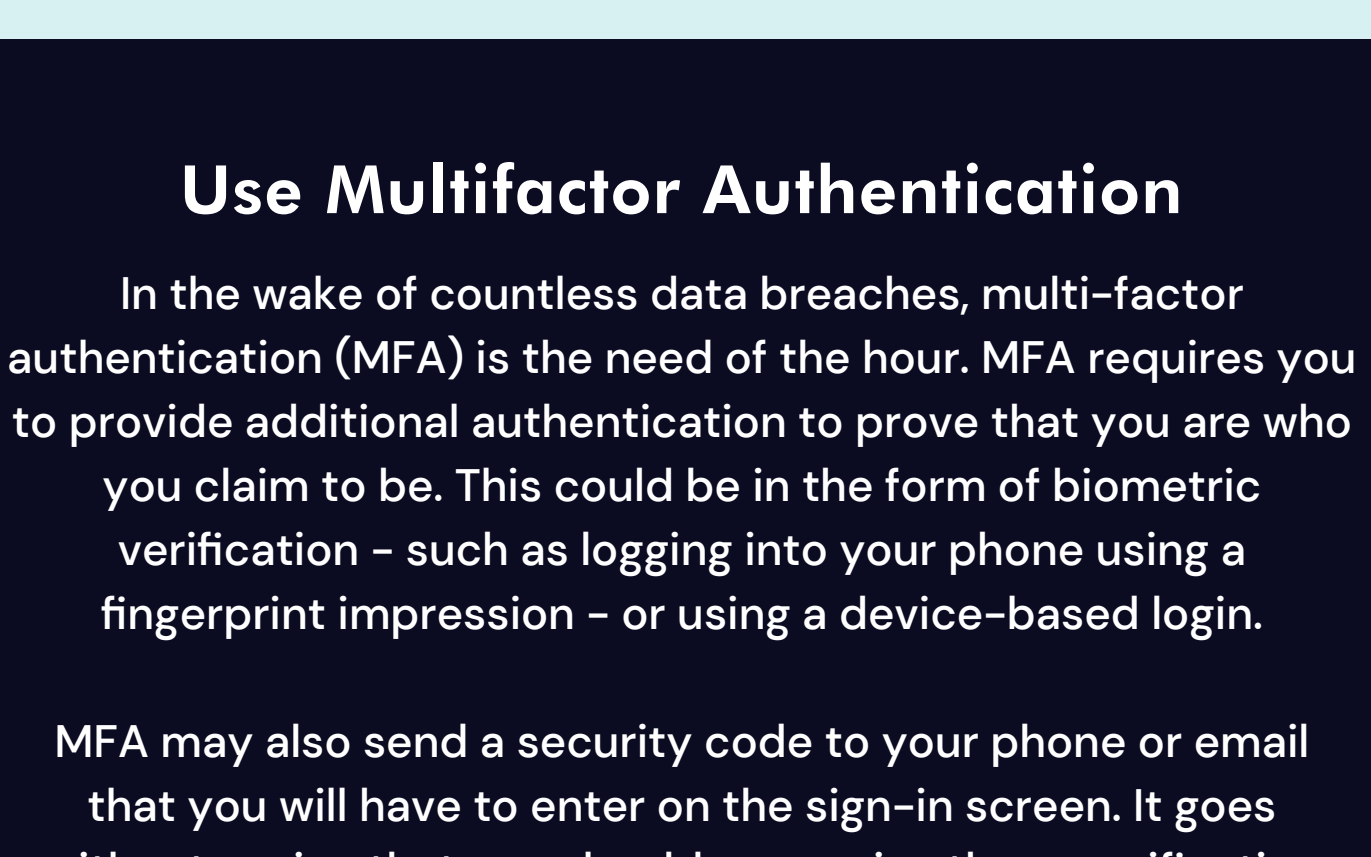
How to tell if your password is truly strong? You can test your password strength by using any online testing tool, like the one at passwordmonster.com. The website shows you how long it will take to crack your password. Some of the strongest passwords require several trillion years to crack – making it futile for hackers to continue their efforts in brute forcing attempts.

Remember, if your password is easy to crack in the span of a few hours, then it's time to change it before someone cracks it open!



Never Use Dictionary Words

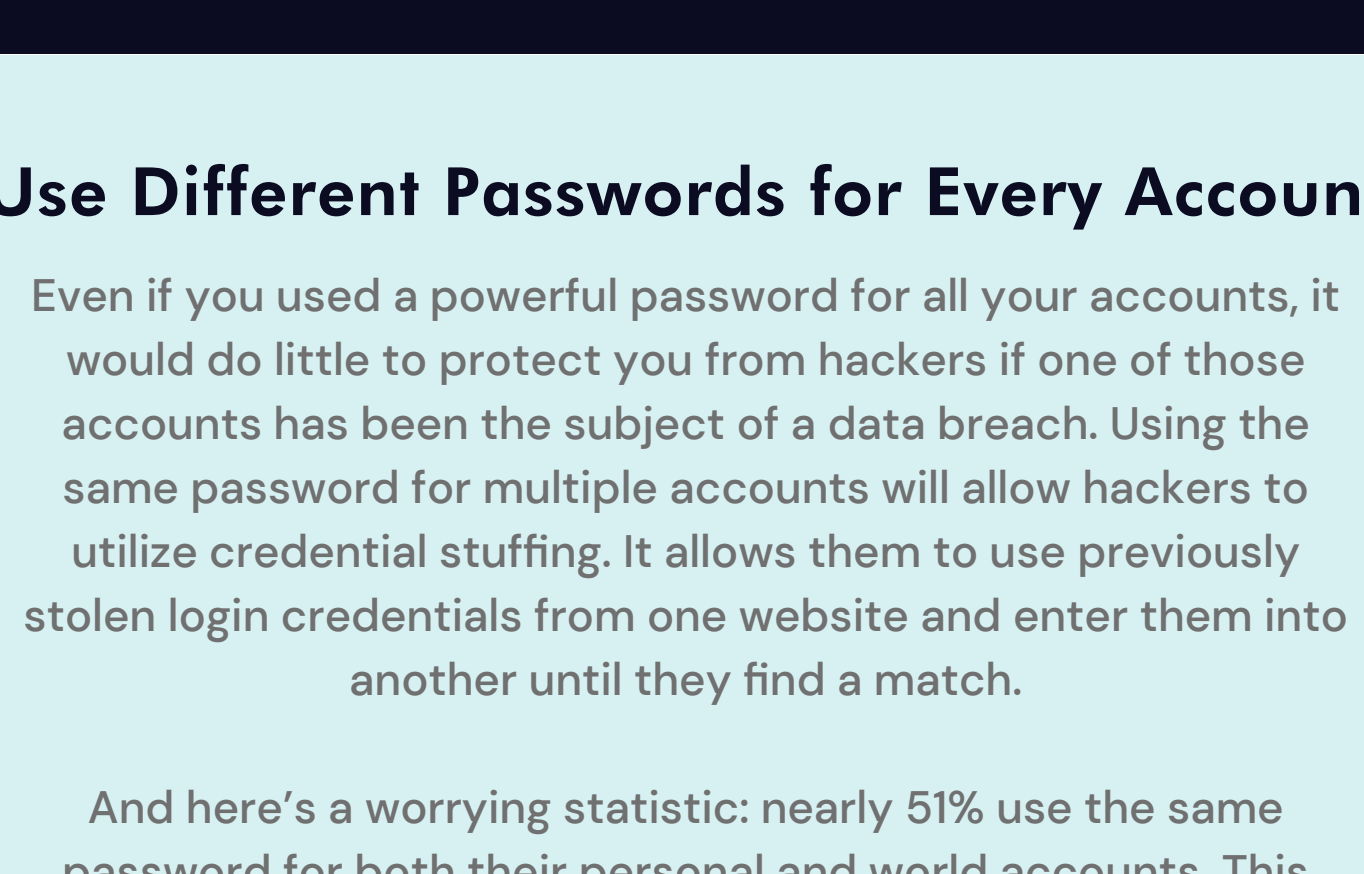
There are various programs, including ones that you can start using yourself, that search through a database of several dictionaries across many languages to crack passwords. You can render these attacks useless by not selecting dictionary words.



Use Multifactor Authentication

In the wake of countless data breaches, multi-factor authentication (MFA) is the need of the hour. MFA requires you to provide additional authentication to prove that you are who you claim to be. This could be in the form of biometric verification – such as logging into your phone using a fingerprint impression – or using a device-based login.

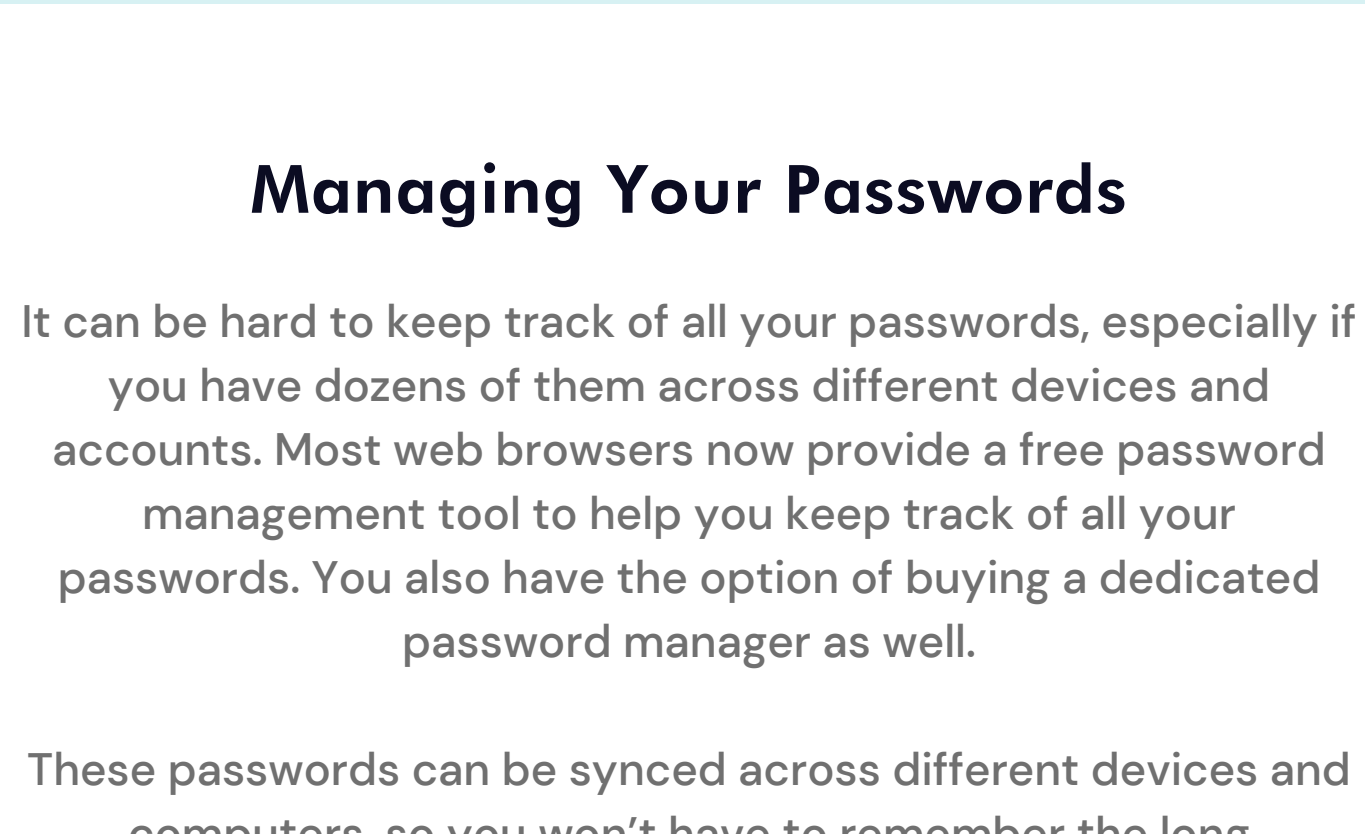
MFA may also send a security code to your phone or email that you will have to enter on the sign-in screen. It goes without saying that you should never give these verification codes to anyone!



Use Different Passwords for Every Account

Even if you used a powerful password for all your accounts, it would do little to protect you from hackers if one of those accounts has been the subject of a data breach. Using the same password for multiple accounts will allow hackers to utilize credential stuffing. It allows them to use previously stolen login credentials from one website and enter them into another until they find a match.

And here's a worrying statistic: nearly 51% use the same password for both their personal and world accounts. This makes hacking attacks incredibly easy, especially if the password was obtained by a phishing attack.

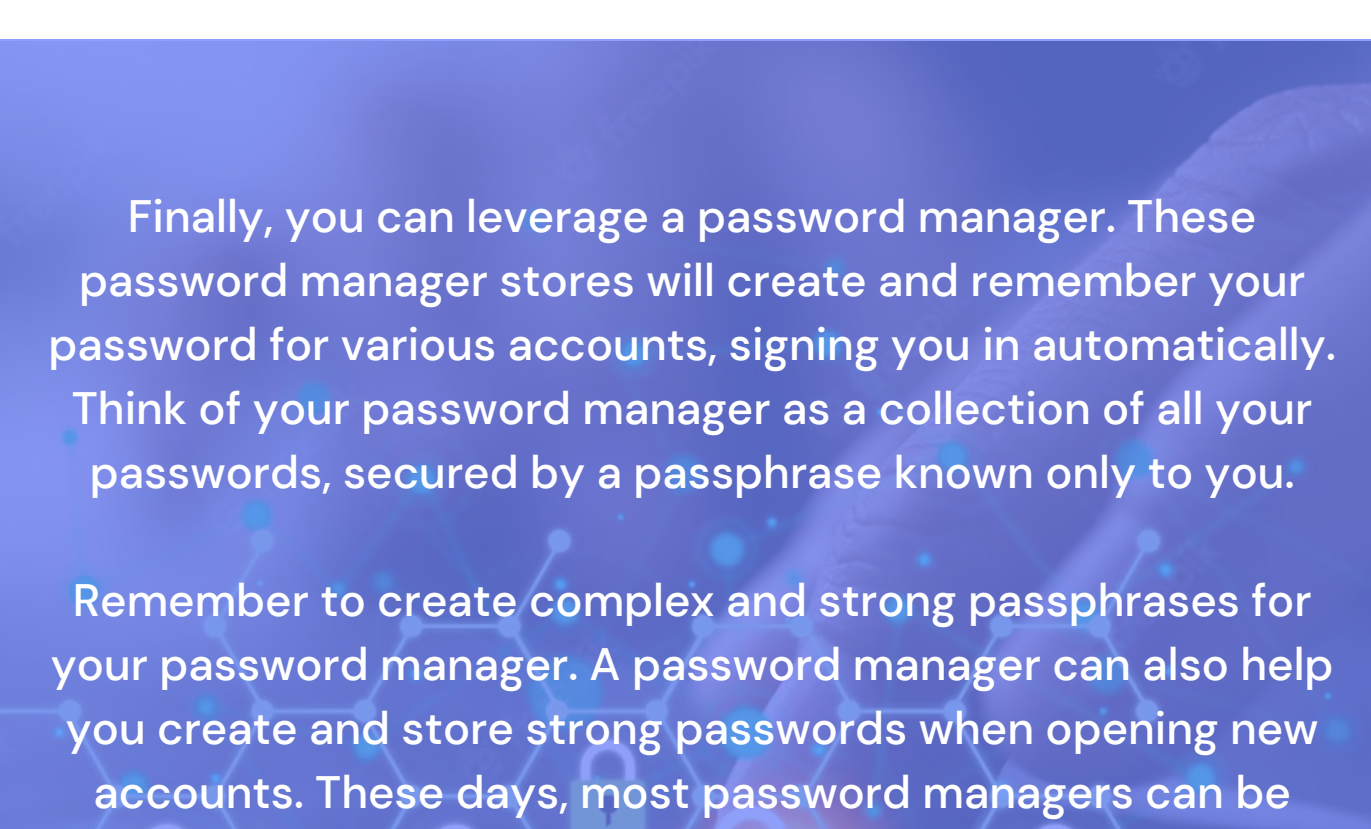


Managing Your Passwords

It can be hard to keep track of all your passwords, especially if you have dozens of them across different devices and accounts. Most web browsers now provide a free password management tool to help you keep track of all your passwords. You also have the option of buying a dedicated password manager as well.

These passwords can be synced across different devices and computers, so you won't have to remember the long credentials every time. These features are incredibly safe to use as long as your browser itself is secure. Remember, if anyone accesses your web browser, they can be inside your accounts in the span of a few clicks.

As a precaution, you should enable password protection on your desktop computer and mobile devices. This should prevent anyone else from accessing your passwords through your browsers.



Finally, you can leverage a password manager. These password manager stores will create and remember your password for various accounts, signing you in automatically. Think of your password manager as a collection of all your passwords, secured by a passphrase known only to you.

Remember to create complex and strong passphrases for your password manager. A password manager can also help you create and store strong passwords when opening new accounts. These days, most password managers can be synced across multiple devices with encryption, letting you take your passwords anywhere in the world.

Some of the most popular and well-respected password managers are LastPass, 1Password, and Dashlane. These services let you manage an unlimited number of passwords across multiple accounts.

Wrapping Up

So there you have it, an in-depth look at password management best practices. For more information on our cyber security services, please talk to our consultants at Microsys.

Get In Touch With Microsys