

Hackers love easy targets; don’t be an easy target

The only thing between all your personal and financial information and a hacker is a password. Password Managers are a great tool to help you create stronger and unique passwords for every site.

By **BRETT CORPORON** and **ZAK BRATTON**

In this digital age, convenience usually trumps security, putting your identity, finances, and client data at risk. But a password manager, as recommended by security experts, provides both convenience and increased security.

Password managers are programs that store all of your passwords, regardless of how simple, random, long or short it may be, and protects them under one single password. Once a user visits a website and enters their login information, the password manager captures the information for future logins.

This eliminates the need for the user to remember the credentials in the future. Now, only the master password has to be remembered to log in to the manager itself and access the entirety of passwords.

If a user is creating a new account or password on a website, the password manager has the capability to create a secure, randomly-generated password, allowing the user to move through the process more efficiently.

The goal, of course, would be to have completely different passwords for each site with a high character count and mix of uppercase and lowercase letters, numbers, and symbols, to ensure maximum security.

The password manager would keep track of all these passwords in a single hub, encrypting them for security, and eliminating the need to burn them into your brain or log them on a sheet taped underneath your keyboard.

This allows stronger and more unique passwords for every single site, and makes it much more difficult for hackers to guess or use brute force attacks to access you or your clients’ information.

A perfect analogy would be someone trying to unlock your vehicle with a set of keys on a keyring. If there are only five keys and each is marked corresponding to what it opens, house, truck, shed, etc., it makes short work for the individual to access the vehicle.

On the flip side, a keyring with 40 keys, all very different cuts, shapes and no distinguishing identification, would be much harder to crack.

This raises two questions: “How do I know if a password is considered ‘strong’? And “What if my passwords aren’t up to snuff?”

The good news is, many password managers offer a feature to generate passwords at the click of a mouse. These programs may also include a feature to audit any current passwords to let the user know how susceptible it is by identifying the strength as weak, medium or strong by hacker standards.

Many password managers support a variety of operating systems: Windows, macOS, Linux, as well as mobile devices. Plugins for web browsers such as, Chrome, Firefox, Safari, and Internet Explorer, are also supported.

Truly the silver lining can be defined by one factor: cost. While it may be possible to find a free password manager, most do charge a fee, typically in a yearly or monthly subscription.

Paying the subscription can give users access to premium features such as the ability to sync passwords across all devices, priority customer support or additional encrypted storage space, among other things. Other developers may require users to pay a one-time fee to use their product.

In this case, it varies from program to program and comes down to an individual user’s needs and circumstances.

For an in-depth look at password protection and general security, the [United States Computer Emergency Readiness Team \(US-CERT\)](#), a subset of the U.S. Department of Homeland Security, has published a slew of articles on the subject.

The US-CERT is tasked with protecting citizens against cyber threats and their articles provide general information for non-technical computer users, as well as concentrated information for control system users, government users, and home and business users.

Password managers help to deter hackers and secure your identity, finances, and client data, and are a cost-effective, convenient alternative to remembering or writing down the password for hundreds of individual websites.