Issues in Information Systems
Volume 26, Issue 2, pp. 267-280, 2025

DOI: https://doi.org/10.48009/2_iis_121

Facing your digital footprint on college campuses

Reese Martin, *Robert Morris University, reesegelstonmartin@gmail.com*
Sushma Mishra, *Robert Morris University, mishra@rmu.edu*

Abstract

As digital technology becomes increasingly integrated into daily life and organization operation, cybersecurity has now been a major concern. Despite the implementation of security policies, noncompliance by individuals remains a vulnerability. This research explores the role of post-security education in shaping students understanding of cybersecurity, with a particular focus on cybersecurity common practices and self-protection online. This study seeks to identify knowledge gaps among students and examines how a student's academic major may influence their comprehension of digital security practices.

Keywords: assessment of learning in IS, cybersecurity awareness, digital self-protection, curriculum development

Introduction

Organizations all over the world have been using technology to communicate and run the overall functions of daily operations. This area of new technology has benefited every organization by the productivity and collaboration that it provides. As this technology becomes more active in individuals' daily lives the importance of security and protection of information online becomes more apparent. Cell phones with internet access are nearly universal in the U.S., with 97% of Americans owning one. (Pew Research, 2024) Such access has allowed for the connection of oneself to the internet and to each other daily. Organizations in regard to internet usage have options for better protecting individuals such as security policies but many individuals do not comply with the specified behaviors. (Bada et al, 2019) These security measures are in place to better protect the organization from cyber-attacks. However, if the policies are too restrictive, it can cause individuals to want to bypass them. For example, if the hosting organization blocks a music streaming service or a social media application it can provide a reason to bypass the security for individuals to access it.

The gap in securing personal information online can largely be attributed to shortcomings in the education system, including a lack of emphasis on digital security in both secondary and post-secondary institutions. The focus of this paper will be on post-secondary education and the student body's understanding of cybersecurity concepts such as common practices (password, browsing, antivirus software, VPN) and self-protection (social media use, trust, privacy). By identifying where knowledge gaps exist, this research aims to support both students and educators in pinpointing areas where the education system can be improved. Strengthening digital security education at the university level will not only benefit individuals but also better prepare future professionals for the cybersecurity challenges they may face in the workforce. The central research question of this study is how does a student's academic major influence their understanding

of cybersecurity? This question will help uncover whether students in certain disciplines such as computer science are better equipped with cybersecurity knowledge compared to those students in other disciplines. This analysis will help to better understand what implications this has for the future of educational strategies.

Background

This section highlights the previous research and understanding of college students and cybersecurity. There are two sections involved with better understanding and protecting individuals on college campuses, those being cybersecurity basics and self-protection online. Overall, there are few studies that focus on the students attending universities and colleges while having a focus on their majors in relation to cybersecurity.

Cybersecurity Common Practices

The action of implementing a successful cybersecurity awareness program is more than just asking questions. The overall focus of a security awareness program is not to train students or individuals on the security concepts to protect themselves but rather to focus attention on security concerns and respond accordingly. (Bada et al, 2019) Overall, this creates a rift between the students expecting to learn about security online and the reality of cyber awareness programs. Items such as phishing attacks are targeting everyone through phone numbers and emails. This threat to universities and individuals is a major concern, especially with online coursework. Phishing and social engineering are not understood by students at universities with one study having only 30.8% of the participants of the study recognizing what phishing can do. While 69.2% do not recognize what phishing is. (Erendor, 2022) This can take away the protection of many students' accounts with single-factor authentication.

Password security because of the large number of accounts that one has to access passwords has become more commonly reused. Along with reused passwords, there is an increasing number of students who have simplistic words or identifiable information as their passwords to important web pages such as banks. Even when there is a breach of information and individuals are urged to change passwords, they sometimes keep it the same or change it to another password that is currently being used. (Alqahtani, 2022) These areas are important for the security of companies and individual protection such as password management.

The use of antivirus software on students' laptops are critical to protect projects, resumes, and other critical information to keep up with the demands of all the coursework. An assessment of the student body at Majmaah University revealed that over 30% of students have no antivirus software installed on their systems which would open the door for corruption and viruses. This belief is that there is no threat and that their passwords would secure the system. This concern allowed for the study to ask about firewalls as they are also a defense against viruses. The majority of this study did not understand what a firewall was or the action to turn it on and off. (Alharbi & Tassaddiq, 2021) The protection that firewalls and antivirus software provide should be critical to individuals' understanding of security on devices.

Self-Protection Online

Protecting oneself online has become more complex as technology develops. This is through the use of AI tools and the overall impact that it has been having on everyone’s daily lives. One example of this is within McAfee’s Cybersecurity Artificial Intelligence Report which focuses on the impact that AI voice cloning has on scamming people. In the report the United States has voice cloning happening to 14% of the individuals interviewed. Then 23% of individuals in the US are sharing their voice online more than twice a week. (Chole et al, 2023) This mass volume of oneself sharing one's voice online is what is enabling hackers to manipulate AI voice cloning. Another report by Norton LifeLock back in 2019 identified many

areas where individuals are experiencing cybercrime along with threats to privacy online. A shocking 69% of the American sample claimed that they accept certain risks to their online privacy to create a more convenient experience. There are also 4 out of 5 people who feel that regardless of what they do to protect themselves online that information is still getting to the companies and that they have lost control at protecting their information. (Norton LifeLock, 2020) All of these areas are creating a numbing effect on online security and the protection of one's information.

Another source that includes the overwhelming amount of information needed to protect oneself online is the Pew Research Center. They found that most Americans feel that regardless of what they do to protect themselves it does not make that much of a difference. Along with that 56% of the survey group frequently click agree without reading the content in privacy policies. (Mcclain, 2023) This can create a disconnect between focusing on training on the protection of data and online communication. The continued push for protection online is both in the professional and personal lives of every person that accesses the internet.

Methodology

This section includes the method of collecting data and identifying the findings. The method of choice will be a survey of students in various majors at Robert Morris University. Efforts will be made through communication in clubs and events to gain individual interest and response. Along with gathering information through clubs, the survey went out with an email explaining the importance and request for participation. The survey itself will consist of questions that will focus on four sections: demographic information, General Cybersecurity Awareness, Self-Protection Online, and end-of-survey questions. These four sections were designed to not only measure current knowledge but also provide insight into how students relate to their digital environments both personally and academically. Having demographic information and end-of-survey questions included in the survey will allow to better analyze the impact that cybersecurity is having on the student body here at Robert Morris University.

Data collection was conducted over the course of February 2025, with the survey officially closing at the end of the month. This timeline allowed for adequate distribution and participation across various student networks. The following section presents the sample of questions included in the survey that was sent to students:

Table 1. Sample Questions in Categories That Were Presented in the Study

Demographic Information	Cybersecurity Common Practices	Self-Protection Online
What is your age?	How familiar are you with common cybersecurity practices such as password management, safe browsing, or antivirus software?	Do you use any of the following to protect your online presence? (Select all that apply)
What is your gender?	How often do you update your passwords across different platforms?	When browsing online, do you check for signs of secure websites such as HTTPS or the lock symbol in your browser?
What level of study are you pursuing?	Do you know what a firewall is and how to access it through your device?	How often do you review your privacy settings on social media platforms?
What year are you currently?	How comfortable are you to connect to a public Wi-Fi network?	How confident are you that your privacy is secured when using social media platforms?
What is your field of study?	How aware are you of phishing attacks or other online scams?	

End of Survey Questions
How confident are you that your education or workplace training has effectively provided you with cybersecurity knowledge?
Is there anything else you would like to share about your understanding of technology or cybersecurity? (If nothing write N/A)

Once the survey results are collected, the data clean-up process will proceed as follows. First, the data will be organized into three sections: the baseline group (Computer & Information Systems majors), the test group (all other majors), and the overall group (all the majors together). This division of data will enable a clean analysis of each group's understanding of cybersecurity and self-protection online. Next, the questions will be categorized into four sections: demographics, cybersecurity common practices, self-protection online, and end-of-survey questions. This would allow the information to be segmented to better understand the results within each category. After analyzing the data through these divided sections breaking up the cybersecurity common practices and self-protection online responses across the different academic departments: School of Data Intelligence and Technology, Rockwell School of Business Data, School of Education and Social Sciences, School of Communication and Media, School of Engineering and Science, and School of Health Professions. This analysis will allow us to better understand how a student's academic major influences their understanding of cybersecurity.

Results

Upon completion of the month-long collection of data by reaching out to organizations here at Robert Morris University along with email solicitation the survey received 73 responses. Within the 73 survey responses, the baseline group consists of 19 respondents, and 54 respondents for the test group. The data was also organized by academic department to help better identify the overall understanding of cybersecurity in different academic groups. The academic departments are organized by the following: School of Data Intelligence and Technology, Rockwell School of Business Data, School of Education and Social Sciences, School of Communication and Media, School of Engineering and Science, and the School of Health Professions. The demographics of the participants were first included to better understand the type of information being examined.

The majority of respondents in the survey fall within the 21-24 age range across the two groups. This age range is particularly relevant as it aligns with the current year and educational level, helping better understand the older student population specifically. Additionally, most participants are seniors, with 36.8% in the baseline group and 44.4% in the test group identifying as seniors. The education level helps assess participants' understanding of the information. Both groups mostly identified undergraduate students, with 57.9% of the baseline group and 85.2% of the test group identifying as undergraduate students. Additionally, there is a significant difference in gender distribution between the two groups. The baseline group is predominantly male, with 78.9%, while the test group is predominantly female, with 63%. The gender distribution in cybersecurity and information technology majors reveals an imbalance between females and males. Promoting greater female participation should be a top priority, especially as the field of information security continues to evolve.

Cybersecurity Common Practices

The importance of cybersecurity in the modern workforce is underscored by the need to effectively protect business infrastructure from a range of potential cyber-attacks. With human factors often being the weakest link in both cybersecurity and network security it is crucial that individuals receive proper training on

cybersecurity before entering the workforce. (Negussie Tolossa, 2024) Analyzing the findings from this research will provide valuable insights into areas where improvements are needed to better secure business infrastructure. Also, by extension, safeguard the growing role that technology plays in everyone's daily lives. Cybersecurity threats can come from various attack vectors, making the need for understanding and recognizing these threats more critical than ever. Recognizing majors outside of cybersecurity at a university like Robert Morris and how they are learning about cybersecurity can better identify any gaps of information that should be better covered while in post-secondary education. The questions that individuals were asked involved cybersecurity practices focused on the security of password management, firewall accessibility, Wi-Fi connections, and attacks such as phishing towards an individual or company.

The first group of questions that was asked beyond the demographic information was some common cybersecurity practices which can see right away that there is a gap between the baseline and test group. Identifying areas of improvement is done through grouping responses in both the baseline and test groups. The overall response with cybersecurity concepts has the baseline group sitting at 94.7% of responses. This should make sense through the studies that involve proper password management and antivirus protection of devices. Among the test group the various school departments, excluding information technology and cybersecurity, the school of health professions had the least familiarity with common cybersecurity concepts, with 44.4% of participants reporting limited knowledge. Along with the least familiar, the most familiar excluding information technology and cybersecurity are the Rockwell School of Business Data, with 81.9% of participants reported to be familiar with common cybersecurity practices. This contrast highlights the varying levels of cybersecurity awareness across various academic disciplines.

Proper password management and updating passwords are needed to better protect the infrastructure that a network sits on. Having the method of password management and updating passwords can be frustrating to users as some believe there is no reason to change passwords. A survey conducted by USENIX found that while people can buy into security advice, they are sometimes unable or unwilling to go through with the protection of their passwords. (Habib et al, 2018) This understanding reflected in the baseline group as they update their passwords regularly at 57.9%. the academic department that had the most frequent password changes was the School of Engineering and Science at 27.3%. Along with the most frequent password changes, the school that rarely or never changed its passwords is the School of Health Professions with 88.9% of participants. These statistics are to be expected as a poll from Google found that around 44% of internet users rarely, if ever change their passwords. (Howarth, 2023) Some solutions to this issue could be to implement multi-factor authentication methods to have layered security within accounts. This method Robert Morris has adapted through having users that use the network to have multi-factor authentication enabled.

Accessing the basic functions of individual devices is crucial for better-protecting organizations, especially those providing company devices to employees. A key area of focus in cybersecurity education is ensuring that users understand and can effectively manage their devices' security features. For instance, understanding what a firewall is and how to access it can allow individuals to better secure their devices along with company devices. The understanding of the data collected highlights a critical gap in understanding. In the baseline group, 42.1% of participants were unsure of what a firewall is and how to access it on their devices. The test group that the highest academic scoring department out of them is the School of Communication and Media with 60% of participants understanding what a firewall is and how to access it. In comparison, the lowest school to understand firewall accessibility is the School of Health Professions with 77.7% disagreeing. Device security starts with the individual user. By promoting awareness of the various ways users can protect their own devices, organizations can have a stronger security posture.

Another important aspect of business operation is where the user is accessing business information. With the world of today having remote work employees can almost do their work from anywhere on the planet if they have a strong internet connection. Connecting to public Wi-Fi can be extremely dangerous because of the way that the information is presented across the network. It can be easily captured by individuals who want to steal or compromise information about organizations and users. Without any protection such as a VPN or ways to encrypt your data, it can be compromised. Within our survey, this concern was reflected in differing comfort levels among groups. In the baseline group, 31.6% of respondents indicated that they were somewhat comfortable connecting to a public network. This compared to the test group the academic departments revealed varying levels of awareness or caution. The School of Engineering and Science had the highest percentage of respondents who were not comfortable connecting to a public network at 54.6%. This is possibly an indicator of a stronger understanding of cybersecurity risks. On the other hand, the highest levels of comfort were observed in the School of Communication & Media and the School of Education and Social Sciences, where 60% of respondents each reported feeling comfortable using public networks. Given these trends, increasing awareness of dangers associated with public network connections is essential for proper information security.

Finally, the last question that was asked regarding common practices within cybersecurity was that of phishing attacks and other online scams. Living in the 21st century the rise of online transactions has grown exponentially and continues to increase bringing both convenience and new risks. This growth has created more opportunities for cybercriminals to exploit users, particularly through methods such as phishing or other online scams. In a study comparing the analysis of phishing they described it as one of the most frequent examples of fraud that is found on the internet. (Alkhalil, 2021) These scams have a focus on deceptive communication to the individual trying to reveal sensitive information. The baseline group had an astounding 94.8% of participants cautious about and can identify phishing attacks. The high understanding of phishing attacks is also represented in the test group. Including academic departments and their understanding of phishing attacks has a positive result for multiple departments. Two departments scored 100% with them being the School of Communication and Media & School of Education and Social Sciences. These results indicate a strong level of cybersecurity awareness within these departments regarding phishing and online scams that are present. In contrast, the school with the least amount of understanding of phishing attacks is the School of Health Professions with 11.1% not aware at all. This raises concerns about potential vulnerabilities within the teaching and highlights the need for targeted cybersecurity awareness initiatives to ensure all students are equipped to recognize and respond to online threats.

Self-Protection Online

Shifting the focus to protecting oneself online can benefit organizations as better self-protection practices should relate to better information security. The digital age can provide many conveniences but in turn, provide a higher understanding of security and technology to properly protect oneself online from the dangers that are there. Applying their understanding of cybersecurity concepts, individuals were asked a series of questions that related to the protection practices that they do online. This includes identifying various cybersecurity countermeasures, implementing proper browser protection, and understanding privacy features that social networking platforms have with user data.

The first question related to self-protection online was about the types of tools that individuals use to protect themselves. These tools include antivirus software, virtual private networks (VPN), strong passwords that have unique passwords for each account or have a password manager, multi-factor authentication (MFA), or none of the above. This question was to select all that apply so the best method of analyzing is by number rather than percentage. Something to also note is that every student at Robert Morris University has to by IT policy have MFA enabled on their accounts. So, the expectation is that MFA should have the number

identified being the same as the total number of participants. This is unfortunately not the case with both the baseline and test groups. The baseline group does have 100% of participants select MFA as something they use regarding protection online. In relation to the test group, 90.7% of participants selected that they use MFA. The hypothesis is that it is not the fault of the students but rather the understanding of what is an MFA and what it does to their accounts.

Browser security is another important layer of security online that one can use. Specifically making sure that the connection to the website is over port 443 or HTTPS allows for the communication to be encrypted. Without the protocol, the website operates over port 80 which does not encrypt traffic, which allows for interception of clear text. Without proper protection there are attacks such as man-in-the-middle, cross-site scripting, and session hijacking. (Satish & Chavan, 2017) The baseline group scored 79% of participants within frequently or always checking for signs of a secure connection to a website such as HTTPS. The test group describes the academic departments in the analysis of browser security and connectivity revealed some surprising results. The highest scoring group was the School of Health Professions with 66.6% of individuals reporting that they sometimes or always check for signs of secure websites connections such as HTTPS. This level of awareness contrasts sharply with the School of Engineering and Science where 45.5% of respondents reported that they rarely or never checked for secure connections. This significant difference highlights an interesting disconnect between general cybersecurity knowledge and the application of self-protection online. While the School of Engineering and Science showed a strong understanding of broader cybersecurity concepts, their understanding might be in the gap of everyday digital behavior. Addressing this disconnect would allow for more comprehensive cybersecurity awareness and application in daily activities.

Privacy on social media is an increasingly important concern, particularly with the growing number of people who are actively using these platforms. Social media are supposed to provide people with an area to connect across the globe, allowing individuals from all backgrounds and nationalities to connect and communicate in a shared digital space. Users that own social media accounts have been reported that 49% have accessed the application multiple times a day. (Auxier & Anderson, 2021) This highlights the critical need for strong security measures. When asked how often you review privacy settings on social media platforms, 57.9% of participants in the baseline group reported doing so regularly or very regularly. Among the various academic departments, the School of Engineering and Science scored the highest with a review of privacy settings on social media with 36.4%. The academic department that has the least activity on reviewing privacy settings is the School of Health Professions at 44.4%. This suggests that while some users are taking steps to protect their information through security measures on social media, there is still a substantial need for education and awareness around privacy awareness on social media.

In relation to social media, the goal was to gauge the overall confidence that social media is securing users' information online. This confidence level should be relatively low as anything that is posted on social media is out there forever to be located by cybercriminals. The baseline group expressed low confidence, with 57.9% of participants indicating this. In relation the test group by academic departments showed a concerning trend. The department with the highest percentage of students who do not trust their privacy on social media is the School of Communication and Media at 60%. This suggests that communication majors understand potential privacy risks on social media, as interacting with networks aligns with their field of study. Then in comparison, the lowest scoring department is the School of Education and Social Sciences with 40% having somewhat or very confident that their privacy is secured. This disparity could suggest that students in education and social sciences may not engage as critically with social media platforms as the mechanisms that run them.

End of Survey

Ending the survey, the participants were asked about the level of confidence they felt that their education or workplace training has provided them with cybersecurity knowledge. The baseline group claimed that 73.7% felt somewhat or very confident with their cybersecurity knowledge. The test group had a shocking response as the academic department that had the highest scoring was that of the School of Communication & Media at 80% of somewhat to very confident. This would be expected as they scored high on the other questions and both categories of the survey. The unexpected result was in the lowest scoring school as it was the School of Engineering & Science 36.4% felt not very or at all confident. As the highest scoring school overall was the School of Engineering & Science it is interesting that they were found to have the lowest confidence level.

Along with asking about the confidence level of the education system on cybersecurity knowledge participants were also asked the question of is there anything else you would like to share about your understanding of technology or cybersecurity? This resulted in the ability of the students to provide personal feedback on their overall understanding and knowledge of technology. Some responses are the following: "Never taught anything", "My natural laziness as a human being results in me not taking the appropriate steps to protect myself online", "I do not have a lot of knowledge about this but I think it would be very valuable to know", and "I am still in the process of learning more through an Intro to Cybersecurity class, but it's more or less basic outline and hearing stuff from cyber friends." These responses pose an interesting viewpoint as much of the knowledge that comes from securing one's information comes from wanting to understand how things work.

Discussion

Overall, the data highlights varying levels of cybersecurity awareness and education across different academic departments, indicating that students' understanding of these practices is influenced by their field of study. These levels show that some groups of majors have a stronger sense of these common practices that would overall benefit the companies that they are going to be working for. The highest scoring academic school for cybersecurity common practices is tied with the School of Engineering & Science and the School of Communication & Media. This represents the understanding and importance that cybersecurity has promoted within these schools. Engineering and communication students often engage with technology and digital platforms as part of their academic training, which may naturally lead to greater awareness and competency in online safety and data protection. Meanwhile, the lowest scoring academic school overall is the School of Health Professions. A possible explanation for this could be the demanding nature of the health professions curriculum particularly for nursing majors who are often balancing rigorous coursework with clinical responsibilities. The overall heavy and demanding workload associated with nursing may leave little room for additional subjects like cybersecurity, even if those topics are becoming more apparent in healthcare.

Meanwhile the impact of online activity daily allows cybercriminals the ability to create a profile and through OSINT attempt to break into organization systems. This method has allowed organizations to attempt to educate their employees more about online protection and the impact that can benefit them. Continuing to promote self-protection online should always be a top priority as today's world revolves around the use of the internet and social media. The result of the survey is that the School of Engineering & Science and the School of Communication & Media are the highest scoring schools. This directly reflects the common cybersecurity practices as they were also the highest scoring schools. The close relationship between technology, engineering, and communication disciplines demonstrates the positive impact of embedding cybersecurity education into academic programs. In relation, the lowest scoring school was the

School of Health Professions which also relates to the cybersecurity common practices. Overall scoring reflected the same in both categories of focus in the survey. This is closely aligned with the fact that outside of cybersecurity and information technology, there is not the same level of exposure or emphasis on digital security, ultimately affecting their understanding and application of best practices.

Cybersecurity Common Practices					
	How familiar are you with common cybersecurity practices such as password management, safe browsing, or antivirus software?	**How often do you update your passwords across different platforms?**	**Do you know what a firewall is and how to access it through your device?**	**How comfortable are you to connect to a public Wi-Fi network?**	**How aware are you of phishing attacks or other online scams?**
Highest Scoring School	Rockwell School of Business Data | 81.9%	School of Engineering and Science | 27.3%	School of Communication and Media | 60%	School of Engineering and Science | 54.6%	School of Communication and Media & School of Education and Social Sciences | 100%
Lowest Scoring School	School of Health Professions | 44.4%	School of Health Professions | 88.9%	School of Health Professions | 77.7%	School of Communication and Media & School of Education and Social Sciences | 60%	School of Health Professions | 11.1%

Self-Protection Online			
	When browsing online, do you check for signs of secure websites such as HTTPS or the lock symbol in your browser?	**How often do you review your privacy settings on social media platforms?**	**How confident are you that your privacy is secured when using social media platforms?**
Highest Scoring School	School of Health Professions | 66.6%	School of Engineering and Science | 36.4%	School of Communication and Media | 60%
Lowest Scoring School	School of Engineering and Science | 45.5%	School of Health Professions | 44.4%	School of Education and Social Sciences | 40%

End of Survey	
	How confident are you that your education or workplace training has effectively provided you with cybersecurity knowledge?
Highest Scoring School	School of Communication and Media | 80%
Lowest Scoring School	School of Engineering and Science | 36.4%

Table 2. Overall Results of the Highest and Lowest Scoring Schools

Students in college are focusing on many aspects of a critical time in their lives. Trying to become professionally and academically successful, joining clubs and extracurricular activities, working, if need be, and attempting to socialize can overwhelm most. With so much of a student's life spent online with digital platforms from submitting assignments to communicating with professors there is an increase in

online threats. Learning common cybersecurity skills and online protection can help the average student from being a victim of scams or threats. Increasing the general curriculum or opportunities for workshops relating to cybersecurity and online protection could help ensure that students are informed in the digital world they rely on daily.

Implications

As mentioned above, there are some limitations to this study, one of the main challenges being the number of responses collected. Overall, there were 73 responses, which included both the baseline and test groups. Breaking down the data into these respective groups showed that the baseline only had 19 responses and 54 in the test group. This data was then divided even further based on academic departments, as this was the most effective way to analyze trends and patterns across different disciplines. If further research was conducted the focus should be to increase the population size to include more individuals from each of the different academic departments. Along with students, expanding the groups to professors and staff of Robert Morris University. This expansion of information would allow the ability to better understand the knowledge of cybersecurity at a university level. Another limitation is the method of data analysis, due to limited knowledge in analyzing the responses. If future research was conducted working with someone who understands data analysis more would allow for more in-depth analysis of the data collected.

Conclusion

Working with organizations in 2025 has shown that the majority of them use some form of technology for their operations. This growth in technology has allowed cybercriminals the ability to steal or cause damage to these organizations sometimes without entering the place of work. Individuals who work at these organizations now have to better understand and be able to protect themselves with the devices they have access to. This is where the importance of understanding which groups understand technology at a university level. It allows the individuals who are going to be tasked with securing information and devices with the knowledge of which groups to put more emphasis on when training. The survey that was used in this study aimed to look at students at Robert Morris University and their understanding of cybersecurity and self-protection online. The data collected was from 73 respondents and showed that there was a correlation between the different majors and academic departments and their level of understanding. By gaining a clearer understanding of how a student's field of study influences their knowledge of cybersecurity, organizations can better prepare future professionals to safeguard information and infrastructure.

References

"2019 NortonLifeLock Cyber Safety Insights Report | NortonLifeLock." www.nortonlifelock.com, 2020, www.nortonlifelock.com/us/en/newsroom/press-kits/2019-norton-lifelock-cyber-safety-insights-report/ .

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of majmaah university. Big Data and Cognitive Computing, 5(2), 23. doi: https://doi.org/10.3390/bdcc5020023

Alkhalil, Zainab, et al. “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy.” Frontiers in Computer Science, vol. 3, no. 1, 9 Mar. 2021, pp. 1–23, www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full .

Alqahtani, M.A. Factors Affecting Cybersecurity Awareness among University Students. Appl. Sci. 2022, 12, 2589. https://doi.org/10.3390/app12052589

Auxier, B., & Anderson, M. (2021). Social media use in 2021. *Pew Research Center*, *1*(1), 1-4.

Bada, M., Sasse, A. M., & Nurse, J. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behavior? ArXiv.org. https://arxiv.org/abs/1901.02672

Chole, Vallabh, et al. Beware the Artificial Impostor a McAfee Cybersecurity Artificial Intelligence Report. 2023.

Habib, Hana, et al. Open Access to the Proceedings of the Fourteenth Symposium on Usable Privacy and Security Is Sponsored by USENIX. User Behaviors and Attitudes under Password Expiration Policies User Behaviors and Attitudes under Password Expiration Policies. 2018.

Howarth, Josh. “50+ Password Statistics: The State of Password Security in 2023.” Exploding Topics, 6 Feb. 2023, https://explodingtopics.com/blog/password-stats .

Mcclain, Colleen, et al. “How Americans View Data Privacy.” Pew Research Center: Internet, Science & Tech, 18 Oct. 2023, www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ .

M. E. Erendor and M. Yildirim, "Cybersecurity Awareness in Online Education: A Case Study Analysis," in IEEE Access, vol. 10, pp. 52319-52335, 2022, doi: 10.1109/ACCESS.2022.3171829 . keywords: {Computer security;Computer crime;Information security;Social networking (online);Cyber Attack;Awareness;cyberattacks;cybersecurity;Manas University;students},

Negussie Tolossa, Dawit. “View of IMPORTANCE of CYBERSECURITY AWARENESS TRAINING for EMPLOYEES in BUSINESS.” Vidyajournal.org, 2024, www.vidyajournal.org/index.php/vidya/article/view/206/96 .

Pew Research Center. “Mobile Fact Sheet.” Pew Research Center, Pew Research Center, 31 Jan. 2024, www.pewresearch.org/internet/fact-sheet/mobile /.

Satish, P. S., & Chavan, R. K. (2017). Web browser security: different attacks detection and prevention techniques. International Journal of Computer Applications, 170(9), 35-41.

Appendix

Demographic Information

		Overall N	Overall %	Baseline N	Baseline %
Age	Between 18 - 20	35	48	9	47.4
	Between 21 - 24	38	52	10	52.6
Sex	Male	34	46.5	15	78.9
	Female	38	52.1	4	21.1
	Non-Binary	1	1.4	0	0
Education Level	Undergraduate	57	78.1	11	57.9
	Graduate	11	15.1	5	26.3
	Integrated graduate	4	5.4	2	10.5
	Graduated	1	1.4	1	5.3
Current Year	Freshman	11	15.1	2	10.5
	Sophomore	12	16.4	4	21.1
	Junior	16	21.9	4	21.1
	Senior	31	42.5	7	36.8
	Graduate	2	2.7	1	5.3
	Graduated	1	1.4	1	5.3
		Overall N	**Overall %**	**Baseline N**	**Baseline %**
Major by Academic Department	School of Data Intelligence and Technology	32	43.8	19	100
	Rockwell School of Business	11	15.1	0	0
	School of Education and Social Sciences	5	6.8	0	0
	School of Communication and Media	5	6.8	0	0
	School of Engineering and Science	11	15.1	0	0
	School of Health Professions	9	12.4	0	0

Cybersecurity Common Practices Findings

Q: How familiar are you with common cybersecurity practices such as password management, safe browsing, or antivirus software?

Responses	Baseline N	%
Very Familiar	13	68.4
Somewhat Familiar	5	26.3
Neutral	0	0
Somewhat Unfamiliar	1	5.3
Not Familiar	0	0

Q: How often do you update your passwords across different platforms?

Responses	Baseline N	%
Very Regularly	1	5.3
Regularly	3	15.8
Occasionally	7	36.8
Rarely	8	42.1
Never	0	0

Q: Do you know what a firewall is and how to access it through your device?

Responses	Baseline N	%
Strongly Agree	1	5.3
Agree	9	47.3
Natural	1	5.3
Disagree	2	10.5
Strongly Disagree	6	31.6

Q: How comfortable are you to connect to a public Wi-Fi network?

Responses	Baseline N	%
Very Comfortable	0	0
Somewhat Comfortable	6	31.6
Neutral	3	15.7
Not Very Comfortable	6	31.6
Not Comfortable	4	21.1

Q: How aware are you of phishing attacks or other online scams?

Responses	Baseline N	%
Very aware & can identify easily	14	73.7
Fairly aware & cautious about it	4	21.1
Somewhat aware but not always sure	1	5.2
Slightly aware but unsure	0	0
Not aware at all	0	0

Self-Protection Online Findings

Q: Do you use any of the following to protect your online presence? (Select all that apply)

Responses	Baseline N	Baseline %	Test N	Test %
Antivirus Software	13	23.6	22	19.1
Virtual Private Network (VPN)	8	14.5	9	7.8
Strong Passwords (Unique Passwords or a Password Manager)	15	27.4	33	28.7
Multi-Factor Authentication (MFA)	19	34.5	49	42.7
None of the Above	0	0	2	1.7

Q: When browsing online, do you check for signs of secure websites such as HTTPS or the lock symbol in your browser?

Responses	Baseline N	Baseline %
Always	9	47.4
Frequently	6	31.6
Sometimes	2	10.5
Rarely	1	5.3
Never	1	5.3

Q: How often do you review your privacy settings on social media platforms?

Responses	Baseline N	Baseline %
Very Regularly	3	15.8
Regularly	8	42.1
Occasionally	6	31.6
Rarely	1	5.3
Never	1	5.3

Q: How confident are you that your privacy is secured when using social media platforms?

Responses	Baseline N	Baseline %
Very Confident	1	5.3
Somewhat Confident	2	10.5
Neutral	5	26.3
Not Very Confident	7	36.8
Not Confident	4	21.1

End of Survey Findings

Q: How confident are you that your education or workplace training has effectively provided you with cybersecurity knowledge?

Responses	Baseline N	Baseline %
Very Confident	6	31.6
Somewhat Confident	8	42.1
Neutral	2	10.5
Not Very Confident	2	10.5
Not Confident	1	5.3