

# Secure the Network

**Gr. 8-12 Activity Write Up**

# Secure the Network

<b>Terms of Use</b>	<b>2</b>
<b>Activity Summary</b>	<b>3</b>
<b>Learning Outcomes</b>	<b>3</b>
<b>Logistics (Timing, Group Sizing, Materials)</b>	<b>4</b>
<b>Safety Considerations</b>	<b>5</b>
<b>Curriculum Links</b>	<b>7</b>
<b>Activity Procedure</b>	<b>8</b>
To Do in Advance	8
Opening Hook	9
Section 1: Cyber Scams	10
Section 2: Cyber Security	12
Section 3: Social Media Accounts x Privacy	13
Reflection & Debrief	14
<b>Delivery Recommendations</b>	<b>15</b>
<b>Delivery Adaptations</b>	<b>17</b>
Modifications	18
Extensions	18
<b>References &amp; Gratitude</b>	<b>20</b>
<b>Appendices</b>	<b>22</b>
Appendix A: Career & Mentor Connections	22
Appendix B: Background Information	23
Appendix C: Additional Resources	27



## 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](http://www.actua.ca) and on social media: [Twitter](#), [Facebook](#), [Instagram](#) and [YouTube](#)!



# Secure the Network

## Activity Summary

In this activity, participants will learn how cybercriminals attempt to steal information from unsuspecting users using various online and offline scams. After learning about different ways cybercriminals use clickbait and phishing strategies, participants will use their knowledge to become cyber detectives. Participants will leave with strategies that they can use to be proactive about various threats when online.

Developed by Actua, 2022.

Delivery Environment	Activity Duration	Intended Audience	Tech
In-Person	1 hour & 30 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. <b>Facilitators should have access to a laptop, projector, speakers, and a screen or blank wall to project onto.</b></p> <ul style="list-style-type: none"><li>• Projector</li><li>• Speaker</li><li>• Screen/Blank Wall</li><li>• Laptops/Tablets</li></ul>

## Learning Outcomes

Following this activity, participants will:


- Recognize various cyber scams and phishing attempts, and know how to avoid them.






- Gain knowledge of preventative measures to cyber threats.
- Use best practices to be smart and proactive while exploring online and connecting with others.

TOOLSETS	SKILLSETS	MINDSETS
<b>Knowledge, resources, and experiences</b> <ul style="list-style-type: none"> <li>• Clickbait</li> <li>• Phishing</li> <li>• Privacy</li> <li>• Personal information</li> </ul>	<b>Digital skills, STEM skills, and essential employability and life skills</b> <ul style="list-style-type: none"> <li>• Digital literacy</li> <li>• Using devices</li> <li>• Being safe and responsible online</li> <li>• Communicating online</li> <li>• Critical thinking</li> <li>• Analysis</li> </ul>	<b>Digital intelligence, community action, and computational thinking</b> <ul style="list-style-type: none"> <li>• Understanding your relation to technology</li> <li>• Privacy management</li> </ul>

## Logistics (Timing, Group Sizing, Materials)

Section Title	Est. Time	Group Size	Materials
<b>Opening Hook</b>	10 minutes	<i>Whole Group</i>	<b>Facilitators</b> <ul style="list-style-type: none"> <li>• Board &amp; Board Marker</li> </ul>
<b>Section 1: Cyber Scams</b>	20 minutes	<i>Individual; Whole Group</i>	<b>Facilitators</b> <ul style="list-style-type: none"> <li>•  Security Awareness Episode...</li> <li>• <a href="#">Phishing and Clickbait Examples Slide Deck</a></li> </ul>



Section Title	Est. Time	Group Size	Materials
			<b>Per Participant</b> <ul style="list-style-type: none"> <li>Laptop/Tablet</li> <li><a href="#">Phishing Quiz</a></li> </ul>
<b>Section 2: Cyber Security</b>	20 minutes	<i>Individual; Whole Group</i>	<b>Facilitators</b> <ul style="list-style-type: none"> <li> 5 Tips for Cybersecurity Safe...</li> </ul> <b>Per Participant</b> <ul style="list-style-type: none"> <li>Laptop/Tablet</li> <li><a href="#">Cyber Security Arcade Game</a></li> </ul>
<b>Section 3: Social Media Accounts x Privacy</b>	30 minutes	<i>Whole Group; Individual; Small Group</i>	<b>Facilitators</b> <ul style="list-style-type: none"> <li> Live My Digital for students: ...</li> <li> Digital footprints   Michelle ...</li> </ul> <b>Per Participant</b> <ul style="list-style-type: none"> <li>Account Defenses Activity Page (<i>Appendix C</i>)</li> </ul> <b>Per Small Group</b> <ul style="list-style-type: none"> <li><a href="#">A Guide to Staying Safe on Facebook</a></li> <li>Laptop/Tablet</li> </ul>
<b>Reflection &amp; Debrief</b>	10 minutes	<i>Individual; Whole Group</i>	<b>Facilitators</b> <ul style="list-style-type: none"> <li><a href="#">How to stay safe on social media</a></li> </ul> <b>Per Participant</b> <ul style="list-style-type: none"> <li>Post-It Notes (3 different colours) &amp; Writing Utensil</li> </ul>



## 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 discussions 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 your 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"><li>• <b>Think ahead and be ready to adapt:</b><ul style="list-style-type: none"><li>◦ Determine your <b>delivery method</b> and leverage ideas from the delivery recommendations and adaptations sections.</li><li>◦ While <b>estimated times</b> are provided, it will be helpful to think about how much time you would like to spend on different activities and discussions.</li><li>◦ While <b>group sizes</b> (individual, pairs, groups) are suggested, many activities are flexible for whatever will work in your classroom.</li></ul></li><li>• <b>Prepare for the content:</b><ul style="list-style-type: none"><li>◦ Have <b>answers in mind</b> to share with participants for the various reflection questions asked.</li><li>◦ Examine the provided videos and read/explore the provided materials in <i>Appendix C</i> to determine if they are <b>suitable</b> for your participants.</li></ul></li><li>• <b>Equipment:</b><ul style="list-style-type: none"><li>◦ Ensure device, screen and projector are set up.</li><li>◦ Prepare participant devices.</li></ul></li></ul>
Opening Hook	<ul style="list-style-type: none"><li>• Prepare the space so that there is room for participants to move freely without obstruction.</li></ul>



Section Title	Preparation
<b>Section 1: Cyber Scams</b>	<ul style="list-style-type: none"> <li>Familiarize yourself with the <a href="#">Phishing Quiz</a>.</li> </ul>
<b>Section 2: Cybersecurity</b>	<ul style="list-style-type: none"> <li>Familiarize yourself with the <a href="#">Cyber Security Arcade Game</a>.</li> </ul>
<b>Section 3: Social Media Accounts x Privacy</b>	<ul style="list-style-type: none"> <li>Print out the <i>Account Defenses Activity Page (Appendix C)</i></li> </ul>

## Opening Hook

1. Have participants line up at one side of the room. You will read different statements about online safety and participants will take a step depending on how they relate to it (if they are unsure, then they will just stay put):
  - a. Statements:
    - i. **Statement 1: If you make sure to log out of public devices (library, school, etc.) after using it, move 1 step forward.** You don't want to keep your personal information accessible on public devices that anyone has access to.
    - ii. **Statement 2: If you use a unique password for every account, move 2 steps forward.** Using a different password for every account is best practice! It prevents credential stuffing (where people plug in the same username and password for all of your accounts).
    - iii. **Statement 3: If you use multi-factor authentication, move 2 steps forward.** An external request that acts as additional security to protect your account (e.g., a code sent as a text, an email confirming your identity).
    - iv. **Statement 4: If you use the auto-fill feature to fill in personal information, move 1 step backwards.** It is good practice not to



store personal information on your devices - imagine if it gets stolen?

**v. Statement 5: If you press “update” ASAP when you get a software update notification, move 1 step forward.** Always do updates once it becomes available, this will help to fix any bugs or issues that can result in a security breach.

**vi. Statement 6: If you have an anti-virus software on one of your devices, move 3 steps forward.** This is important to have installed on your devices and it can flag breach attempts too. It is also important to do software updates ASAP.

**vii. Statement 7: If you have detected a phishing scam before, move 1 step forward.** Sometimes phishing attempts are obvious, other times they are sneaky. Either way, you avoided the risk of sharing personal information.

**viii. Statement 8: If you use a VPN when using public Wi-Fi, move 2 steps forward.** VPN = “Virtual Private Network” that provides additional privacy and security online by encrypting the data exchanged through that connection and enabling anonymous web browsing. You still need to be careful of suspicious links/files that could infect your device though!

**2.** Being online can be fun and educational if we know what to be aware of.

Create a brainstorm on the board around the question **“What are some risks you can experience while online?”**

**a.** Possible responses: click bait, cyberbullying, phishing attempts, having your personal information stolen, being catfished by a stranger.

**3.** In another colour, add to the brainstorm around the question **“What are some strategies we can use to prevent these risks?”**

## Section 1: Cyber Scams

This section will be well set up if cyber scams like clickbaits and phishing are mentioned in the opening hook brainstorm. Here, participants will learn more about these scams and strategies to keep their devices secure.



1. Play this video for participants:

 Security Awareness Episode 4: Phishing and Ransomware


(StaySafeOnline.org, 2:33s).

- a. **“What mistake did Dave make that led them to having to pay the ransom?”**
  - b. **“How can you avoid a situation like this?”**
  - c. **“What strategies were shared?”**
2. Facilitate the [Phishing and Clickbait Examples Slide Deck](#).
    - a. For each example, discuss if they thought it was a scam and what the red flags were.
    - b. See *Speaker Notes* for information to point out in each example.
  3. Share this [Phishing Quiz](#) for participants to do (individually, in pairs, in groups).
    - a. **Note:** Name: cybersmart; Email: [cybersmart@gmail.com](mailto:cybersmart@gmail.com).
  4. Ask participants to share key takeaways and strategies that this exercise taught them about keeping their inbox safe (or ones they learned outside of this activity).
    - a. *Possible responses:* hover over all links before clicking to double check the URLs; review the sender’s email address to check for anything suspicious; check for spelling and grammar errors, spam/junk filter, etc.
    - b. Inboxes can exist for more than just emails. It is also important to be mindful of the links sent to you on social media or text (Do you know the person who sent it? Is it a link that you would trust?).
  5. Discuss the following next steps that can help participants and their parents if they do accidentally give out personal and sensitive information (share these in the chat):
    - a. Contact the platform (e.g., if banking information is shared, then contact the bank);
    - b. Contact the local police service;
    - c. Contact the [Canadian Anti-Fraud Centre](#)
      - i. If time permits, head to the site and show participants the numbers on the right side of the screen (“Impact of COVID-19 Fraud” and “Impact of Fraud so far This Year”).



## Section 2: Cyber Security

1. Play this video for participants:  

 5 Tips for Cybersecurity Safety brought to you by Mayim Bialik (IBMorg, 5:45s).

  - a. **Note:** Participants can write down some of the tips they are unaware of.
2. “What are some strategies you’ve learned so far (from the video or other sessions) that will help you be a responsible digital user?”
  - a. Prompts: cyber scams; making a more secure network; sharing information
  - b. Possible responses: *keep profiles private, avoid sharing personal information, only allow followers that you know, create strong and unique passwords for all of your accounts, do not believe everything you read online, do not click everything you see online, etc.*
3. Have participants play this [Cyber Security Arcade Game](#). The goal of the game is to answer all 12 questions *correctly* (see Appendix C: Delivery Materials for questions and answers).
  - a. Here are the rules:
    - i. Destroy the Viruses (hit spacebar on keyboard or A on screen, use keyboard or in-game arrows to move the ship).
    - ii. Avoid the aliens. If you get hit 3 times the game is over.
    - iii. Take your time to answer the questions correctly (use the arrows on keyboard or dial on screen to choose the correct number associated with the answer). **Note:** The question and options will disappear when they have to choose their answer.
    - iv. Move forward by pressing the spacebar/arrow on the keyboard or A on the screen.
  - b. **Note:** An alternative game is [Cybersecurity Lab \(NOVA Labs\)](#) (Google Chrome is the recommended browser).



### Section 3: Social Media Accounts x Privacy

- How true is this saying: **“Nothing ever gets deleted from the internet”?**

Connect this to the idea of Digital Footprint:

▶ Live My Digital for students: Digital Footprint talks about using the digital footprint to your advantage.

- Play this spoken word poem on the effects of our digital footprints:

▶ Digital footprints | Michelle Sadrena Pledger | TEDxHollywood

- a. **“What do you agree with? What have you heard before?”** E.g., We do not need to co-exist solely by an internet connection.
- Think about the accounts you’ve created (for school, work, your personal life). Many apps are improving their security measures so that people feel more confident about their information staying secure. **“What are some cyber security strategies you use or have learned when it comes to posting online, or having accounts?”**
  - You can think of your privacy security as having 3 lines of defenses: account settings, privacy settings, and defining your community. Have participants fill out the Account Defenses Activity Page (*Appendix C*) individually using the strategies that they currently use in the appropriate sections. Examples below:

First line - login settings	Second line - privacy settings	Third line - community
<ul style="list-style-type: none"><li>• 2 factor authentication</li><li>• Alerts about unrecognized logins</li><li>• Strong passwords</li><li>• Watch out for scams or phishing</li><li>• Regular security check ups</li></ul>	<ul style="list-style-type: none"><li>• User name details</li><li>• Manage location settings</li><li>• Undo and delete personal information</li><li>• Review your timeline and tags</li><li>• See how your profile appears to others</li></ul>	<ul style="list-style-type: none"><li>• Friending, following</li><li>• Unfriending, unfollowing</li><li>• Blocking</li><li>• Reporting fake accounts</li></ul>



<ul style="list-style-type: none"> <li>• End-to-end encryption</li> <li>• App ratings</li> </ul>	<ul style="list-style-type: none"> <li>• Understand the data policy</li> <li>• Control who can see what you share (public page but with customized story settings for close friends).</li> <li>• Control who can find you (anyone, friends of friends, phone number)</li> <li>• Adjust ad settings</li> <li>• Reporting photos/videos that violate your privacy</li> </ul>	
--	--	--

- **“Where can you anticipate a breach in your defenses?”**

Participants may not use Facebook, but this guide has tips that are important for any type of social media or account: [A Guide to Staying Safe on Facebook](#) (developed by Women’s Aid, National Network to End Domestic Violence, and Facebook). Put participants into groups and have them explore the guide.

- “What strategies do you currently use?”**
- “Which do you think are the most important?”**

## Reflection & Debrief

1. Play this video for participants: [How to stay safe on social media](#) (Office of the Privacy Commissioner of Canada, 2:34s).
2. Give each participant 3 differently coloured post-it notes to write down the strategies a-c below. Have participants put up their post-it notes on a board/wall and discuss some of the responses.



- a. A strategy they will share with their friends and family.
  - b. A strategy they weren't aware of.
  - c. A strategy they already knew about.
- 3. Discuss the different careers listed in *Appendix A: Career & Mentor Connections*.
- 4. Encourage participants to be a Cyber Smart Ambassador and share this knowledge (and poster) 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)
<b>General</b>	
<ul style="list-style-type: none"> <li>Encourage participants to unmute themselves or type in the chat based on what is easiest for them to communicate.</li> <li>Leverage a tool where participants can all participate online during discussions (e.g., Mentimeter, Jamboard, etc).</li> <li>Make note of any links that need to be shared and be prepared to share them in the chat.</li> <li>Use polls or other group interactions to check in and keep up engagement.</li> </ul>	<ul style="list-style-type: none"> <li>Leverage boards to do brain storms/write down participant responses.</li> </ul>





Remote (Online)	Unplugged (Low/No Tech)
<b>Opening Hook</b>	
<ul style="list-style-type: none"> <li>• Use poll/raise hand function if it exists, use the chat if the statement is applicable, or have participants just reflect on the statement.</li> <li>• 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).</li> </ul>	<ul style="list-style-type: none"> <li>• Activity can be done as-is unplugged.</li> </ul>
<b>Section 1: Cyber Scams</b>	
<ul style="list-style-type: none"> <li>• Use the laser pointer option when facilitating the slide deck.</li> <li>• 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).</li> </ul>	<ul style="list-style-type: none"> <li>• Print out examples from the slide deck for participants to analyze.</li> <li>• Focus on discussion: develop a list as a class of cyber security strategies. Come prepared with additional strategies to add to their suggestions.</li> </ul>
<b>Section 2: Cyber Security</b>	
<ul style="list-style-type: none"> <li>• Display a <a href="#">virtual stopwatch</a> (countdown option) on your screen so that participants know how much longer they have to play.</li> <li>• Display the game on the screen to show participants how to play before giving them time to play</li> </ul>	<ul style="list-style-type: none"> <li>• <i>Game Board (Appendix C):</i> Describe the rules of the game using the <a href="#">Low/No Tech Game Board Instructions Slide Deck</a></li> <li>• Distribute a game board for each participant (alternatively, they can play in pairs or groups).</li> </ul>



Remote (Online)	Unplugged (Low/No Tech)
on their own.	<ul style="list-style-type: none"> <li>• Participants can repeat the game multiple times (the goal is to understand what the different terms are).</li> <li>• At the end, ask participants to share their tallied points (the higher the number, the more secure the network)</li> </ul>
<b>Section 3: Social Media Accounts x Privacy</b>	
<ul style="list-style-type: none"> <li>• Display the worksheet. Ask participants to grab a spare piece of paper to copy it on.</li> </ul>	<ul style="list-style-type: none"> <li>• Print out the poem for participants to read.</li> <li>• When thinking about accounts, remind participants that it is not only about social media accounts. You can have an account for Google, for your student accounts, YouTube and Netflix.</li> </ul>
<b>Reflection &amp; Debrief</b>	
<ul style="list-style-type: none"> <li>• Consider using a collaborative tool (e.g., Jamboard, Google Doc, Mentimeter).</li> </ul>	<ul style="list-style-type: none"> <li>• Activity can be done as-is unplugged.</li> </ul>



## 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.

#### OPENING HOOK

- Tally the points rather than taking steps and discussing scores at the end (alternatively, you can provide an opportunity for participants to reflect on their scores and how they can improve rather than sharing it).

#### SECTION 1: CYBER SCAMS

- Do the Phishing Quiz together as a whole group (or go through at least one together as an example).
- Review less of the examples in the Slide Deck/ have participants work in groups.

#### SECTION 2: CYBER SECURITY

- Play in pairs or small groups.

#### SECTION 3: SOCIAL MEDIA ACCOUNTS X PRIVACY

- Print out the poem for participants to follow.



## Extensions

### SECTION 1: CYBER SCAMS

- Play [Missing Link Game](#) (Texas A&M University)

### SECTION 2: CYBER SECURITY

- Participants can copy the code from the [Microsoft MakeCode Arcade Game](#) and edit it to create their own game for cyber security.

### SECTION 3: SOCIAL MEDIA ACCOUNTS X PRIVACY

- Participants can compare what the three defenses would be like for a public account vs. a private account on their worksheet.

### 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

- Binary Tattoo. (2017, June 19). *Glossary of Internet Scams and Fraud Terminology*.  
<https://www.binarytattoo.com/glossary-of-internet-fraud-and-scam-terminology/>
- BleepingComputer. (2018, January 11). *Remove the Amazon Rewards Event Web Page*. <https://bit.ly/37piROX>
- Canva. (n.d.). *Create a Design*. <https://www.canva.com/>
- Canadian Centre for Cyber Security. (2020, April 21). *Don't Take the Bait: Recognize and Avoid Phishing Attacks*.  
<https://www.cyber.gc.ca/en/guidance/dont-take-bait-recognize-and-avoid-phishing-attacks>
- Canadian Centre for Cyber Security. (2020, April 21). *Glossary*.  
<https://www.cyber.gc.ca/en/glossary>
- Common Sense Education. (2019, January 11). *Teen Voices: Oversharing and Your Digital Footprint* [Video file]. <https://www.youtube.com/watch?v=ottnH427Fr8>
- Federal Trade Commission Consumer Information. (2019, May). *How to Recognise and Avoid Phishing Scams*.  
<https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>
- GDST. (2016, July 1). *Live My Digital for students: Digital Footprint* [Video file].  
<https://www.youtube.com/watch?v=OBq2YYV3Bts>
- Goodwill Community Foundation. (n.d.). *What is Clickbait?*  
<https://edu.gcfglobal.org/en/thenow/what-is-clickbait/1/>
- IBMorg. (2020, January 22). *5 Tips for Cybersecurity Safety brought to you by Mayim Bialik* [Video file]. <https://www.youtube.com/watch?v=ZOtQ21hXJ7k>
- Iluli by Mike Lamb. (2019, October 2). *Phishing Attacks - how to avoid the bait* [Video file]. <https://www.youtube.com/watch?v=XsOWczwRVuc>
- Imperva. (n.d.). *Phishing Attacks*.  
<https://www.imperva.com/learn/application-security/phishing-attack-scam/>
- Kaspersky. (n.d.). *What is VPN? How It Works, Types of VPN*.  
<https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>
- NOVA Labs. (n.d.) *Cybersecurity Lab*. <https://www.pbs.org/wgbh/nova/labs/lab/cyber/>
- Office of the Privacy Commissioner of Canada. (2020, June 30). *Video for Canadians: How to stay safe on social media*.  
[https://priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookie/online-privacy/social-media/video\\_sm/](https://priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookie/online-privacy/social-media/video_sm/)
- Panda Security. (2019, April 2). *10 Social Media Scams and Hot to Spot them*.  
<https://www.pandasecurity.com/en/mediacenter/panda-security/social-media-scams/>



PCS Business Systems. (n.d.). *Malware, phishing, spyware and viruses - what's the difference?* <https://www.pcs-systems.com/different-cyber-threats/>

Security Boulevard. (2019, November 26). *Dropbox Phishing Scam: Don't Get Fooled by Fake Shared Documents*.  
<https://securityboulevard.com/2019/11/dropbox-phishing-scam-dont-get-fooled-by-fake-shared-documents/>

Search Security. (2014). *Phishing Definition*.  
<https://searchsecurity.techtarget.com/definition/phishing>

StaySafeOnline.org. (2020, April 6). *Security Awareness Episode 4: Phishing and Ransomware* [Video file]. [https://www.youtube.com/watch?v=D\\_yAYhjNE-0](https://www.youtube.com/watch?v=D_yAYhjNE-0)

Tech Radar. (2017, November 14). *You need a VPN when accessing public Wi-Fi - here's why*.  
<https://www.techradar.com/news/public-wi-fi-and-why-you-need-a-vpn>

TEDx Talks. (2014, July 24). *Digital footprints | Michelle Sadrena Pledger | TEDxHollywood* [Video file].  
<https://www.youtube.com/watch?v=NIgyTp4Nd4M>

Tech Xplore. (2020, March 27). *Router phishing scam targets global fear over coronavirus*.  
<https://techxplore.com/news/2020-03-router-phishing-scam-global-coronavirus.html>

Windsor Public Library. (2017, February 16). *Spotting a Phishing Attempt*.  
<https://www.windsorpubliclibrary.com/?p=47291>

Women's Aid, National Network to End Domestic Violence, and Facebook. (n.d.). *A guide to staying safe on facebook*.  
[https://www.womensaid.ie/assets/files/pdf/a\\_guide\\_to\\_staying\\_safe\\_on\\_facebook.pdf](https://www.womensaid.ie/assets/files/pdf/a_guide_to_staying_safe_on_facebook.pdf)



## 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

Binary Tattoo has put together a “[Glossary of Internet Fraud and Scam Terminology](#)” that is a strong resource for all facilitators to familiarize themselves with.

### PHISHING SCAMS

According to the [Canadian Centre for Cyber Security](#), phishing is an attack where cyber criminals contact you (call, text, email, use social media) to trick you into sharing private information or clicking on a malicious link/downloading malware. These attempts are usually generic mass messages but they can seem like they are sent from a legitimate, trustworthy source (ex. school or bank). Depending on what you share or provide access to, a scammer may have multiple pieces of private information (phone numbers, address, birthday, banking information, etc.) that they can use to steal your identity, passwords and money.

#### SOMETHING MAY BE PHISHY IF:

- You don't recognize the sender's name, email address, or phone number (e.g. very common for spear phishing)
- You notice a lot of spelling and grammar errors
- The sender requests your personal or confidential information
- The sender makes an urgent request with a deadline
- The offer sounds too good to be true



#### WATCH OUT FOR:

- Attachments
- Hidden links
- Spoofed websites
- Log-in pages
- Urgent requests

#### PROTECT YOUR INFORMATION AND INFRASTRUCTURE:

- Verify links before you click them
- Avoid sending sensitive information over email or texts
- Call the sender to verify legitimacy (e.g. if you receive a call from your bank, hang up and call them)
- Back up information so that you have another copy
- Apply software updates and patches
- Use anti-phishing software that aligns with the Domain-based Message [Authentication](#), Reporting, and Conformance (DMARC) policy
- Filter spam emails
- Block IP addresses, domain names, and file types that you know to be bad
- Reduce the information you post online (e.g. phone numbers and extensions for employees)

Canadian Centre for Cyber Security (2020, April 21). *Don't Take the Bait: Recognize and Avoid Phishing Attacks*. Retrieved from <https://www.cyber.gc.ca/en/guidance/dont-take-bait-recognize-and-avoid-phishing-attacks>

### The 3 main reasons why hackers or people phish are:

- 1) Access (to accounts or information).
- 2) Money (gaining access to credit cards/bank info, locking a device/system with ransomware).
- 3) Chaos (to stir trouble).





- a) The phishing scam itself is tricking you into sharing info - the reasons are to do damage to your finances, your reputation, or your company/school/system you have access to.

These are some signs that may help you recognize a phishing scam:

- Often tell a story to trick you into clicking a link/opening an attachment.
  - e.g., Eligible for a refund, make a payment, confirm personal information, there's an issue with your account.
  - It often involves emails containing links to websites that have malware.
- Generic greeting (e.g., Hi User).
- You don't recognize the sender's name, email address, or phone number.
- May look like the message is from a company you know (you may or may not have an account with this company).
- A lot of spelling and grammar errors.
- The sender requests personal or confidential information.
- The sender makes an urgent request with a deadline.
  - The sender may even be someone you know but the request in the email seems odd, or is something you would not normally receive from this person.
- The offer sounds too good to be true.

These are some strategies to protect yourself from phishing attacks (combined from information shared by the [Canadian Centre for Cyber Security](#) and the [Federal Trade Commission](#)):

- Use security software to protect your devices (and update automatically).
- Use multi-factor authentication on your accounts.
- Verify links before you click them.
- Avoid sending sensitive information over email or texts.
- Call the sender to verify legitimacy (e.g., if you receive a call from your bank, hang up and call them).
- Filter spam emails.



- Reduce the information you post online (e.g., phone numbers and extensions for employees).

## MALWARE

The [Canadian Centre for Cyber Security](#) describes malware as malicious software created to gain access/damage computer systems, without the owner's consent and sometimes, without their knowledge. Phishing attempts can take you to a link/have you download something that is infected with malware. Scammers use malware as an attempt to go after your identity, passwords and money.

Types of malware:

- **Spyware:** hard to detect and collects information without you knowing.
- **Viruses:** program that replicates itself in the computer's memory and spreads.
- **Worms:** runs independently and self-replicates to cause damage (ex. deleting files, sending documents via email, etc).
- **Trojans:** disguised as legitimate software.
- **Ransomware:** encrypts your files and makes you pay to have them decrypted.

## CLICKBAIT

Clickbait is a misleading form of false advertisement that is designed to get the attention of a user and encourage them into clicking something. It can look like a headline meant to appeal to your emotions and curiosity to entice you to click on an article, image or video.

Clickbait itself is a common term for using enticing titles to get you to click (e.g., "Doctor's hate this woman's anti-aging secret.. find out why!") - it is often used as an advertising technique and is not always nefarious, **however in some cases they can be an elaborate effort to scam people (e.g., directing them to a nefarious website with malware, or fooling individuals into donating to a fake charity).**

Websites that use clickbaits often value getting visits over the quality and credibility of the information it shares. It can be harmful when used in combination with fake news, and can be spread widely on social media.



[Goodwill Community Foundation \(Learn Free\)](#) shares information on how to recognize clickbaits:

- Often outrageous headlines.
- Vague headlines and images that let your imagination run (ex. You won't believe what this teacher said to their classroom).
- The headline tells you how to feel.




## Appendix C: Additional Resources

### SECTION 1: CYBER SCAMS

Activity Slide Deck(s)

- [Phishing and Clickbait Examples Slide Deck](#)

Video(s)


-  Security Awareness Episode 4: Phishing and Ransomware (StaySafeOnline.org, 2:33s)

Website(s)

- [Phishing Quiz](#)

### SECTION 2: CYBER SECURITY

Video(s)

-  5 Tips for Cybersecurity Safety brought to you by Mayim Bialik (IBMorg, 5:45s)

Website(s)

- [Cyber Security Arcade Game](#)
  - Q & A for Cyber Security Arcade Game (*see below*)

Low/No Tech Activity Alternative(s)



- Game Board (*see below*)
- [Low/No Tech Game Board Instructions Slide Deck](#)

### SECTION 3: SOCIAL MEDIA ACCOUNTS X PRIVACY

Activity Page(s)

- Account Defenses Activity Page (*see below*)

Video(s)

-  Live My Digital for students: Digital Footprint
-  Digital footprints | Michelle Sadrena Pledger | TEDxHollywood

Website(s)

- [A Guide to Staying Safe on Facebook](#)



## REFLECTION & DEBRIEF

Website(s)

- [A Guide to Staying Safe on Facebook](#)
- [How to stay safe on social media](#) (Office of the Privacy Commissioner of Canada, 2:34s)



## Q & A for Cyber Security Arcade Game

Question	Message
<p>Your friend asks for your password to your school login. What do you do?</p> <ol style="list-style-type: none"> <li>1. Share it duh, they're your friend.</li> <li><b>2. Keep it private and find another way to help.</b></li> </ol>	<p>Your password is private! It should not be shared with anybody (even if you use different passwords for all accounts).</p>
<p>You get an email asking you to reset your password to one of your gaming accounts. What do you do?</p> <ol style="list-style-type: none"> <li>1. Click link ASAP to change it.</li> <li>2. Delete email.</li> <li><b>3. Read carefully and look for hints that it could be a scam.</b></li> </ol>	<p>YES! This could be a phishing attempt. Inspect the email for spelling mistakes, double check sender email, and hover over links. Go to the app directly rather than through the link provided.</p>
<p>You need to make a password for an account. Which should you follow?</p> <ol style="list-style-type: none"> <li><b>1. Make a passphrase with no personal info.</b></li> <li>2. Make it random and short.</li> <li>3. Have your name somewhere so it's easy to remember.</li> </ol>	<p>Make sure all your passwords are different and are passphrases without any personal info (no dates, names, etc.).</p>
<p>You have a social media account where you share life updates. You will:</p> <ol style="list-style-type: none"> <li>1. Keep it public.</li> <li>2. Make it private but accept everyone.</li> </ol>	<p>Widely sharing personal life updates (like birthdates, locations, interests) can potentially be used to hack you. Be mindful about what you share and who you share it with.</p>

<p><b>3. Make it private and only accept people you know.</b></p>	
<p>Which is the strongest password?</p> <ol style="list-style-type: none"> <li>1. STEM</li> <li>2. Stem123!</li> <li><b>3. StemIsTheBest1*</b></li> </ol>	<p>YAY! This is an example of a passphrase with a number and symbol! It makes it hard for guessing or brute-force attacks to be successful.</p>
<p>Somebody makes a comment to you on YouTube that makes you feel weird. What do you do?</p> <ol style="list-style-type: none"> <li><b>1. Report, Block and tell a trusted adult.</b></li> <li>2. Ignore and close the window.</li> <li>3. Reply and tell your friends.</li> </ol>	<p>It is always important to be kind online but a message that makes you uncomfortable should be shared with a trusted adult. Reporting and blocking is also important.</p>
<p>You almost got a virus from downloading a pdf but you didn't trust the site. You should remember to:</p> <ol style="list-style-type: none"> <li>1. Download antivirus software.</li> <li><b>2. Download antivirus software and update regularly.</b></li> <li>3. Not surf the web anymore.</li> </ol>	<p>It isn't enough to just have antivirus software, it must be updated regularly. The same goes with any device updates! This helps secure your accounts.</p>
<p>You got a pop-up on a website saying you won \$1000. All you have to do is fill out a form. What should you do next?</p> <ol style="list-style-type: none"> <li>1. Celebrate and complete the form.</li> <li>2. Only share mandatory details.</li> <li><b>3. Ignore. You did not apply for any draws.</b></li> </ol>	<p>Messages from unknown senders that are urgent or too good to be true are often an attempt to steal private information. It is important to be aware and pay attention when online.</p>

<p>Your parents use the same password for all their accounts. Is this safe?</p> <ol style="list-style-type: none"> <li>1. Of course, it's a strong password.</li> <li><b>2. No, each password should be strong AND unique.</b></li> </ol>	<p>All your passwords should be unique! That way, if one is stolen then your other accounts are okay.</p>
<p><b>True (1)</b> or F (2)</p> <p>You should not log in to one of your accounts using public Wi-Fi, like at Tim Hortons or McDonalds.</p>	<p>It is best not to access personal accounts (like your school or bank) on unsecured public Wi-Fi.</p>
<p><b>True (1)</b> or F (2)</p> <p>You should be empowered to be online. Used wisely, it is a great tool to learn, share and connect.</p>	<p>The internet allows us to access lots of information (in a way our parents didn't have growing up). This is wonderful! We just need to make sure to fact check and ask questions.</p>
<p><b>True (1)</b> or F (2)</p> <p>Cybersecurity is a growing field with lots of demand.</p>	<p>Yes! To start, check out cybersecurity engineer, web developer and security analyst.</p>



## Cyber Security Game Board

START	You downloaded Norton Security (an antivirus software) that luckily stopped a virus before any damage was done. <div>+ 5 points</div>		You shared your password in a phishing attempt. Update all passwords and report the scam! <div>- 2 points</div>		Server earned <div>+ 1 point</div>	A worm destroyed the storage in your computer. Remember to download a reliable firewall to prevent this in the future! <div>- 2 points</div>		
	You received an email telling you that you won a laptop. You click a link in it and accidentally download a virus. <div>- 2 points</div>		You remember not to log on to any accounts when you were connected to mall Wi-Fi. <div>+ 2 points</div>		Database earned <div>+ 1 point</div>			
A virus is stopping you from using your computer. Remember to download antivirus software and keep it updated! <div>- 5 points</div>	Server earned <div>+ 1 point</div>	You identified a phisher trying to get you to share your birthdate and address. You reported it. <div>+ 5 points</div>		You did not have the latest update for your antivirus software and a virus made its way onto your hard drive. Remember to always update your software! <div>- 2 points</div>		Firewall earned <div>+ 1 point</div>	Storage earned <div>+ 1 point</div>	You accidentally activated a trojan virus by clicking an application you thought was a game. <div>- 3 points</div>
Your servers crashed!  Return to the start (and lose all points)	You tried to download a free game but downloaded malware instead. Remember to think carefully about the links you click on! <div>- 5 point</div>		Database error <div>- 1 point</div>	You accidentally downloaded malware, but you frequently back up your data so you did not need to pay to get access to your files again. <div>+ 1 point</div>		Database earned <div>+ 1 point</div>		
	Firewall error <div>- 1 point</div>	Server earned <div>+ 1 point</div>	You filled a form from an unknown sender to claim a prize and downloaded ransomware. Remember to think about spam/junk mail! <div>- 5 point</div>		You double check emails to ensure they are not scams in disguise. <div>+ 2 points</div>			
END	You verified a source of a download and saw that it was untrusted. You avoided downloading a trojan virus. Great eye! <div>+ 3 point</div>		You illegally downloaded a movie with a virus and now you have ads all over your browser. Be mindful about what you do online! <div>- 5 point</div>		Storage earned <div>+ 1 point</div>	You illegally downloaded a movie with a virus and now you have ads all over your browser. Be mindful about what you do online! <div>- 5 point</div>		

## Account Defenses Activity Page

You can think of your privacy security as having 3 lines of defenses: **account settings** (e.g., 2 factor authentication), **privacy settings** (e.g., manage location settings), and **defining your community** (e.g., reporting fake accounts). Fill out the graphic using the strategies you use in the appropriate sections.

