PASSWORD MANAGERS—SECURITY

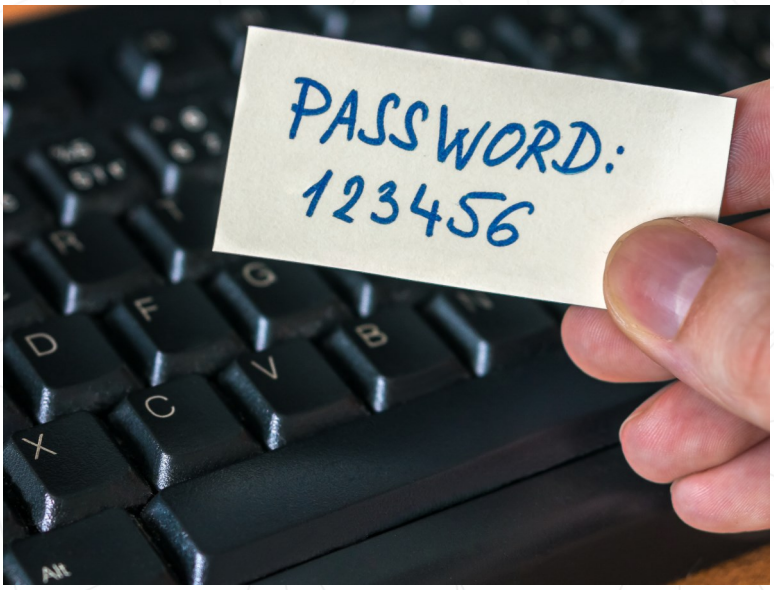
SEPTEMBER 2019

ITSAP.30.025

Trying to use different and complex passwords for every website, account, and application can be challenging. If you are experiencing password overload, you may become careless. Maybe you keep all your passwords written down or reuse the same, easy to remember password. You can use a password manager to help you create, store, and remember your passwords.

By using a password manager, you don't need to remember dozens of passwords. They promote the use of complex passwords and discourage password reuse. Even though password managers provide a number of advantages, these tools present some risks to user's information which we will outline in this document.

A password manager exists as a password vault and stores a user's usernames and passwords for different websites, applications, and services. Password managers have unique features, design, and vulnerabilities. There are two main types of password managers: browser-based and stand-alone.



BROWSER-BASED VS. STAND-ALONE PASSWORD MANAGERS

Browser-based password managers are convenient. They are built in to your web browser and do not require you to remember a long master password. They use the "remember me" feature when you log-in to a website. This creates vulnerabilities when another user has access to this device. Browser-based password managers don't always sync to other devices. This forces you to remember your passwords when logging in on other devices. For optimal security, you must keep your browser up to date.

Stand-alone password managers require local or cloud-based installation of software and account creation to access the service. They tend to be more secure than browser-based and they allow for a complex master password and typically offer two-factor authentication. They also have more advanced features such as alerts if a website is compromised, and flagging weak passwords. You can also sync the passwords stored across your devices.

Regardless of which type you choose to use, we recommend you use two-factor authentication whenever possible.

TWO-FACTOR AUTHENTICATION

For an extra layer of security, we recommend using password managers that require two-factor authentication.

With threats becoming more sophisticated (e.g. keylogging and phishing attacks), your main password can be hacked easily. That's why two methods of authentication, something you know and something you have (e.g. a password and a token, a password and a fingerprint), are better than one when it comes to password security. For example, two-factor authentication may require an additional code to log in to an account; this code can be emailed to you or provided through an automated phone call.

Not all two-factor solutions are equal—but all will improve your overall cyber security posture.

SECURITY CONSIDERATIONS

Password managers are an attractive target –a one stop shop if you will. Although password managers have many benefits, such as helping you cope with password overload, there are also risks associated with using them, the greatest risk being compromise of all your accounts at once. If a password manager is compromised, all the stored account passwords will be exposed. If you choose to store passwords for sensitive accounts (e.g. your online banking account), then your level of risk is increased accordingly. We recommend that you evaluate the value of the accounts you are storing in the password manager, and take every precaution you can if you decide to use a password manager.

Many security considerations need to be evaluated before using a password manager. Several attacks from threat actors can affect your passwords stored in a password manager. Using brute force, a threat actor can attempt to gain access to your master password. If you must write down your master password, ensure it is properly stored (e.g. a locked safe), and limit the number of people with access to it.

TIPS FOR USING PASSWORD MANAGERS

- **Use password managers that:**
  - support two-factor authentication
  - prompt you to change old passwords
  - flag weak or reused passwords
  - store legitimate web links and notify you about compromised websites
  - integrate with your phone, computer, tablet, and other devices
- **Install updates regularly for password managers**
- **Use the password manager to generate passwords for you**
- **Avoid using the same password for multiple sites**
- **Do not store passwords for sensitive accounts (e.g. banking, email)**
- **Do not share your master password**
- **Have a plan to recover your passwords when your computer fails and you lose access to your password manager**

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (CCCS) at **cyber.gc.ca**