The Future of Engineering Education
2024 Annual Conference & Exposition
Oregon Convention Center
Portland, OR . June 23 - 26, 2024
ASEE
Paper ID #42307

Empowering Community-Driven Cybersecurity Education: A Framework for the Cybersecurity Ambassador Program

Dr. Doug W. Jacobson, Iowa State University of Science and Technology

Doug Jacobson is a University Professor in the Department of Electrical and Computer Engineering at Iowa State University. He is currently the director of the Iowa State University Center for Cybersecurity innovation and Outreach.

Empowering Community-Driven Cybersecurity Education:

A Framework for the Cybersecurity Ambassador Program

Work in Progress

Background

In an era where digital technology permeates every aspect of our lives, from personal communication to global commerce, educating the public has never been more critical. Traditionally, cybersecurity education has relied on awareness campaigns and simplistic top-ten lists. However, these approaches fall short. Imagine being handed a checklist of security tasks—patch updates, antivirus signatures, firewall exceptions—without context or relevance to our daily lives. It's akin to giving someone a toolbox without explaining how the tools work or when to use them.

The focus needs to be on security literacy. Security literacy is applying computer security best practices when faced with a novel situation and being proactive, not reactive, in the face of new threats. Security literacy is not just a list of tasks to perform but a context and knowledge for making value-based decisions regarding cyber security. It encompasses recognizing and protecting oneself from cyber threats, understanding the importance of maintaining digital privacy, and applying safe online practices in daily activities.

The need for security literacy arises from the ubiquitous nature of digital interactions and transactions in our daily lives. Our digital footprint is expansive, from online banking and shopping to social media engagement and remote work. This expansion brings myriad security risks, including identity theft, financial fraud, data breaches, and privacy violations. The consequences of these risks are not just individual; they extend to societal levels, impacting economic stability, public safety, and national security. As cyber threats evolve in sophistication, the gap between technical security measures and the general public's understanding of these threats widens, leaving individuals and communities vulnerable to digital exploitation.

Security literacy is the missing piece—a holistic understanding of practical computer security. It's not just about memorizing rules; it's about empowering individuals to make informed decisions. Here's why it matters:

1. **Context Matters**: Security literacy places knowledge within context. Instead of isolated bullet points, it provides the "why" behind security practices. When faced with a novel situation, users armed with context can apply best practices effectively.
2. **Daily Relevance**: Our screens constantly buzz with alerts—patch updates, suspicious emails, and malware threats. But these notifications often lack clarity. Security literacy bridges the gap by teaching users to evaluate risks and benefits. It's about making value-based decisions, not blind compliance.
3. **Proactivity, Not Reactivity**: Rather than reacting to threats, security literacy empowers proactive measures. It equips individuals to safeguard their digital lives preemptively, whether they're students, professionals, or everyday users.

In summary, security literacy is essential in the digital age for technology enthusiasts and everyone interacting with digital systems. We can foster a digitally secure and resilient society by delivering this education in a context that resonates with the general public.

The goal of the paper's author has long been to provide security literacy to every citizen of the State of Iowa. In doing so, the author produced a book [1], created a website to support security literacy [2], developed a course within the university, and has given over a hundred talks across the state. While these efforts were successful, they only reached a small number of people. This realization led to the creating of the Cybersecurity Ambassador Program at Iowa State University.

Program Structure

Iowa State University introduced and developed The Cybersecurity Ambassador Program under the umbrella of the Iowa Cyber Hub [3] to foster a network of informed and resilient digital citizens. Created in 2017, the Iowa Cyber Hub is an initiative developed by educators and industry professionals in Iowa. It serves various constituents, including students, employees, managers, educators, and others, by providing cybersecurity resources and guidance. The hub aims to enhance knowledge and career development in cybersecurity within the state and offers a variety of resources and opportunities. The Iowa Cyber Hub is dedicated to securing the state and expanding the cybersecurity workforce.

Launched in October of 2023, the Cybersecurity Ambassador Program [4] empowers students to promote basic cybersecurity concepts and practices within their communities. Through this campaign, students will develop and deliver content that educates and raises awareness on key cybersecurity issues that affect people's daily lives.

This ground-breaking program seeks to foster a network of trained ambassadors based in schools, 4H clubs, community colleges, universities, and other groups who will advance cybersecurity knowledge and practices within their communities. The campaign equips ambassadors with essential cybersecurity knowledge and skills that they can use to help their families, friends, and community members stay safe online. Ambassadors can access a library of engaging and interactive content such as videos, social media posts, infographics, and flyers to share cybersecurity best practices and tips with their audiences. Ambassadors are also encouraged to create materials to be included in the library. This initiative will promote digital safety, enhance community engagement, and foster leadership and communication skills among students.

By participating in the Cybersecurity Ambassador Program, students gain a deeper understanding of cybersecurity concepts and how to apply them to their personal and professional lives. They will also develop valuable communication and leadership skills as they work to educate others on this critical topic.

Ultimately, this program aims to create a network of local chapters of Cybersecurity Ambassadors who can promote basic cybersecurity literacy in their communities and help prevent cyber threats such as identity theft, cyberbullying, and online scams. With students at the forefront of this effort, the Cybersecurity Ambassador program has the potential to make a significant impact in promoting a safer digital future for all.

The **cybersecurity ambassador program's mission** is to "Cultivate a community of well-informed and proactive cybersecurity ambassadors who, through education and advocacy, play a pivotal role in promoting a safer and more secure digital society."

The **cybersecurity ambassador program's vision** is "To establish a resilient digital ecosystem where individuals, empowered with cybersecurity knowledge, collaborate to protect and enhance the security and privacy of their communities."

Program Objectives

- **Education & Awareness:** To disseminate critical cybersecurity information and foster a culture of vigilance and precaution.
- **Community Engagement:** To engage with various community segments, encouraging active participation in cybersecurity initiatives.
- **Collaboration & Networking:** To foster collaboration among cybersecurity professionals, enthusiasts, and the community.
- **Innovation & Development:** To encourage cybersecurity innovation, developing new and engaging ways to promote cybersecurity.
- **Capacity Building:** To build a cadre of trained and certified cybersecurity ambassadors and trainers who will spearhead various community outreach initiatives.
- **Leadership and Skill Development:** This campaign offers students a golden opportunity to develop crucial leadership and communication skills as they spearhead efforts to raise awareness about cybersecurity in their communities.

We created a Cybersecurity Ambassador Pledge, a testament to the core values that anchor the Cybersecurity Ambassador Program. This pledge embodies the ethos of our mission – to educate, protect, and inspire proactive digital citizenship. By adopting this pledge, our ambassadors affirm their dedication to upholding the highest digital safety and ethics standards and serving as pillars of trust and knowledge within their communities.

Cybersecurity Ambassador Pledge

As Cybersecurity Ambassadors, we commit to upholding the highest standards of ethical conduct and promoting a culture of safety, respect, and inclusivity within our community. We strive to:

1. ***Promote Awareness:** Actively work towards raising awareness about the importance of cybersecurity and helping others understand the risks and protections associated with digital environments.*

2. ***Empower Others:*** *Utilize our knowledge and skills to empower others, acknowledging my community's diverse capabilities and needs and striving to ensure that everyone can access and benefit from cybersecurity resources and education.*
3. ***Maintain Confidentiality:*** *Respect and protect the privacy and confidentiality of information entrusted to us, understanding the gravity of the responsibility we hold.*
4. ***Lead by Example:*** *Demonstrate exemplary digital citizenship, leading by example and encouraging others to follow suit, thus creating a culture of respect and safety online.*
5. ***Pursue Knowledge:*** *Remain committed to continually updating our knowledge and understanding of the ever-evolving cybersecurity landscape, ensuring that the information we share is current and accurate.*
6. ***Collaborative Spirit:*** *Embrace the spirit of teamwork, recognizing that cybersecurity is a collective effort, and provide assistance, encouragement, and support to fellow ambassadors and community members alike.*
7. ***Act with Integrity:*** *Confront digital ethics challenges with honesty and responsibility, not for personal gain but for the collective good, serving as a trustworthy guide in an evolving digital landscape.*
8. ***Uphold the Mission:*** *Uphold the mission and vision of the Cybersecurity Ambassador Program, striving at all times to be a credible, reliable, and enthusiastic ambassador.*

Components of the Program

This section discusses the program's various components, including ambassador chapters, support materials, and websites to support the program. Figure 1 shows the elements of the program.

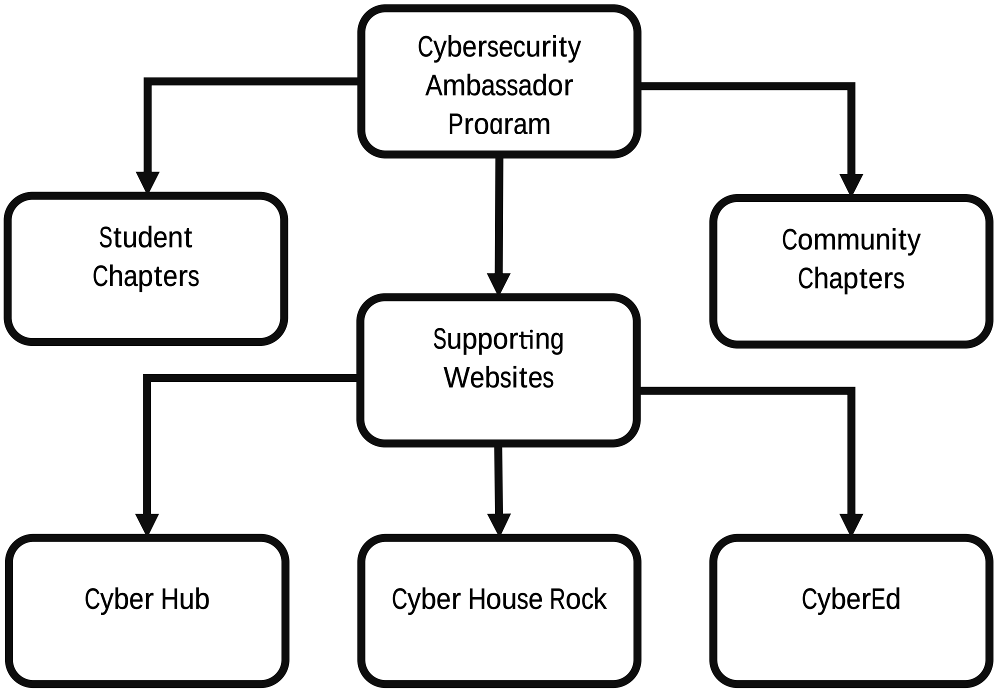

Figure 1: Elements of the Ambassador Program

To cultivate comprehensive cybersecurity awareness, the Cybersecurity Ambassador Program has established two distinct types of chapters: Student Chapters and Community Chapters. The rationale behind establishing separate student and community chapters lies in their unique spheres of influence and operational dynamics. This bifurcation is rooted in the understanding that different demographics and environments require tailored approaches to effectively convey and implement cybersecurity principles.

Student Chapters are primarily based in institutions such as high schools, colleges, universities, or other student groups like 4H. These chapters focus on ingraining cybersecurity awareness among the youth. The educational setting provides a fertile ground for these chapters to integrate cybersecurity education into the existing curriculum, extracurricular activities, and peer-to-peer interactions. A Cybersecurity Ambassador Program student chapter functions as a mini-hub within educational institutions like high schools or universities. Its primary role is to disseminate cybersecurity knowledge among peers. This chapter's members organize workshops, seminars, and interactive learning sessions tailored to their fellow students, fostering a culture of digital safety and awareness within their academic communities. These chapters bridge the complex world of cybersecurity and the student body, simplifying and localizing information to suit the unique needs of their educational environment.

In contrast, Community Chapters extends its reach beyond academic confines, targeting a broader audience that includes adults, seniors, and professionals. These chapters are pivotal in addressing the diverse cybersecurity needs of various community groups, often transcending the basic digital literacy provided in academic settings. Community chapters of the Cybersecurity Ambassador Program operate within broader local settings such as neighborhoods, towns, or cities. They focus on raising cybersecurity awareness among the general public, encompassing a diverse audience with varied levels of digital literacy. Activities conducted by community chapters include public workshops, awareness campaigns, and informational sessions at community centers or local events. These chapters are crucial in translating cybersecurity knowledge into practical, everyday applications. This ensures that all community members, regardless of age or professional background, can navigate the digital world safely and securely.

Recruitment, selection, and support of ambassadors

The Cybersecurity Ambassador Program employs a two-pronged approach to establishing chapters and recruiting ambassadors. This approach caters to student and community-based groups, ensuring a broad and impactful reach.

Student Chapters: These chapters are primarily formed within youth organizations such as schools, universities, and 4H clubs. The student chapter model relies heavily on these organizations to recruit students who are enthusiastic about cybersecurity. The recruitment process is integrated into the fabric of these institutions, leveraging existing networks and student activities. By doing so, the program ensures that the message of cybersecurity literacy resonates with the youth, fostering a culture of digital safety and awareness from an early age. We are leveraging existing relationships and programs to recruit chapters. For example, the community colleges are all part of the Iowa Cyber Hub, we are working with the State of Iowa STEM Council to reach all schools, and we have been running statewide cyber defense competitions since 2005 for both community colleges and high schools. In addition, we have already enlisted the state 4H leadership to create chapters within 4H.

Community Ambassadors: Unlike the student chapters, community ambassadors are recruited from a wider pool, typically through various technology and IT groups. The selection of community ambassadors follows a more formal application process. This process assesses candidates' backgrounds, expertise, and commitment to cybersecurity education. The aim is to ensure that those selected possess the necessary knowledge and the zeal to educate and empower their communities in cybersecurity matters. Since the program's announcement, we have had over 20 professionals inquire about becoming an ambassador. We will start the selection process in the summer of 2024.

Support and Materials

Once recruited, all ambassadors, whether part of student chapters or community ambassadors, have access to a wealth of resources and training. This support structure is critical for enabling ambassadors to effectively convey cybersecurity knowledge and practices within their communities. The types of support are described below.

Training and Educational Materials: Ambassadors are provided with access to a comprehensive library of educational content. This includes videos, social media posts, infographics, and flyers that provide best practices and tips for cybersecurity. Such materials are instrumental in facilitating the ambassadors' educational efforts, allowing them to communicate complex cybersecurity concepts in an engaging and accessible manner.

Interactive Platforms: The program also includes interactive platforms like the Cyber House Rock and CyberEd websites, which offer a variety of engaging content. These platforms serve dual purposes: they are a resource for ambassadors to enhance their understanding and a tool they can use in their community outreach activities.

Collaborative Contribution: One unique aspect of the program is the encouragement of ambassadors to contribute to the material development. This collaborative approach ensures the content remains relevant and updated and fosters a sense of ownership and engagement among the ambassadors.

Events and Networking: The program also includes opportunities for ambassadors to participate in events like the CyberEd-Expo. These events offer platforms for sharing experiences, presenting new materials, and networking with peers and experts in the field. Such interactions are pivotal for the continuous growth and development of ambassadors.

Program Websites: The materials and resources outlined above are disseminated through three specialized websites. Each of these websites contributes uniquely to the overarching goal of the Cybersecurity Ambassador Program, forming an integrated network of resources that support both the ambassadors in their educational endeavors and the public in gaining a better understanding of cybersecurity. Together, they represent a comprehensive approach to raising cybersecurity awareness and competence across various sectors of society.

Iowa Cyber Hub Website:

The Iowa Cyber Hub [3] is the primary portal for all information related to the Cybersecurity Ambassador Program. It is the starting point for anyone looking to understand the program's scope, objectives, and structure.

The site features comprehensive documentation developed with ChatGPT's assistance, offering detailed insights into the program's workings. From guiding principles to operational strategies, the Iowa Cyber Hub is a valuable information repository for prospective ambassadors and the general public. The site also maintains a web page presence for each chapter organized by county, thus allowing chapters to promote their upcoming events and as a way for groups to request presentations.

CyberEd Website:

The CyberEd website is designed to serve the educational needs of Cybersecurity Ambassadors. The site content is divided into four sections, each offering different educational materials. The goal is to create a dynamic educational hub that is continually evolving to include the latest information and resources in cybersecurity. A discussion of how the materials are developed is provided later in the paper.

The first section contains learning modules. Each module will contain materials that the ambassadors can utilize. We will also include lesson plans that provide activities and other information that ambassadors can use to help present the materials. This section of the website is under construction. However, we have identified the following topics for initial development.

1. **Cybersecurity Fundamentals:** "Learn the essentials of cybersecurity, including standard terms, concepts, and the rationale behind adopting cybersecurity measures."
2. **Types of Threats:** "Identify and understand the various cybersecurity threats, the risks they carry, and their potential impact on digital safety."
3. **Web Security:** "Discover the importance of securing websites and web applications, focusing on practices that protect user data and prevent unauthorized access."
4. **Email Security:** "Explore mechanisms that protect email content, safeguarding against unauthorized access and various forms of email-centric cyberattacks."
5. **Safe Online Habits:** "Study practices that enhance online safety, emphasizing routine actions and precautions that help maintain a secure digital environment."
6. **Mobile and IoT Security:** "Examine security protocols for mobile devices and Internet of Things (IoT) products, highlighting strategies to mitigate associated risks."
7. **Privacy and Data Protection:** "Understand the principles of data privacy and methods to ensure the confidentiality, integrity, and availability of personal information."
8. **Social Engineering:** "Learn about techniques used in social engineering attacks and the human factors that contribute to the success of these exploitation strategies."
9. **Network Security:** "Focus on methods to protect network infrastructures, including preventive measures, intrusion detection, and response strategies."

10. **Cybersecurity in Different Sectors:** "Review the application of cybersecurity frameworks and strategies in various industry sectors, acknowledging their unique requirements and challenges."
11. **Incident Response and Recovery:** "Learn the systematic approach to respond to cybersecurity incidents, focusing on immediate action, mitigation strategies, and recovery processes."
12. **Emerging Technologies and Risks:** "Keep abreast of the latest technological advancements and their corresponding cybersecurity challenges and risks.

The second section will contain sector-based materials. We currently have videos and informational materials that are targeted at farmers. The video series features Famer Frankie, who experiences various cyber situations and is faced with various choices. The videos help put cybersecurity in context and relate to farmers. The county extension offices have used the material to help teach cybersecurity concepts to farmers. They have found that by using the videos and supporting materials, they can add cybersecurity to an existing program, like ag lending.

The following section contains our tutorials page, featuring a curated selection of videos and instructional materials. These resources offer detailed guidance on specific cybersecurity tasks and a deeper exploration of internet technologies. From executing security measures to understanding intricate concepts, these straightforward tutorials provide factual, in-depth information for skill enhancement. The content is suitable for various learning levels and is designed for direct application and clear comprehension.

The last section is a series of videos written like short news stories. It is called the Adversarial News Network (ANN). These are designed to describe cybersecurity events in terms the public can understand. These would be used to help explain relevant cybersecurity events in an engaging way to show the potential impact of a cybersecurity incident.

Cyber House Rock Website:

The Cyber House Rock website is targeted at the general public and aims to make cybersecurity education both accessible and engaging. This platform is where multimedia meets cyber education, featuring creative content such as videos and interactive segments. By presenting cybersecurity concepts in a relatable and enjoyable format, the Cyber House Rock website provides a method to break down the complexity of digital safety into easily digestible and memorable content. The video content is divided into three types: cyber house rock, cyber tales, and how-to videos. Unlike the cybered website, the materials on this website are designed to be viewed by the public without an ambassador's aid. However, ambassadors might use some of these videos to support the learning materials during a presentation.

The "Cyber House Rock" video series stands as a cornerstone of the Cybersecurity Ambassador Program's public outreach efforts, drawing inspiration from the iconic and educational "Schoolhouse Rock" [7] series. This innovative series is designed to distill complex cybersecurity concepts into engaging, easily digestible multimedia content, making learning about digital safety enjoyable and memorable for all ages. Loosely based on the classic

"Schoolhouse Rock" format, "Cyber House Rock" uses catchy tunes, fun animations, and straightforward lyrics to explain various topics. However, it diverges by focusing specifically on the nuances of cybersecurity. The series covers a broad spectrum of issues, from understanding the basics of online privacy to recognizing and responding to cyber threats like phishing and malware. Each video in the collection is crafted to appeal to a broad audience, ensuring the messages resonate well beyond the traditional classroom setting. By blending education with entertainment, "Cyber House Rock" effectively lowers the barrier to understanding cybersecurity, making it more accessible to the general public and reinforcing the importance of being vigilant and informed in the digital world.

We have prototypes of several videos and are currently working to add animations to the songs. A few examples include:

Title	Topic	Title	Topic
Cyber House Rock	Theme Song	Malware Mansion	Types of Malware
I'm Just a Password	Strong Passwords	Phishing Boat Blues	Threats
Do the Two-Step	MFA	Email Rail	How Email Works
Password Parade	Password Keeper		

The Cyber Tales are short videos similar to the Farmer Frankie videos, except the situations and characters are not specific to a sector. Many of the videos also have a corresponding document that contains a summary of the situation and mitigation strategies.

The how-to videos overlap the how-to videos presented on the cybered website. These are designed to be more in-depth and help the viewer understand how technologies work.

The site also includes the innovative "Ask Captain Cyber," designed to provide a place to ask questions and look up answers to questions asked by others through the knowledge base. This unique platform acts as a digital cybersecurity consultant, where users can submit their queries and receive detailed, easy-to-understand responses from Captain Cyber, an animated character serving as the friendly face of cybersecurity expertise. What sets "Ask Captain Cyber" apart is its approachability and user-focused design. The site addresses common cybersecurity questions and delves into specific scenarios that users might encounter in their daily digital interactions. From tackling basic queries about creating strong passwords to more complex concerns regarding online privacy and data protection, Captain Cyber provides answers in a conversational and accessible manner, making it an ideal resource for people of all ages and digital literacy levels.

Material development

Creating and keeping the materials current is one of the more challenging aspects of teaching a topic like cybersecurity. This section will discuss how materials were created using ChatGPT and plans for using materials from other sources. We will also discuss the role of the ambassadors in developing new materials.

In addition to the educational materials described above, we created a brand identity for the program. The brand identity is designed to be simple and something we can put on our printed and promotional materials. For example, each ambassador will receive a name tag with the ambassador logo on it. We have created tote bags and other items that have the logo to give away. The logo for this program is shown below, along with the current logo for Cyber House Rock:

CYBERSECURITY
EDUCATE
EMPOWER
PROTECT
AMBASSADOR

The Iowa State University CyberEd group [8] oversees the creation of the educational materials. The CyberEd group comprises faculty and students from across campus working together to create and deliver cybersecurity education and outreach to Iowa and beyond. The mission of the CyberEd group is to provide cybersecurity education opportunities to all citizens. The CyberEd group is funded through various methods, including university funding (full-time support staff and the author's time), grant funding, and donations. A more detailed description of the financing and sustainability of the ambassador program is provided later.

CyberEd focuses on the following:

- **Literacy and Outreach:** Cybersecurity education for all.
- **Pathways:** New educational options for students, graduates, and professionals to earn cybersecurity degrees and credentials tailored to their career goals.
- **Exercises:** Cyber-focused exercises designed to provide scenario-based learning opportunities.
- **Training:** Specialized cybersecurity modules for educational and training purposes.
- **Learning Materials:** The design of innovative materials to help students learn cybersecurity and apply it to their career and degree goals.

The CyberEd group employs a multifaceted approach to developing educational materials, leveraging a blend of public resources, original content, and contributions from ambassadors. The group harnesses publicly available cybersecurity resources from sources like CISA [9], FBI [10], FTC [11], and others, ensuring learners can access diverse information from reputable sources. When these public materials are foundational, the CyberEd group supplements them with additional support materials, such as user-friendly guides, practical exercises, and discussion points, to enhance comprehension and engagement.

Furthermore, as described above, the group is dedicated to creating original, tailor-made content that addresses specific cybersecurity topics and scenarios relevant to the program's audience.

This content is not only informed by current trends and best practices in the field but also by the real-world experiences and insights of the ambassadors themselves.

Encouraging ambassadors to contribute to material development serves a dual purpose: ensuring the content is practical and relatable. It fosters a sense of ownership and engagement among the ambassadors. This collaborative and inclusive approach to content creation allows the CyberEd group to offer a rich, comprehensive suite of cybersecurity learning tools that are authoritative and adaptable to the needs of different learners.

In the spring of 2024, we held a CyberEd-Expo where student ambassadors presented materials they had developed to the CyberEd group for feedback. They first presented a plan in the fall of 2023 of what types of materials and lessons they were planning, and we provided initial feedback. The goal is to make these materials available to other ambassadors.

The CyberEd group utilized ChatGPT to develop the framework and some content for the ambassador program materials, as described above. Below is a description of how ChatGPT was used for the various parts of the program. I also want to acknowledge that ChatGPT helped create the description below of how ChatGPT supports the program. By including this, I intend to help show the power of using AI. I edited the responses to help make them more readable and to put them in first person. It should also be noted that the project went from an initial idea in September 2023 to kick off at the end of October 2023 and likely would not have been developed that quickly without AI.

1. Creating the Cybersecurity Ambassador Program

a. Development of the Charter:

- ***Initial Consultation:*** *I began by consulting ChatGPT to understand the fundamental components of an effective charter for a cybersecurity ambassador program. ChatGPT provided insights into key elements such as the program's mission, objectives, roles and responsibilities, and governance structure.*
- ***Drafting the Charter:*** *Utilizing the information, I worked with ChatGPT to draft a comprehensive charter. This included defining the scope of the program, outlining the roles of ambassadors, and establishing guidelines for operations and decision-making processes.*

b. Formulating the Pledge:

- ***Ideation:*** *I sought ChatGPT's assistance in brainstorming ideas for a pledge that would resonate with the ambassadors. The focus was on commitment to cybersecurity best practices, ethical behavior, and continuous learning.*
- ***Drafting the Pledge:*** *ChatGPT helped in drafting a concise and impactful pledge, ensuring it encapsulated the core values and responsibilities of the ambassadors.*

c. Guidelines for Starting a Chapter:

- ***Framework Development:*** *ChatGPT provided a step-by-step guide on how to start a local chapter of the cybersecurity ambassador program. This included advice on recruitment, setting up organizational structures, and conducting initial meetings.*
- ***Resource Compilation:*** *Additionally, ChatGPT assisted in compiling the resources and tools necessary for chapter leaders to manage and grow their local communities effectively.*

2. Creation of the Cyber House Rock Music Series

a. Lyric Creation:

- ***Brainstorming Sessions:*** *I used ChatGPT to brainstorm and create catchy, informative lyrics that would engage listeners while educating them about cybersecurity.*
- ***Refinement:*** *ChatGPT helped refine the lyrics, ensuring they were educational, rhythmic, and thematically consistent with the music genre.*

b. Development of Additional Video Ideas:

- ***Expansion of Concepts:*** *After the initial set of videos, I collaborated with ChatGPT to come up with innovative ideas for additional videos, focusing on emerging cybersecurity topics and trends.*
- ***Storyboarding:*** *ChatGPT assisted in developing storyboards for these videos, outlining the visual and narrative flow.*

c. Creation of the Phishing Series:

- ***Conceptualization:*** *ChatGPT played a crucial role in conceptualizing a series specifically focused on phishing. This included defining the scope, target audience, and key messages.*
- ***Content Development:*** *I worked with ChatGPT to develop engaging and informative content for the series, ensuring it was accurate and easy to understand for a broad audience.*

3. Developing the "Ask Captain Cyber" Concept

a. Conceptualization:

- ***Character Creation:*** *ChatGPT helped create the character of "Captain Cyber," a knowledgeable and approachable figure in cybersecurity.*
- ***Role Definition:*** *We defined the role of Captain Cyber as a virtual guide and mentor, answering questions and providing insights on cybersecurity matters.*

b. Initial Questions and Answers for the Knowledge Base:

- ***Question Compilation:*** *I used ChatGPT to compile a list of frequently asked questions (FAQs) that Captain Cyber would address. These ranged from basic cybersecurity concepts to more complex issues.*
- ***Answer Formulation:*** *ChatGPT was instrumental in formulating clear, concise, and accurate answers to these questions, ensuring they were informative and accessible to a wide audience.*

c. Knowledge Base Expansion:

- ***Continuous Update:*** *ChatGPT was used to regularly update and expand the knowledge base, incorporating new questions and answers as the field of cybersecurity evolved.*

4. Development of Learning Modules for the CyberEd Part of the Project

a. Identifying Educational Needs:

- ***Needs Assessment:*** *Initially, I engaged ChatGPT in discussions to identify the key educational needs and knowledge gaps among the cybersecurity ambassadors. This involved understanding the varying levels of expertise and the specific challenges they might face.*
- ***Target Audience Analysis:*** *ChatGPT helped analyze the target audience, primarily the ambassadors, to tailor the learning modules according to their learning styles and requirements.*

b. Topic Selection for Learning Modules:

- ***Brainstorming Topics:*** *Utilizing ChatGPT, I brainstormed a wide range of topics relevant to cybersecurity. This included foundational cybersecurity principles, advanced threat detection, incident response, and emerging technologies like AI and blockchain in cybersecurity.*

- ***Relevance and Applicability:*** *ChatGPT assisted in ensuring that the topics chosen were relevant to the current cybersecurity landscape and applicable to the practical scenarios that ambassadors might encounter.*

c. Structuring the Modules:

- ***Module Framework Development:*** *I worked with ChatGPT to develop a structured framework for each learning module. This included defining learning objectives, key takeaways, and interactive elements like quizzes and practical exercises.*
- ***Content Creation:*** *ChatGPT was instrumental in creating detailed content for each module. This content was designed to be engaging, informative, and easy to understand, focusing on real-world applications.*

Current Status of the Project

The project launched in late October of 2023. The program has successfully garnered commitments from 4H, four high schools, three community colleges, and my university to establish student chapters. These chapters will serve as pivotal centers for educating young minds about the importance of cybersecurity.

Additionally, there has been a surge of interest from various parts of the state in starting community chapters. These chapters will be crucial in broadening the program's reach to a broader range of community members, ensuring cybersecurity awareness permeates every level of society. We are working with ag extension and our manufacturing extension group to establish community chapters.

As mentioned above, we held our first CyberEd-Expo, where two of our schools presented new learning materials that can be included on our cybered website.

Funding and Sustainability of the Cybersecurity Ambassador Program

With its comprehensive structure and far-reaching objectives, the Cybersecurity Ambassador Program requires a robust financial plan to ensure its success and sustainability. Initially seeded by Iowa State University, the program has benefitted significantly from the university's backing in terms of both financial support and staff resources. The university's involvement is not limited to funding; it extends to providing essential infrastructure and personnel support, crucial for the program's foundational operations. As the director of the Iowa State University Center for Cybersecurity and Outreach, the author has a portion of their professional responsibilities to oversee and guide the program's development. The center has a staff person dedicated to supporting outreach activities. Moving forward, we are exploring several options for long-term funding, as outlined below.

1. **Private Funding:** A notable $50,000 in private funding marks a strong start for the program. This initial capital is instrumental in covering the program's early-stage expenses, such as developing training materials, setting up online platforms, and organizing initial outreach events.
2. **Corporate Sponsorship:** The program has attracted interest from various corporate entities keen on sponsoring cybersecurity initiatives. These companies will be

approached to provide financial assistance and contribute valuable industry insights and expertise. We are working with the university foundation on a strategy to obtain private donations.

3. **State Funding:** Efforts are underway to secure state funding to align the program with regional cybersecurity and educational goals. State funding would not only bring in financial resources but also reinforce the program's legitimacy and widen its scope of influence.
4. **Grants and External Funding Opportunities:** The program will seek grants and funding from cybersecurity-focused institutions and government agencies. Such funding sources can provide substantial financial backing and are often aligned with the program's objectives of fostering cybersecurity literacy.
5. **Partnerships with Educational and Tech Companies:** Collaborations with tech and educational companies can bring in both financial and material resources. Since launching the program, we have discussed partnerships with several security technology companies. Partnerships can include donations of equipment, software, and access to proprietary training resources.

Ensuring Program Continuity

In addition to diverse funding streams, the Cybersecurity Ambassador Program's sustainability hinges on demonstrating continuous impact and relevance. Regular assessments, impact reports, and adaptability to the evolving cybersecurity landscape will be critical in securing ongoing support from existing and potential funders. The program's affiliation with Iowa State University and the CyberEd group provides a solid foundation for academic and research-based credibility, further enhancing its appeal to sponsors and funders.

The program's financial and operational sustainability will depend on its ability to blend educational goals with community engagement, forming partnerships beyond financial support into knowledge exchange, skill development, and community building.

Digital Badges and Micro-Credentials: A Comprehensive Recognition System

Another exciting development is the introduction of digital badges for ambassadors. These badges will serve as a recognition of their skills, training, and contributions, further incentivizing participation and engagement in the program. This system provides ambassadors with tangible proof of their expertise and encourages a sense of achievement and progress. The planned introduction of micro-credentials by Iowa State University is a strategic enhancement to the program. These credentials, particularly those aligned with the 8 NACE Career Readiness Competencies [12], offer a structured way to recognize the ambassadors' development in highly valued skills in the workforce. This alignment not only underscores the practical value of the program in terms of career development but also integrates the program's objectives with broader educational and professional standards.

These badges symbolize achievement, acknowledging each ambassador's skills, training, and contributions. These badges could be tiered, reflecting the increasing complexity and level of involvement in the program – from basic awareness to advanced cybersecurity practices and leadership roles. There are several benefits to micro-credentials and digital badges, as outlined below:

1. **Enhanced Career Opportunities:** For student ambassadors, these digital badges and micro-credentials can be a significant addition to their resumes, showcasing their commitment and proficiency in cybersecurity. This recognition can be instrumental in differentiating them in the job market, particularly in fields where cybersecurity awareness and skills are increasingly in demand.
2. **Recruitment and Retention:** Earning recognized credentials is a powerful recruitment tool for the program. It attracts individuals who are not only interested in cybersecurity but also in enhancing their professional skill set. Furthermore, this system aids in retaining ambassadors by offering them clear pathways for advancement and recognition.
3. **Validating Skills and Knowledge:** The digital badges and micro-credentials provide a tangible and verifiable means to validate the skills and knowledge gained by the ambassadors. This is especially important in cybersecurity, where practical skills and up-to-date knowledge are paramount.
4. **Building a Portfolio of Skills:** Ambassadors can accumulate a portfolio of badges and credentials that demonstrate a wide range of competencies, from technical knowledge to leadership and communication skills. This holistic skill set is beneficial professionally and personally, as it fosters a comprehensive understanding of digital security.

The introduction of digital badges and micro-credentials within the Cybersecurity Ambassador Program is a strategic initiative that promises to enrich the ambassadors' learning experience, provide them with valuable professional tools, and enhance the overall appeal and effectiveness of the program.

Future Plans and Conclusions

As the Cybersecurity Ambassador Program continues to evolve and expand, several key initiatives are on the horizon to enhance its scope and efficacy. The ongoing development of educational materials remains a cornerstone of the program. With a focus on continuous innovation, we plan to regularly update and introduce new content that addresses emerging cybersecurity trends and threats. This effort includes creating more interactive modules and real-life case studies that provide ambassadors and learners with hands-on, practical cybersecurity experiences. The program has hired five undergraduate students as summer interns to develop the additional materials.

The Cyber House Rock initiative, a key component of our Cybersecurity Ambassador Program, is poised for a significant expansion to enrich its offerings and reach. We are assembling a team of singers and animators to take the AI-generated lyrics and produce an extensive series of educational yet entertaining videos to realize this vision. By expanding the range and number of videos, we aim to cover a broader spectrum of cybersecurity topics, ensuring that there is a Cyber House Rock video for almost every aspect of digital safety and security. This expansion is not just about quantity; it's about enhancing the quality and diversity of the content, making cybersecurity education more accessible, memorable, and enjoyable. Integrating animation and music production will bring these concepts to life, creating an immersive learning experience that resonates with viewers and encourages them to engage more deeply with cybersecurity. Through Cyber House Rock, we are redefining the approach to cybersecurity education, making it a creative and engaging journey for everyone.

Our program will significantly advance by integrating artificial intelligence into "Ask Captain Cyber." This AI augmentation, supervised by cybersecurity experts, aims to provide more dynamic, personalized responses to user queries. The enhancement will improve the accuracy and relevance of the information provided and offer a more engaging and responsive user experience. This development aligns with our goal to make cybersecurity advice more accessible and effective for a broader audience.

The expansion of student chapters remains a crucial objective. Recognizing the vital role of youth in shaping a cyber-aware future, we are committed to establishing more student chapters across various educational institutions. These chapters will act as hubs for peer-led learning, fostering a culture of digital safety and responsibility from an early age. We aim to have at least 24 student chapters signed up by fall.

Additionally, working in collaboration with CIRAS (Center for Industrial Research and Service) and extension services, we aim to create more community chapters. This expansion will ensure that cybersecurity education reaches beyond academic settings into the wider community, encompassing various demographics and professions. We aim to have at least five community chapters in place by the end of summer.

In summary, the Cybersecurity Ambassador Program is making significant strides in contributing to the broader landscape of cybersecurity education. Our emphasis on local engagement, diversity of participation, and practical learning experiences underpins the program's success. As we look to the future, we are inspired to explore new pathways and initiatives that will continue to strengthen the cybersecurity knowledge and practices of individuals and communities alike. Our vision is a digitally secure future where cybersecurity is understood and embedded in every netizen's daily actions. With the collective effort of our ambassadors, partners, and supporters, we are confident that this vision will become a widespread reality.

Overall, the Cybersecurity Ambassador Program is rapidly gaining momentum. We aim to foster a culture where cybersecurity is not just a concept but a practiced norm. The enthusiasm and commitment from educational institutions, communities, and corporations reinforce the program's relevance and potential impact.

References

[1] Jacobson, D., & Idziorek, J. (2013). Computer Security Literacy: Staying Safe in a Digital World (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/b13707

[2] Security literacy website, [Online]. Available: http://www.security-literacy.org/ [Accessed: 29-April-2024].

[3] Cyber hub website, [Online]. Available: https://www.iowacyberhub.org/ [Accessed: 29-April-2024].

[4] Cyber Ambassador program, [Online]. Available: https://www.iowacyberhub.org/ambassadors/ [Accessed: 29-April-2024].

[5] CyberEd web site, [Online]. Available: https://www.cyio.iastate.edu/cybered/ [Accessed: 29-April-2024].

[6] Cyber house rock web site, [Online]. Available: https://cyberhouserock.cyio.iastate.edu/ [Accessed: 29-April-2024].

[7] School house rock, [Online]. Available: https://en.wikipedia.org/wiki/Schoolhouse_Rock! [Accessed: 29-April-2024].

[8] CyberEd group's website, [Online]. Available: https://www.cyio.iastate.edu/cybered/ [Accessed: 29-April-2024].

[9] Parent and Educator Resources | CISA, [Online]. Available: https://www.cisa.gov/resources-tools/resources/cybersecurity-awareness-program-parent-and-educator-resources. [Accessed: 08-Feb-2024].

[10] Internet Crime Complaint Center, "Complaint Choice," IC3, 2024. [Online]. Available: https://www.ic3.gov/Home/ComplaintChoice/default.aspx [Accessed: 08-Feb-2024].

[11] Online Privacy and Security, Federal Trade Commission, 2020. [Online]. Available: https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security. [Accessed: 08-Feb-2024].

[12] NACE Career Readiness Competencies [Online]. Available: https://www.naceweb.org/career-readiness/competencies/career-readiness-defined [Accessed: 22-Mar-2024]