Journal of Cybersecurity Education, Research and Practice

Volume 2022 | Number 1 Article 6

July 2022

Cybersecurity Educational Resources for K-12

Debra Bowen
National University, dbowen@nu.edu

James Jaurez
National University, jjaurez@nu.edu

Nancy Jones
National University, njones2@nu.edu

William Reid
National University, wreid2@nu.edu

Christopher Simpson
National University, csimpson@nu.edu

Cybersecurity Educational Resources for K-12

Abstract

There are many resources to guide successful K-12 cybersecurity education. The objective of these resources is to prepare skilled and ethical cybersecurity students at the earliest level to meet the demands of higher-level programs. The goal of this article is to provide, as a starting point, a list of as many currently popular K-12 educational resources as possible. The resources provided are broken into five categories: 1) Career Information, 2) Curriculum, 3) Competitions, 4) CyberCamps, and 5) Labs and Gaming. Each resource listed has a link, the K-12 levels that are supported, whether the resource is free or has a cost, and a shortlist of topics or, for camps and competitions, the dates available. There are many teaching and learning resources for K-12 students. However, there are very few sources that combine a variety of these resources into one document. Even though this is not an exhaustive list of resources, it should be a helpful starting point as to what is available for the K-12 levels.

Keywords

Cybersecurity, K-12, Ethics, Curriculum, Competitions. Camps, Labs, Gaming

INTRODUCTION

The cybersecurity skills gap continues to be an issue that is contributing to a shortage of cybersecurity professionals. In addition, it is creating challenges for educational institutions at all levels to keep pace with the necessity to educate students in cybersecurity at a much earlier level. Even though the number of schools designated as Centers of Academic Excellence (CAE) is growing, the ability to prepare enough cybersecurity students cannot meet the demands of the industry (Tsado, 2019). Students need to be introduced to cybersecurity concepts earlier in the educational process. According to Hachey (2020), students who start earlier have a better chance of staying in STEM. An introduction to ethics and responsible computer usage as early in the educational process as possible will give students and educators confidence to properly explore cybersecurity topics. An opportunity to close the skills gap earlier could start by providing a collection of educational resources to assist those teaching and learning cybersecurity at the K-12 level. K-12 refers to kindergarten through 12th grade, encompassing approximately five to 18 years old. There are many teaching and learning resources for K-12 students. However, there are very few sources that combine a variety of these resources into one document.

The goal of this article is to provide, as a starting point, suggested educational resources that are currently available at the K-12 levels. The resources listed were either known by one of the authors or selected after research and vetting to make sure the resource was valid and up to date. Please note that the resources in each table are not listed in any type of preference, but rather alphabetically. Also, the emphasis on resources is centered in the United States. Since cybersecurity practices could affect environments in unpredictable ways, we would like to begin by mentioning ethics in cybersecurity.

ETHICS IN CYBERSECURITY

Ethics play a critical role in whether a school even offers cybersecurity courses, pathways, or resources. An inherent danger in teaching cybersecurity to young people is that their social development may be heavily influenced by curiosity and peer recognition, which could lead to high-risk behavior (Blanken-Webb et al., 2018). This potential for students to utilize knowledge and tools in inappropriate, mischievous, or perhaps even criminal ways compounds the necessity for foundations of ethical behavior as a prerequisite for providing resources and content to young people. Balanced with the engagement and career potential of cybersecurity academic and job paths, this strong foundation in ethics courses provides the necessary tools to ensure K-12 students operate their skills safely and effectively (Macnish & van der Ham, 2020).

As with many career paths, the individual must decide whether to use their knowledge and potential in constructive or potentially destructive ways (Christen et al., 2020). However, unlike many other STEM fields, cybersecurity delves into tools, techniques, and procedures (TTP) that are powerful enough to affect computing systems as well as the organization and social environment (Martin, 2017). By offering students a pathway to understanding values, behaviors associated with actions that are good and desirable, educators can provide the framework for students to best understand attitudes, preferences, and interests as both subjective and objective in the cybersecurity field. According to Martin (2017), even elementary concepts such as the distinction between white, black, and gray hat hackers delineate the expectations and responsibilities of even the novice cybersecurity professional.

The cybersecurity field sometimes necessitates an individual selecting a team and then exhibiting and articulating the chosen use of their knowledge and skills. Introducing ethical concepts as early as possible within the academic pathway for cybersecurity allows students to realize and cement the purpose and parameters of the TTPs they will acquire during their special educational pathway. Separating the understanding of confidentiality, integrity, and availability (CIA), as well as the difference between safety and security, demonstrates to students that professional actions and responsibilities can align ethical behavior to functional purpose within the field by contrasting normal risk of operations with the harm caused by adversarial individuals (Christen et al., 2020; Manjikian, 2017). Furthermore, students begin to see that concepts of red team activity and white-hat (ethical) hacking are tools used to understand threat actors and adversaries by utilizing value conflict within rules of engagement to understand and defend against the cybersecurity opponent (Martin, 2017).

RESOURCES CURRENTLY AVAILABLE

After collecting numerous resources, it was apparent that providing general categories would be needed for ease of use. Based on content type, the resources were broken into five categories: 1) Career Information, 2) Curriculum, 3) Competitions, 4) CyberCamps, and 5) Labs and Gaming. Each resource listed provides a link, the K-12 levels that are supported, whether the resource is free or has a cost, and a shortlist of topics or, for camps and competitions, the historical time period available.

Career Information

As mentioned previously, there is a growing shortage of qualified cybersecurity professionals and practitioners. As with many careers, the earlier a student is introduced to the discipline, the more interest they have in pursuing similar careers

as adults. However, this could be especially challenging for students with cybersecurity interests since it is not traditionally covered in K-12 curriculum. While educators can obtain the skills to teach the range of K-12 students, the industry will need to take the lead in establishing career paths by providing internships, apprenticeships, training programs, and recruiting and hiring opportunities. Table 1 contains some useful cybersecurity career resource websites for the K-12 levels.

Resource	K-12 Levels	Free / Pay	Content Type
Career Discovery Cybersecurity Experience https://sites.google.com/view/cybercareerdiscovery/introduction-to-this-exploration	9-12	Free	• Career Journey • Teacher Resources (Lesson plans, labs, videos)
Common Core State Standards Initiative http://www.corestandards.org/	K-12	Free	• Standards per State • Mathematics Standards K-12 • English Language Arts Standards K-12
Cybersecurity Guide https://cybersecurityguide.org/	9-12	Free	• Career guide for students • Tips for parents
K12 CyberTalk https://k12cybertalk.org/	K-12	Free	• Careers: Season 1, Show 12 • Environment for K-12 students to learn and explore cybersecurity
NICCS https://niccs.cisa.gov/formal-education/students-launch-your-cyber-career	9-12	Free	• Career Options • Career Paths • Scholarships • Colleges
SANS Cyber Aces https://www.cyberaces.org/careers.html	9-12	Free	• 20 Top Information Security Jobs

Table 1: List of Cybersecurity Career Resources

Curriculum

To begin solving the increasing cybersecurity talent shortage, educators need to teach the next several generations of potential cybersecurity professionals, starting as early as possible in the K-12 educational system. Prepared educators can confidently teach cybersecurity curricula in a way that empowers students. By

learning and teaching cybersecurity skills and concepts in a classroom, educators are providing students with knowledge, skills, tools, and confidence. These can be carried forward so that students become lifelong learners with the potential to succeed in future cybersecurity training, education, and careers.

One of the challenges of teaching cybersecurity to K-12 students is that K-12 methods are different from higher education methods. However, both are expected to accomplish the same goals (Chase, 2020). Many educational resources provide curriculum guidance and content for educators. Table 2 contains useful websites which provide cybersecurity curriculum resources for different K-12 levels.

Resource	K-12 Levels	Free/Pay	Content Type
Clark Center https://clark.center/home	9-12	Free	• Curriculum Guidance • Content-teachers • Content-students • Videos & Labs
CodeHS https://codehs.com/info/curriculum/pathways/k-12	K-12	Free	• Teaching Platform • Curriculum • Courses • K-12 Pathways
CSTA Standards https://www.csteachers.org/Page/standards	K-12	Free / Pay	• Content-teachers • Professional Development • Reports & Publications
Cyber.Org https://cyber.org	2-12	Free	• Content-teachers • Courses • Activities
Cybersecurity Education Resource Directory (CARD) https://www.caeresource.directory/home	9-12	Free	• Categorized collection of cybersecurity education resources
Hacker High School https://hackerhighschool.org	6-12	Free / Pay	• Self-guided Curriculum • Practical Exercises • Lessons / Courses
National Cryptologic Foundation (NCF) https://cryptologicfoundation.org/what-we-do/educate/high-school-cybersecurity-curriculum-guidelines.html	9-12	Free (registration required)	• Curriculum Guidelines • Reading Material • Events

NCYTE https://www.ncyte.net/resources/cybersecurity-curriculum	9-12	Free (membership required)	• Cyber Curriculum • Lessons / Modules • Faculty Development
NICCS https://niccs.cisa.gov/formal-education/integrating-cybersecurity-classroom	K-12	Free	• Curricula • Professional Dev • Programs • Student Resources
Teach Cyber https://teachcyber.org	9-12	• Free • Pay (workshops)	• Cyber Curricula • Sample Lessons • Workshops • Course Material

Table 2: List of Cybersecurity Curriculum Resources

Competitions

Cybersecurity competitions are a fun and practical way for students interested in cybersecurity to increase their skills in realistic situations. Competitions include students using security and administrative tools to fight threats and solve challenges within a specific time limit. Students may also gain experience working on a team during competitions and are exposed to ethics and policy practices. There is a wide variety of cybersecurity competitions, including competitions focused on areas like hacking, solving puzzles, attacking or defending a system, secure coding, forensics, and cryptography, just to name a few. Some competitions allow individuals to participate or require a team, and some recent events allow remote participation.

Most competitions start at the middle school level, with very few at the K-5 levels. Participating in cybersecurity competitions is a significant opportunity for students to network and improve their cybersecurity technical and non-technical skills. Competitions often include participation from leading cybersecurity experts and can lead to future scholarship opportunities or internships and job possibilities. Table 3 contains several cybersecurity competitions for the K-12 levels. Please note that most have at least annual competitions, and all will require registration. The registration dates indicated are historical, so it is important to verify the actual dates on the respective websites.

Resource	Historical Registration Date (Online or Onsite)	Free/Pay	K-12 Levels
CyberPatriot www.uscyberpatriot.org/competition/Competition-Overview/competition-overview	• Registration opens early April • Online competition except for onsite Finals	Teams $165-205 (See site for fee waivers)	6-12

Cyberstart America: National Cyber Scholarship Competition https://www.cyberstartamerica.org/	• Registration opens late October • Online competition	Free	9-12
eCYBERMISSION https://www.ecybermission.com/	• Registration opens mid-August • Online competition	Free	6-9
High School Capture the Flag (HSCTF) https://hsctf.com/	• Held in mid-June • Online competition	Free	6-12
National Cyber League (NCL) https://nationalcyberleague.org/	• Registration opens late January • Online competition	$35	9-12 (Age 13+)
NDIA: SoCal Cyber Cup https://www.ndia-sd.org/ndiasdevents/socal-cyber-cup-challenge/	• Registration opens mid-January • Online competition	Free	6-12
picoCTF 2021 Competition https://picoctf.org/	• Registration opens early February • Online competition	Free	6-12 (Age 13+)
US Cyber Challenge: Cyber Quests https://www.uscyberchallenge.org/	• Registration and quiz open late February • Online challenges	Free	9-12

Table 3: List of Cybersecurity Competitions

CyberCamps

Developing students' interest in cybersecurity at the K-12 level can be a challenge if they have very little experience in the field. CyberCamps, sometimes referred to as Cyber Boot Camps, are camps that provide an exciting way to explore cybersecurity and learn fundamental technical and non-technical skills. In addition, exposure to cybersecurity in camps could affect a student's future choice of higher learning majors or even future careers (Hernandez et al., 2020).

CyberCamps are usually hosted annually by a variety of organizations at many locations across the United States or held virtually. Locations and dates may vary from year to year, so it is important to check the website of a favorite cybercamp periodically. Registration and cost per student, if applicable, will vary depending on the individual cybercamp being offered. Table 4 contains several popular cybercamps for the K-12 levels, though there are too many to list. Also, a great place to search would be a local university or college. Please note that the dates indicated are historical.

Resource	Locations/Dates (Online or Onsite)	Free / Pay	K-12 Levels
Cyber.Org https://cyber.org/events	Varies for camps, bootcamps, workshops, and conferences	Free	• 9-12 • Teachers
CyberPatriot https://www.uscyberpatriot.org/afa-cybercamps/attend-a-camp	A list of locations and dates posted in the first week of May	Varies	6-12
GenCyber Camps https://www.gen-cyber.com/camps/	• Online • Onsite	Free	• 8-12 • Teachers
Khan Academy Kids https://khankids.zendesk.com/hc/en-us/articles/360060247272-2021-Launch-summer-learning-with-Camp-Khan-Kids	• Throughout July • Online	Free	K-2
USCC Cyber Summer Camp https://www.uscyberchallenge.org/cyber-camps	• Must participate in Cyber Quests Spring or Fall to be eligible for that Cyber Camps • Online camps	$185	9-12

Table 4: List of Popular CyberCamps

Labs/Gamification

Hands-on cybersecurity labs provide students with real-world training in a safe learning environment. Labs can motivate students to learn and help build confidence, which could keep students interested in cybersecurity. Even though the benefits of hands-on labs could enhance student learning, lab environments are frequently proprietary, involve specific software, and may require registration, often at a cost (Simpson et al., 2019). In addition, most labs only address the high school level in their K-12 offerings.

Gamification has become increasingly widespread to reach lower K-12 levels. When educators introduce gamification to course material, a student's retention of the topic increases (Krause et al., 2015). While there is still a long way to go with free K-12 gamification availability, there are some current resources educators can take advantage of immediately. Table 5 provides a few cybersecurity labs and gaming resources, which include free labs for the K-12 levels.

To reach a wider community, Immersive Labs created the Neurodivergent Digital Cyber Academy. This academy provides a platform so the neurodivergent community can develop the skills for a career as a cybersecurity professional.

Resource	K-12 Levels	Free/Pay	Lab Topics
Blue Team Labs https://blueteamlabs.online	9-12	Free / Pay	• Incident response • Security Operations • Reverse Engineering
Center for Infrastructure Assurance and Security (CIAS): Culture of Cybersecurity https://www.cultureofcybersecurity.com/kids/kids-activities/	K - 12	Free / Pay	• Activity Sheets • Educational Card Games • Electronic Games
Clark Center https://clark.center/home	9 - 12	Free	• Python Controls • Scripting Basics • Data
CyberStart America https://www.cyberstartamerica.org/	9 – 12 (Age 13+)	Free (Registration required)	• Cryptography • Social Engineering • Linux • Reverse Engineering
Immersive Labs Neurodivergent Digital Cyber Academy https://ndca.immersivelabs.online/register	9-12	Free (Registration required)	Core cybersecurity skills
INTERLAND https://beinternetawesome.withgoogle.com/en_us/interland	2 - 6	Free	Teaches fundamentals of digital citizenship and safety
Nova Labs https://www.pbs.org/wgbh/nova/labs/lab/cyber	6 - 12	Free / Pay (Registration required)	• Crack passwords • Craft Code • Defeat Malicious Hackers
TryHackMe https://tryhackme.com/ Note: Includes “hacking” labs	9-12	Free / Pay	• Cyber basics • Linux • Windows

Table 5: List of Cybersecurity Lab and Gaming Resources

CONCLUSION

Many resources could be used to guide successful K-12 cybersecurity education. Since these are the cybersecurity professionals of the future, educators need to be aware of as many opportunities as possible to prepare them. The intention is to prepare skilled and ethical cybersecurity students at the earliest level to meet the demands of higher-level STEM programs. However, the industry is continually changing, and with a plethora of resources that are constantly being updated, it was the goal of this article to provide a starting point with as many educational resources in one location as possible. This was not intended to be an exhaustive list.

REFERENCES

Blanken-Webb, J., Palmer, I., Deshaies, S.-E., Burbules, N. C., Campbell, R. H., & Bashir, M. (2018). A case study-based cybersecurity ethics curriculum. In *2018 Workshop on Advances in Security Education (ASE 18).* https://www.usenix.org/system/files/conference/ase18/ase18-paper_blanken-webb.pdf

Chase, J., Uppuluri, P., Denny, E., Patterson, B., Eller, J., Lane, D., ... & Onuskanich, R. (2020, July). STEAM Powered K-12 Cybersecurity Education. In Journal of The Colloquium for Information Systems Security Education (Vol. 7, No. 1, pp. 8-8). https://cisse.info/journal/index.php/cisse/issue/view/12

Christen, M., Gordijn, B., & Loi, M. (2020). The Ethics of Cybersecurity (p. 384). Springer Nature. https://library.oapen.org/bitstream/handle/20.500.12657/22489/1007696.pdf?sequence=1

Hernandez, J., Qu, X., Yuan, X., & Xu, J. (2020). Engaging Middle and High School Students in Cybersecurity through Summer Camps. In *2020 ASEE Southeastern Annual Section Conference*. https://sites.asee.org/se/wp-content/uploads/sites/56/2021/01/2020ASEESE8.pdf

Hachey, A.C. (2020). Success for all: fostering early childhood STEM identity, *Journal of Research in Innovative Teaching & Learning*, 13(1), 135-139. https://doi.org/10.1108/JRIT-01-2020-0001

Krause, M., Mogalle, M., Pohl, H., & Williams, J. (2015, March). A playful game changer: Fostering student retention in online education with social gamification. In Proceedings of the Second (2015) ACM Conference on Learning @ Scale (L@S '15) (pp. 95–102). Association for Computing Machinery. https://doi.org/10.1145/2724660.2724665

Macnish, K., & van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in Society*, 63, 101382. https://www.sciencedirect.com/science/article/pii/S0160791X19306840

Manjikian, M. (2017). *Cybersecurity ethics: an introduction*. Routledge.

Martin, C. D. (2017). Taking the High Road White hat, black hat: The ethics of cybersecurity. *ACM Inroads*, 8(1), 33–35. https://cs.utm.utoronto.ca/~zingarod/inroads317.pdf#page=35

Simpson, C., El-Gayar, O., & Bishop, D. (2019). Automated Deployment of Cybersecurity Labs in Cloud Computing Environments. In *2019 25th Americas Conference on Information Systems* https://scholar.dsu.edu/cgi/viewcontent.cgi?article=1064&context=bispapers

Tsado, L. (2019). Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach. *Journal of Cybersecurity Education, Research and Practice*, 2019(1), 4. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1050&context=jcerp