

# 01. Internet Safety and Digital Identity





# Table of Contents

01.

## Intro

You can describe the  
topic of the section here

02.

## Internet Safety Basics

You can describe the  
topic of the section here

03.

## Digital Citizenship

You can describe the  
topic of the section here



04.

## Password Etiquette

05.

## Digital Footprint and Privacy



# Welcome to Internet Safety and Digital Identity!

With the ever growing world of technology and the everyday use of the internet it is important you understand what it means to be online and how to stay safe.



# What are we working on?



## Objective

Understand what happens to our information online and how to stay safe.



## Why is this important

The internet offers incredible opportunities but also poses risks. Understanding how to protect yourself online is crucial.



## Are you at risk

If you are online you are at risk of malicious software of threat actors.

# 02. Internet Safety Basics

## Topics Covered:

**Strong Passwords:** Create and manage secure passwords.

**Privacy Settings:** Safeguard your personal information on social media and websites.

**Avoiding Scams:** Recognize common online scams and how to avoid them.





# Creating Strong passwords

A strong password will consist of letters, numbers, and symbols. Below are some good tips to follow for your passwords/

- Combination of letters, numbers, symbols
- Minimum of 16 characters
- No personal info and never share it

Alternatively you can use a trusted password manager!



<https://www.passwordmonster.com/>



What goes online, stays online. So be careful what to share so it doesn't fall into the wrong hands. Here is some things not to share:

- Address, Location, Travel Plans
- Full birthdate, Phone Number, Full Name
- Passwords and personal facts

Now some exceptions can be made for secure account creation but generally avoid sharing personal information.



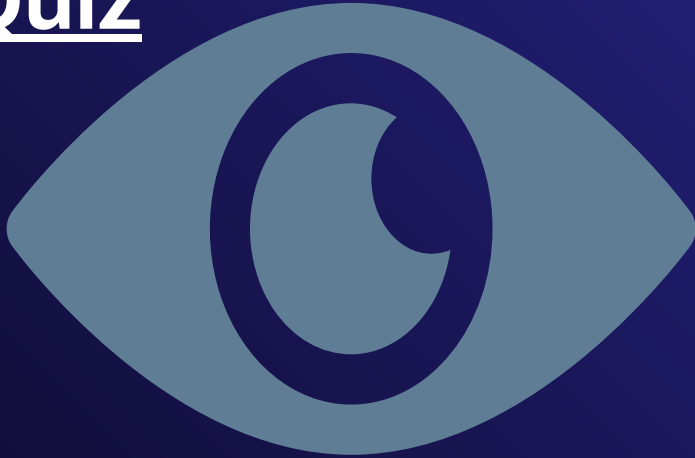
# What to keep private?



<https://services.priv.gc.ca/quiz/en/youth>



# Avoiding Online Scams Quiz



How can we spot an online scam before we fall for it?

- To good to be true
- Verify sender email or number
- Research first
- Grammar issues or poor formatting
- Sense of urgency or free offer

By following these tips, you can better protect yourself and others from falling prey to online scams and fraudulent activities.



03.

# Digital Citizenship



# What is digital Citizenship

Digital citizenship refers to the responsible and ethical use of technology, encompassing the behaviors, norms, and rules for appropriate online interactions. It involves engaging with digital tools, platforms, and communities in a way that promotes safety, respect, and positive contributions to the digital world.



# Why you should care!

Your digital footprint is the trail of data you leave behind from online activities.

Positive actions, such as showcasing achievements, volunteering, and respectful interactions, can enhance your digital reputation.

Colleges, employers, and others often research applicants online, making it important to manage your digital footprint carefully.

Example: Imagine posting about a volunteer project or sharing a thoughtful comment on a blog—these actions can positively influence how others perceive you online.



# A couple ways to maintain good digital citizenship

## Respect Others

Treat others online with kindness and respect, avoiding cyberbullying or engaging in disrespectful behavior.

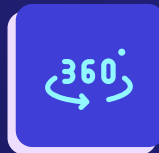


## Protect Personal Information

Safeguard your personal information by being cautious about what you share online.

## Think Before You Post

Before posting or sharing online, consider the potential impact of your words and actions. Content shared online can be permanent.

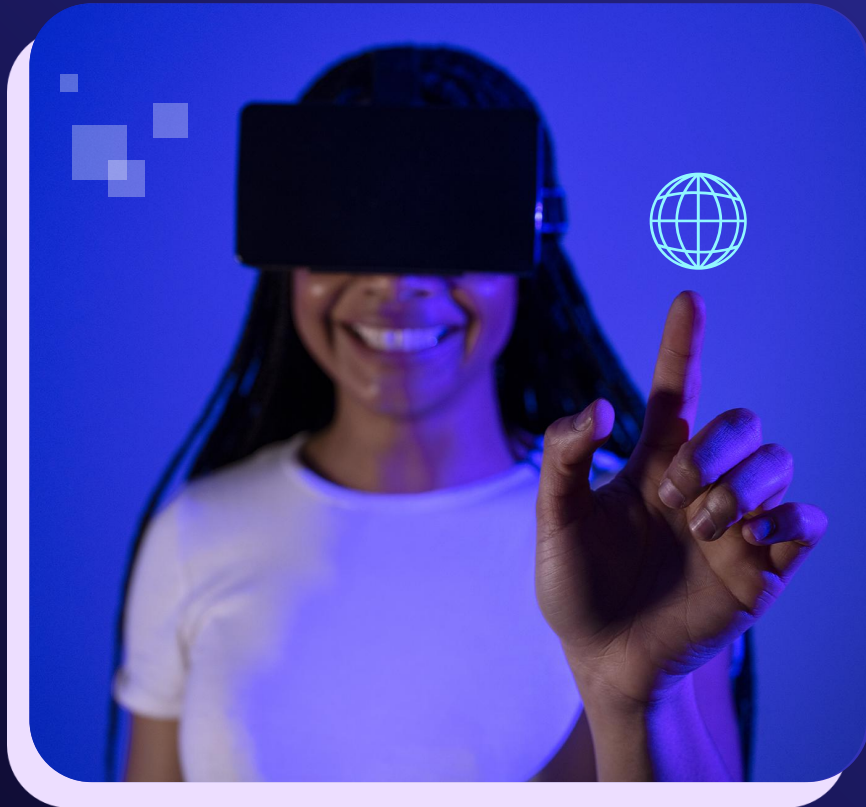


## Verify Information

Verify the accuracy and credibility of information before sharing it online. Misinformation can spread quickly and contribute to misunderstandings or harm.

# 04. Password Etiquette





# What is password etiquette?



Password etiquette is the Do's and Don'ts of handling and storing your passwords.



# Golden Rules



## Never Share...

Never share your passwords, this includes in a message, on paper, or any form of sharing.



## Use Strong and unique passwords

A combination of letters, symbols, and numbers, try to aim for over 16 characters if possible.



## Use a password manager if possible

A password manager is an essential tool in this age to keep your accounts secure.



# Discuss

## Questions

- Is Jason123 a strong password? Why or why not?
- A friend asks to borrow my game account and needs my login details, what should I say?





# 05. Digital Footprint and Privacy



**Your digital footprint is the trail of data you create while using the internet. It includes your online activities, interactions, and the content you share.**





# How it affects you

## Why?



our digital footprint can influence your reputation and opportunities, including college admissions and job applications.

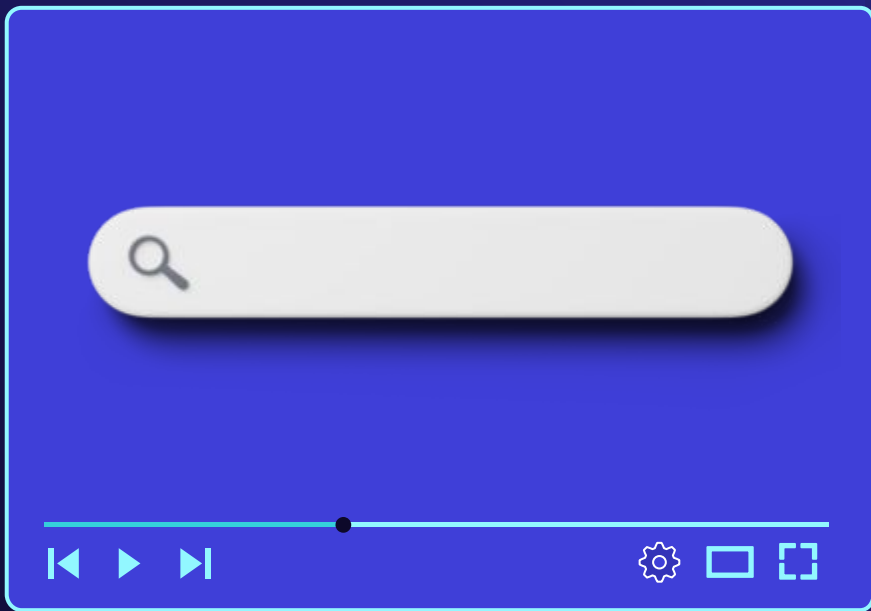
## How?

Regularly review privacy settings on social media platforms and adjust them to control who can see your information.

## When?

When browsing the internet be cautious about sharing personal details online, such as your full name, address, phone number, or financial information.





# Activity

Try googling your name or social media profiles and see if you can find any trail of your digital footprint.





# Thank you!

CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics and images by **Freepik**

