Secure the Network

Gr. 5-7 Activity Write Up

Actua | 111 Murray Street, Ottawa, ON K1N 5M5 | www.actua.ca | 613 234 4137

actüa
Youth · STEM · Innovation
Jeunesse · STIM · Innovation

Secure the Network

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!

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.

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)*	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.** • Projector • Speaker • Screen/Blank Wall • Laptops/Tablets

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
Knowledge, resources, and experiences • Clickbait • Phishing • Privacy • Personal information	**Digital skills, STEM skills, and essential employability and life skills** • Digital literacy • Using devices • Being safe and responsible online • Communicating online • Critical thinking • Analysis	**Digital intelligence, community action, and computational thinking** • Understanding your relation to technology • Privacy management

Logistics (Timing, Group Sizing, Materials)

Section Title	Time	Group Size	Materials
Opening Hook	10 minutes	*Whole Group*	**Facilitators** • Clickbait Image *(Appendix C)*
Section 1: Cyber Scams	20 minutes	*Individual; Whole Group*	**Facilitators** • Stay Safe from Phishing an... • Phishing and Clickbait Examples Slide Deck **Per Participant** • Laptop/Tablet • Phishing Quiz
Section 2: Cyber Security	20 minutes	*Individual; Whole Group*	**Facilitators** • 5 Tips for Cybersecurity Saf... **Per Participant** • Paper & Writing Utensil • Laptop/Tablet • Google's Interland (Reality River)
Reflection & Debrief	10 minutes	*Whole Group; Individual*	**Per Participant** • Laptop/Tablet • Canva Poster

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 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

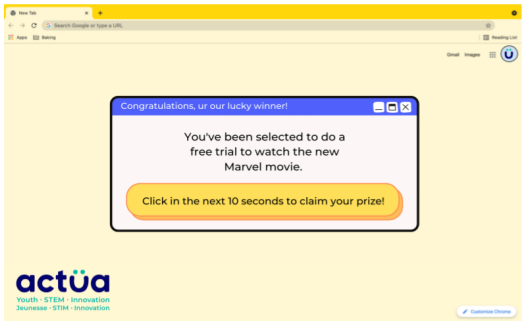
Section Title	Preparation

General	• **Think ahead and be ready to adapt:**
	  ○ 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:**
	  ○ 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 *Appendix C* to determine if they are **suitable** for your participants.
	• **Equipment:**
	  ○ Ensure device, screen and projector are set up.
	  ○ Prepare participant devices.

Opening Hook	• Prepare *Clickbait Image (Appendix C)* to display or project
Section 1: Cyber	• Familiarize yourself with the Phishing Quiz.

Section Title	Preparation
Scams	
Section 2: Cyber Security	• Familiarize yourself with Google's Interland (Reality River) (***Note:*** The game has sound but this is not required, it is a voice that reads the words on the screen).
Reflection & Debrief	• Familiarize yourself with the Canva platform (***Note:*** No account needed to create).

Opening Hook



1. Project the *Clickbait Image (Appendix C)* so that it is the first thing participants notice when they walk into the room.
2. Set the scene: You were just browsing online before class and this message popped up. Apparently you have the chance to win a new phone! Ask **"What do you all think? Should I spin the wheel?"**
3. Reveal the truth: this is an example of a common cyber scam (clickbait) that you'll learn more about later (see Background Information in *Appendix B* for more information).
4. Being online can be fun and educational if we know what to look out for. Start a brainstorm on the question **"What are some risks you can experience while online?"**
    a. *Possible responses: clickbait, cyberbullying, phishing attempts, having your personal information stolen, being catfished by a stranger.*
5. In another colour, add to the brainstorm around the question **"What are some strategies you know about that we can use to prevent these risks?"**

Section 1: Cyber Scams

The photo shared at the start is an example of clickbait, a common cyber scam. Let's learn more about clickbaits and another common cyber scam called phishing.

1. Play this video for participants: Stay Safe from Phishing and Scams (Google for Education, 3:14s) to share key strategies and things to beware of when it comes to scams.
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.
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, etc.
5. Discuss the following next steps **that can help participants and their parents if they do accidentally give out personal and sensitive information:**
    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

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 on everything that’s online, etc.
3. Share this link for participants to play for 10 minutes: Google’s Interland (Reality River) - there are other games, but focus on Reality River.
    a. As participants play, ask them to make note of the smart decisions they can make online, especially ones that might be new to them.
    b. ***Note:*** Depending on the device and internet connection the game may be slow. If participants experience this, HD Graphics can be turned off. The gear icon in the bottom right corner of the screen allows you to turn HD graphics off. Warn participants that this will reset their progress. We recommend playing the game without HD graphics turned on.

Reflection & Debrief

1. Participants can create a PSA poster on Canva that they can share with their friends and family informing them about how to be cyber smart online. Tip: show them how to create a new project and the different editing features.
    a. ***Note*:** Consider having participants share their poster with others.
2. Discuss the different careers listed in *Appendix A: Career & Mentor Connections*.
3. 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)
General	
• 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.	• Leverage boards to do brain storms/write down participant responses.
Opening Hook	
• 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).	• Focus on oral storytelling or print out the image.

Remote (Online)	Unplugged (Low/No Tech)
Section 1: Cyber Scams	
• Use the laser pointer option when facilitating the slide deck. • 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).	• Print out examples from the slide deck for participants to analyze.
Section 2: Cyber Security	
• Display a virtual stopwatch (countdown option) on your screen so that participants know how much longer they have to play. • Display the game on screen to show participants how to play before giving them time to play on their own.	• *Game Board (Appendix C)*: Describe the rules of the game using the Low/No Tech Game Board Instructions Slide Deck • Distribute a game board for each participant (alternatively, they can play in pairs or groups). • Participants can repeat the game multiple times (goal is to understand what the different terms are). • At the end, ask participants to share their tallied points (the higher the score, the more secure the network)
Reflection & Debrief	
• Craft a poster with key takeaways on paper rather than on Canva.	• Craft a poster with key takeaways on paper rather than on Canva.

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: 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 Reality River as a group or demonstrate how to play for the first few minutes.
    - The second question is timed. This may be stressful for some participants if they take longer periods to read or type.

Extensions

SECTION 1: CYBER SCAMS

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

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. (n.d.). *Glossary*. https://cyber.gc.ca/en/glossary/Ransomware

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 Commision Consumer Information. (2019, May). *How to Recognise and Avoid Phishing Scams*. https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Goodwill Community Foundation. (n.d.). *What is Clickbait?* https://edu.gcfglobal.org/en/thenow/what-is-clickbait/1/

Google for Education. (2017, June 25). *Stay Safe from Phishing and Scams* [Video file]. https://www.youtube.com/watch?v=R12_y2BhKbE

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/

Kapersky. (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/

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

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

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

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.

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

OPENING HOOK

Image(s)

- Clickbait Image *(see below)*

SECTION 1: SCAMS

Activity Slide Deck(s)

- Phishing and Clickbait Examples Slide Deck

Video(s)

- Stay Safe from Phishing and Scams (Google for Education, 3:14s)

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)

- Google's Interland (Reality River)

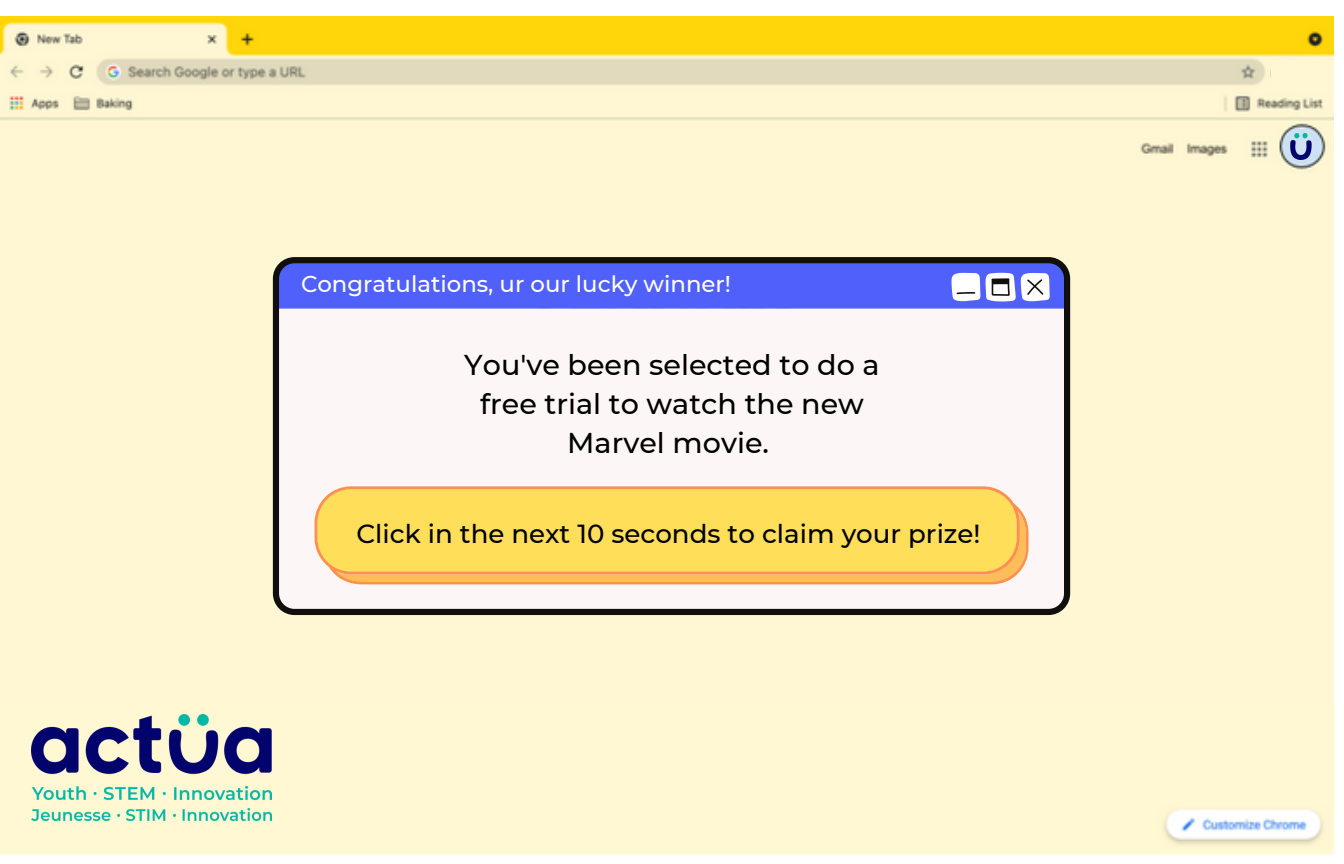
Low/No Tech Activity Alternative(s)

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

REFLECTION & DEBRIEF

Website(s)

- Canva Poster


New Tab
Search Google or type a URL
Apps
Baking
Reading List
Gmail
Images
Congratulations, ur our lucky winner!
You've been selected to do a free trial to watch the new Marvel movie.
Click in the next 10 seconds to claim your prize!
actüa
Youth · STEM · Innovation
Jeunesse · STIM · Innovation
Customize Chrome

actüa
Youth · STEM · Innovation

Cyber Security Game Board

START	You downloaded Norton Security (an antivirus software) that luckily stopped a virus before any damage was done. + 5 points		You shared your password in a phishing attempt. Update all passwords and report the scam! - 2 points	Server earned + 1 point	A worm destroyed the storage in your computer. Remember to download a reliable firewall to prevent this in the future! - 2 points
A virus is stopping you from using your computer. Remember to download antivirus software and keep it updated! - 5 points	Server earned + 1 point	You received an email telling you that you won a laptop. You click a link in it and accidentally download a virus. - 2 points	You remember not to log on to any accounts when you were connected to mall Wi-Fi. + 2 points	Database earned + 1 point	
	You identified a phisher trying to get you to share your birthdate and address. You reported it. + 5 points	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! - 2 points	Firewall earned + 1 point	Storage earned + 1 point	You accidentally activated a trojan virus by clicking an application you thought was a game. - 3 points
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! - 5 point	Database error - 1 point	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. + 1 point	Database earned + 1 point	
	Firewall error - 1 point	Server earned + 1 point	You filled a form from an unknown sender to claim a prize and downloaded ransomware. Remember to think about spam/junk mail! - 5 point	You double check emails to ensure they are not scams in disguise. + 2 points	You illegally downloaded a movie with a virus and now you have ads all over your browser. Be mindful about what you do online! - 5 point
END	You verified a source of a download and saw that it was untrusted. You avoided downloading a trojan virus. Great eye! + 3 point		You illegally downloaded a movie with a virus and now you have ads all over your browser. Be mindful about what you do online! - 5 point	Storage earned + 1 point	