Grades
4-6

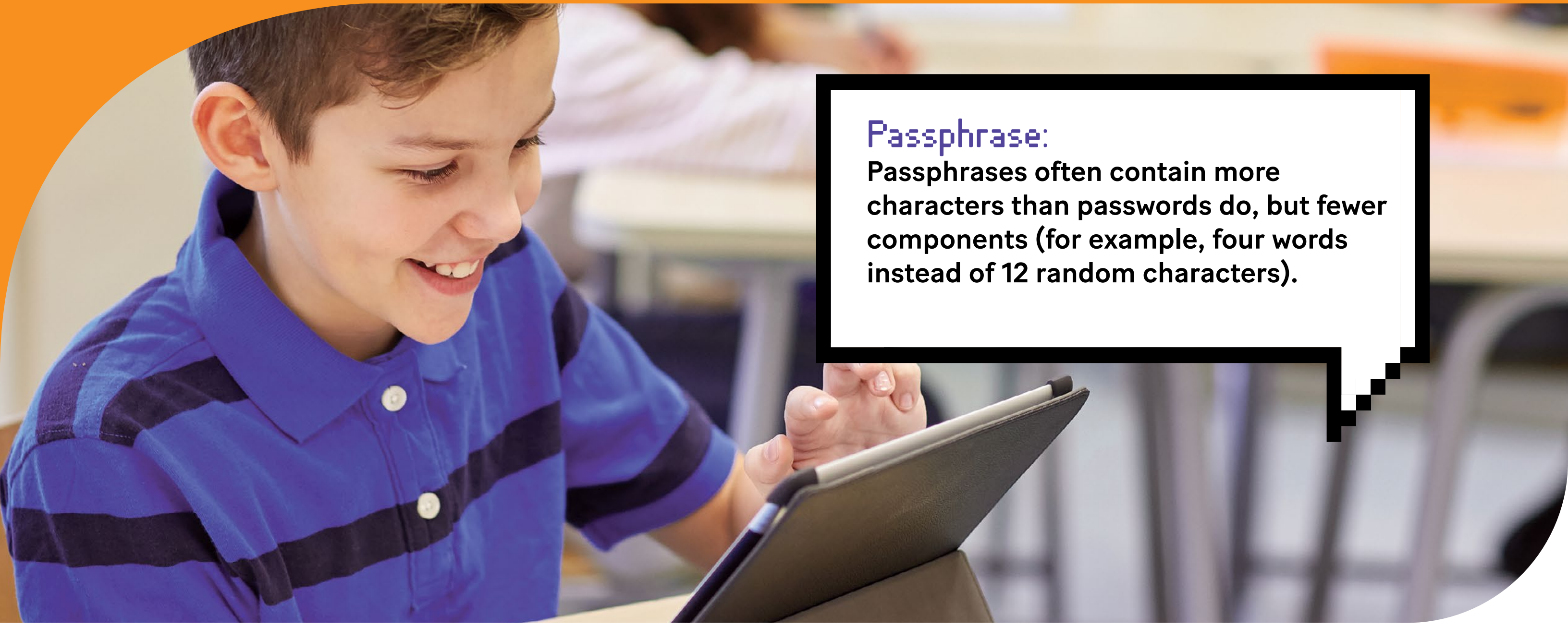
Privacy Online: Passcodes

ROGERS
cybersecure
catalyst

What are passcodes? Passcodes (also known as “passwords”) are like keys for keeping personal and private information safe from others. Personal information includes things like kids’ hobbies, favourite food, etc.; whereas private information includes details that can identify kids, such as street address, phone number, date of birth, etc. Although personal information alone is generally not enough to identify someone, when it’s shared alongside private information and ends up in the hands of the wrong person, it can be used to guess passcodes, and unlock access to online accounts and profiles (e.g., a passcode using a kid’s school team jersey number can be easily guessed at). Passcodes can be a series of random words put together, a memorable phrase, or a combination of words, numbers and symbols unique to the user – like a fingerprint!

Kids might use passcodes for school profiles such as a school-specific email address, or at home for personal YouTube or online gaming profiles – and it’s important that their passcode for each is different, yet strong. Passcodes should be mindfully cared for and never shared, or else kids risk losing access and control over their profiles, damaging their reputation, or having their identity stolen.

This resource offers information and guidance for parents/guardians on how to understand and communicate with kids about good passcode practices, creating strong and secure passcodes, protecting them from others, and managing them carefully.



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

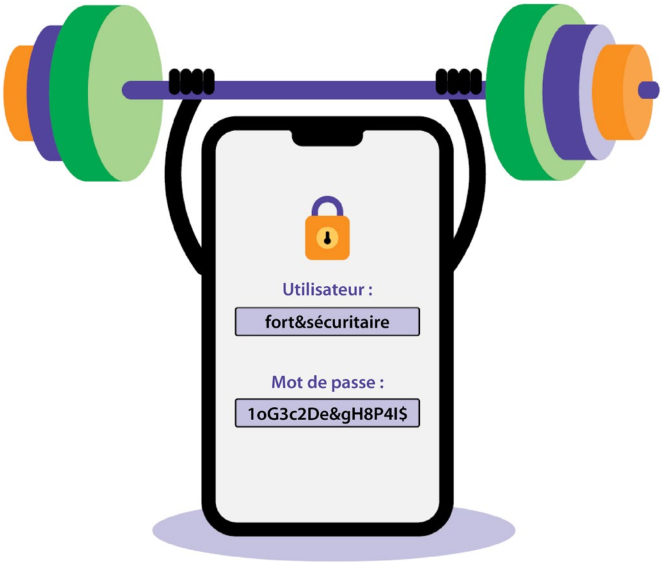
A DEFINITION

Creating strong passcodes

Passcodes protect kids, and prevent others from accessing the personal and private information stored in their online profiles. In order to do this, kids must understand how to create strong passcodes. Following the simple passcode rules below will help keep the entire family safe and secure online:

- **Longer is stronger!** Long passcodes are harder for others to guess. Most online 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. If kids are having a hard time thinking of a passphrase, encourage them to use words that rhyme, or create an image in their mind or a joke!



Utilisateur :
fort&sécuritaire

Mot de passe :
1oG3c2De&gH8P4I$

- **Never use any personal or private information** in a passcode or passphrase, such as information that someone might already know or easily get from someone else. For example, if Alex's favourite dessert is ice cream, then iloveicecream would be an easy passcode to guess!

- If a passcode contains numbers (which is highly recommended!), parents/ guardians should insist that kids **do not repeat numbers** like '777' or use a number count like '123' / '321', or a significant date like a birthdate or phone number. These are too easy to guess!

- **Create passcodes with a variety of characters!** Parents/guardians should ask kids to include uppercase letters (ABC) and lowercase letters (abc), numbers (123) and symbols (!, @, #). Using all four types makes for a super strong passcode!

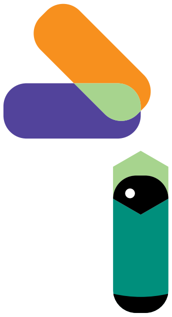
Remember this!

The same rules apply when creating usernames and screen names. It's unsafe to have real first and/or last name, ages, gender, location, etc., as screen names or usernames are publicly viewable. Be creative!

B RELEVANCE

Protecting passcodes

Creating a strong passcode is very important, but that's only the first step kids can take to keep devices and accounts safe; the second step is for kids to keep their passcodes to themselves! Here are some ways kids can protect themselves and their passcodes:



- **Always use a unique passcode** for each profile because, if a passcode is stolen from one account, other accounts will still remain protected!
- **Do not reuse old passcodes** – even if the old passcodes were for other accounts or profiles. If anyone knew or guessed them then, they can now use old passcodes to log into other accounts.
- **Be sure that each passcode is very different from each other**, because similar passcodes – though not the same – can be easily guessed. For example, it wouldn't be a good idea to use "@catCOMPUTER5" and then "@catPHONE5".
- Best practice is to **change passcodes** from time to time. Kids can set a date in their calendar to do this, because even strong passcodes can eventually be guessed. And of course, be sure to make the new passcode completely different from all others!

Tip:

There are websites that provide an idea of just how strong a passcode is, as well as approximately how long it would take to someone or a computer system to guess it! Try it here:

Kaspersky Password Check
https://password.kaspersky.com/

- **Don't share passcodes with friends,** not even best friends! Depending on individual household rules, passcodes should be shared with parents/guardians only, for emergency purposes.

Hacked:
Someone gained access to an account, profile or device without permission.

- **Avoid logging into accounts on other people's devices,** as passcodes can be easily retrieved. If absolutely necessary, kids should be sure to log out of profiles and devices when finished.
- **Don't allow websites to "remember" or store passcodes.** Often, websites and Internet browsers will ask to the user to save login credentials, such as usernames, emails, passcodes or addresses, for convenient future login. Although this may seem convenient, it could put personal or private information at risk.
- **Be aware of physical surroundings!** Kids need to watch out for others trying to look at their passcodes as they type it into their computer or other devices.
- **Never log into profiles when on public Wi-Fi,** such as free Wi-Fi available at a restaurant or hotel, because this makes it easy for someone connected to the same Wi-Fi to steal passcodes.
- **Avoid playing free games or doing fun quizzes online that ask any personal or private information, or ask to link to other online accounts like social media profiles.** These games are often an attempt to access information that could lead to revealing a passcode.
- If kids realize or suspect that any of their profiles have been hacked, parents/guardians should ask them to **change their passcode immediately!**

Conversation Starter:

Why is it important to protect our online accounts/profiles? What kinds of information could be stolen if passcodes are shared?

C CALL TO ACTION

Managing passcodes

For kids, managing a lot of profiles, usernames and passcodes can be dif cult. Parents/guardians can consider using an online family passcode manager for individual family passcodes. Depending on individual household rules, passcodes should be shared with parents/guardians only, for emergency purposes.

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.

ACTIVITY 1

Activities are a useful way for kids to test and demonstrate their knowledge on the topic covered in this resource. Have them try the activities themselves, and offer support when needed.

Privacy Online: Passcodes Word Search

Can you find the keywords related to privacy online: passcodes? As you find the words listed below, think about what they mean, what you've learned, and how you can help share this information with others!

Y	N	U	M	P	C	V	Z	S	Z	C	B	J	M	B
T	T	K	W	R	H	P	S	Y	T	H	U	C	L	R
Y	C	C	F	E	I	H	Y	W	S	F	O	R	T	F
A	R	O	D	N	F	R	M	P	I	E	M	V	K	M
G	E	M	O	S	F	A	B	Y	M	N	O	Y	A	K
P	E	P	Y	E	R	S	O	L	C	S	T	G	C	R
V	R	T	S	I	E	E	L	P	G	D	D	P	A	T
V	Q	E	N	G	S	D	E	R	A	K	E	R	R	S
D	X	S	G	N	E	E	S	O	A	E	P	I	A	W
S	A	Z	L	E	K	P	S	T	R	L	A	V	C	U
Q	N	H	C	M	V	A	G	E	C	B	S	E	T	D
Q	B	D	K	E	V	S	E	G	J	X	S	I	E	Y
R	Y	F	N	N	Z	S	W	E	G	F	E	O	R	L
I	B	H	M	T	V	E	Q	R	J	Q	K	S	E	W
P	U	P	K	S	H	H	L	A	U	U	G	H	S	L

Information

Accounts

Protect

Passphrase

Private

Strong

~~Characters~~

Symbols

Create

Password

Numbers

ACTIVITY 2

Check your understanding!

Fill in the blanks using the words provided.

immediately

device

Wi-Fi

remember

1 Websites should NOT .... your passcodes.

2 Never store passcodes in or on your ....

3 Change your passcode .... if you get hacked.

4 Do not sign into your profiles when on free public ....

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.

D 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/.

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

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

Toronto Metropolitan University

ROGERS cybersecure catalyst