Civilizing Cybersecurity: No Kid Left Behind in the Digital Age

I will be applying to the *Instructional Innovations* category of this award.

**Description of Technology**

*NOVALabs* is a free digital platform featuring a series of online educational labs geared towards grade 6-12 students. NOVALabs involves students as "citizen scientists". NOVALabs acts as a bridge that connects students to current research completed by scientists and IT professionals. My submission will focus on the *Cybersecurity lab* which can be accessed [here](#). Each lab features four components. The first is an interactive problem-solving game component where students have practice skills and concepts presented. Students are tasked with protecting their tech startup from cybersecurity threats (the game will be the main focus on this proposal). Secondly, a *video and quiz* section works to consolidate learning. The “meet the expert” section presents individuals who are actively engaged in the field. The *educator’s guide* presents teachers with additional resources to extend the students’ learning. Students can use a guest account or creating an account using their school Gmail account. Creating an account allows student progress to be saved so students can return to their unfinished lab. Finally, I have attached a Google slides *presentation* with links (or see appendix B) that highlights the key components of the lab. This serves as a teacher reference and as a resource to show students how the cybersecurity lab is set up.

**Context**

The Cybersecurity lab is designed for students from grades 6-12. The Cybersecurity lab promotes student understanding of cyber threats and defences with a strong focus on precautions everyone can take to keep their digital lives safe. The Cybersecurity lab can be connected to a variety of subject areas including science, literacy, and social studies. The lab can be used at home and at school. The Cybersecurity lab incorporates technology on two levels. Students discover how technology is used to maintain and establish a safe digital landscape. Challenges are made possible through technology and gamification. There are 4 challenges with 3 different levels of difficulty that include:

- **Coding**: program a robot to navigate a maze using Blockly drag-and-drop commands.
Civilizing Cybersecurity: No Kid Left Behind in the Digital Age

- **Password cracking:** face a series of “password duels” that teach the basics of how attackers might try to crack their passwords.
- **Social engineering:** navigating through scam emails, websites and phone calls and identify tactics that can promote safe online digital interactions.
- **Network cyber battles:** earning resources to buy cyber defences to protect their companies against a series of cyber attacks.

**Content and Connection to Curriculum and Competencies**

Through the completion of the Cybersecurity lab, students are engaged in computer coding, logical reasoning, critical thinking, and vulnerability detection to solve various problems that parallel the day-to-day jobs of cybersecurity professionals. The Cybersecurity lab connects to Big Ideas of Ontario science curriculum: "to relate science and technology to society and the environment". I have chosen this big idea because this lab provides a practical example that promotes digital literacy and prompts students to inquiry critically about their presence on the internet. This activity connects to one or more of the 21st century global competencies because of its well-rounded approach for innovative instruction. Through the completion of the process, students engage in problem-solving as they complete cybersecurity challenges. They must use their creativity to contribute unique solutions while taking risks to tackle problems presented. Finally, students engage in active citizenship as they learn about how to create a positive digital footprint and they may engage in local and global initiatives to make a difference.

**Educational Rationale**

I used the Cybersecurity Lab activity when I worked as a STEM program facilitator for girls in grades 6-8. The Cybersecurity lab was a success with the girls because they enjoyed the challenge of protecting a tech startup from cyber threats. Though I have been exposed to many technology resources, I decided to focus my submission on a cyber safety-focused resource. This decision was primarily driven after the technology class I took in the MT program. After I learned about the importance of culturing a community of learners that can take ownership over their digital lives, I decided that this was an important resource that I want to share with educators to help spread the important message of cyber safety. Research has shown that digital literacy is a critical skill we should be teaching in today's classrooms due to the
Civilizing Cybersecurity: No Kid Left Behind in the Digital Age

advancement of technology. (Hague and Payton, 2011; Lorenz, Kikkas, Laanpere and Laugasson, 2016). The biggest pedagogical rationale I took for using this resource is that I wanted to optimize student buy-in. Video games have been shown to be successful in fostering cybersecurity awareness and used frequently for training (Alotaibi, Furnell, Stengel, and Papadaki, 2016; Kritzinger, 2015). Therefore I believe that using the Cybersecurity lab can promote students to initiate learning outside of their regular structured school day.

Inclusivity/Equity/Diversity

This technology can be used to support approaches in differentiated learning in both content and process differentiation. In terms of content differentiation, each of the videos has closed captioning and the game can be used with voice-over apps to promote auditory and visual understanding. For process differentiation, each student has a choice as to which of 4 categories of challenges they want to focus on so they have multiple ways of demonstrating their understanding. Because each of the categories has multiple levels that students can work on, this allows all students at all ability levels experience success. Students that have trouble reading texts on the screen may have issues navigating the instructions at times. To support those students and make the activity for equitable and inclusive for them, teachers can employ cooperative learning techniques. Teachers can pair up students that require additional support with students and make the activity a group task. I believe this activity fits in with the principles for Universal Design for Learning as it stimulates motivation for learning. Additionally, the final assignment allows students to demonstrate their learning in various ways (see below).

Detailed Instructions

Time:

● 3-4 hours over 1-2 weeks

Materials

● The Cybersecurity Lab is accessible on web browsers that support HTML5 for example Chrome and Safari browsers.

Learning Goals:

● Students will be able to explain computer science terminology related to coding, password protection, social engineering, and network security.
Civilizing Cybersecurity: No Kid Left Behind in the Digital Age

- Students will be able to navigate a robot through a maze using Blockly code in the Coding Challenge
- Students will use analytical reading skills to distinguish among phishing attempts, fraudulent websites, and phone scammers in the Social Engineering Challenge
- Students will use logical reasoning to create strong passwords in the Password-Cracking challenge

Minds On

- Have students watch the video titled Cybersecurity101
- As a class create a class word cloud on Menti for the following question: “What are some ways we can protect ourselves on the internet?”
- Discuss why Cybersecurity is important to everyone
- Activity extension: complete a KWL (What I Know, want I want to learn, What I learned) chart

Action

- Explain to students that in the game, they will be completing four challenges related to Cybersecurity and describe the four challenges.
- Instruct students to complete all the Level 1 challenges in the game and ask students to remember some tips that they learned.
- In small groups, students complete a placemat activity where students list some of the tips they learned during the lab. Use a Google Docs document to write down ideas.
- Allow students to complete the remaining two levels for the four different challenges while the teacher provides guidance as necessary.
- Activity extension: allow students to design their own maze for the coding challenge, or instruct students to write their own phishing email.

Consolidate

- Students should complete the video quizzes and turn in their lab report as their exit slip.
- Final project: Students will create awareness for cyber safety using multimedia approaches. See appendix A for student self-assessment checklist and teacher assessment rubric. Examples may include:
Civilizing Cybersecurity: No Kid Left Behind in the Digital Age

- Design a poster that highlights the importance of safe online practices to bring awareness to the school community. Posters can be displayed around the school.
- Create a skit in the form of a personal service announcement. Skits/videos can be shown at a school assembly.
- Become a cybersecurity lab “expert”, volunteer in various classrooms to make presentations and show other students how to work through the cybersecurity lab.

Evidence of Learning Outcomes

To assess learning outcomes and ensure learning is presented during each part of the lesson, I have taken an approach that focuses on using assessment for, as, and of learning. Assessment of the students for learning will take place in the minds-on activity. I will use the word cloud created on the Menti Meter platform to assess students' pre-existing knowledge around cybersecurity. The assessment as learning takes place in the class during brainstorming of cyber safety tips and completion of the videos and quizzes. The formative assessment focuses on identifying if students have fully understood the ideas presented in the lab. Students demonstrate their ability to think critically and apply problem-solving protocols. This provides an opportunity for students to identify the key components and concepts presented in the lab. Finally, assessment of learning occurs in the final project where students demonstrate what they have learned and create a piece of work that brings awareness to cybersecurity. See appendix A for the student self-assessment checklist and the teacher assessment rubric. This final project supports the development of active citizenship as part of the 21st-century global competencies.

Other Considerations

This lab has many components which can be confusing for students to navigate through. For teachers to be able to support students, it is recommended that teachers take some time to explore and work through some of the problems presented. Because the lab is accessed through the internet, students may be distracted from the task. It is important to
review procedures for appropriate web use. By reviewing guidelines, it serves as a deterrent for inappropriate behaviour.

**Personal Professional Learning**

After completing this activity with grade 6-8 students, I understand the need for innovative teaching practices to educate students about cyber safety. Because the digital landscape permeates the lives of students, students need to learn how to protect themselves. As a new graduate from the MT program, I would use the prize money received from this award in two ways. First I would invest some of the money in technology-focused games and tools that I can bring into future classrooms to inspire learning. It is important that I continue to refine and expand my teaching pedagogy related to technology, thus I plan to use the prize money to help pay for the technology additional qualification course to achieve that goal. Thank you for the time spent in reviewing my submission.
References


Appendix A: Cyber Security Awareness (Final Project Assessment)

**Student Checklist (Self-Assessment)**

I have...

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summarized the big idea of from the Cybersecurity lab activity</td>
<td></td>
</tr>
<tr>
<td>Created a piece of work that communicates the importance of cyber</td>
<td>safety to the school community</td>
</tr>
<tr>
<td>Explained 2 pieces of advice for staying safe on the internet</td>
<td></td>
</tr>
</tbody>
</table>
Civilizing Cybersecurity: No Kid Left Behind in the Digital Age

**Cyber Security Awareness Rubric (Teacher Assessment)**

<table>
<thead>
<tr>
<th>Knowledge &amp; Understanding</th>
<th>Level 4</th>
<th>Level 3</th>
<th>Level 2</th>
<th>Level 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student demonstrates a thorough understanding of the evidence that explains the importance of cyber safety</td>
<td>Student demonstrates a considerable understanding of the evidence that explains the importance of cyber safety</td>
<td>Student demonstrates some understanding of the evidence that explains the importance of cyber safety</td>
<td>Student demonstrates a limited understanding of the evidence that explains the importance of cyber safety</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
<th>Level 4</th>
<th>Level 3</th>
<th>Level 2</th>
<th>Level 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student makes connections between evidence studied in class and pieces of advice with thorough effectiveness</td>
<td>Student makes connections between evidence studied in class and pieces of advice with considerable effectiveness</td>
<td>Student makes connections between evidence studied in class and pieces of advice with some effectiveness</td>
<td>Student makes connections between evidence studied in class and pieces of advice with limited effectiveness</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Thinking</th>
<th>Level 4</th>
<th>Level 3</th>
<th>Level 2</th>
<th>Level 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student's proposed work demonstrates a high degree of critical thinking</td>
<td>Student's proposed work demonstrates a considerable critical thinking</td>
<td>Student's work demonstrates some critical thinking</td>
<td>Student's work demonstrates limited critical thinking</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Communication</th>
<th>Level 4</th>
<th>Level 3</th>
<th>Level 2</th>
<th>Level 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student expresses ideas and content with thorough effectiveness</td>
<td>Student expresses ideas and content with considerable effectiveness</td>
<td>Student expresses ideas and content with some effectiveness</td>
<td>Student expresses ideas and content with limited effectiveness</td>
<td></td>
</tr>
</tbody>
</table>
Accessing the [Cybersecurity Lab](https://www.nova-labs.org/cybersecuritylab/)

The cybersecurity lab has multiple components.

The hands-on component lies in the “Game” where students participate in challenges to learn about cybersecurity.
Additional Resources (Details on slides 17-20)

- Cyber Video Quizzes:
  - can be used as a formative assessment to check understanding
- Meet the Experts:
  - extend the learning for students as they learn about professionals in the field
- Video Library:
  - focuses on particular concepts that students may be interested about

Cybersecurity Lab Game Play: Set Up

- Students can access using their Google account or use a guest account (no login)
**Game Play:** Selecting an Avatar and Choosing a Company

- Students select an avatar and a company they represent.
- Students choose a company they will “defend” against cybersecurity threats.

---

**Game Play: Goal**

- By completing challenges students gain...
  - Additional users for their company
  - Coins to buy cyber defenses
- 3 levels in the game for additional challenges and learning!
Game Play: Challenges

Each level contains 3 challenges:

- Coding: Navigate a maze using Blockly drag-and-drop commands.
- Password cracking: face a series of “password duels” that teach the basics of how attackers might try to crack their passwords.
- Social engineering: navigating through scam emails, websites and phone calls and identify tactics that can promote safe online digital interactions.

Game Play: Coding Challenges

- Students use block coding to program a robot to complete selected tasks
- Students are guided through the tasks with tips
- As students complete challenges, they gain more users and cyber coins
**Game Play: Coding Challenge**

- As students complete the tasks, they get more complicated.

**Game Play: Password Cracking Challenge**

- Students learn about how to design safe and strong passwords.
**Game Play: Password Cracking Challenge**

- Students learn about the ways that passwords can be hacked

![Password Cracking Challenge]

**Game Play: Social Engineering Challenge**

- Students complete challenges and learn about phishing emails, faulty sites, and other scams
- Students work to identify differences between the phishing email and real emails

![Social Engineering Challenge]
**Game Play: Social Engineering Challenge**

- After completion of the tasks, students are given explanations about the phishing websites and tactics hackers use to create scam websites and emails.

---

**Game Play: Completion of Level 1**

- Students have the option to replay puzzles to earn addition stars which will buy coins for the cyber attack challenge.
Game Play: Network Protection Challenge

- Students decide how they want to spend their coins to buy new cyber defenses
- These cyberdefenses will protect their company against the next round of attacks

Game Play: Network Protection Challenge Outcomes

- After buying the defenses, the company gets “attacked”
- Students will see how their cyber defenses held up again the attack
- Explanations will be given
- Students lose some users in areas with weaker defense
Civilizing Cybersecurity: No Kid Left Behind in the Digital Age

Teacher Resources: **Lesson Plan**

- Teachers have access to full lesson plans that describe:
  - Learning goals
  - Minds on
  - Action
  - Explanation
  - Consolidation

Teacher Resources: **Additional Videos**

- Cybersecurity 101
- Cyber Codes
- The Secret Lives of Hackers
- A Cyber Privacy Parable
- Cybersecurity Lab

Videos have accompanying discussion questions that can be assigned to check for comprehension
Civilizing Cybersecurity: No Kid Left Behind in the Digital Age

Teacher Resources: Videos and Quizzes

- As a formative assessment, the multiple choice questions can help teachers assess their learning
- Students can use this as a self-check for learning

Teacher Resource: Cybersecurity Glossary

- The glossary can be used by teachers to support learning...
  - Quiz for students
  - Support ELL learners by translating these terms
  - Additional learning activities (ex. flashcards)

---

**NOVA CYBERSECURITY LAB GLOSSARY**

The Cybersecurity Lab contains terms that may be unfamiliar to educators and students. In the game, these terms are highlighted with definitions that appear as mouse-overs. Below is a list of these terms and their definitions.

- **Antivirus software**
  - Computer programs that can block, detect, and remove viruses and other malware.

- **Backdoor**
  - Extra copies of computer files that can be used to restore files that are lost or damaged.

- **Bandwidth**
  - The amount of data that can pass through a network or part of a network per second.

- **Botnet**
  - Multiple computers on a network that are infected with a program that can be controlled remotely. The infected computers are usually used to cause damage that couldn’t be achieved with a single computer.

- **Computer network**
  - Two or more interconnected devices that can exchange data.

- **Computer virus**
  - A computer program that can copy itself and cause harm in various ways, such as stealing private information or destroying data.

- **DDoS**
  - A distributed denial of service attack attempts to make an online service, like a website, unavailable by overwhelming it with a flood of traffic from a team of computers.

- **Doom**
  - A fictional virus modeled after the Blaster virus. Like Blaster, Doom is able to damage physical infrastructure.