Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

Best practices for passphrases and passwords

February 2024

ITSAP.30.032

You have passwords for everything: your devices, your accounts (like banking, social media, and email), and the websites you visit. By using passphrases or strong passwords you can protect your devices and information. Review the tips below to learn how you can create passphrases, strengthen your passwords, and avoid common mistakes that could put your information at risk.

For passwords, we recommend that you use a minimum of 12 characters. Keep in mind that websites and applications have different password creation rules that you will have to follow (for example, letters, numbers, punctuation marks and special characters that a password must and must not contain). This will impact your ability to follow our recommended guidance.

Use passphrases

We recommend that you use passphrases, as they are longer and easier to remember than a password made up of random, mixed characters. A passphrase is a memorized phrase consisting of a sequence of mixed words with or without spaces. Your passphrase should be at least 4 words and 15 characters in length. For example, you might create a passphrase by using association techniques, such as scanning a room in your home and creating a passphrase that uses words to describe what you see (for example, "Closet lamp Bathroom Mug").

Protect passphrases and passwords

Threat actors send **phishing** emails to trick you into giving your personal information and, in some cases, installing malware, such as a keylogger. If a **keylogger** is installed on your device, a threat actor can use it to capture the keystrokes you use when entering your passphrases and passwords. Phishing attacks are common, but you can protect yourself by reading the tips in Spotting malicious email messages (ITSAP.00.100) and Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101) .

Create complex passwords

Use a password that is as complex as possible if you cannot use a passphrase (for example, when a website requires that your password is less than 15 characters). A password made up of lowercase and uppercase letters, as well as numbers and special characters, is more complex than a password containing only lowercase letters.

You can also think up a phrase and then use the first letters of each word to create a complex password that is more memorable. For example, the phrase "My jersey number when I played competitive soccer was 27!" can be used to remember the password "Mj#wlpcsw27!".

Use passcodes or personal identification numbers

A passcode or personal identification number (PIN) is a sequence of numbers that is at least 4 digits. Passcodes use a minimum of 4 digits because there are other protection mechanisms in place to protect your device or account. For example, to access your bank account, a threat actor would need to know your PIN or passcode and have physical access to your bank card. Always make sure your PIN is made of random numbers.

AWARENESS SERIES

Cat. No. D97-1/30-032-2024E-PDF
ISBN 978-0-660-68243-3

Multi-factor authentication

Multi-factor authentication strengthens your device and account security. Multi-factor authentication makes accounts more secure by requiring at least two items of authentication such as something you know, something you have, or something you are (like a password and a token or a password and a fingerprint) to log in. If you use multi-factor authentication, you could use a password that is 6 to 8 characters in length because the extra authentication adds another layer of protection.

Not all multi-factor solutions are equal, but all will improve your overall cyber security posture. Your organization should have user authentication policies that balance security with usability. For more information on multi factor authentication see Secure your accounts and devices with multi-factor authentication (ITSAP.30.030).

Protect passwords, passphrases and personal identification numbers

Passphrases, complex passwords, passcodes, and PINs must be handled and stored carefully so that they are not compromised. Keep the following tips in mind:

- Be aware of your surroundings when entering passwords, passphrases, passcodes, or PINs in public
- Do not enter passwords when using public Wi-Fi
- Use a different password, passphrase, or PIN for each device and account, especially for accounts with sensitive information
- Do not give out passwords, passphrases, passcodes, or PINs online or over the phone
- Do not share passwords, passphrases, passcodes, or PINs with others, even family
- Log off and sign out of accounts and websites when you are done using them
- Ensure your sensitive accounts, such as those used for banking or for the Canada Revenue Agency, are protected by the strongest passphrase or password possible

Avoid common password mistakes

If created and protected properly, passwords, passphrases, or PINs are an effective way to protect your devices, accounts, and information. Below are some examples of common mistakes to avoid:

- Do not use easily guessed passwords, passphrases, or PINs, such as “password”, “let me in”, or “1234”, even if they include character substitutions like “p@ssword”
- Do not use common expressions, song titles or lyrics, movie titles, or quotes
- Do not use your personal details such as your birthday, hometown, or pet’s name
- Do not use the passwords assigned by the vendor when installing or enabling new hardware or software
- Do not use passwords found on known data breaches

For more advice on passwords, see Rethink your password habits to protect your accounts from hackers (ITSAP.30.036).

Know the reasoning behind the rules

The rules around creating passphrases and passwords exist for a reason. If you’re not careful to take precautions with your passphrases and passwords, threat actors can choose from an ever-growing list of methods to break into your devices and accounts, and access your information. Many of these methods use a password hash, which is an encoded version of your clear text password. The hash is what is often used to verify your passwords on apps and websites.

Threat actors can use the following methods:

- **Brute force** is a method of trial and error where all common passwords are entered until one works. This method usually uses password dictionary tables.
- **Rainbow tables** are precompiled lists of password combinations and their associated hashes. These are used to match a known hash to a password that grants access to an account.

Shorter passwords are much easier to hack. You can make it more difficult for threat actors to hack into your devices and accounts if you use lengthy passphrases or more complex passwords.

Password managers

If you feel overwhelmed by the number of passwords that you have, you can use a password manager to generate and track your many passwords. To protect the passwords stored on a password manager, consider the following tips:

- Use a password manager to store passwords for your lower sensitivity accounts but not for sensitive accounts such as those with administrative privileges or banking credentials
- Use a strong password and multi-factor authentication to secure a password manager
- Ensure the password manager is from a secure website and that it is updated regularly

Before using a password manager, check out Password managers: Security tips (ITSAP.30.025).

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**