Cybersecurity for Young Learners

Extending the Reach of the Cybersecurity Workforce Pipeline via Early Awareness & Education

Rebecca Hoffart
All Saints Cathedral School, St. Thomas, US Virgin Islands

ABSTRACT

Past efforts to expand cybersecurity workforce pipeline have focused heavily on adult learners. This project demonstrates that the pipeline can be extended to reach undertargeted populations such as early learners. This approach will introduce more people to cybersecurity as a career choice, build their confidence in skills, and increase cybersecurity awareness to build a general population better prepared to self-defend.

The poster provides an overview of a successful project and highlights examples of the work, metrics, success measurements, and samples of student cybersecurity products. Projects like this provide important steps to implementing an effective and comprehensive cybersecurity education program for grades K-12.

INTRODUCTION

- Cybersecurity education is underway in certification and undergraduate programs, and national pre-college programs such as the Air Force Association's CyberPatriot and NSA's Day of Cyber.
- Maximizing the pipeline means adding initiatives for younger learners and within formalized school curriculum. Successful models need to be identified in order to move forward.
- In this project, a first grade class of 12 students was introduced to both programming and core cybersecurity concepts. A variety of methods was applied to deepen understanding (game-based learning, videos and multimedia, modeling, project-based learning, differentiation). Students illustrated core cybersecurity concepts by coding animations using Scratch, Jr.

CORE CONCEPTS (from the 2016 CSTA K-12 Computer Science Standards)

- Personal Information: Sharing and Securing
- Cyberbullying & Online Safety
- Computer & System Protection

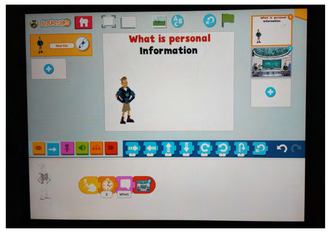
RESULTS

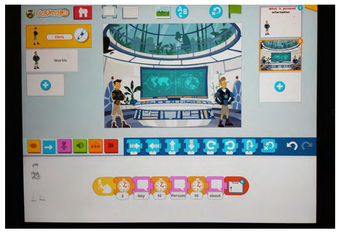
Despite the young age of the students (6-7 years), they demonstrated recognition of the importance of cybersecurity.

- Cybersecurity quiz results reflected mastery of the concepts.
- 100% of students achieved a certificate for mastering the Security Showdown game from the AFA CyberPatriot Program Elementary School Cyber Education Initiative (ESCEI).
- Student project animations demonstrate knowledge, impart a sense of ownership, and provide tools for teaching others.

SUCCESS MEASURES

STUDENT PROJECT SAMPLES





MATERIALS & TOOLS

Despite the young age of the students (6-7 years), they demonstrated recognition of the importance of cybersecurity.

- ScratchJr. Lesson Plans
- BrainpopJr. Internet Safety Video and Extension Materials
- AFA CyberPatriot Program Elementary School Cyber Education Initiative (ESCEI)

PROCEDURE

1. Introduce and practice coding in ScratchJr.
2. Introduce core cybersecurity concepts and test for understanding.
3. Present model project(s).
4. Students create their own version of the model and share with others.

CONCLUSION

When provided with well-constructed lessons that are sound both pedagogically and in content, early learners can grasp core cybersecurity concepts. Projects like this support the curriculum development work which must take place in order to formalize and implement a K-12 cybersecurity education program.

Excerpt from BrainPopJR. Internet Safety Video Transcript

ANNIE: Well, Rocket Ron is *definitely* a stranger. If a stranger contacts you or makes you feel uncomfortable, tell a teacher or a grown-up.

Threat-Driven Approach

MOBY: Beep.

Managed Security Service Provider

Moby raises his hand to get help from a grown-up at the school. Annie's teacher comes over to help.

ANNIE: They can keep the stranger from bugging you by blocking their e-mails or instant messages.

Incident Response

A dialog box asks if Moby wants to block Rocket Ron. The teacher clicks "yes" and then closes the instant message box.

ANNIE: Sometimes I get e-mails from people that pretend to know me or tell me I've won a big prize. If I don't know the sender, I don't open the message.

Phishing

Social Engineering

Annie's inbox shows she has an e-mail from someone named David. The subject says "Annie, you've won a new computer!!" She deletes the e-mail.

ACKNOWLEDGEMENTS & DISTINCTIONS

- This work has been supported by the CECOR K-20 Cybersecurity Workforce Pipeline Consortium, which was established by U. S. Department of Energy/National Nuclear Security Administration's Minority Serving Institutions Partnerships Program (MSIPP).
- Related work was also presented at the Computer Science Teachers Association Summer, 2017 International Conference.
- The National CyberWatch Center honored this work with its inaugural "Innovations in Cybersecurity Education" award in the category of Student Learning Aid.

REFERENCES

2017 Global Information Security Workforce Study, Frost & Sullivan and (ISC)2 (https://iamcybersafe.org/research_millennials/)
Securing our Future: Closing the Cyber Talent Gap, Raytheon (https://www.raytheon.com/cyber/rtnwcm/groups/iis/documents/content/rtn_278205.pdf)
State of Cyber Security 2017, ISACA (https://www.isaca.org/cyber/Documents/State-of-Cybersecurity-infographic_res_eng_0217.pdf)
Thomas, J. (2000). *A Review of Research on Project Based Learning*. Buck Institute for Education. Bie.org

WEB SITES FOR PROJECT TOOLS

1. Scratch Jr. (https://www.scratchjr.org/teach/activities)
2. BrainpopJr. (brainpopjr.com)
3. ESCEI (uscyberpatriot.org)