The Importance of Password Managers

Take a moment to think about how many online accounts you have. What do the passwords for these accounts look like? Perhaps you reluctantly had to create an account to access a particular service, and in that process, you quickly typed in a password you already use for a different account. Or maybe you created a new, unique password, since you understand the dangers of password reuse.

Let's say the new password you choose for the account is something like "murphy" (weak password, I know!) Given access to a computer, anyone (and I mean *anyone*) can install a password cracking software (i.e. John the Ripper) in under 5 minutes. Given that your password is just a single word, it would take John the Ripper less than a second to crack your password and access your account.

How about we take it a couple steps further. Say you capitalize the first letter and add four random numbers to the end of the password, making the password "Murphy9283"—I can certainly attest to the fact that I've created many passwords with that exact format in the past. Given the addition of a capitalized letter and 4 random digits, the time it takes to crack this new password has gone up to a whopping 4 whole minutes!

But that's not enough. Sometimes the website will tell you to add a special character to the password. Sounds easy enough, but we don't want to add too many special characters because it'll make the password harder to remember. Let's add a percent symbol to the end of the password, which means our password now has a capital letter, numbers, and a special character—enough to satisfy even the strictest online requirements for creating a password. This brings the total time to crack our password up to about 40 minutes, meaning it would take less than an hour for a bad actor to get access to our account.

It may not take long for a hacker to guess our password, but what if we have two factor authentication? Or what if our account simply gets locked out after a few incorrect password attempts? These are two common pitfalls that lead individuals to not worry about weak passwords, but both layers of protection can be circumvented by a determined attacker.

1 Cracked Password Risks

With respect to account lockouts, at first glance this seems like an effective way to prevent brute-force password attacks (i.e. repeatedly guessing your password until it's correct). However, many companies cannot fully implement this feature due to its potential of being exploited by hackers. For example, if a bad actor were to gain a list of various valid usernames (with no knowledge of their password), they could intentionally trigger account lockouts for each user, causing a huge headache for the company (and the user) as they would be forced to deal with many password resets at once.

As for two-factor authentication, while this is an effective means of preventing someone from gaining access to your account if they have your password, it is by no means a completely bulletproof measure. If you have browser cookies that remember your two-factor authentication (so you only need to use 2FA once when you login to a new device, and not every single time you login), hackers

The Importance of Password Managers

wouldn’t even need to interact with the two-factor authentication. Having a weak password also means that hackers only need to focus on bypassing the two-factor authentication, instead of having to first crack the password (which sums up to two layers of security).

But what does this all mean? Clearly our requirements for what constitutes a “strong” password needs to change, but then how would we keep track of all of those passwords? It’s already hard enough remembering an insecure password like “Murphy9283%”, and it becomes even more challenging when we need to create a unique password for every single account.

This is where password managers come in. Password managers help generate and store complex, unique passwords for each of your online accounts, helping you ensure that all your passwords are secure and single use; the best part is, you don’t need to memorize each and every password! All you need to do is create and keep track of a single, complex password that grants you access to the password manager. Password managers make it extremely easy to create new logins through the use of browser extensions, and it’s easy to import existing logins from places such as your browser.

But a single place to keep all your passwords sounds a bit unsafe, right? What happens if someone guesses the password to your password manager, or somehow hacks the place where all the passwords are stored?

With regards to someone hacking your password manager (without knowledge of your master password), that would be a virtually impossible scenario. For popular choices like Bitwarden, all the information within the password manager is encrypted (essentially scrambled) on your computer *before* it’s sent to an external server or cloud—the only way to unscramble the information is to use your master password, which essentially serves as the “key” for your password manager lock. This ensures that even if someone were to hack the password manager’s database, they would not be able to make sense of anything without the master password for each account.

2 Popular Password Managers

As for ensuring that no one gets access to your master password, that responsibility lies on you. Make sure to create a complex, lengthy, and unique password that would be very hard to guess and ensure that no one else has any knowledge of the password. Despite our previous discussions about how easy it is to crack most passwords, it is not too difficult to create an extremely secure password. An example (iterating on our previous password) could be “MurphyLawNice4690$”, which would take several centuries for a hacker to guess. While it isn’t innately difficult to generate complex passwords like these, the challenge lies in creating unique ones for each of your accounts and keeping track of them all, which is where a password manager comes in handy.

All in all, password managers are a vital tool that help ensure good password practices while prioritizing user convenience. The password manager I personally use is Bitwarden, although there are many different options to choose from that are all equally safe. Regardless of the number of online accounts you have or your technical abilities, password managers can benefit almost anybody and take very little time to setup, so download one today!