Education, Policies, and Cybersecurity: Explaining the Complicated World of Cyberspace to Newcomers and the General Public

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Jason Lee

November 3, 2023

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Prof. Pedro Augusto P. Francisco, Department of Engineering and Society

Introduction

Congressional lawmakers have shown us time and time again that their level of internet literacy is low to nearly non-existent. Whether it is discussing how Facebook makes money off of its website (Put Congressional hearing here) or passing laws that make encryption of data illegal (More sources here), members of Congress are not well educated in the medium of technology. This becomes an issue when dealing with cybersecurity, especially if it comes to sensitive information or even a national election. Computer literacy (the ability to use computers effectively) is usually learned through one of two methods: informally (at home) and formally, in a classroom setting (Hoffman, p. 222). However, formal education is shown to only accompany skills related to their work, which could be as simple as creating presentations or as complex as creating a web page (with the latter being a much rarer occasion). Informal education addresses everything that a person would be interested in doing on the internet (such as using social media, running and maintaining a website, or using complex computer programs for creative endeavors). In order to protect the public and keep cybersecurity awareness high, we need one of two approaches: getting better formal education that addresses important cybersecurity topics, or increasing the amount of resources and interest in cybersecurity in order to increase people informally educating themselves. Since the latter is more difficult to maintain a standard, this paper will address the first approach.

Currently, formal cybersecurity education and training is only given to those who have to work with sensitive data, or those who are very deeply ingrained in the field of computer science. Computer science education (for most schools) is put to the side as a possible elective, rather than a subject of study unlike many others that came before it. The problem is that cybersecurity is a multidisciplinary subject that must be explored in order to fully grasp and understand what is happening (Use that one citation). In a world where technology is growing at a rapid pace, with aritifical intelligence speeding up its course, falling behind on being educated in this field slows down innovation and ultimately leaves us vulnerable.

In our currently digital world, whether many of our everyday items have an internet connection, having a baseline knowledge of computer science and awareness of common threats can reduce the risk of massive data breaches, widespread damage from nation-state attacks, and other costly cybercrimes.

Learning how to formally and effectively educate the masses on cybersecurity is a massive first step in getting to the next step in research and development. We have effective methods and policies written out by the NIST and other reputable sources for workplace network safety, but we don't have standards of education nor policies to keep the general internet safe from cybercriminals (NIST article). To keep society safer, we must be able to explain simple and complex computer science concepts in an easy-to-understand format, and develop a cybersecurity standard or policy that can keep the general populace safe on the internet.

My research question is: Why it is so difficult to educate the public on topics of both internet and network security? This report will address the technical aspects of Cybersecurity and Cybersecurity Policies, and the STS topic of Public Education on Cybersecurity Literacy.

Cybersecurity and Cybersecurity Policies and Education

In our growingly connected society, we've seen that, while the technologies and innovations that surrounds us grows, the most common methods of delivering malicious programs remains the same: spam, phishing, and malicious downloads (Jang-Jaccard and Nepal, 2014, p.976). Spam refers to unsolicited emails or messages sent anonymously to users. Phishing refers to acquiring sensitive information, such as usernames, passwords, or other forms of authentication, by pretending to be a trusted party. All of these methods rely on some sort of psychological manipulation or social engineering, which, according to IBM, are attacks that manipulate people into making mistakes that “compromise their personal or organizational security” (IBM, n.d.). It has been observed that the best way to defend against any types of cyberattacks is to educate those who are at risk of these attacks with structured policies and procedures (Li et al., 2019). Teaching best practices for cybersecurity is the recommended way to ensure a more readily defended system, which means that comprehensive public cybersecurity education should mean that there would be a decrease in malware attacks throughout the country.

Since sweeping public education is more difficult to implement, I will focus on our university’s curriculum, particularly when it comes to cybersecurity education. BACS and BSCS have a significant difference in curriculum, but one particular point is concerning: Advanced Software Development, the first course where security in application design is first discussed, is not required for BA students. While Intro to Cybersecurity and other security related courses are available as electives, there exists the possibility that a UVA student will completely bypass all of these courses and go into the workplace being unaware of possible cyberthreats. In order to combat this possibility, and in order to make security a main focus for future UVA undergrads, I propose a change to the curriculum that includes a higher focus on safe practices and security-oriented design.

Two additional courses should be added to the curriculum. The first should focus on “The Internet of Things” and the prevention of attacks through smart devices (which are notorious for being weakpoints in any home security operation). Internet of Things (or IoT) refers to devices that can exchange data through a network, and this area of “Things” have expanded from smartphones to automobiles and fridges (Shafiq et. al, 2022). While it is convenient to have these devices connected and easily accessible, it is an additional source of data and sensitive information that could be stolen or even hijacked. Teaching safe design practices for devices that are not personal computer should be taught regardless of whether you are BA or BS. The second course should be offered to all students, regardless of major, and focus on social engineering and digital safety. By teaching each and every engineering student about the possibility of data breaches, it should foster a more security-focused student body and, consequentially, a defensively aware workforce. By addressing these two topics (and more), we can grow a better educated generation of workers and (hopefully) lawmakers.

The Issue with Teaching Cybersecurity

My research question is “Why is it so difficult to educate the general public and lawmakers about cybersecurity?” Congressional efforts to bolster our cybersecurity defenses have been lackluster, especially due to a lack of any catastrophic attacks on critical infrastructure (Murray, Zeadally, and Flowers, 2012). Since they lack the incentive to make positive changes for cybersecurity, government policies have been slow in catching up to the current state of information. However, according to Ferdinando (2016), “Change is needed to ensure better security for our networks, including starting with the most important factor: the human element.” Ferdinando discusses this in terms of culture, but I would like to address the difficulties within cybersecurity education in general, and why it’s different to many other subjects.

In order to discuss cybersecurity, you must go beyond simply looking at code, computer systems, and network systems. According to Hytönen, Trent , A., & Ruoslahti, “Cyber security awareness includes understanding computers, ethics, law, and public policy, which are very relevant to building and using intelligent systems" (2022). Due to the many different disciplines that must be addressed, simply educating people on how malware works is not sufficient. Along with the multidisciplinary knowledge, educators must have a baseline level of computer literacy, which requires either more expert in the field (hiring more CS faculty) or comprehensive training for other disciplines' professors instead (Rahman et al., 2020). Both of these options are costly, and difficult to justify in a short-term basis. Along with this, the difficulty lies within keeping these professors up to date on current threats and recent trends, as the field rapidly evolves in response to ground-breaking innovations (Crick et al., 2020).

Analysis will be done via meta-analysis of different cybersecurity policies and papers on the difficulties of teaching cybersecurity. By compiling these policies and papers on the issues behind training, I hope to reach a common consensus and a starting point to begin constructing a well-written, easy-to-digest curriculum.

Evidence that will be collected will pertain mostly to the shortcomings of teaching, the more complicated and difficult to explain portions of cybersecurity, and techniques to simplify teaching complex computer topics to a general audience. This evidence will mostly be in the form of research papers, standards and policies, and different cybersecurity curriculums from around the country. Analysis will be done to find what techniques are common in teaching novel concepts, such as analogies or applications to everyday life, as well as things to avoid when designing an effective educational policy.

Conclusion

To conclude, I will research the problems behind teaching cybersecurity to a general populace, and how we as a university could begin to tackle this problem before it reaches critical mass. To prevent the possibility of attacks on critical infrastructure, we must bolster and keep our policies current and relevant. To educate future lawmakers and the general public on the possibilities of a catastrophic attack, we must overcome the complications with comprehensive cybersecurity training. With my following paper and my technical report, I hope that the faculty takes my viewpoints to heart, and bring a generation of university alumni that are prepared to defend themselves in cyberspace.

References:

Alghamdi, M. I. (2021). Digital forensics in cyber security—recent trends, threats, and opportunities. Cybersecurity Threats with New Perspectives.

Crick T., Davenport J. H., Hanna P., Irons A. and Prickett T., "Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes," 2020 IEEE Frontiers in Education Conference (FIE), Uppsala, Sweden, 2020, pp. 1-9, doi: 10.1109/FIE44824.2020.9274033

Ferdinando, L. (2016). Cybersecurity: How Safe Are We As A Nation? (Doctoral dissertation, Georgetown University).

Hoffman, M., & Blake, J. (2003). Computer literacy: Today and tomorrow. *Journal of Computing Sciences in Colleges*, *18*(5), 221-233.

Hytönen, E., Trent , A., & Ruoslahti, H. (2022, June). Societal impacts of cyber security in academic literature. Research Gate. https://www.researchgate.net/publication/361218720_Societal_Impacts_of_Cyber_Security_in_Academic_Literature_-_Systematic_Literature_Review

IBM (n.d.). *What is Social Engineering?* https://www.ibm.com/topics/social-engineering

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior. International Journal of Information Management, 45, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Muhammad Shafiq, Zhaoquan Gu, Omar Cheikhrouhou, Wajdi Alhakami, Habib Hamam2, "The Rise of “Internet of Things”: Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks", *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 8669348, 12 pages, 2022. https://doi.org/10.1155/2022/8669348

Murray A., Zeadally S. and Flowers A., "An assessment of U.S. legislation on cybersecurity," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, Malaysia, 2012, pp. 289-294, doi: 10.1109/CyberSec.2012.6246106.

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), 378-382.