Password Managers

I use several online resources that keep me somewhat up to date on technology issues, and a YouTube provider (Dave's Garage) had an informative discussion about password managers. Password manager software has been around for some years, and it was quite a surprise when he recommended the password manager services that the Chrome Browser or Microsoft Edge provides.

His arguments were fairly compelling. He notes that Google, for example, only has access to encrypted copies of the passwords, and that the original user and the user's device has the encryption key needed to unscramble them. Secure passwords are created automatically, for the user, when they are needed, and are auto-filled, when they need to be used. Google and Microsoft both have a compelling business need to keep their password manager services safe, because failing to do so would have a dramatically bad impact on their reputation. And . . . the service is free of charge.

Okay . . . everything has a downside, so I've done a bit of poking around. My first effort was to google: "Has the google password manager ever been hacked?" The response confirmed that there are concerns about the Google Password Manager. Among the concerns is that if a person has access to your device, they will have access to your passwords. Malware attacking the Chrome Browser or the installed extensions was also a concern, as well as Google's reputation with privacy concerns.

Proton, a company which provides email service said to be more secure than others, points out that Google's security cannot be verified, they may lose all of your passwords, and among other things, Google's reputation with privacy and data sharing with their advertisers.

There were other concerns about what happens if you are locked out of your Google account (which can happen), and a number of other issues.

***A key point**: The password used for the service managing your passwords must be, in itself, a secure password!!! It does no good to have a weak password protecting your repository of passwords.*

I guess I don't have any magic answers, today (or any other day, for that matter). I do know that secure passwords (long passwords with random letters, numbers, and punctuation) are a must-have thing. Such passwords are hard to remember, and a password manager makes the task easier.

Use secure passwords. Computers are fast, and can crack even a difficult password a matter of milliseconds.

I wanted to demonstrate how fast modern computers can do things. Since I didn't want to come up with a boatload of dry statistics, I made a Powerball drawing simulator, and it's results are below.

The program that generated this was written in Java, written by a Java student, who is halfway through his class, as his first non-classwork project. It was not specifically optimized for speed, and was run on a 10-year old office-grade desktop computer. Keep this in mind, since a hacker or other bad actor would likely run speed-optimized software on a speed-optimized machine.

Please note that this program made and evaluated 4.7 MILLION Powerball drawings PER SECOND. It could've been password guesses, instead!!!

Powerball Simulation
Running Time = 1 minute

Total drawings: 282080841 (Drawings per second: 4701347)
The ticket is: 1 68 38 54 45 and PB 22

Type	Times won	Expected	Actual
Match 5 + PB	3	0.000000342 %	0.000001064 %
Match 5	25	0.000008556 %	0.000008863 %
Match 4 + PB	301	0.000109514 %	0.000106707 %
Match 4	7857	0.002737838 %	0.002785372 %
Match 3 + PB	19276	0.006899354 %	0.006833502 %
Match 3	486695	0.172485166 %	0.172537431 %
Match 2 + PB	402352	0.142586229 %	0.142637134 %
Match 1 + PB	3065826	1.087192868 %	1.086860776 %
Match PB	7359595	2.60960334 %	2.609037638 %

Credits:
https://youtu.be/dGwmIwG6IwY?si=9EQkjNCWdmkxfIqR
https://proton.me/blog/google-password-manager-security
https://www.google.com/search?q=Has+the+google+password+manager+ever+been+hacked

software, parts and service: youfoundterry.com