



Being Online

Gr. 8-12 Activity Write Up

Being Online

Terms of Use	2
About Actua	2
Activity Summary	3
Learning Outcomes	3
Logistics (Timing, Groups Size, Materials)	4
Safety Considerations	6
Curriculum Links	7
Activity Procedure	8
To Do in Advance	8
Opening Hook	9
Section 1: Digital Footprint	9
Section 2: Who are Others Online?	12
Section 3: Digital Wellbeing	12
Reflection & Debrief	14
Delivery Recommendations	14
Remote (Online)	14
Unplugged (Low/No Tech)	14
Delivery Adaptations	16
Modifications	16
Extensions	17
References & Gratitude	19
Appendices	21
Appendix A: Career & Mentor Connections	21
Appendix B: Background Information	22
Appendix C: Additional Resources	26



Terms of Use

Prior to using this activity or parts thereof, you agree and understand that:

- It is your responsibility to review all aspects of this document and the associated activity write ups, and ensure safety measures are in place for the protection of all involved parties.
- Any safety precautions contained in the “Safety Considerations” section of the write-ups are not intended as a complete list or to replace your own safety review process.
- Actua shall not be responsible or liable for any damage that may occur due to your use of this content.
- You may adapt the content for your program (remix, transform, and build upon the material), providing appropriate credit to Actua and indicating if changes were made. No sharing of content with third parties without written permission from Actua.

About Actua

Actua is Canada's leading science, technology, engineering and mathematics (STEM) youth outreach network, representing a growing network of over 40 universities and colleges across the country. Each year 350,000 young Canadians in over 500 communities nationwide are inspired through hands-on educational workshops, camps and community outreach initiatives. Actua focuses on the engagement of underrepresented youth through specialized programs for Indigenous youth, girls and young women, at-risk youth and youth living in Northern and remote communities. For more information, please visit us online at www.actua.ca and on social media: [Twitter](#), [Facebook](#), [Instagram](#) and [YouTube](#)!



Being Online

Activity Summary

Participants will explore their online identity and discuss the various intentions of other users online. Key topics that will be discussed include digital footprint, social media, oversharing and digital wellbeing. Participants will leave with a stronger understanding of how to interpret the online behaviours of others, as well as how to carefully consider the importance of being aware of their digital footprint.

Developed by Actua, 2022.

Delivery Environment	Activity Duration	Intended Audience	Tech
In-Person	1 hour & 45 mins	Grades 8-12 (Ages 14-18)	<p>Certain activities will require a laptop/tablet. With modifications, it is possible to run this entire lesson in pairs/groups. Facilitators should have access to a laptop, projector, speakers, and a screen or blank wall to project onto.</p> <ul style="list-style-type: none">• Projector• Speaker• Screen / Blank Wall• Laptops/Tablets

Learning Outcomes



Following this activity, participants will:

- Understand their digital footprint and online behaviour can be interpreted.
- Use and share key strategies to be smart and responsible while online.
- Identify what information should not be shared on the internet and know how to prevent/limit over sharing of personal information (privacy management).
- Understand how to promote digital wellbeing.



TOOLSETS	SKILLSETS	MINDSETS
Knowledge, resources, and experiences <ul style="list-style-type: none"> • Online identity • Digital citizenship • Social media • Digital footprint 	Digital skills, STEM skills, & essential employability and life skills <ul style="list-style-type: none"> • Digital literacy • Being safe and responsible online • Communicating online 	Digital intelligence, community action, and computational thinking <ul style="list-style-type: none"> • Understanding your relation to technology • Digital wellness • Privacy management

Logistics (Timing, Groups Size, Materials)

Section Title	Est. Time	Group Size	Materials
Opening Hook	10 minutes	<i>Whole Group</i>	Facilitators <ul style="list-style-type: none"> • Board & Board Marker Per Participant <ul style="list-style-type: none"> • Laptop/Tablet
Section 1: Digital Footprint	PART 1: Digital Footprint Management 15 minutes	<i>Whole Group; Individual</i>	Facilitators <ul style="list-style-type: none"> •  Live My Digital for studen... Per Participant <ul style="list-style-type: none"> • Paper & Writing Utensil
	PART 2: Oversharing 20 minutes	<i>Whole Group</i>	Facilitators <ul style="list-style-type: none"> •  Teen Voices: Oversharing ... • Board & Board Marker • Oversharing on Profiles Slide Deck
	PART 3: Social Media Reflection 15 minutes	<i>Whole Group</i>	Facilitators <ul style="list-style-type: none"> • Digital Footprint Map Example • Board & Board Marker



Section Title	Est. Time	Group Size	Materials
Section 2: Who are others online?	15 minutes	<i>Whole Group; Individual</i>	Per Participant <ul style="list-style-type: none"> Laptop/Tablet Imposter (Choose Your Own Adventure)
Section 3: Digital Wellbeing	20 minutes	<i>Whole Group; Individual</i>	Facilitators <ul style="list-style-type: none"> Digital Wellbeing Memes Slide Deck Social Media Icons (Appendix C) Per Participant <ul style="list-style-type: none"> Colouring Utensil & Paper Laptop/Tablet Meta: Promoting Safety and Expression TikTok: Wellbeing Guide
Reflection & Debrief	10 minutes	<i>Whole Group</i>	<ul style="list-style-type: none"> N/A

Safety Considerations

Safety considerations have been provided below to support safety during this activity, however they are not necessarily comprehensive. It is important that you review the activity and your delivery environment to determine any additional safety considerations that you should be implementing for the delivery of these activities.

Emotional Safety

The goal of this Cyber Smart project is to equip participants with the tools and knowledge to understand online behaviours and make safe decisions.

- Facilitators should understand that participants have different lived experiences and prior knowledge about cyber safety, cyber security and digital citizenship. This activity may involve or lead to discussion of sensitive topics, such as cyberbullying and other online risks. Facilitators should always keep the participants' emotional safety in mind in these discussions, and defer to training from their institution and training received for this project.
- Facilitators should focus on guiding discussion toward an appreciation for healthy and safe online behaviours, and empowering participants to make responsible, informed and smart choices.

Online Safety

Some components of this activity require the use of devices connected to the internet.

- Facilitators should review the provided videos and read/explore provided websites and materials to determine if they are suitable for their participants.
- Where applicable, facilitators should remind participants to stay on task and only use links provided within this activity.
- Facilitators should also model and encourage appropriate online behaviour by all participants in the group (e.g., using chat boxes to answer and ask questions, using positive and encouraging language, using devices for the purpose of the task).



Curriculum Links

Each of these activities align with these components found in the Canadian Computer Science Framework:

Cyber Security

- Starting learners should be able to define cybersecurity and create safe passwords using effective criteria. Proficient learners should be able to describe common cyber attacks and identify malicious content, apply prevention practices and assess the role that people play in creating, preventing, and minimizing the impacts of cyberattacks as well as consider how they affect people and society (p. 24).

Data: Data Governance

- Starting learners should be able to identify ways that their digital or physical activity creates digital data and learn how to adjust privacy settings on commonly used digital tools. Proficient learners should be able to discover who owns the digital data they produce, as well as assess provincial, national and Indigenous data governance laws/agreements and be able to advocate for their data rights and the rights of others (p. 26).

Technology and Society: Ethics, Safety & the Law

- Starting learners should be able to identify strategies to protect their personal data and identity online. Proficient learners should be able to define and apply basic copywriter principles, explain privacy concerns, and assess the effects of computer crime/hacking on self and society (p. 28).

Activity Procedure

To Do in Advance

Section Title	Preparation
General	<ul style="list-style-type: none"> • Think ahead and be ready to adapt: <ul style="list-style-type: none"> ◦ Determine your delivery method and leverage ideas from the delivery recommendations and adaptations sections. ◦ While estimated times are provided, it will be helpful to think about how much time you would like to spend on different activities and discussions. ◦ While group sizes (individual, pairs, groups) are suggested, many activities are flexible for whatever will work in your classroom. • Prepare for the content: <ul style="list-style-type: none"> ◦ Have answers in mind to share with participants for the various reflection questions asked. ◦ Examine the provided videos and read/explore the provided materials in <i>Appendix C</i> to determine if they are suitable for your participants. • Equipment: <ul style="list-style-type: none"> ◦ Ensure device, screen and projector are set up. ◦ Prepare participant devices.
Section 1 Part 2: Oversharing	<ul style="list-style-type: none"> • Familiarize yourself with the Oversharing on Profiles Slide Deck.
Section 2: Who are others online?	<ul style="list-style-type: none"> • Familiarize yourself with the “choose your adventure” game: Imposter.
Section 3: Digital Wellbeing	<ul style="list-style-type: none"> • Familiarize yourself with the Digital Wellbeing and Safety resources developed for two popular social media platforms: Meta and TikTok



Opening Hook

1. Ask participants the following questions:
 - a. **“What was the last thing you shared online?”**
 - b. **“What do you think you would find if you Googled your name?”**
2. If suitable, have participants actually Google their names to see what comes up. Regularly searching your name is a good practice in managing your digital footprint.

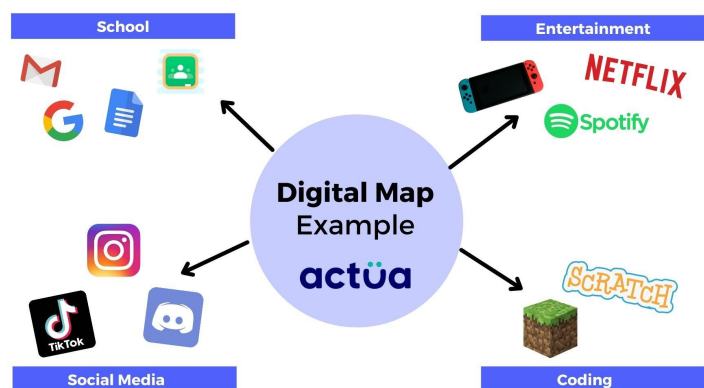
Section 1: Digital Footprint

PART 1: DIGITAL FOOTPRINT MANAGEMENT

1. Ask participants to guess how long the average person under 25 years old spends online every day. Answer: About 7 hours!
2. Start a brainstorm on the board with the answers to participants' responses to: **“What does *being online* mean to you?”**
 - a. Additional prompts: What do you do online? What can you do on the internet?
 - b. Possible responses: scrolling through social media, making TikToks, watching videos on YouTube, streaming movies on Netflix, online gaming (e.g., League of Legends, Minecraft), video calling friends, searching online.
3. Ask participants **“What do you know about the term ‘Digital Footprint’?”**


This is the trail of data you create when using the internet (e.g., the website you visit, posts you make, emails you send).

4. Digital Footprint Mapping: Distribute blank paper and a writing utensil. Participants will write their name in the centre and think of all the ways they have been connected to the internet in the last week (see example on the right).



- a. If time permits, consider having participants compare their digital footprint to someone who might live in a rural and remote location where connectivity is challenging.
5.  [Live My Digital for students: Digital Footprint](#) (GDST, 4:52s)

PART 2: OVERSHARING

1. Ask participants **“How would you define oversharing?”** (see *Background Information in Appendix B* for more information).
2. Play this video for participants:
 [Teen Voices: Oversharing and Your Digital Footprint](#) (Common Sense Education, 3:34s).
3. Start a brainstorm on the board with the answers to participants’ responses to: **“What kind of information should you keep private (offline AND online)?”**
 - a. **Note:** Include the following examples in addition to what participants might share:
 - i. Full name, email address, your favourite sport, school name, parent’s name, birthday, relationship status (and other examples of personal data that can potentially be used to identify a person).
4. Ask participants **“What are the risks of oversharing?”**
 - a. *Possible responses:* your information can be stolen (e.g., birthdays, locations, full name), accounts created in your likeness, recruiters/coaches can see things you might find embarrassing, and that could impact your chance of getting into a school/career/sports team; oversharing between friends can result in hard feelings and broken trust.
 - b. **Note:** Answers can also take a more serious tone, including being kidnapped or stalked. It is important to bring up the importance of being mindful about what you share and who you share it with.
5. Facilitate the [Oversharing on Profiles Slide Deck](#). Participants will try to find information on the profile that a cybercriminal might find interesting (see *Speaker Notes* under each slide for more information).
 - a. After each slide, start a whole group discussion on what information they thought cybercriminals would find interesting from these profiles.



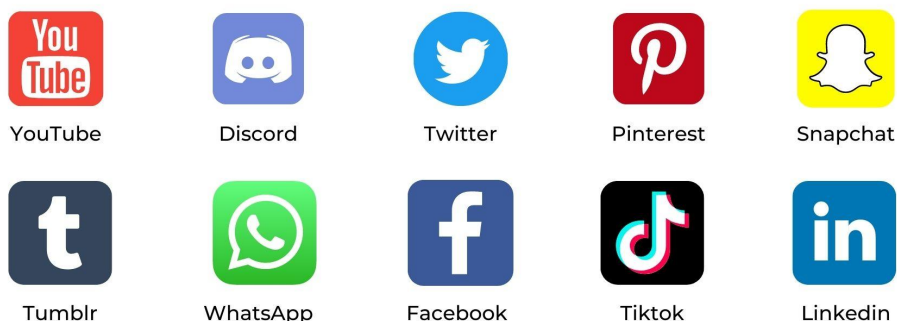
- b. Ask participants to suggest strategies to help us keep our accounts more secure (prevention tips/security fixes).
 - i. Possible responses: making accounts private (update privacy settings) - none of these accounts were private and some posts were made to the public; use discretion whenever posting (use the Grandma Rule/Future Me Rule!); only allow followers that you know; revise profile content regularly.
 - ii. See Background Information in Appendix B for more information.

PART 3: SOCIAL MEDIA REFLECTION

1. Ask participants **“What is social media?”**
2. Display the *Social Media Icons* (Appendix C). **“How many of these are you familiar with? How many of these do you have an account with? What made you want to make an account?”**

actüa

Social Media Examples



3. Do a brainstorm as a group on both the pros and cons of social media.
 - a. Possible responses (pros): allows you to connect with people from different backgrounds, find groups of people you relate to (e.g., LGBTQ+ communities), connectivity, etc.
 - b. Possible responses (cons): comparisons, impact on mental health, can become addictive, etc.
 - c. **Note:** This discussion could be extended by having participants compare two types of accounts (e.g., Meme page (9gag) vs. educational page (e.g., National Geographic): Who created the content? Is it kind? What kind of information do they share?

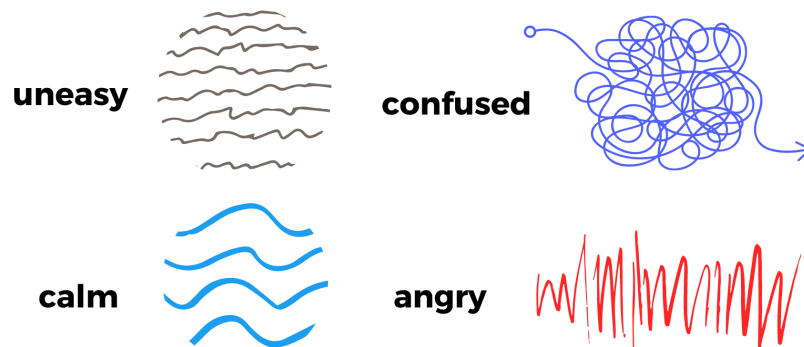
Section 2: Who are Others Online?

1. Ask participants **“Why might someone try to change aspects of their identity - or even be someone entirely different - online?”**
 - a. Possible responses: cybercriminals trying to trick you into sharing personal information, sometimes this is easier to be your authentic self online where you can be anonymous.
 - b. See Background Information in Appendix B for more information.
2. Give participants 10 minutes to play this “choose your adventure” game: [Imposter](#) (Twine Story hosted on Itch.io). Their task is to make the most cyber smart choices in each scenario.
 - a. **Note**: This can be done individually, in pairs or in groups.
3. Ask participants **“What can you do if someone makes you uncomfortable when you’re online/you suspect someone is an online imposter?”**
 - a. Possible responses: report the account (**Note**: All social media applications have a method by which you can anonymously report an account so the person who owns the account won't know you reported them), if you know the person who is trying to add you, ask them in person if that is truly them, tell a trusted adult (e.g., parent, guardian, teacher), ignore the person, do not respond to them, block or mute the person, take a screenshot to save and collect evidence of imposter; ensure you have privacy settings on all of your accounts.

Section 3: Digital Wellbeing

1. Ask participants **“How much time would you say you spend on a device? How much of that time is spent on social media?”**
2. Take participants through the [Digital Wellbeing Memes Slide Deck](#). **“Are any of these memes relatable? Why?”**
3. Distribute paper and colouring utensils for them to draw their feelings abstractly using a colour, shape, line style. **“In your experience, how do you feel after being online?”** (e.g., scrolling through social media, bingeing your favourite episodes, or doing schoolwork). See the image below for examples.





4. Distribute devices and have participants explore the following Digital Wellbeing and Safety resources developed for two popular social media platforms: [Meta](#) (Facebook, Instagram, Whatsapp) and [TikTok](#). Discuss the following questions:
 - a. **“Did you know that these types of features existed?”**
 - b. **“What is something new to you?”**
 - c. **“What is something that could be improved?”**
5. Continue the discussion by asking participants **“What are some healthy choices you make while online? What are some healthier choices you can make while going online in the future?”**
 - a. **Note:** In addition to the responses participants share, include the following:
 - i. Balance time online
 1. Take regular breaks from the screen
 2. Find time to do hobbies without a device
 - ii. Social media use
 1. Take control of your notifications
 2. Avoid using social media before bed
 3. Be intentional when you use social media (vs. mindless scrolling)
 4. Follow people and pages you enjoy
 5. Keep your online bubble safe and positive

Reflection & Debrief

1. Discuss the following question(s) with participants to help them reflect on themselves and their online experiences (these could be shared with the entire group/in small groups/written down):
 - a. **“How would you compare your offline self to your online self?”**
 - b. **“Who do you want to be online? Who do you want to be offline? How are they similar, why might they be different?”**
 - c. **“Why would you say it is important to focus on real world interactions and not just online interactions?”**
2. Discuss the different careers listed in *Appendix A: Career & Mentor Connections*.
3. Encourage participants to be a Cyber Smart Ambassador and share their learnings from this activity with their friends and family.

Delivery Recommendations

How might you deliver this content in different settings? Every activity has been designed for in-person delivery. Here, we provide recommendations for remote learning (online) or unplugged (no tech).

Remote (Online)	Unplugged (Low/No Tech)
General	
<ul style="list-style-type: none">• Encourage participants to unmute themselves or type in the chat based on what is easiest for them to communicate.• Leverage a tool where participants can all participate online during discussions (e.g., Mentimeter, Jamboard, etc).• Make note of any links that need to be shared and be prepared to share them in the chat.• Use polls or other group interactions to check in and keep up engagement.	<ul style="list-style-type: none">• Leverage boards to do brain storms/write down participant responses.



Remote (Online)	Unplugged (Low/No Tech)
Opening Hook	
<ul style="list-style-type: none"> Activity can be done as-is online. Since you will not be present in the room with participants, if you choose to let them search their names online, gently remind participants to be mindful of any links they might click after searching their name. 	<ul style="list-style-type: none"> Focus on the discussion pieces.
Section 1: Digital Footprint	
<p>Part 1: Digital Footprint Management</p> <ul style="list-style-type: none"> Activity can be done as-is online. <p>Part 2: Oversharing</p> <ul style="list-style-type: none"> Activity can be done as-is online. For brainstorming, consider doing a verbal discussion or use a collaborative tool (e.g., Jamboard, Google Doc, Mentimeter). While slides are shared, ask participants to record notes (on paper or their devices). <p>Part 3: Social Media Reflection</p> <ul style="list-style-type: none"> Activity can be done as-is online. 	<p>Part 1: Digital Footprint Management</p> <ul style="list-style-type: none"> Majority of the activity can be done as-is unplugged. If unable to play the video, examine separately and share key takeaways with participants. <p>Part 2: Oversharing</p> <ul style="list-style-type: none"> Activity can be done as-is unplugged. <p>Part 3: Social Media Reflection</p> <ul style="list-style-type: none"> Activity can be done as-is unplugged.
Section 2: Who Are Others Online?	
<ul style="list-style-type: none"> Consider doing the Twine Story as a whole group and using a polling option to see which route students would want to take. 	<ul style="list-style-type: none"> Put participants in groups and create different scenarios to assign to each group to create their own story (each story should use cyber smart choices).

Remote (Online)	Unplugged (Low/No Tech)
Section 3: Digital Wellbeing	
<ul style="list-style-type: none"> Activity can be done as-is online. 	<ul style="list-style-type: none"> Print out the memes or focus on the discussion question. Print the pages of the Digital Wellbeing and Safety websites for Meta and TikTok. Put participants into groups to discuss the questions.
Reflection & Debrief	
<ul style="list-style-type: none"> Activity can be done as-is online. For brainstorming, consider doing a verbal discussion or use a collaborative tool (e.g., Jamboard, Google Doc, Mentimeter). 	<ul style="list-style-type: none"> Activity can be done as-is unplugged.

Delivery Adaptations

How might you adapt the time, space, materials, group sizes, or instructions to make this activity more approachable or more challenging? **Modifications** are ways to make the activity more accessible, **extensions** are ways to make the activity last longer or more challenging.

Modifications

GENERAL

- Ensure captions are on during videos played.
- Provide computer mice where laptops are in use.
- Use pairs/groups instead of having participants work individually.

SECTION 1: DIGITAL FOOTPRINT

- Part 1: Digital Footprint Management**
 - Create your own example to show participants.



- Create a map as a class instead of individually.
- **Part 2: Oversharing**
 - Do one profile with participants to give them an idea of what could be produced.
 - Participants can work in pairs/groups.
 - Reduce the number of profiles you have participants analyze.

SECTION 2: WHO ARE OTHERS ONLINE?

- Do Twine story as a whole group and read the story out loud.

Extensions

GENERAL

- **Computer Science Connection:** Generate discussions on artificial intelligence.
 - Many online accounts on platforms like Twitter are run by bots, which are computer controlled programs. They use existing photos from the internet and generate content.
 - Have you ever interacted with a bot? They tend to re-use or repost information and share very few personal details.

SECTION 1: DIGITAL FOOTPRINT

- **Part 2: Oversharing**
 - Play "[Fight Back](#)" (Battle the Werewolf: Part of a series of online games created by Texas A&M Information Technology to test online security knowledge and safe tech habits).
 - Analyze different celebrities and see what they can learn with 6 clicks? [Real-Life Stories - 6 Degrees of Information](#) (NetSmartz, 7:26s)
 - Discuss *why* people overshare might overshare: [Your brain on likes: The science of oversharing online](#) (CBC Radio).

SECTION 3: DIGITAL WELLBEING

- Have participants create their own memes (there are many web-based meme generators - you will want to find one appropriate for your participants).



REFLECTION & DEBRIEF

- Participants can create a [Canva Poster](https://www.canva.com/posters/templates/campaign/) to share strategies with their friends and families on what cyber smart steps we can take when interacting with new users online. Share this link with them <https://www.canva.com/posters/templates/campaign/>. It will be helpful to explore Canva to get an idea of how to use this resource yourself.
 - Quickly show them how to create a new project and the different editing features they can use. If helpful, choose a suitable Canva template rather than have them find one themselves/have them draw it out.
 - Participants can draw their creations on paper rather than on Canva.
 - If time permits, have participants share their work.

References & Gratitude

- Canadian Centre for Cyber Security. (2022, January). *Digital Footprint*.
<https://cyber.gc.ca/en/guidance/digital-footprint-itsap00133>
- Canadian Centre for Cyber Security. (2020, July 3). *Social Media Account Impersonation*.
<https://cyber.gc.ca/en/guidance/social-media-account-impersonation>
- Common Sense Education. (2019, January 12). *Teen Voices: Oversharing and Your Digital Footprint* [Video file].
<https://www.youtube.com/watch?v=ottnH427Fr8>
- Cyber Degrees. (2020, April 9). *How to Become a Security Software Developer*.
<https://www.cyberdegrees.org/jobs/security-software-developer/>
- GDST. (2016, July 1). *Live My Digital for students: Digital Footprint* [Video file].
<https://www.youtube.com/watch?v=OBg2YYV3Bts>
- Government of Canada. (2020, August 25). *Cybercrime Intelligence Analyst* [Job Posting].
<https://emploisfp-psjobs.cfp-psc.gc.ca/psrs-srfp/applicant/page1800?toggleLanguage=en&poster=1449726>
- Government of Canada. (n.d.). *Social Media (Get Cyber Safe)*.
<https://www.getcybersafe.gc.ca/en/secure-your-accounts/social-media>
- Jisc. (n.d.). *Digital Wellbeing*.
<https://www.digitalcapability.jisc.ac.uk/what-is-digital-capability/digital-well-being/>
- Meta. (n.d.). *Promoting safety and expression*.
<https://about.facebook.com/actions/promoting-safety-and-expression/>
- Office of the Privacy Commissioner of Canada. (2020, January). *Are your online friends who they say they are?*
<https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/fs-fi/friend-ami/>
- Office of the Privacy Commissioner of Canada. (2018, January 10). *Discussion Topic #7: Online impersonation: prevent people from hijacking your account and pretending to be you*.
https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/topic-sujet/dt_07/
- Rasmussen College. (2018, October 1). *Everything You Need to Know About Becoming a Cyber Security Analyst*.
<https://www.rasmussen.edu/degrees/technology/blog/becoming-cyber-security-analyst/>
- Texas A&M University. (n.d.). *7 Tips for Safe Social Networking*.
<https://it.tamu.edu/security/safe-computing/identity/safe-social-networking.php>
- TikTok. (n.d.). *Well-Being Guide*.
<https://www.tiktok.com/safety/en-ca/well-being-guide/>
- University of San Diego. (n.d.). *Master of Science in Cyber Security*.
<https://onlinedegrees.sandiego.edu/should-you-become-a-cyber-security-e>



[ngineer/](#)

U.S. Army Cyber Command. (2018, February 13). *Cybersecurity Fact Sheet: Social Media Imposters*.

<https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/1440824/cybersecurity-fact-sheet-social-media-impostors/>

Viswanathan, U. (2021, May 6). *Stay safe on social*. McGill University.

<https://www.mcgill.ca/cybersafe/article/stay-safe-social>

Appendices

Appendix A: Career & Mentor Connections

ROYAL CANADIAN MOUNTED POLICE: CYBERCRIME INTELLIGENCE ANALYST

- A cybercrime intelligence analyst specializes in cybercrime, and uses that knowledge to develop strategies to identify criminal trends and patterns. They use this information to design strategic intelligence products, and provide expert advice on complex criminal investigations.

CYBER SECURITY PROFESSIONAL (INFORMATION SECURITY PROFESSIONAL)

- A cyber security professional identifies threats and vulnerabilities in various systems and softwares. They apply their knowledge to design security measures and implement solutions to defend against cybercrime, such as hacking and malware. These measures come in the form of technology and organizational processes.

CYBER SECURITY ANALYST (INFORMATION SECURITY ANALYST)

- A cyber security analyst monitors a company's computer networks and systems. In order to further protect the company from threats and breaches, they plan and implement security measures.

SECURITY SOFTWARE DEVELOPER

- A security software developer designs and integrates security software tools, develops systems, and tests vulnerabilities in their designs.

Appendix B: Background Information

DIGITAL FOOTPRINT

The [Canadian Centre for Cyber Security](#) (2022) defines digital footprint as “the trail of data you create while using the Internet. This trail of data comes from the websites you visit, the emails you send, and the information you submit or download online.”

They go on to mention that our digital footprints are built actively and passively:

- “Active digital footprint: Data left through intentional actions, such as posting on social media, filling out online forms, or agreeing to browser cookies.”
- “Passive digital footprints: Data left unintentionally or unknowingly. This data is often collected by monitoring tied to your IP address. Websites and applications may install cookies on devices without disclosure, use location tracking, or log your activities.”

OVERSHARING

Whether posting on social media or making new connections online, oversharing can put you at risk of identity theft and even threaten your physical safety. It is recommended that users do not share their personal data publicly online.

Personal Data

Personal Data is any information about you. Personally identifiable information is any information that can be used alone or in combination with other information that can identify you. Examples include:

- Full name
- Email address
- The sport you play
- School Name
- Dad's name
- Birthday
- Relationship Status

To many, it is obvious that posting information about your credit card is a big security risk, but so is posting an image with your location. These are some things



to consider when sharing online because you never know who is on the other side of the screen ([Stay Safe Online](#), 2021):

Risks of Oversharing

- Exposing your location publicly or to strangers can put you at risk of:
 - Criminals learning where you live, study and work
 - Spear-phishing emails (targeted attempt to steal sensitive information)
 - Theft of property (if you indicate you're on vacation, the takeaway is that your valuables are unattended)
- Identity theft or account infiltration (sharing information like birth date or schools can be used to reset passwords if this information is used in your identification questions).

Strategies

- Create a strong, unique password.
- Use two factor authentication.
- Avoid sharing ([Get Cyber Safe Government of Canada](#), 2020):
 - Personal information: phone number, emails, addresses, work details, school
 - Informative pictures: backgrounds that reveal license plates, street signs, etc.
 - Geotagged photos: automatically attached locations of where photos are taken.
 - Exciting news: Vacation, big purchases, events where you are away from home.
 - Banking/financial info: name of bank, card number, etc.
- Tips for Safe Social Networking ([Division of Information Technology](#), n.d.):
 - Keep your location private.
 - Review and manage your privacy settings periodically to limit the visibility of what you share.
 - Use discretion and be responsible when connecting with people online and sharing information.
 - Use the "Future Me" Rule: ask yourself if you *from the future* would want to see this. Think of yourself as a parent, as someone applying

to school/jobs, or as someone who is already a working professional. If the answer is no, you probably shouldn't post it.

- Employers, coaches, and school administrators are using social networking sites to "get to know" and weed out applicants. Don't let those certain photos cause problems for you in the future.
- What you post might also affect others besides yourself, whether it's a photo that includes other people or comments about someone you know.

ONLINE IMPOSTERS

Online imposters are users that imitate someone else and claim to be someone they are not - this can be someone that you know, or even you. You are at risk even if you do not have a social media account because an imposter can steal your information and create an account in your likeness, pretending to be the victim. A social media imposter's intentions will vary, but can include the intent to ruin someone's information or trick others into sharing private/personal information ([U.S. Army Cyber Command](#), 2018).

Be cautious about strange communication

1. They try to offer you something that is "too good to be true" (e.g., You won \$1000, just share your information to get the prize).
2. They ask you for personal information.
3. They try to get you to click on a link (links can download secret applications that can be used to transmit your location or someone else access to the media on your device).
4. They ask you to meet some of their friends.

What to do if you suspect an imposter profile

According to the [Canadian Centre for Cyber Security](#), many platforms, including Facebook, Twitter and Instagram, have a reporting system. It is important to report an account you think may be a fake/ imposter account on the social media platform you found them on.

How to reduce vulnerability to social media imposters

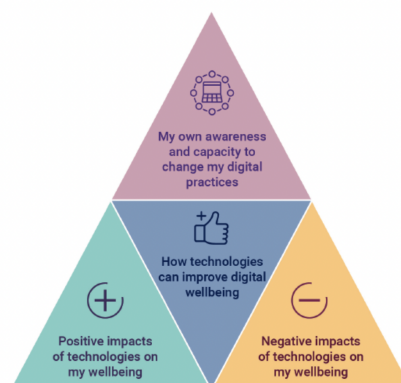
The Government of Canada and the U.S. Army Cyber Command outlines the following strategies:

- Conduct routine searches across social media platforms for your name. Include like or close spellings, as imposters often use similar spellings to remain undetected.
- Review your privacy settings often.
- Keep private information private.
- Be mindful of who you interact with online.

You can also use Google to ‘reverse image search’ any public picture of yourself to make sure no one else has used it as a profile photo.

DIGITAL WELLBEING

[Building Digital Capability](#) defines this as a “term used to describe the impact of technologies and digital services on people’s mental, physical, social, and emotional health.” See image (Jisc 2019: Model showing four aspects of digital wellbeing for individuals).



Digital wellbeing can be viewed by multiple perspectives. Building Digital Capability goes on to explain the individual and societal/organization perspective:

- “Individual perspective: personal, learning and work contexts: this involves identifying and understanding the positive benefits and any potential negative aspects of engaging with digital activities and being aware of ways to manage and control these to improve wellbeing.”
- “Societal or organisational perspective: providers of digital systems, services and content have a responsibility for ensuring that these are well managed, supported, accessible and equitable. They also need to empower and build capability in users so that all who engage with them are equipped to do so in a way that supports and/or improves their wellbeing.”



Appendix C: Additional Resources

SECTION 1: DIGITAL FOOTPRINT

Activity Slide Deck(s)

- [Oversharing on Profiles Slide Deck](#)

Video(s)

-  Live My Digital for students: Digital Footprint (GDST, 4:52s)
-  Teen Voices: Oversharing and Your Digital Footprint (Common Sense Education, 3:34s)

SECTION 2: WHO ARE OTHERS ONLINE?

Website(s)

- [Imposter \(Choose Your Own Adventure\)](#)

SECTION 3: DIGITAL WELLBEING

Activity Slide Deck(s)

- [Digital Wellbeing Memes Slide Deck](#)

Infographic(s)

- Social Media Icons (*see below*)

Website(s)

- [Meta: Promoting Safety and Expression](#)
- [TikTok: Wellbeing Guide](#)





Social Media Examples



YouTube



Discord



Twitter



Pinterest



Snapchat



Tumblr



WhatsApp



Facebook



Tiktok



Linkedin