



**Grades  
7-12**

# Privacy Online: Passcodes



**ROGERS  
cybersecure  
catalyst**



**Passcodes, often referred to as passwords, are key to keeping personal and private information safe. Personal information includes facts about an individual, such as hobbies, favourite food, etc.; whereas private information includes details that can be used to identify an individual, such as street address, phone number, date of birth, etc. Both personal and private information, if in the hands of the wrong person, can be used to guess or “crack” passcodes, and gain access to online accounts, such as online banking or emails. For instance, if you’ve posted online about your favourite celebrity/athlete and use that person’s name in a passcode, that passcode can be easily guessed. Passcodes can be a series of random words strung together, a memorable phrase, or a combination of words, numbers and symbols; regardless of how it’s put together, it should be unique to you – just like a fingerprint!**

**Passcodes are needed for your safety and security, and to protect your privacy. Strong passcodes, as well as a different passcode for each account, stop others from getting into your accounts and devices by dishonestly authenticating you. Passcodes should be carefully cared for and never shared. Otherwise, you risk losing your accounts, damaging your reputation, or having your identity stolen.**

**In this resource, you’ll learn tips on how to create a secure and memorable passcode, ways to protect your passcodes, how attacks work and how to manage your passcodes.**





# DEFINITION

## Creating strong passcodes

Passcodes protect your privacy and prevent other people from accessing your accounts and private information. This is important so that people can't pretend to be you, go through your stuff, steal from you, damage your online image, or even get you in trouble. For this reason, it's important that you follow some simple passcode rules to keep safe and secure, and your passcode impossible to guess:

- **Longer is stronger!** Long passcodes are harder for others to guess, and hackers to decode. Most accounts require a minimum passcode length of 10 characters; however, a recommended length is 12-15 characters.
- **Use a passphrase!** A passphrase can be a few random words used together that are easy to remember.
- **Never use any personal or private information** in your passcode or passphrase – information that someone might already know or easily obtain – because identity thieves can use it to impersonate you.
- If your passcode contains numbers (highly recommended!), **do not repeat the numbers** like '777' or use a number count like '123', or a significant date like '010101' if your birthday is January 1, 2001. These are too easy to guess!
- **Create passcodes with a variety of characters!** Including capital letters (ABC) and small letters (abc), numbers (123) and symbols (!, @, #). Using all four types makes for a strong passcode.

### Characters:

Characters in a passcode refer to symbols consisting of letters in upper (capitals) and lower (small) cases, figures from 0 to 9 and characters such as !, #, ^, \*, \$, %, etc.







### Passphrase:

Passphrases often contain more characters than passwords do, but fewer components (for example, four words instead of 12 random characters).

### Mnemonics:

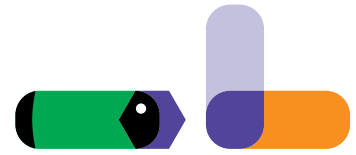
Pronounced "ne-mon-ics"; also known as a memory device, such as a pattern of letters, ideas or associations that assists in remembering something.



# Creating a strong passcode: Helpful tips

Having a hard time coming up with strong and secure passcodes? Try these helpful tips:

- You might want to use a **memory or learning technique** like mnemonics to help you create and remember strong passcodes. For example, the quote "Just be yourself, there is no one better" – Taylor Swift, 2016 becomes: Jby,tisnob-TS,2016.
- **Mixing and matching languages!** For example, the passphrase "The cat eats three jewels!" in English, Spanish, Italian, French becomes: The,Gato,Mangia,3BIJOUX!
- **Make it poetic!** Try creating a passcode or passphrase with alliteration or rhyme! For example: "Loud.lemurs.laughed.lightly!"

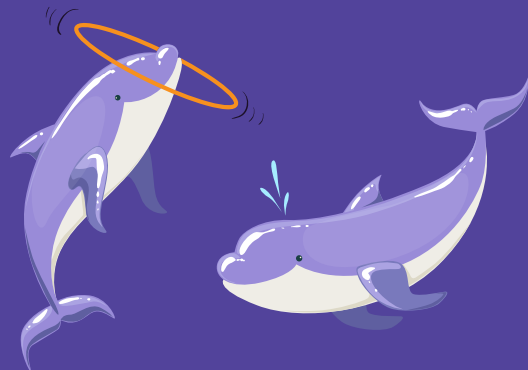


## Alliteration:

The occurrence of the same letter or sound at the beginning of adjacent or closely connected words.

## Remember this!

When creating a passphrase, choose words you can imagine in your head so they can be easily recalled. For example **LoudLemursLaughed**





**Virtual Private Network (VPN):**  
Allows you to create a secure connection to another network over the Internet privately. **HOWEVER:** Free services come with hidden costs!



## Protecting your passcodes

Creating a strong passcode is very important, but won't be effective unless you keep it safe, and keep it to yourself! Here are some ways to protect yourself and your passcode:

- **Do not share passcodes with anyone**, not even your best friend in order to continue an online game streak, or to show your commitment to the friendship!
- Be sure to **let your parents/guardians know where you store your passcodes**, in case of an emergency.
- **Do not allow websites, web browsers and programs to 'remember' or 'store' your passcodes**, as they can be easily compromised if breached.
- **Do not log into accounts on other people's devices**, as your passcodes can be easily retrieved. If you must, be sure to log out when you finish.
- **Type your passcodes away from peering eyes**, especially when logging in around groups of people, like at a library or in class.



- **Never log into your accounts when on a public Wi-Fi or when using free Virtual Private Network (VPN),** as all your user and passcode information can be acquired.
- **Never store passcodes in or on your device.** Consider using a passcode manager instead!
- **Do not use any personally identifiable information** in your usernames. Like your name, gender, location or birthday. For example: MissLilly2002
- **Treat secret questions like passcodes!** Choose questions and create answers that do not reveal your real personal information, as these can be easily guessed by someone who knows you or potentially follows you on social media.
- **Avoid playing games or doing quizzes that ask you for any personal or private information, or ask to link to your accounts,** like Facebook. These games are a form of phishing for information that could lead to you unknowingly revealing your passcode.
- **Sign out of your accounts and lock your devices** when you're not using them so that no one else can access them.

#### Passcode manager:

A computer program that allows users to store, generate and manage their personal passwords for online services. It also assists in generating and retrieving strong passwords.

#### Phishing:

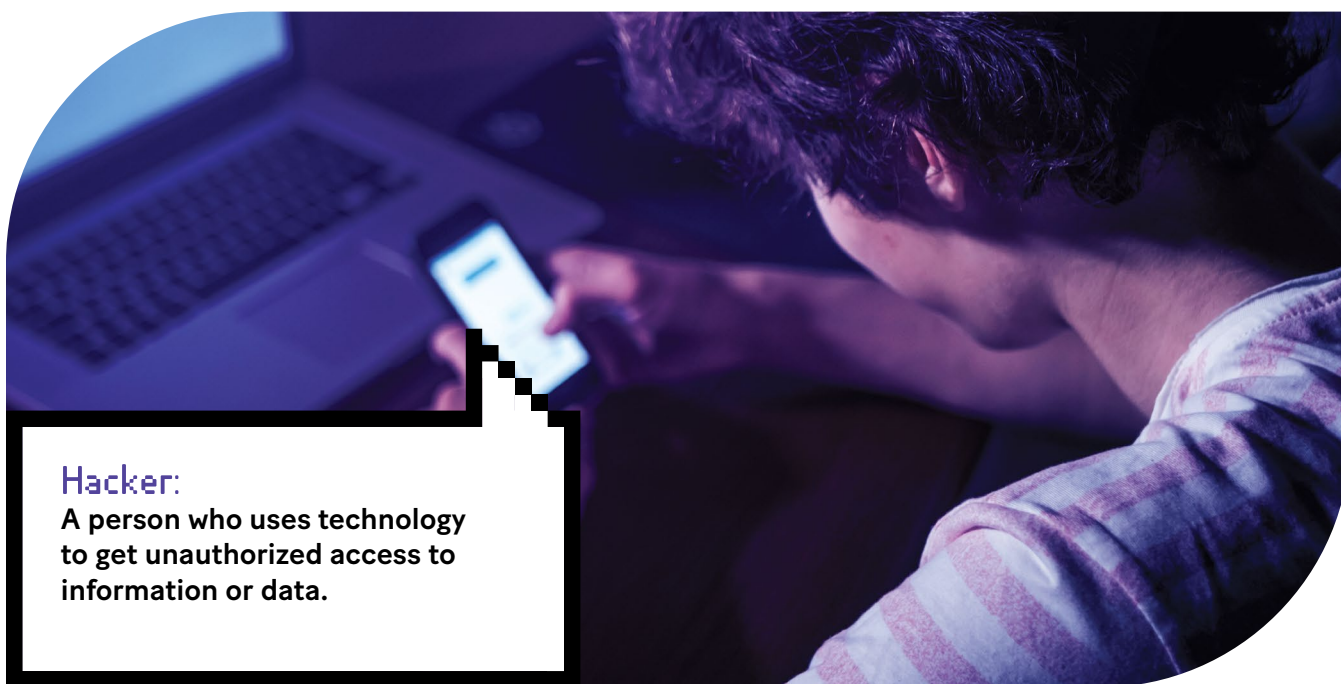
Pronounced "fishing"; a fraudulent attempt or a scam by an Internet user to get private or personal information to use illegally.

#### Reflect on your understanding:

Why do you think people would feel pressured into sharing their passcodes? What are the risks of sharing your passcodes with others?







### Hacker:

A person who uses technology to get unauthorized access to information or data.

## Cracking the code: How attacks work

You might feel that you're either too unimportant or have nothing to hide or steal, or you might not even care if your account gets taken over. The reality is, hackers use bots to crawl the web searching for vulnerabilities or holes in security – and they're not selective about who they find. You have your personal identity to worry about because someone can pretend to be you and cause many complications for you by posting inappropriate things on your accounts, asking your friends/family for help or money, or locking you out of all of your accounts.

There are two ways your accounts can become vulnerable to hacks and attacks:

1

Your accounts become vulnerable to **passcode guessing attacks** when you set up weak passcodes.

2

When your accounts are **compromised in data breaches**, your accounts and personal information become vulnerable.

### Data breaches:

When an account or database gets hacked, and usernames, passcodes and other stored confidential information are revealed.







Let's take a look at three common guessing attacks:

- **Dictionary attacks:** This type of attack uses computerized dictionaries of all languages to guess a passcode. It also uses collected lists of hacked passcodes, and strings of words in book titles, slogans, song lyrics, newspaper articles, etc.
- **Brute force attacks:** All passcodes can eventually be cracked by a brute force attack, but the time it can take will be determined by how safe your passcode is. Weak passcodes can be guessed in less than a minute, whereas strong passcodes can take years or decades to crack.
- **Targeted attacks:** Attackers get a lot of information about people online, and know that some of this personal information is often used in passcodes. It's easy for attackers to access this information, even though they don't know the victim personally.



### Did you know?

A security expert who wanted to make users aware that their data had been compromised created a website where you can safely type in your email to see if it has ever been compromised.

### Try it yourself!

Type the following website in your browser address bar: <https://haveibeenpwned.com/>

If your email has been compromised, scroll down the page on the website and it will give you details as to where it was hacked from.

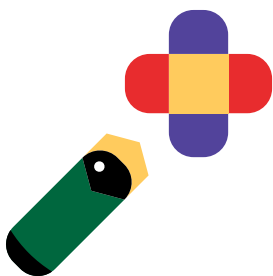


## It's up to you!

### Managing your passcodes

Now that you know how to create a strong passcode, protect that passcode and are aware of the types of data attacks, it's important to be aware of how to manage your passcodes – all of them!

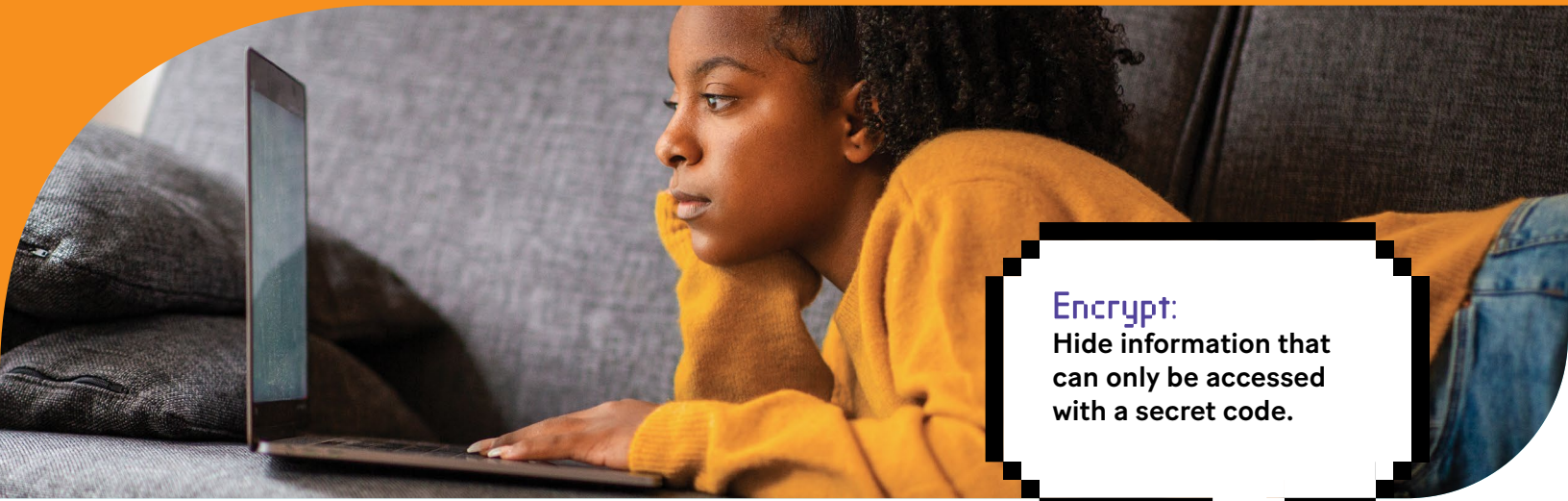
- **Never use the same passcode, security question or security answer** for multiple accounts. Why not? Because, if one account gets hacked, your other accounts using the same username, email or passcodes won't become easily hackable!
- **Occasionally change your passcodes.** Worried you won't remember to do it? Try setting a date on your calendar.
- **Do not reuse old passcodes!**
- **Store your passcodes of ine and off your devices.** Consider using a secure passcode manager tool (more information below) to generate and store complex passcodes for each of your accounts. **Use Multi-Factor Authentication (MFA)** whenever it's available. This provides an extra layer of protection, because you'll need to fi rst confirm on another device (such as your phone) that it's you trying to log in before being given access. Someone who knows the passcode won't be able to access the account with MFA, and you'll be notified of the attempt.



#### Multi-Factor Authentication (MFA):

A security feature that verifies a user's identity by requiring two or more pieces of evidence ("factors") or credentials such as numerical codes, answers to unique security questions, etc.





### Encrypt:

Hide information that can only be accessed with a secret code.

## Passcode managers

Keeping track of so many usernames, passcodes and their accounts can lead to passcode overload. Passcode managers attempt to solve this issue by encrypting all your passcodes and login information – and to access all your logins, you simply need to create and enter one strong master passcode.

Here are some criteria to consider while investigating passcode manager software. Decide which criteria are most important to you, and pick your top passcode manager. Sign up and get started!

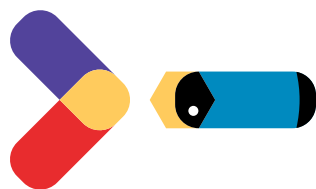
- ✓ Account recovery ease
- ✓ Passcode changing
- ✓ How data are stored/protected
- ✓ Sharing capabilities
- ✓ Works with multiple platforms and multi-factor authentication apps
- ✓ Ability to organize all accounts
- ✓ Includes emergency access
- ✓ Dark web monitoring
- ✓ Support
- ✓ Total cost per year

Technology has a lot of positive uses, but you need to empower yourself with the skills needed to enjoy surfing the Internet safely. Every possible passcode combination can be cracked sooner or later. The question is: How long will it take to crack?





## Activities



Activities are a useful way for you to test and demonstrate your knowledge on the topic covered in this resource.

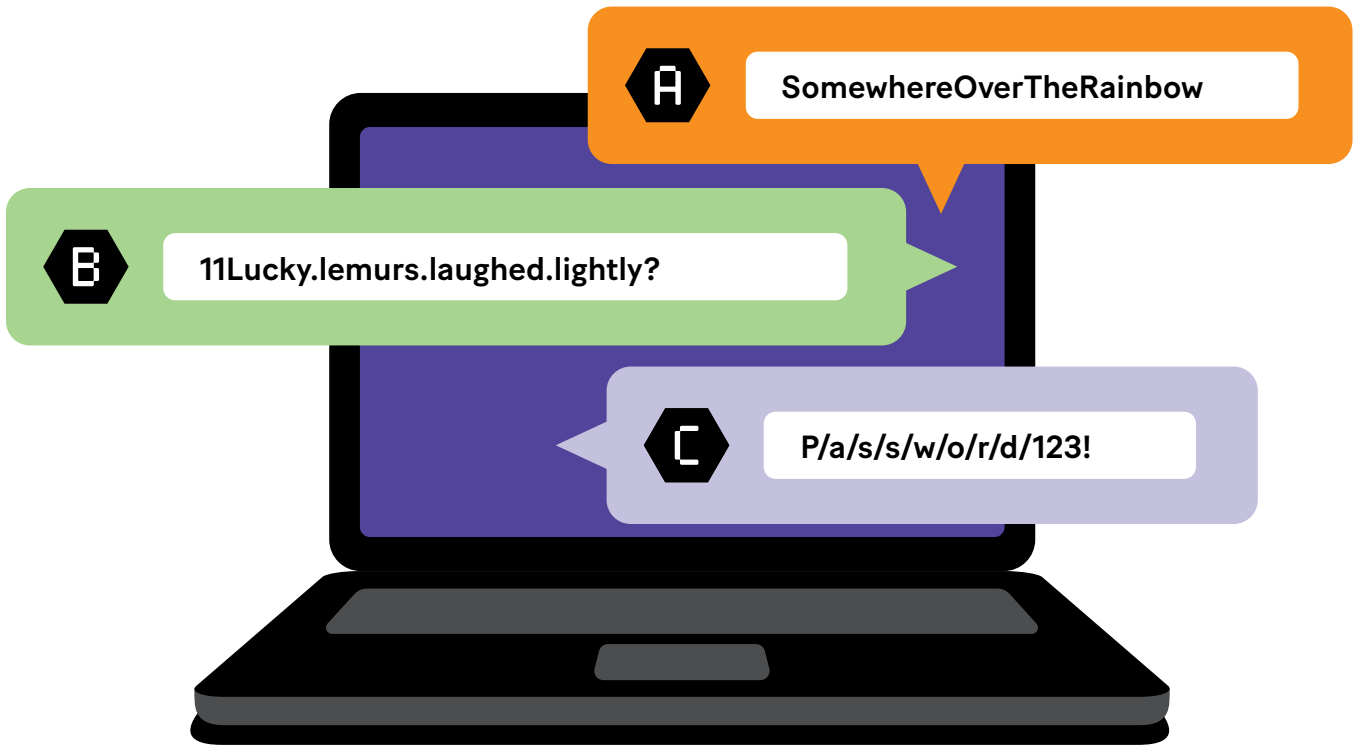




# ACTIVITY 1

## Passcode Rankings

Of the sample passcodes provided below, rank them from strongest to weakest, and explain your reasoning.



1	.....	WHY?.....
2	.....	WHY?.....
3	.....	WHY?.....



Answer Key: :  
1st: Passcode B (long, uncommon, several numbers & symbols  
2nd: Passcode A (long, but no symbols or numbers, song lyrics are easier to guess)  
3rd: Passcode C (too common! Even if separated by symbols)

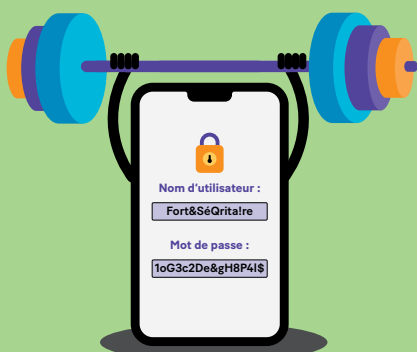


# ACTIVITY 2

## Practicing Passcode Creations

Using the phrase below, and the tips provided in this resource, try creating your own sample strong passcodes.

Phrase	Exemple de mot de passe
Three Musketeers	 <div>3Musket33rs!</div> 
Add me on Instagram!	
"May the Force be with you." – Star Wars, 1977	
«I solemnly swear I am up to no good.» – Harry Potter and the Prisoner of Azkaban	



Want to test the strength of the passcodes you created? Try using the free Kaspersky Password Checker; it will tell you how hack-resistant the password is, and if it's appeared in any databases of leaked passwords in the past.

**Kaspersky Password Checker\*:**  
<https://password.kaspersky.com/>

\*Note: Kaspersky doesn't collect or store passcodes you enter on the site.





## FOR MORE INFORMATION

For more information on cybersecurity, or to continue the conversation and learning process, visit the Canadian Centre for Cyber Security website:  
[cyber.gc.ca/en/](https://cyber.gc.ca/en/).

For more information on Passphrases, passwords and PINs, visit the Government of Canada's website:  
[getcybersafe.gc.ca/en/secure-your-accounts/passphrases-passwords-and-pins](https://getcybersafe.gc.ca/en/secure-your-accounts/passphrases-passwords-and-pins)

### Kids Help Phone:

Contact by text message at 686868 or by phone at 1-800-668-6868 from across Canada, 24 hours a day, 7 days a week; or access their resources online: [kidshelpphone.ca](https://kidshelpphone.ca)



