Aims / Introduction (What)

o What you aim/propose to do

o Frame the topic and explicitly link to worldviews

o Thesis statement that presents your project/ argument

• Significance / Background (Why)

o Build the case for why this is relevant

o Citations

o Explain to us why this is meaningful to you (and to others)

o Context

• Methods (How)

o Be specific!

o Explain how, when, where, and what you propose to do

o Details

How much cyber security knowledge do teenagers have today, and what is the best way to teach them what they lack through an educational website?

What missing critical pieces of cyber security knowledge can be provided to teenagers through an informational website?

I am researching how much cyber security knowledge teenagers have today because I want to find out what knowledge or skills they are lacking in order to create an educational website to teach them how to be safe online and follow safe security practices in their online lives.

Problem you can’t ignore, can’t stick your head in the sand

You can’t opt out of cyber in your life today, it is virtually impossible not to have a digital footprint, and as such you can be subject to cyber crime such as scams, identity fraud, and malware.

Outline

1. Introduction
   1. Unless one educates themselves or has access to education about cyber security, they will not know how to protect themselves and their data online.
2. Background
   1. My cyber security education has made me a better person and I enjoy teaching others about cyber security
3. Significance
   1. If teenagers today know how to act safely online, this practice will become more common throughout time and eventually become default practice
4. Methods
   1. Research, design, games, quizzes

Unless one educates themselves or has access to education about cyber security, they will not know how to protect themselves and their data online. The youth of today are well-versed in the technological age. However, they are not being explicitly taught proper cyber hygiene and are prone to fall victim to scams, identity fraud, and malware.

I propose making an educational website for teenagers to teach them the cyber security practices they lack. In today's technological age, one can only opt out of cyberspace if he decides to go off the grid and live without technology. Today, people rely on technology for almost every aspect of their lives: for work, school, and social life, connected via invisible threads of networks and applications. Therefore, nobody can afford to be lax in cyber security because it is crucial to today's world. However, cyber security practices are not being explicitly taught in most schools today. The youth in this digital age are well-versed in using technology but do not know proper security practices, so they fall victim to scams, identity fraud, and malware. Studies show that the teens' most missed cyber practices are recognizing phishing emails, password management, social media safety, and general security and privacy settings. i

The increased victimization of the "digital natives" is because they use the internet much more than the older generations. They use dating apps and shop online much more often than others, so by the frequency of use, they come across more scams than most other internet users. ii I am also part of Gen Z, but I have not fallen victim to a scam because I know what to look for and what could happen. Generation Z has not had the cyber security awakening that Gen Y did in 2015 when President Obama called cyberspace "the Wild West," pointing out the dangers of being online and the potential threats that lurk in websites and internet transactions. iii So, the younger generation does not feel unsafe online because they are unaware of the risks.

I understand how vital cyber security knowledge and the education of proper cyber security practices are. I enjoy volunteering at a cyber competition event every year that the Crimson Defense Cyber Security Club hosts for high schoolers, and it shows me how vital cyber security knowledge is to the younger generation because these teenagers will grow up to become functioning, contributing members of society. If younger generations learn proper online security practices, they will grow up knowing how to stay safe online and hand their knowledge to future generations. Cyber security education will become the default practice.

My research will help me create a website that teenagers would want to visit to learn about cyber security. Furthermore, it will help me find data on what specific categories of cyber security teenagers are missing so that I can focus on those crucial to protecting one's information online. Knowing that teens' lack of education comes primarily from a false sense of security online will help me create information that shows them what could happen. For example, I will have a trivia page on "what's the worst that could happen," showing them the consequences of clicking on suspicious links or what someone could do with their stolen identity. I want to create a comprehensive educational website to teach my users what could go wrong and how to identify potential scams online. I will accomplish this through an interactive game where they learn to identify a phishing scheme and know the key attributes to watch out for. I have also researched how teenagers prefer to consume information online and know they do not want to be overwhelmed by details because that would lose their interest. iv I am designing my website to teach them in small modules. I will have a few games where they learn password security, how to identify scams, and what information is safe to post online. I will also have quizzes where they test their overall cyber security knowledge, and at the end of the quiz, they can see what areas they could improve in and go to those sections to learn more. My website can be part of the foundation that creates the new wave of cyber security experts who will share their knowledge with those after them.

i Radhakrishnan, Satish & Rajendran, Lavanya. (2023). Information Security Practices and Intervention Among Teenagers. Journal of Computer Information Systems. 1-15. 10.1080/08874417.2023.2270453.

ii Ohlheiser, A.W. “Gen Z Falls for Online Scams More than Their Boomer Grandparents Do.” *Vox*, 21 Sept. 2023, www.vox.com/technology/23882304/gen-z-vs-boomers-scams-hacks. Accessed 01 Feb. 2024.

iii Debb, Scott M., et al. “A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults.” *International Journal of Cybersecurity Intelligence and Cybercrime*, 28 Feb. 2020, pp. 42–55, doi:10.52306/03010420gxuv5876.

iv Anthony S. Chow, et al. “Youth as Design Partners: Age-Appropriate Websites for Middle and High School Students.” *Journal of Educational Technology & Society*, vol. 15, no. 4, 2012, pp. 89–103. *JSTOR*, http://www.jstor.org/stable/jeductechsoci.15.4.89. Accessed 29 Jan. 2024.