Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

Password managers: Security tips

February 2024

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. Both of these password habits put you and your accounts at risk. For more information on best practices for passwords see Rethink your password habits to protect your accounts from hackers (ITSAP.30.036) and Best practices for passphrases and passwords (ITSAP.30.032).

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 users' 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. If you decide to use a password manager, you should research different vendors in order to make an informed choice about which is right for you.

Types of password managers

There are 2 main types of password managers: browser-based and stand-alone.

Browser-based password managers

Browser-based password managers are convenient. They are built into your web browser and do not require you to remember a long primary password. They use the "remember me" feature when you log-in to a website. This creates vulnerabilities when another user has access to that same 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

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 primary 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 activate multi-factor authentication (MFA) whenever possible. For more information on multi-factor authentication see Secure your accounts and devices with multi-factor authentication (ITSAP.30.030).

AWARENESS SERIES

Cat. No. D97-1/30-025-2023E-PDF
ISBN 978-0-660-68382-9

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, they also present some risks. The greatest risk being the compromise of all your accounts at once. If a password manager is compromised, through your account or through a vendor compromise, all the stored account passwords will be exposed. If you choose to store passwords for sensitive accounts (like your online banking account), then your level of risk increases 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 primary password. If you must write down your primary password, ensure it is properly stored (such as in a locked safe), and limit the number of people with access to it.

Multi-factor authentication

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

With threats becoming more sophisticated (like keylogging and phishing attacks), your main password can be hacked easily. That's why using MFA authentication is better than a single password where the factors can include something you know, something you are, or something you have. For example, you can combine a password with a token, a fingerprint, or an additional code to access your password manager.

Tips for using password managers

- **Use password managers that:**
  - support multi-factor authentication
  - encrypt passwords so only you see them, making the passwords unreadable even to the vendor (known as zero knowledge architecture)
  - prompt you to change old passwords
  - flag weak or reused passwords
  - disclose how they protect your passwords
  - store legitimate web links and notify you about compromised websites
  - notify you if your password appears within a known data breach
  - integrate with your phone, computer, tablet, and other devices
- **Use a strong primary passphrase or password:**
  - passphrases are memorized phrases of at least 4 words (with or without spaces) and are a minimum of 15 characters in length
  - passwords are at least 12 characters in length and includes upper and lower case letters, numbers and special characters
- **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 (such as banking and email accounts)**
- **Do not share your primary 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**