Building an Educational Website Dedicated to Increasing Cybersecurity Awareness for All Ages

---

A Master's Thesis Project

Presented to the School of Arts & Sciences

State University of New York

Polytechnic Institute

Utica, NY

In Partial Fulfillment of the Requirements for the Master of Science degree

Elizabeth Hanselmann December 2022

SUNY POLYTECHNIC INSTITUTE

DEPARTMENT OF INFORMATION DESIGN AND TECHNOLOGY

CERTIFICATE OF APPROVAL

Approved and recommended for acceptance as a thesis in partial fulfillment of the requirements for the degree of Master of Science in Information Design and Technology.

_____

Date

_____

Dr. Kathryn Stam- Thesis Advisor

_____

Date

_____

Dr. Ryan Lizardi- Second Reader

Table of Contents

Abstract

As technology advances, so does the need for appropriate safety measures. When people are not given the proper tools and education to combat today's existing cyber threats, they leave themselves and others vulnerable. Antivirus software and other tools can help fight these cyber attacks, but the human firewall remains the strongest defense. Using a blog format as well as existing research, I have examined the pitfalls that tend to affect certain groups of people and created a resource to help educate them.

Description

A master's thesis project presented to the Department of Communications and Humanities, SUNY Polytechnic Institute, in partial fulfillment of the requirements for the degree of Master of Science in Information Design and Technology.

Introduction

This project exists as an in depth analysis on the different types of cyber attacks in existence today, and the trainings, awareness, and protective measures that are currently or need to be implemented. In these analyses I focused on younger generations' (Gen Z and Millenials) usage of the internet, specifically social media, and examine how their practices compare to those of older generations (Gen X and Baby Boomers). Given that younger generations have had arguably the greatest exposure to the internet and its resources, are they better-equipped to combat cyber attacks? Or are they more likely to be the victims of an attack because they tend to see the internet as a playground and have their guards lowered? People of all ages today have few qualms about sharing their personal information online (names, addresses, jobs, current locations, etc.); I addressed the narrative that younger people tend to be more "tech savvy", when these same young people are sharing their entire private lives on social media (TikTok, specifically) and risking more privacy and safety than they may initially realize.

My research objective was to use existing literature to first analyze the change in internet behavior across generations, if any. I examined the cause behind those behavior changes and determine if internet safety and cybersecurity are stronger or weaker based on their user base. In examining the effectiveness of cyber attacks, I used data from cybersecurity firms, as well as sources that have analyzed this information from a non-corporate lens.

My research questions included, but were not limited to, the following: How has internet usage changed as it becomes a more normal part of development? To what extent is internet safety taught in schools? Are older generations more wary or more trusting than their younger counterparts? To what extent has social media lowered people's guard? Are people more likely to share personal, private information online? Are they even more likely to do so if they believe that it will help them gain followers or fame?

This project took the form of a website (blog) accompanied by a written analysis. My anticipated goals were to shed light on the importance of internet safety and cybersecurity in an age where technology is rapidly improving and where hyper-vigilance is increasingly necessary. Using various resources on similar topics, I examined the generational differences in internet use regarding purpose and motivation, preconceived notions of the internet and surrounding safety, and the effectiveness of various cyber attacks on different age groups.

My expected results were that I would find different age groups equally at risk to cyber attacks, though in different ways. For example, older generations may fall prey to phishing attacks at higher rates, but younger generations are more likely to tie their identity to the internet and disregard any necessary boundaries for their privacy. The obstacles that I expected to run into were primarily a lack of existing research and literature on this topic.

Literature Review

As I plan to focus my research on the current practices of social media and how they relate to cybersecurity, I will be referencing a variety of sources. The sources that I have found and collected for this project each focus on a different central theme of my overall project. The four main themes include: Cybersecurity Practices, Generational Variances in Technology Usage, Adolescent Habits Regarding Internet Usage, and Security Practices and Issues Regarding Social Media. I will use the cited sources to investigate the cybersecurity practices of different generations as they use social media. Are certain age groups more wary of what they post online? Are younger social media users better equipped to deal with the threats they face online, or have they become more trusting and complacent because they have grown up in a more technology-filled world?

The majority of these sources (and others of similar background and relevance) still acknowledge the unknowns of the internet. Because this is still such a new phenomenon, particularly the spike of social media usage during the Covid-19 pandemic that skyrocketed an already high use of the platforms, there are many unanswered questions. What are the long-term effects of prolonged exposure? How do we protect people who see the internet as a safe haven rather than recognize the inherent dangers?

The sources I have examined study people of various generations and their respective internet habits, how those generational habits differ, and ongoing cybersecurity issues as well as effective practices against them. The collective research

concludes that while each generation is as equally susceptible to online attacks as the next, these attacks and vulnerabilities vary in the forms they take. While the research points to similar weaknesses among users, unanswered questions remain regarding the influence that constant, lifelong exposure to the internet has on a person. This refers to the influence as a whole, but with specific regard to this project, how the influence affects a users' cybersecurity liability.

Cybersecurity practices

KnowBe4 is a cybersecurity firm that provides its clients with the latest news in cybersecurity, internet safety training, and a wide range of knowledge base articles regarding internet safety. Using this as a resource, I will establish a standard of cyber hygiene and safety best practices, as well as common threats in an online environment (e.g. phishing, spear phishing, and social engineering).

Though its targeted audience is primarily businesses and their employees, KnowBe4 is a platform for all parties to learn how to better protect themselves in the digital age. With a wide variety of free resources, KnowBe4 stays up-to-date on current threats, security practices, and end-user weaknesses, particularly when it comes to social engineering, or "the art of manipulating, influencing, or deceiving you in order to gain control over your computer system." As a baseline resource, KnowBe4 provides a broad scope of information on cybersecurity, while other sources in this paper focus on more particular areas of interest.

Generation Variances in Technology Usage

These sources place more focus on the generational differences in technology use. I will use these to highlight the existing generational divide in technology and examine any existing cybersecurity risks.

Calvo-Porral and Pesqueira-Sanchez focus on different generations' technology usage, including what their respective usage looks like, and the motivators behind them. Specifically targeting Generation X and Millennials, Calvo-Porral and Pesqueira-Sanchez found that there are indeed notable differences between the two. Generation X's and Baby Boomers' technology usage tends towards the practical, placing more importance on things such as finding information, banking, and simple communication. Younger generations' usage, however, beginning with millennials, but more prominent among Gen Z, focuses more on technology for entertainment and for "hedonic" purposes (TikTok, Instagram, and BeReal are examples).

"Generational differences in online safety perceptions, knowledge, and practices" continues the topic of generational differences in technology use, but steers its focus towards cybersecurity. Specifically, it addresses how different generations (Silent and GI generation (SGI), Baby Boomers, and Millennials) differ in their views on online safety. While all groups have some level of wariness when it comes to cyber safety, this paper found that older age groups have less faith and trust in technology, including security

resources. As such, they take fewer precautions when navigating the online world, putting themselves in more danger due to their wariness. Even with these results, the paper concludes that online safety training is still necessary for each generation that was studied.

"Revisiting the Digital Divide: Generational Differences in Technology Use in Everyday Life" also places its main focus on the generational differences in technology usage, also concluding that older generations tend to be less comfortable using technology. More differences were found as age gaps became more significant. The paper concluded that younger age groups are more likely to feel uncomfortable without their phones, and are less likely to be frustrated by technology. "Many groups, from condominium associations to religious congregations and other non-profit organizations, have transitioned to primarily using electronic communication, thus it is important to understand that the oldest adults in the group may be less likely to be included in this type of exchange." Furthermore, as technology advances, older groups of people are more likely to be left behind if they are unable to adapt.

Adolescent Habits Regarding Internet Usage

These sources highlight social media habits for teens specifically, while examining privacy and addiction issues. These papers focus more on data privacy, and I used these to take a closer look at how these habits affect cybersecurity practices.

One of the biggest concerns about TikTok, a popular social media platform, is the privacy of the children who use it. TikTok is incredibly popular with tweens, teens, and young adults, but how safe is it? De Leyn, De Wolf, Vanden Abeele, and De Marez interviewed tweens and their parents to gain an understanding of their perceptions of privacy and how the platform is used. The study concluded that while tweens were aware that a sense of privacy protection was necessary, their concerns were more so focused on their activity being exposed to friends and classmates. A more tangible exposure was the biggest concern for these tweens, rather than an unknown threat such as phishing or another kind of scam.

"Fear of Missing Out as a Predictor of Problematic Social Media Use and Phubbing Behavior among Flemish Adolescents" discusses Fear-Of-Missing-Out, or FOMO, as it relates to addictive behaviors online. FOMO refers to the anxiety that something interesting or fulfilling may be happening elsewhere. This is often prompted by seeing others' posts on social media. This study argues that social media also seems to help with this anxiety: "One way of satisfying these needs… is through the use of social media applications, because the dynamic nature of social media applications provides users with a consistent stream of social and informational rewards." Social media may offer a quick relief to FOMO. More likely, however, it exacerbates the anxiety, provides a seeming relief, and prodding the anxiety again, keeping users in an unending cycle.

Continuing the trend of examining online privacy and technology addiction, Meral explores the data privacy issues of TikTok, while also looking at the addiction issues that come with the application. “TikTok application, the fastest-rising short video-sharing website, is examined. As a result of the literature review, it is observed that TikTok application also had ethical violations issues like lack of private data safety, not sufficient precautionary system barriers for the young generation, and addiction risk.” As seen in previously-referenced papers, social media is incredibly effective when it comes to grabbing users’ attention and keeping them coming back to the platform. These addictive patterns, combined with apparent data privacy issues, make the need for cybersecurity education for all ages an increasingly important topic.

Security Practices and Issues Regarding Social Media

These articles highlight data privacy and security practices as they relate to social media, specifically with adolescents. I will use these sources to examine how social media handles security concerns, not including the users’ own practices. Regardless of how a user conducts themselves on social media (using their real name, sharing personal information, etc.), how safe is any shared information in the first place? What are the best practices to take to further ensure online safety?

“On Privacy and Security in Social Media – A Comprehensive Study. Procedia Computer Science” focuses on data mining, or “the process of finding anomalies, patterns and correlations within large data sets to predict outcomes.” Data mining is

often used by large sites to gather data on their users. The gathered data can be used to target advertisements, and even to influence users to adjust their behavior a certain way. “It has been observed that privacy concerns are very feeble in the social networking sites and the users' endeavors to make the appropriate changes on their social media privacy is substantially lower than other mode of security operations.”

Al-Turjman and Deebak discuss the various types of cyber attacks, specifically relating to social networks. They focus on the targets, the reasoning behind selecting those targets, and the methods for attacking them. Dividing social networking sites into two parts, the users and the site itself, Al-Turjman and Deebak examine attacks, weaknesses, and countermeasures for these attacks, providing suggestions and outlines for security practices.

“Reframing Current Debates on Young People's Online Privacy by Taking into Account the Cultural Construction of Youth” works to debunk the myth that younger people (Millennials, Gen Z) are cavalier about their online privacy and protection. “Recent scholarly work, however, debunked the myth that teenagers do not value privacy anymore by uncovering how they manage sensitive information in their everyday life.” However, even if younger people are aware that they should be protecting their privacy, other research (such as De Leyn, T., De Wolf, R., Vanden Abeele, M., & De Marez, L. (2022)) shows that they may not have a large enough scope of how their information can be compromised.

Methods

With this project, I plan to examine and compare the social media and cybersecurity habits of Gen Z, Millennials, and Gen X to determine any differences in the generations' approaches to technology use. Using Wix as a website builder and using KnowBe4 as a cybersecurity resource, I will build a website that acts as an informational resource, addressing the specified generations and any gaps in internet safety that seem to be trending with the respective groups.

I plan on answering my project and research questions through researching and analyzing existing literature. I will use KnowBe4, a cybersecurity firm, to establish existing threats and best practices for cybersecurity. Using existing sources regarding users' social media habits (ex. Calvo-Porral, C. and Pesqueira-Sanchez, R., Mengtian Jiang, Hsin-yi Sandy Tsai, Shelia R. Cotten, Nora J. Rifon, Robert LaRose & Saleem Alhabash, Volkom, M.V., Stapley, J.C., & Amaturo, V.), I will analyze how these users approach cybersecurity and address any potential gaps in safety in the website I design. Using existing sources on security issues as they specifically relate to social media (ex. K, S., K, D. & N, S., Al-Turjman, F., & Deebak, B. D., Tom De Leyn, Ralf De Wolf, Mariek Vanden Abeele, and Lieven De Marez), I will address common threats and instruct users on ways to defend against them.

This blog will be created using the website designer, Wix, creating separate pages and sections focusing on prominent cyber threats today, as well as ways to combat them. This site will include information on common traps and pitfalls online, how

users of varying age groups are targeted, and will provide direction on navigating today's online world safely.

Project Outcomes

From the sources I have cited, there is a consensus in the varying uses of social media among different generations, especially as it relates to cybersecurity. KnowBe4 states, “Younger and older people differ in their susceptibility to different types of social engineering attacks, according to researchers at Avast (a cyber security firm). Younger people tend to fall for scams distributed through social media apps, while older people are more likely to fall for banking and tech support scams.” While no generation is more or less susceptible to cyber attacks than any other, the forms these attacks take differ greatly depending on the target. I myself can confirm from work in IT, specializing in cybersecurity, that there are victims of every age. The attacks are adjusted to target the user’s main use of technology; for younger generations the attacks would likely be via social media, while older generations may be attacked with “urgent” phishing emails regarding their bank account. Conclusions from my other cited sources (Calvo-Porral, C. et al., Mengtian Jiang et al., Volkom, M.V. et al.) have concluded the same regarding Gen Z vs. Millennial vs. Gen X vs. Baby Boomer technology habits and their respective security susceptibilities. Further sources (De Leyn, T. et al. (2022), Franchina, V. et al., Meral, K. Z., K, S., K, D. & N, S., Al-Turjman, F. et al., De Leyn, T. et al. (2019)) expand on these topics, specifically regarding younger generations’ (Gen Z and Millenials) technology habits and internet privacy.

Given the research and conclusions presented in these sources, I am more precisely able to address these generations in my final website project. Sections of the

website will explore and explain both common threats for specific generations, as well as ways to raise awareness and combat those threats.

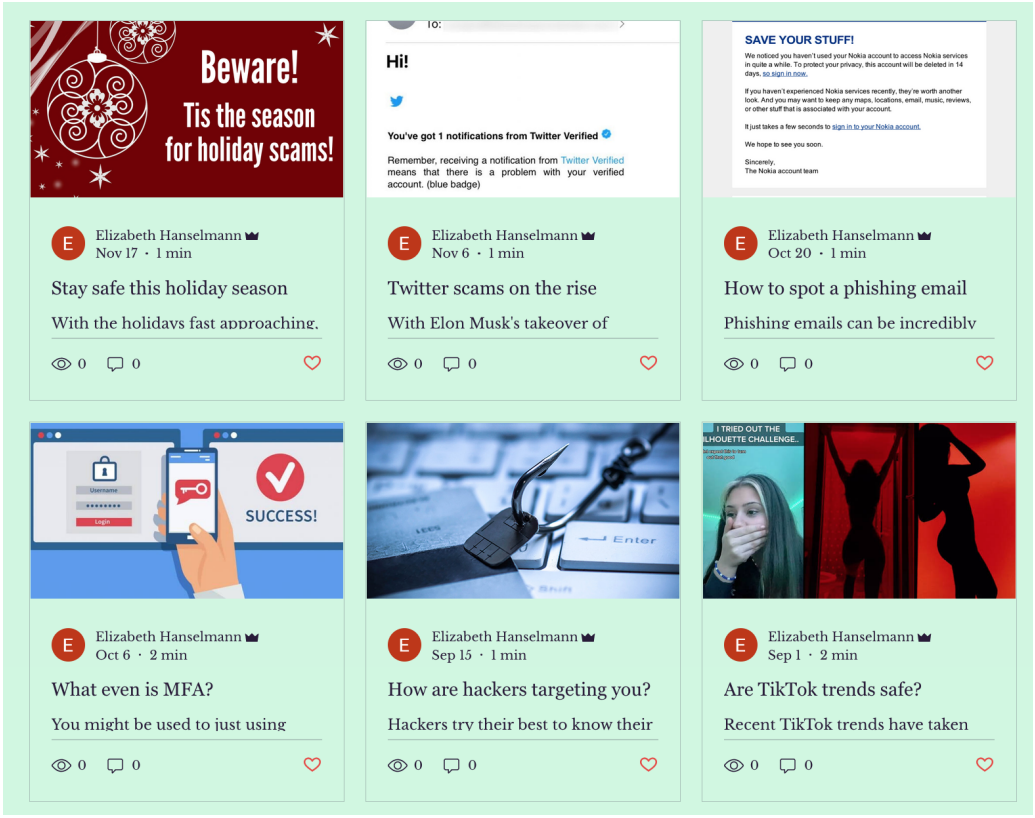
Discussion

There are numerous resources that discuss cybersecurity and online safety (KnowBe4, Sophos, Avast, etc.), but these resources are more often than not trying to sell a product or market their content to businesses. With my project specifically, I wanted to create an accessible resource for all users, especially those who are not given workplace-mandated training.

As technology continues to advance, the hope remains that sites and resources like mine will become more common, and that people will more readily equip themselves with the tools to navigate the internet safely.

Final Project

https://emhanselmann.wixsite.com/my-site



Conclusions and Future Outlook

Research shows that there is no one group or generation that is more susceptible to cyber attacks (phishing, spear phishing, social engineering, etc.) than any other. However, research also shows that these attacks differ in that they are specifically tailored as they target each group. Further research would logically trend as different generations' technology usages change, making note of the most common habits so as to prepare people for further cyber attacks as the attacks themselves evolve. As technology is always evolving, so will the attacks and pitfalls, and so must the research.

Additional areas of study might focus on the long-term effects technology has on the generations that grow up submerged in it specifically as it relates to online privacy. As we are only now able to see these effects as children grow up, what different behaviors are we seeing, if any, as they relate to the concept of privacy and security on the internet?

References

www.KnowBe4.com

Al-Turjman, F., & Deebak, B. D. (2021). Security in Iot social networks. Academic Press, an imprint of Elsevier. https://www.sciencedirect.com/book/9780128215999/security-in-iot-social-networks

Calvo-Porral, C. and Pesqueira-Sanchez, R. (2020), "Generational differences in technology behaviour: comparing millennials and Generation X", Kybernetes, Vol. 49 No. 11, pp. 2755-2772. https://www.researchgate.net/publication/337471708_Generational_differences_in_technology_behaviour_Comparing_Millennials_and_Generation_X#:~:text=Research%20findings%20indicate%20that%20Millennials,utilitarian%20purposes%20and%20information%20search.

De Leyn, T., De Wolf, R., Vanden Abeele, M., & De Marez, L. (2022). In-between child's play and teenage pop culture : tweens, TikTok & privacy. JOURNAL OF YOUTH STUDIES. https://doi.org/10.1080/13676261.2021.1939286 https://www.researchgate.net/publication/352304026_In-between_child's_play_and_teenage_pop_culture_tweens_TikTok_privacy

De Leyn, T., De Wolf, R., Vanden Abeele, M., & De Marez, L. 2019. Reframing Current Debates on Young People's Online Privacy by Taking into Account the Cultural Construction of Youth. In Proceedings of the 10th International Conference on Social Media and Society (SMSociety '19). Association for Computing Machinery, New York, NY, USA, 174–183.

https://doi.org/10.1145/3328529.3328558

https://dl.acm.org/doi/10.1145/3328529.3328558

Franchina, V., Vanden Abeele, M., van Rooij, A. J., Lo Coco, G., & De Marez, L. (2018). Fear of Missing Out as a Predictor of Problematic Social Media Use and Phubbing Behavior among Flemish Adolescents. International journal of environmental research and public health, 15(10), 2319. https://doi.org/10.3390/ijerph15102319

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6211134/

K, S., K, D. & N, S. (2016). On Privacy and Security in Social Media – A Comprehensive Study. Procedia Computer Science, 78:114–119. doi: 10.1016/j.procs.2016.02.019

https://www.sciencedirect.com/science/article/pii/S1877050916000211

Mengtian Jiang, Hsin-yi Sandy Tsai, Shelia R. Cotten, Nora J. Rifon, Robert LaRose & Saleem Alhabash (2016) Generational differences in online safety perceptions, knowledge, and practices, Educational Gerontology, 42:9, 621-634, DOI: 10.1080/03601277.2016.1205408

https://www.researchgate.net/publication/304573129_Generational_Differences_in_Online_Safety_Perceptions_Knowledge_and_Practices

Meral, K. Z. (2021). Social Media Short Video-Sharing TikTok Application and Ethics: Data Privacy and Addiction Issues. In M. Taskiran, & F. Pinarbaşi (Eds.), Multidisciplinary Approaches to Ethics in the Digital Era (pp. 147-165). IGI Global. https://doi.org/10.4018/978-1-7998-4117-3.ch010

https://www.researchgate.net/publication/349911843_Social_Media_Short_Video

-Sharing_TikTok_Application_and_Ethics_Data_Privacy_and_Addiction_Issues/citations

Volkom, M.V., Stapley, J.C., & Amaturo, V. (2014). Revisiting the Digital Divide: Generational Differences in Technology Use in Everyday Life. North American Journal of Psychology, 16, 557. https://www.greeleyschools.org/cms/lib2/CO01001723/Centricity/Domain/2387/Revisiting%20the%20Digital%20Divide.pdf