College Students' Cybersecurity Behaviors

Anaya Henry
Junior Seminar 1
November 15, 2023

Table of Contents

→ Thesis Introduction

→ Abstract

→ Background of Study

→ Purpose of Study

→ Method(s)

→ Research Questions

→ Literature Review

→ Methodology

→ Conclusion

→ References

Thesis Introduction

The increasing frequency of cyber risks and the prevalence of digital technology in educational settings have made it more important than ever to comprehend and address college students' cybersecurity behaviors and practices. We know a lot about this topic from earlier research, but there is still much we don't know about how college students' cybersecurity behaviors have changed over the past five years in response to shifting technological environments, new threats, and the global shift to online learning. Most of the recent studies focuses on dated data but may not adequately reflect the dynamic nature of students' cybersecurity activities in the digital age.

By studying the recent five-year cybersecurity practices and routines of college students, this study aims to close this gap. We'll look at how students use technology, their knowledge of cybersecurity best practices, what influences their choices regarding online security, and the difficulties they have in protecting their online reputations. By filling in this important knowledge gap, my research aims to offer current perspectives that can educate academic institutions, policymakers, and cybersecurity practitioners on methods to improve students' cybersecurity awareness and practices, ultimately resulting in a safer online learning environment.

Abstract

The purpose of this research is to provide up-to-date insights into the cybersecurity practices of college students and to identify the key issues they face in the digital age. By doing so, this study aims to inform educational institutions, policymakers, and cybersecurity practitioners about strategies to enhance student cybersecurity awareness and practices, thus contributing to a safer online educational environment. The significance of this study lies in its potential to improve the effectiveness of cybersecurity education programs, the development of targeted policies, and the fostering of a more secure digital learning environment.

This study will employ a mixed-methods research design, combining both quantitative and qualitative data collection methods. A survey questionnaire will be distributed to a diverse sample of college students to collect quantitative data. Additionally, in-depth interviews will be conducted to gather qualitative insights. Data analysis will involve descriptive statistics for the quantitative data and thematic analysis for the qualitative data, providing a comprehensive understanding of the cybersecurity behaviors and habits of college students within the last five years.

Background of Study

At times, the importance of cybersecurity needed in college settings can be overlooked, especially by students. They may not fully comprehend the potential risks and consequences of cyber threats. Some students may believe they are tech-savvy or that they have a good understanding of online security, leading to overconfidence. This overconfidence can lead them to underestimate the risks. Younger students may not have encountered significant cybersecurity incidents in their past, leading to a lack of experience and understanding about the real-world impact of cyber threats. Some students may have an apathetic attitude toward cybersecurity, feeling that it is not a pressing concern in their daily lives or that it is the responsibility of someone else to address. Overcoming these challenges requires educational institutions to prioritize cybersecurity awareness and education, providing students with the knowledge and tools to protect themselves. Students, in turn, should actively seek information on cybersecurity best practices and consider the potential risks associated with their digital activities. Ultimately, raising awareness and fostering a culture of cybersecurity is essential for addressing the oversight of this important aspect of college life.

Purpose of Study

There's several important purposes of studying student cybersecurity behavior and habits for educational institutions, they include protecting personal and institutional data, avoiding scams, teaching students in protecting identities, understanding personal security and ethical use of technology. Educational institutions, ranging from K-12 schools to colleges and universities, are entrusted with a wealth of sensitive data, making them attractive targets for cyber threats. Protecting this data, fostering a culture of security awareness, and preparing students to navigate the digital landscape responsibly are critical aspects of maintaining a secure and productive educational environment. This literature review explores the multifaceted purposes of studying student cybersecurity behavior and habits in educational institutions, with a focus on safeguarding personal and institutional data, avoiding scams, educating students on identity protection, promoting personal security, and fostering ethical technology use.

Protecting Personal and Institutional Data

It is so important that we teach about protecting personal and institutional data in educational settings. Students often handle sensitive information, both their own and the institution's. Understanding their cybersecurity habits helps institutions protect this data. It enables them to implement better access controls, encryption, and monitoring systems to safeguard personal and institutional information. Educational institutions house sensitive information, including student records, financial data, research findings, and intellectual property. The vulnerability of this data to cyber threats, such as data breaches, ransomware attacks, or unauthorized access, underscores the need to understand how students interact with technology and data.

Avoiding Scams

Most common scams that college students face are phishing attacks, dating scam, scholarship and student loan scams. College students need to exercise caution if an email requesting more personal information than you feel comfortable revealing. Very often, these emails appear to be from a school administration. Using a school administrator as the email sender gives students a comfort in sharing information. If you suspect you've received a phishing email, get in touch with your school's IT staff. Meeting new people and finding love can be facilitated by using well-known dating apps. But not everyone is using these applications for the intended purposes. Students must be cautious who you divulge information to, and make sure they are who they say they are before you meet. Scammers will deceive you into thinking that you have won a scholarship or some extra cash in exchange for a fee.

Teaching Students in Protecting Identities

Identity theft is a pervasive cyber threat that can occur to anyone, especially college students. To protect yourself, avoid oversharing personal information and regularly monitor your credit and financial accounts. Card companies offer free alerts for suspicious activity. If you suspect identity theft, report it immediately and freeze your accounts. Studying student cybersecurity behavior helps institutions identify risky practices that may expose students to identity theft risks.

Understanding Personal Security

Colleges and higher education facilities are generally safe spaces for students, but theft and physical crime can occur. Educators and security staff should develop smart resources and trusted systems to promote personal security, providing students with reliable ways to respond to potential dangers. School administrators and security professionals can strengthen their college's security posture. Different ways faculty can improve students' understanding of personal security is by installing app-based access control, designing intelligent lockdown functions, providing secure student safe zones, and developing an incident reporting system; through IT.

Investigating Unethical Use of Technology

Many students and facilities utilize technology sometimes in negligence; which includes but not limited to using computers and inputting personal information, academic dishonesty, cyberbullying, connecting to unknown use of unauthorized software and tool usage. Educational institutions should establish cybersecurity policies, conduct regular awareness and training programs, and enforce consequences for unethical technology practices to protect the integrity and security of their systems and data.

Method(s)

Research Questions

What are the common cybersecurity risks and threats that students encounter in their academic and personal digital activities?

Do students exhibit different cybersecurity behaviors when using university-owned devices and networks compared to their personal devices and networks?

When using university-owned devices and networks, do you use any extra apps to protect your information from cyber threats?

Literature Review

This paper provides a comprehensive review of studies related to student cybersecurity behaviors and habits. It explores the methodologies employed by researchers in this field, their strengths, and weaknesses. Additionally, it reviews and synthesizes studies related to key variables in order to present what is known, what is controversial, and the gaps in the literature.

A. Evolution of Cybersecurity Risks

B. Cybersecurity Awareness and Behavior

C. Existing Gaps in the Literature

Evolution of Cybersecurity Risks

According to “The Evolution of Cybersecurity” written by the Codeacademy Team; the earliest presence of virtual threats happened around the 1960s and 1970s. Threats were more risky at the time due to limited security; cybersecurity had no definition at the time. Computer systems were expensive during the 1960s and time sharing allowed multiple people to use one large computer, which meant there was a need for security measures in order to prevent unauthorized access to files or computer data. In today’s times the solution of protectings accounts using passwords is still in effect.

Moving towards the 1970s, the earliest version of the internet seemed to be called ARPANET; which gave hackers the chance to explore new ways to hijack technology. The safety of the technology being developed had not been taken into account during this period of fast development and experimentation. The incentive to develop secure systems and software has been limited in view of the wide consensus that ARPANET is a scientific cooperative endeavor.

etc.

Fast forwarding to the 1990s, these were considered “the end of viruses.”. In households, the number of computers connected to the Internet has increased and this is making it more accessible. The result was incompetent script kiddies, individuals who downloaded the code and used it themselves without having to write anything of their own. They can use that code to launch attacks they don’t understand in order to vandalize or destroy targets for fun. Cybersecurity is as much about protecting people as it is about protecting computers, given the interconnected world we live in. Humans are weak and, as with computers, they have vulnerabilities that may be exploited: For example, psychologists use techniques to manipulate the emotions of people in order to achieve access to protected systems; Social engineering is also a powerful tool for hackers.

Cybersecurity Awareness and Behaviors

According to Purdue Global’s 2019 year end record, it was reported that

- More than 2.2 million sensitive records were exposed in the field of education

- A majority of data breaches in the education industry (60%) happened through unauthorized access, which mostly means stolen sign-ins and passwords as opposed to outside hacks.

- Virtually everyone is using the internet one way or another, our society hasn’t been educated on the potential harm that happens if devices are not secured correctly.

etc.

Some ways we can improve cybersecurity awareness is by having training in securing their devices, helping prevent phishing and scams, use of communal workstations safely, and encouragement to use password managers like Dash lane. Dash lane a well-known and trusted password manager that prioritizes security first, for professional and personal use. They are “one of the safest password managers out there”, according to Cybernews.com. Online password managers provide a critical defense against unauthorized access to systems, applications, and data. Applications like these makes it easy to have your passwords safely stored on your computer verse writing it down or having it in your notes.

College students are mostly victim to phishing and email scams, when more than one student receives the email, they trust it more. It is important to be careful of unsolicited attachments, hackers can pretend to be someone familiar. A strong level of security for your computer can be provided by a virus protection program. In addition, this program can scan your computer in a set schedule to monitor for threats when you are on the internet, reading messages or anything like that. Your software can warn you in advance that a site or file is suspicious and if dangerous files are downloaded, it will try to hide the threat. Some software charges for its use (and may have student discounts), while other software is available in free versions, with paid upgrades if you need them.

Existing Gaps in the Literature

With the increasing reliance on social media in educational settings, there is a need for more research into how students and staff use social media platforms and how these practices impact cybersecurity behavior. Understanding the role of social media in cybersecurity habits is crucial in today's digital landscape. With the increasing prevalence of online and remote learning, there is a need for research that specifically addresses the cybersecurity behavior habits of students and staff in virtual educational settings. The dynamics of cybersecurity in these environments may differ significantly from traditional settings. Closing these gaps in the existing literature on cybersecurity behavior habits in educational settings is essential for developing more effective strategies and policies to enhance cybersecurity awareness and practices within educational institutions. Furthermore, addressing these gaps will contribute to creating a safer digital learning environment for students and a more secure educational infrastructure for institutions.

Methodology

Research design is a crucial aspect of any study, including those related to "Student Cybersecurity Behaviors and Habits." The choice of research design impacts how data is collected, analyzed, and interpreted. Given how complex understanding student cybersecurity behaviors is, several research designs are consistent with this study. Here are three common research designs:

- Cross Sectional Survey Design
- Longitudinal Design
- Quantitative Data Collection Methods

Cross-Sectional Survey Design

- A cross-sectional survey design involves collecting data from a sample of students at a single point in time to gain insights into their current cybersecurity behaviors and habits. Surveys can be administered online or in person.
- This design is consistent with the study as it provides a snapshot of the cybersecurity practices of a specific student population. It allows researchers to assess the prevalence of behaviors, knowledge levels, and awareness regarding cybersecurity among students.

    - Purpose:
        - Efficient for collecting data from a large sample.
        - Suitable for assessing the prevalence of specific behaviors.
        - Can incorporate both closed-ended and open-ended questions to gain a comprehensive view.

Longitudinal Design

- A longitudinal research design involves collecting data from the same group of students over an extended period. Researchers conduct multiple assessments at different time points to track changes in cybersecurity behaviors and habits.
- Longitudinal designs are well-suited to investigate changes in student cybersecurity behaviors over time. They can assess the impact of interventions and educational programs on long-term habits.

Purpose:

- Provides insights into changes and trends over time.
- Effective for assessing the long-term impact of interventions.
- Allows for the identification of causal relationships.

Qualitative Data Collection Methods

- In-Depth Interviews:
    - *Description:* Qualitative interviews involve one-on-one or group discussions with students, allowing them to share their experiences, attitudes, and motivations regarding cybersecurity.
    - *Consistency with the Study:* In-depth interviews are consistent with the study as they provide insights into the "why" behind student cybersecurity behaviors and habits.
        - *Purpose:*
        - Rich data that provides depth and context.
        - Reveals the nuances and complexities of student behavior.
        - Allows for the exploration of attitudes and motivations.

- Focus Group Discussions:
    - *Description:* Focus group discussions involve small groups of students discussing cybersecurity-related topics guided by a moderator. These discussions help uncover shared perspectives and group dynamics.
    - *Consistency with the Study:* Focus groups are consistent with the study as they provide insights into the collective behaviors and habits within a group of students.
        - *Purpose:*
        - Encourage interaction and idea-sharing among participants.

etc.

- Open-Ended Surveys:
  - *Description:* While surveys primarily collect quantitative data, they can include open-ended questions where students can provide qualitative responses. These responses offer valuable context to the quantitative data.
  - *Consistency with the Study:* Open-ended survey questions can provide qualitative insights into students' cybersecurity practices while maintaining the efficiency of a survey.
    - *Purpose:*
    - Efficient for collecting both quantitative and qualitative data.
    - Allows for contextual information to complement numerical responses.

Conclusion

In summary, the multifaceted goals of studying students' cybersecurity behavior and habits in educational institutions are a critical part of protecting personal and organizational data, preventing fraud, protecting student and faculty identities, understanding personal safety, and promoting the ethical use of technology.

By better understanding how students interact with technology and the digital world, educational institutions can develop informed strategies to improve cybersecurity, foster a culture of technical responsibility, and prepare students to navigate the ever-evolving cyber landscape safely and ethically. As the digital age continues to evolve, the need for this knowledge becomes increasingly apparent to ensure educational environments and help students become responsible.

References

Smith, J. (2017). Cybersecurity behavior in higher education. Journal of Higher Education Cybersecurity, 5(2), 45-62.

Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information Systems Education Journal (ISEDJ)*, *18*(1). https://files.eric.ed.gov/fulltext/EJ1246231.pdf

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3). https://doi.org/10.1057/s41288-022-00266-6

Elevate Security with Passkeys: A Better Way to Log In. (n.d.). Dashlane. Retrieved November 1, 2023, from https://www.dashlane.com/passkeys

The Evolution of Cybersecurity. (n.d.). Codecademy. https://www.codecademy.com/article/evolution-of-cybersecurity