Removing the Veil: Shining Light on the Lack of Inclusivity in Cybersecurity Education for Students with Disabilities

Felicia Hellems
hellemsf@mail.sacredheart.edu
Sacred Heart University

Sajal Bhatia
bhatias@sacredheart.edu
Sacred Heart University

ABSTRACT

There are currently over one billion people living with some form of disability worldwide. The continuous increase in new technologies in today's society comes with an increased risk in security. A fundamental knowledge of cybersecurity should be a basic right available to all users of technology. A review of literature in the fields of cybersecurity, STEM, and computer science (CS) has revealed existent gaps regarding educational methods for teaching cybersecurity to students with disabilities (SWD's). To date, SWD's are largely left without equitable access to cybersecurity education. Our goal is to identify current educational methods being used to teach SWD's concepts of cybersecurity, evaluate these methods, and classify the observed trends.

KEYWORDS

Cybersecurity, Disabilities, Education, Learning Methods

1 BACKGROUND

Four disabilities were chosen for review based on their impact to cybersecurity concepts. The historic lack of curriculum as well as integrative assistive tools has posed problems for visually impaired or blind (VIB) individuals in learning concepts of cybersecurity [2]. Traits of intellectual disabilities (ID) can include deficits in reasoning abilities and abstraction, which impact the maintenance of a solid security posture [1]. Dyslexia can pose textual comprehension issues and difficulties decoding words, which affect password creation and authentication skills [4]. While autistic characteristics can lead to an increased susceptibility to social engineering attacks, other traits make neurodivergent individuals well suited for careers in cybersecurity, underlining the need for inclusivity [3].

2 RESEARCH METHOD AND KEY FINDINGS

Finding minimal research specific to the field of cybersecurity education, the initial review phase was broad in scope and included literature from the fields of STEM and CS, as certain topics in these fields aligned contextually with key cybersecurity concepts. A focused review directly tied to cybersecurity education was then conducted with attention paid to identified emerging patterns. Upon analysis, two main patterns surfaced. The first was related to the *integration* of materials into the curriculum with methods falling either into a short or long term model. Short term models involved the delivery of methods in the form of camps/workshops that were short in temporal duration. Long term integration models included amendments to current curriculum, creations of guidelines aimed at inclusivity, or adaptations to traditional teaching methods. The second identified pattern was related to the *implementation* of materials into the curriculum with prior work largely delivering these methods via the use of programming/coding or the use of tools.

Research in the field of cybersecurity has focused primarily on VIB individuals involving the use of tools delivered through short term integration models. [2]. One instance was identified related to autism involving a longer term model for increasing the presence of neurodiverse individuals in the cybersecurity field [3]. Research has been done in STEM and CS in the use of robotics for teaching SWD's with positive results and stands as an area from which to draw in creating a framework within the field of cybersecurity that can serve as a response to some of the current deficits in the field.

3 CONCLUSION AND FUTURE WORK

The recent rise in virtual learning requires an increase in the breadth of disabilities for which educational methods are being developed to decrease the observed lack of inclusivity for SWD's in cybersecurity. Examining the successes in related fields with gamification and robotics, there exists an opportunity to explore similar approaches within cybersecurity. Past educational models have created a culture within cybersecurity that has both failed in providing proper accessibility to SWD's as well as in offering the same level of equity as non SWD's. A long term integration model that ensures continuity in cybersecurity education for SWD's will not only address this lack of equity but will aid in creating a more inclusive culture within the field of cybersecurity and a more secure and inclusive society as a whole.

ACKNOWLEDGEMENTS

The authors acknowledge support provided by the National Science Foundation under Award No. 2017371.

REFERENCES

[1] Fifth Edition et al. 2013. Diagnostic and statistical manual of mental disorders. *Am Psychiatric Assoc* 21 (2013).
[2] Jesse R Hairston, Derrick W Smith, Tania Williams, William T Sabados, and Steven Forney. 2020. Teaching Cybersecurity to Students with Visual Impairments and Blindness. *Journal of Science Education for Students with Disabilities* 23, 1 (2020).
[3] Joel Scanlan, Andrew Eddy, Teresa Thomas, Tele Tan, Yi-Ping Phoebe Chen, Paul A Watters, Michael Fieldhouse, Lawrence Fung, and Sonya Girdler. [n. d.]. Neurodiverse Knowledge, Skills and Ability Assessment for Cyber Security. ([n. d.]).
[4] Linda S Siegel. 2006. Perspectives on dyslexia. *Paediatrics & child health* 11, 9 (2006), 581–587.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
SIGCSE 2022, March 3–5, 2022, Providence, RI, USA.
© 2022 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9071-2/22/03.
https://doi.org/10.1145/3478432.3499114