



Being Online

Gr. 5-7 Activity Write Up

Being Online

Terms of Use	3
Activity Summary	4
Learning Outcomes	5
Logistics (Timing, Group Sizing, Materials)	5
Safety Considerations	6
Curriculum Links	7
Activity Procedure	8
To Do in Advance	8
Opening Hook	9
Section 1: Digital Persona	9
Section 2: Oversharing	10
Reflection & Debrief	11
Delivery Recommendations	12
Remote (Online)	12
Unplugged (Low/No Tech)	12
Delivery Adaptations	13
Modifications	13
Extensions	14
References & Gratitude	16
Appendices	17
Appendix A: Career & Mentor Connections	17
Appendix B: Background Information	18
Appendix C: Additional Resources	21



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 how that compares to their offline self) and reflect on the various intentions of other users online. Key topics that will be discussed include digital persona and oversharing. 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.

This activity is part of a series in the cyber smart education suite which includes; Digital Citizenship and You, Being Online, Web Detective, Netiquette, Crack the Code and Secure the Network. Explore [Actua's Cyber Smart Educator Handbook](#) to learn how you can bring cyber smart education into your teaching context.

Developed by Actua, 2022.

Delivery Environment	Activity Duration	Intended Audience	Tech
In-Person	1 hour	Grades 5-7 (Ages 10-13)	<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 how 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).

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 • Privacy management

Logistics (Timing, Group Sizing, Materials)

Section Title	Est. Time	Group Size	Materials
Opening Hook	5 minutes	<i>Whole Group</i>	Facilitators <ul style="list-style-type: none"> • Board & Board Marker
Section 1: Digital Persona	25 minutes	<i>Whole Group</i>	Per Participant <ul style="list-style-type: none"> • Laptop/Tablet • Spreadsheet Avatar OR Avatar Creation Activity Page (<i>Appendix C</i>)
Section 2: Oversharing	25 minutes	<i>Whole Group; Individual</i>	Facilitators <ul style="list-style-type: none"> •  Teen Voices: Oversharing an... • Board & Board Marker



Section Title	Est. Time	Group Size	Materials
			Per Participant <ul style="list-style-type: none"> Laptop/Tablet Meeting New People (Choose Your Own Adventure)
Reflection & Debrief	5 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 discussions 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 [Pan-Canadian K-12 Computer Science Education 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: Digital Persona	<ul style="list-style-type: none">• Determine the best method of creating an avatar with your available resources and delivery method.<ul style="list-style-type: none">○ Depending on the approach you take, you will want to familiarize yourself with Excel or Google Sheets.
Section 2: Oversharing	<ul style="list-style-type: none">• Familiarize yourself with the “choose your adventure” game: Meeting New People.



Opening Hook

1. Ask participants to guess how long the average person under 25 years old spends online every day. Answer: ~ 7 hours.
2. Start a brainstorm on the board with the answers to participants' responses to: **“How do you think people are spending that time online? What does being online mean for you?”**
 - a. *Additional prompts:* What do you do online? What can you do on the internet?
 - b. *Possible responses:* using Google Classroom for online learning, playing games online, using Scratch to learn how to code, playing on my Switch, watching videos on Youtube, exploring movies on Netflix, searching online.


Section 1: Digital Persona

1. Online, an **avatar** (which is also known as a profile picture) is a virtual representation of a user/ user's character/ user's persona. Give participants 10 minutes to create an avatar using the [Spreadsheet Avatar](#) by customizing the colours of each pixel. They can edit their avatar any way they'd like (a reflection of themselves, character from a movie they like, made up design, etc.).
 - a. **Note:** There are a number of ways this activity can be completed:
 - i. *Avatar Creation Activity Page (Appendix C)* could be printed out for participants to colour.
 - ii. [Spreadsheet Avatar](#) can be downloaded and edited by participants.
 1. **Note:** It will be helpful to do a quick tutorial on how to use spreadsheets if participants are not familiar with this tool (e.g., filling in multiple cells with the same colour, filling in single cells with a colour, changing colours, making a copy of the document, duplicating the tab).
2. Create a discussion with participants with the following questions:
 - a. **“How did you decide to design your avatar? Why did you choose that design?”**
 - i. **Note:** Consider having a method to share their creations with others, if they are comfortable sharing their work.



- b. **“Do you think everyone represents themselves online, the way that they appear in person? How might that change how they interact with people online?”**
- i. *Possible responses: they might be more comfortable being their true selves, they might be more comfortable sharing their thoughts (especially if they are anonymous), they might be tricking someone to think they are someone else (to become friends with them, to steal information, etc.).*
 - ii. **Note:** Answers can also take a more serious tone here. It is important to bring up the importance of being mindful about who you are online, but also who others are online.

Section 2: Oversharing

1. Someone can overshare in real life, and online. Ask participants **“How would you define oversharing?”** (see *Background Information in Appendix B* for more information).
2. Play this video:  **Teen Voices: Oversharing and Your Digital Footprint** (Common Sense Education, 3:34s).
 - a. **Note:** This is important for participants to consider for the future, even if they are not currently posting online.
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 can see things you might find embarrassing, and that could impact your chance of getting into a school/career; 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. Give participants 10 minutes to play this “choose your adventure” game: [Meeting New People](#) (Twine Story hosted on Itch.io). Their task is to make the most cyber smart choices in the story (in this story, someone unknown messages the main character while playing online).
 - a. Note:** This can be done individually, in pairs or in groups.
- 6. Ask participants **“What can you do if you interact with someone online who is making you uncomfortable? (e.g., when gaming, examining YouTube comments, etc.)”**
 - a. Possible responses:** *report the account (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 (parent, guardian, teacher), ignore the person and do not respond, block or mute the person, take a screenshot to save and collect evidence of an imposter; ensure you have privacy settings on all of your accounts.*

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. “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.
Opening Hook	
<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.
Section 1: Digital Persona	
<ul style="list-style-type: none"> • Use the Spreadsheet Avatar document. 	<ul style="list-style-type: none"> • Print out the <i>Avatar Creation Activity Page (Appendix C)</i> for participants and have them colour it in (also in the supporting resources below).



Remote (Online)	Unplugged (Low/No Tech)
Section 2: Oversharing	
<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"> Instead of the Twine Story, put participants in groups and create different scenarios about oversharing to assign to each group to create their own story (each story should use cyber smart choices).
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 mouses where laptops are in use.
- Use pairs/groups instead of having participants work individually.

SECTION 1: DIGITAL PERSONA

- Manually colour the avatar (print the *Avatar Creation Activity Sheet (Appendix C)* out for each participant).



SECTION 2: OVERSHARING

- Play [Band Runner - Think U Know](#) instead of Twine Story. This alternative involves music and point collection, with the similar goal of determining online safety knowledge by asking participants to help characters make safe choices.
- Do Twine Story as a whole group and read the story out loud.

Extensions

GENERAL

- **Computer Science Connection:** Generate discussions on artificial intelligence **[think: bots]**.
 - 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 PERSONA

- Show participants some examples from this [New York Times: Avatar Picture Series](#) to further discuss “Why others might use a different persona online?”. Remember to determine what images will be appropriate for your participants before sharing. The buttons to go to the next/previous slide are in the top right corner.

SECTION 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? ([6 Degrees of Information](#)).
- Discuss *why* people might overshare: [CBC - Your brain on likes: The science of oversharing online](#).



REFLECTION & DEBRIEF

- Participants can create a [Canva Poster](#) 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. (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/>
- 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>
- 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>
- University of San Diego. (n.d.). *Master of Science in Cyber Security*.
<https://onlinedegrees.sandiego.edu/should-you-become-a-cyber-security-engineer/>
- 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

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 considerations to keep in mind 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 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 grant 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/an 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.



Appendix C: Additional Resources


SECTION 1: DIGITAL PERSONA

Activity Page(s)

- [Spreadsheet Avatar](#)
- Avatar Creation Activity Page (see below)

SECTION 2: OVERSHARING

Video(s)

-  Teen Voices: Oversharing and Your Digital Footprint (Common Sense Education, 3:34s).

Website(s)

- [Meeting New People \(Choose Your Own Adventure\)](#)



Avatar Creation Activity Page

An avatar is a representation of yourself in a virtual setting (like in a video game). Colour in the pixels below to create your own avatar. You can also find examples at the bottom of this page.

