DAKOTA STATE
UNIVERSITY

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Nadia Halabi Student ID: A00130123

Dissertation Title:
A STUDY OF STEM AND NON-STEM COLLEGE STUDENTS' SMART TV ATTITUDES

Graduate Office Verification: DocuSigned by: Abby Chowning F44C8D9E621C417... Date: 11/30/2023

Dissertation Chair/Co-Chair: DocuSigned by: Stephen Krebsbach 3D7C49A27237465... Date: 11/30/2023
Print Name: Stephen Krebsbach

Dissertation Chair/Co-Chair:____________________ Date: __________
Print Name: ____________________

Committee Member: DocuSigned by: Kyle Cronin 0B9AFA1BE48843C... Date: 11/30/2023
Print Name: Kyle Cronin

Committee Member: DocuSigned by: Dr. Cherie Noteboom 897E512F036A49C... Date: 11/30/2023
Print Name: Dr. Cherie Noteboom

Committee Member: DocuSigned by: Mary Francis CF527B7AF83E4A7... Date: 11/30/2023
Print Name: Mary Francis

Committee Member:____________________ Date: __________
Print Name: ____________________

Submit Form Through Docusign Only
or to Office of Graduate Studies
Dakota State University

DAKOTA STATE
UNIVERSITY

A STUDY OF STEM AND NON-STEM COLLEGE STUDENTS' SMART TV ATTITUDES

(THE TRADE-OFF BETWEEN FUNCTIONALITY AND SECURITY/PRIVACY)

Dissertation Proposal

Doctor of Philosophy

in

Cyber Operations

October 2023

By
Nadia Halabi

Dissertation Committee:

Dr. Stephen Krebsbach
Dr. Kyle Cronin
Dr. Cherie Noteboom
Dr. Mary Francis

ACKNOWLEDGMENTS

Many people have supported and encouraged me on this long journey I would like to express my deep gratitude to my committee members for their guidance throughout my research; my work would not have been completed without all your help over the past two years. I am grateful for Dr. Kresbach’s patience and motivation, Dr. Noteboom’s methodology advice, Dr. Cronin’s support, and Dr. Francis’ comments on my survey questions and manuscript. I would also like to thank all who helped me at DSU: Research and Writing Centers.

I would like to thank my husband, sons, parents, siblings, and friends for their constant encouragement and support. A big thanks to my siblings Susan, and Yadira who gave me comments and encouraged me, especially Susan, who kept pushing me to take the extra step. I would also like to express my gratitude to my supervisor, Josh Kadrmas, and my CISO Michael Gregg for their continuous encouragement. Finally, thanks to all my classmates who were there to listen.

Thank you all. Much appreciated!

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the dissertation describes original work that has not previously been. presented for the award of any other degree of any institution.

Nadia Halabi

ABSTRACT

Internet-of-Things (IoT) usage surged over the past decade, and its advancement of intricate devices brings obvious convenience to users. IoT devices such as Smart TVs offer services and features that are desirable and favorable to consumers. However, all that convenience comes with security and privacy concerns. Smart TVs have been the target of attacks due to their internet connectivity. Moreover, personally identifiable information (PII), browsing history, and watching preferences, are being collected, leaked, and sold.

Previous research showed that users care that their data is protected but have minimal privacy awareness. Moreover, some researchers claimed that even if consumers were made aware of privacy issues, using the smart TVs' functionalities took higher precedence than protecting their privacy. This study will extend previous studies and investigate claims that informing users about privacy does not change their attitudes. The aim is to investigate different groups of students at a small mid-western public institution of higher education: across domains, STEM and Non-STEM programs, junior/senior and freshmen/sophomore students' responses and attitudes will be compared. The research will investigate whether training and exposure to security programs and courses affect students' security and privacy knowledge, awareness, and attitudes.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Background

Technology has changed human life immensely in the last several years (Techresider, 2019). The last decades have changed the composition of home networks. Early home networks consisted of home routers and computers and later gaming consoles added network capabilities. The advent of mobile brought additional devices onto the network in smartphones and tablet devices (Dell, 2012; BCG, 2015). Adding the Internet of Things (IoT) devices to the home network expanded the number of devices on home networks even further. IoT devices' simple interfaces and configurations made it effortless to expand the home network by adding devices with a few clicks (Steve, 2021).

IoT is now the next frontier of technological innovations, it is more than a buzzword. IoT technology has diverse applications across different industries, including healthcare, transportation, energy, and critical structures (Assiris, 2018). Electronic devices in homes or offices can connect to the internet and send and receive data. These devices are becoming more popular among homeowners because they are practical. Hence, more people are acquiring such devices due to their convenience. Smart refrigerators, wearable watches, smartphones, heating and cooling units, light bulbs, satellites, smart monitors, and smart televisions with internet capabilities are becoming the current trend.

IoT device usage has surged over the past decade in business and personal applications (Jovanović, 2021). It is now a core element in our modern world and is expected to become more intertwined in our future lives. In an article in BBC Future by Alex Riley, global IoT usage numbers are estimated to reach more than 125 billion IoT-connected devices by 2030 (Riley, 2020). Our dependence on IoT devices is increasing daily (Alharbi, 2018). Unfortunately, efforts to "secure these applications are slower than our growing dependence on them" (Alharbi, 2018). Currently, the Internet of Things is powered by three emerging technologies: Artificial Intelligence, 5G, and Big Data (Ghosh, 2021).

Smart TVs are contemporary innovations, and their usage has increased drastically over the years (Kovocs, 2021). Smart TVs rose from sixty-seven million units shipped worldwide in 2012 to an estimated 141 million in 2015. The global smart TV market was estimated at $174.78 billion in 2020 and at $190.36 billion in 2021. Another article estimated the smart TV growth rate at 20.8% (Grand Review Research, 2021). In addition, the global smart TV market is expected to grow 11.1% from 2021 to 2028 to reach $397.51 billion by 2028. (Grand Review Research, 2021).

A smart TV is an internet-connected television that incorporates an operating system which offers a wide variety of features, such as streaming services, browsing the internet, listening to music, gaming, and connecting to other wireless devices (Silva, 2022). Problems come with those smart TV services: several security risks are found in the smart TV ecosystem. However, many people are unaware of the security risks, leading to privacy issues. Moreover, some home users may be aware of existing security bugs in smart TVs but think that its advantages outweigh the disadvantages.

Problem Statement and Motivation

Smart TVs are connected to the internet and transmit data back to manufacturers or service providers (Abdugani, 2020). Browsing history, users' behavior, and other data are being collected, leaked, and shared (Abdugani, 2020). Third-party vendors can keep track of users, collect their information, listen to their private conversations, and capture their images using the camera and audio capabilities of the smart TV.

Previous research has shown that users do not want their data to be leaked, shared, and used (Malkin et al., 2018). It has also been found that they have minimal awareness of the security issues about smart TV devices (Aleisa et al., 2017). In other research, even if homeowners were made aware of the dangers, maintaining the functionality of the smart TVs mattered more to them than privacy (Ghiglieri et al., 2017). Ghiglieri et al. claimed that, because of this indifference to security, safeguards need to be put in place by the manufacturers to protect consumers (Ghiglieri et al., 2017). These findings lead to one question: if enhanced security awareness will be there because of an adequate level of security education? Will users then be prompted to choose security measures over convenience? In addition, there is the issue of the “Privacy Paradox.” In one article, the researchers claimed those individuals also do not care about their privacy and that users routinely trade privacy for convenience.

Research Gap

Previous studies showed that researchers tried to raise security and privacy awareness of users concerning their smart TVs interactions by:

- Sending some security information text messages to users (Ghiglieri et al., 2018)
- Telling them about smart TV risks and trying to raise their awareness (Ghiglieri et al., 2018)

- Informing users that their data was collected and may be misused (Malkin et al., 2017)

Even though participants were made aware of the security and privacy issues concerning smart TVs features, users still preferred the convenience of using them over protecting their privacy (Aleisa et al., 2017). Raising users' awareness and prompting them to adopt security measures did not yield optimal results. Researchers then concluded that nothing can be done to change homeowners' attitudes, and it is up to the vendors to take measures and protect the users by adding some security technology to smart TVs (Ghiglieri et al., 2018).

There are gaps in the literature about more rigorous attempts to raise users' awareness and knowledge. Therefore, this research will build upon past literature by addressing the research gap. What is needed is to study those that are already heavily involved in security programs (STEM Programs). Will their education positively influence their security habits and behavior?

Research Goal

The goal of this research is to build on the previous research findings and investigate different groups of students' behavior at a small mid-western public institution of higher education while using smart TVs. Those groups are:

- STEM and Non-STEM would be compared with their security knowledge, awareness, and attitude. The first group is expected to be far better off than the second group.
- Junior and senior students will be compared to freshmen and sophomore students in terms of smart TV knowledge, awareness, and attitude.

In this study, the researcher wanted to investigate STEM students, especially security students, if they were influenced positively to adopt safer measures while using smart TVs. If the results show that this is not the case, then it may support the idea that it is impossible to convince users to be proactive and protect themselves while using smart TV devices. If the result is true, it suggests that more research needs to be done and that users can be trained or taught to be proactive in their security and privacy behavior.

Research Questions and Hypothesis

This research aims to investigate two groups of university students: STEM versus non-STEM, and junior and senior students versus freshmen and sophomore. The research will investigate whether appropriate training and exposure to security courses and programs would affect those students' privacy attitudes. The researcher wants to check if those students were positively influenced by their security courses to acquire privacy habits while using smart TVs.

Question 1 (RQ1): Does security awareness (STEM programs) positively influence students' likelihood of adopting security best practices (knowledge, attitude, awareness) while using smart TVs?

Question 2 (RQ2): Do the two groups junior/senior and freshmen/sophomore students differ considerably in their security awareness, attitude, and knowledge?

The following hypotheses are proposed:

Hypothesis (**H1**): Security awareness due to STEM programs positively influences students' likelihood of adopting security best practices (knowledge, attitude, awareness) while using smart TVs.

Hypothesis (**H2**): The two groups junior/senior and freshmen/sophomore students differ considerably in their security awareness, attitude, and knowledge.

The following null hypotheses are proposed:

Null (H1): STEM programs do not positively influence students' likelihood of adopting security best practices (knowledge, attitude, awareness) while using smart TVs.

Null (H2): Junior/senior and freshmen/sophomore students do not differ considerably in their security awareness, attitude, and knowledge.

Moreover, it will be investigated if being exposed to more than one security course does affect students in their security behaviors and mindset.

The following section describes the research scope and limitations, the survey, the participants, the made assumptions, and the significance of the research.

Research Scope and Limitations

This dissertation aims to find the answers to the previously mentioned research questions and analyze the different college students' security and privacy attitudes toward smart TV devices. The scope of the survey is limited to current undergraduate university students.

The estimated research limitation is the survey sample size. The obtained number of participants was not adequate in the Fall 2022 semester. Consequently, the survey was conducted again in the Spring semester 2023 for four weeks. Some of the limitations were:

- Sampling size was insufficient, therefore the survey had to be re-opened in the Spring 2023 semester.
- The sample was biased toward a specific demographic, and the groups were unbalanced.
- Another limitation is the fact that students who participated in the survey were from only one school, which is not representative of all students.

The Survey and Participants

The paid Survey Monkey online web tool was used to anonymize the data from the participants. Confidential information was not collected. The only personal collected information was age and IP addresses.

The survey questions were targeted toward answering the research questions. If students took security courses or were enrolled in security or STEM programs, did that affect their thinking and behavior? By checking the students' answers, a general idea can be made if STEM majors and/or taking security courses influence students' security behaviors.

Participants were undergraduate students who were above 18 years old. Students less than 18 years old were exited automatically from the survey. The only restriction imposed in the survey is that the participants used smart TVs even with external devices. Those who did not use smart TVs exited automatically from the survey as well. The survey was purely voluntary and relied on the students agreeing to participate and complete the research survey. A percentage of participants started the survey but did not complete it. The participants were from different classes across majors. However, more than a third of the participants were freshmen students. Moreover, although the survey link was sent to different departments and majors across the university, most of the participants were STEM students.

Assumptions, Significance, and Contribution

The researcher expected participants who took the survey to be honest with their responses. In addition, the researcher is assuming that these students' responses closely reflect the attitude of the population of other college students nationwide. The researcher is assuming that the results would be a representation of the US university population.

Currently, smart TVs are being used in many areas: home entertainment, office educational purposes, and business purposes (Lee et al., 2013). Therefore, it is important to address the security and privacy issues related to smart TVs and protect users' privacy. This research will contribute to both research/academics and practice.

Research: The research results will contribute to the knowledge in this area and may help inform the direction of future research efforts.

Practice: The findings of this study will have implications for practice. The findings help practitioners to identify more appropriate ways to raise awareness and influence users to protect their privacy and take significant measures to do that. The university will be prompted to educate new undergraduate students to take security or privacy courses and be better prepared while dealing with smart TV devices.

Definitions

The below terms are defined so the reader has a clear idea of what is meant by the researcher.

Attitude: "Attitude is a psychological tendency which is shown in the evaluation of certain entities with some degree of favor or disfavor" (Alqarni, 2017).

A/V: Is an acronym that stands for Audio/Video or Audio-Visual, and it refers to equipment and applications that deal with sound and sight.

CEC: Is Consumer Electronics Control. Per Wikipedia it is feature of HDMI "designed to control HDMI connected devices by using only one remote controller; so, individual CEC enabled devices can command and control each other without user intervention."

DDoS: Per Cloudflare: A distributed denial-of-service (DDoS) attack is a “malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

OTT: Over-the-top media service, or streaming platforms is a “media service offered directly to viewers via the Internet. OTT bypasses cable, broadcast, and satellite television platform” (Wikipedia).

PII: Personally, identifiable information. It is defined in the U.S. General Services Administration (GSA) as “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.”

Privacy: “Ensures that users’ information is not available to anyone without explicit permission” (Goriawala, 2013).

Security: Is how “users’ information is protected from cybercriminals” (Goriawala, 2013).

SSID: Service set identifier is a unique identifier that allows devices to connect to a Wi-Fi network.

Smart TV: A PC that shows TV programs. “Smart TV = TV + PC” (Lee et al., 2013).

Chapter Summary

In this chapter, the problem statement, motivation, research gap, and goal are addressed by the researcher. The security and privacy issues surrounding the growing use of smart IoT devices in general and smart TVs in specific are debated. The research questions and null hypotheses are outlined in this chapter, along with information about the survey, its scope, and participants, Moreover, the researchers touched on the assumptions made, the significance of this study, and its contribution. In the next chapter, the existing literature review is investigated and presented to the reader.

CHAPTER 2

LITERATURE REVIEW

IoT Smart Homes

The smart home IoT ecosystem has thrived lately and with the advent of all those smart devices, the life of homeowners has become more comfortable (Riley, 2020). During the recent pandemic, those devices became popular and are the new trend (Riley, 2020). But all these technological advancements come with a set of risks (Mazhar et al., 2020). It is crucial for the homeowner to know the threats that come with their smart home IoT devices. According to Mazhar et al. the studies on smart home devices are limited, in fact, most of these devices were inspected in testing environments (2020). One extremely popular IoT device is a smart TV.

As previously mentioned, smart TVs are equipped with unique features such as internet browsing and on-demand media (Alam et al., 2017). Hence, they have multiple usages and services such as connections to Amazon, Hulu, other streaming companies, and games (Willcox, 2019). What makes smart TVs popular is their interaction with users and have gratifying characteristics (Alam et al., 2017). Per Kovocs, users can “stream media services and run apps, browse the internet, access music channels, shop online, and access on-demand video services" (2021).

TV Usage and Popularity

TVs have been essential devices for households for decades. It is a fundamental part of our lives, and some regard it as an essential companion (Kaur, 2019). A TV that connects to the internet is a smart TV (Kovacs, 2021). TVs have been remarkably enhanced recently to the point that it may be challenging to get one that is not “smart” (Hall et al., 2020). Due to IoT and smart device innovations, smart TVs were created in 2007 and have been on the rise since then (Good Home Automation, 2021). More than 70% of homeowners had smart TV per Statista in 2020.

The Deloitte report states, “Consumers’ demand for TV and consumption is fundamentally changing” (2018). Moreover, they added that the landscape and the future of TV broadcasting and streaming videos are unclear (Deloitte, 2018). However, the presence of security and privacy issues in smart TVs is worrisome (Whittaker, 2019). They may be used for spying, hacking, and botnet attacks (TechieGuy, 2020). There are few safeguards in them, if any, to enhance users’ privacy and security. Manufacturers can add protectors at low cost to protect them from security attacks, but little has been done (Privitera, et al., 2018). Instead of technology and hardware fixes, users are left to fend for themselves.

As mentioned, there are security and privacy issues with smart TV devices. These issues are threats to users’ privacy. Sometimes the terms “security” and “privacy” overlap and there is a gray area between them. Per Dictionary.com, security is: “precautions taken to guard against crime, attack, sabotage, espionage.” On the other hand, privacy is “the state of being free from unwanted or undue intrusion or disturbance in one's private life or affairs.”

Some smart TV security-related violations would be:

- Injecting some malware code to cause harm.
- Using smart TV as a medium for botnet attacks.
- Opening back doors for some malicious activity when users download unsafe apps on their devices.
- Keeping track of the use Accessing someone's smart TV login credentials,

Privacy issues are violations of users' confidential information. Some smart TV's privacy violations are:

- Browsing history, search/ pattern, and viewing habits.
- Listening to users' private conversations via smart TV audio.
- Watching users' areas and taking their pictures via the smart TV cameras, if applicable
- Using the audio and camera functionalities of the smart TV for spying purposes.
- Collecting personal information of users and sharing or selling it to another party.
- Leaking sensitive information about users and their families; Identity theft.
- Access browsing history, search patterns and viewing habits
- Collecting children's information and images and selling it to a third party; this is a violation of The Children's Online Privacy Protection Act (COPPA).

Some of the best practices to stop these smart TV privacy violations are:

- Purchasing a smart TV without cameras. In addition, checking the security reviews of the TV before getting it is a smart move.
- Disabling the cameras when not needed. Cameras may be used for spying or taking videos or pictures of the household.
- Turning off the TV when not in use. The audio can run in the background.
- Refraining from downloading apps on smart TVs before checking their security reviews. Some apps have security issues and may open backdoors for hackers.
- Changing the default and admin passwords on the home router Wi-Fi
- Checking the admin password on the TV settings.
- Updating the smart TV's firmware regularly.

Smart TVs are full of vulnerabilities and flaws that malicious users can abuse. The FBI warned users that hackers could take control of the cameras and microphones to spy on smart TV users (Whittaker, 2019). In 2017, the Federal Trade Commission fined Vizio 2.2 million dollars because they were tracking their customers' viewing habits and then selling that information to third parties (Hall et al., 2020).

Streaming Devices (OTT)

Smart TV devices have grown over the years including streaming platforms (or OTT) devices, such as the two popular devices Roku TV and Amazon Fire. These OTTs are substitutes for having multiple channels of TV. Moghaddam et al. (2019) in a large first-scale tracking research examined 2,000 channels on Roku and Amazon Fire TV. They claimed that 69% of Roku channels and 89% of Amazon Fire TV channels had tracking on them. Moreover, they discovered that device IDs several numbers, Wi-Fi MAC addresses, and

SSIDs are often being gathered and transmitted. In addition, they mentioned that disabling the tracking options is unproductive and offers no protection for users. The researchers recommended that OTT should be transparent about the traffic and should offer privacy controls and block clear text connections.

In a similar study Varmarken et al. (2020), mentioned that smart TVs connect to advertising and tracking services (ATSes). They gathered traffic from the top 1000 apps on Roku TV and Amazon Fire. The authors designed a software tool to examine those apps and investigate them. Varmarken et al. mentioned that blocklists do not work and that hundreds of these apps gather PII info and leak it to third parties. In addition, some of the apps prevent users from being able to opt out of ads. The researchers concluded that "Privacy Enhanced Solutions" should be developed for smart TV platforms (Varmarken et al. 2020).

High-Definition Multimedia Interface (HDMI)

The High-Definition Multimedia Interface (HDMI) is the backbone for Audio/Video (AV) connections between video devices. HDMI is a widely used standard for transmitting audio and video signals. While HDMI is considered secure, there are some potential security threats that users are not aware of.

In an article, researchers investigate the security threats to the High-Definition Multimedia Interface (Rondon et al., 2021). They mentioned that almost 10 billion HDMI devices are used to distribute A/V signals. The researchers mentioned that the Consumer Electronics Control (CEC) protocol is a vital part of the HDMI protocol, which allows HDMI devices to share an "HDMI distribution to communicate and interact with each other." While there are security mechanisms that protect network components, this is not the case for CEC. Rondon et al. mentioned that the CEC protocol was insecure and that this may give the adversary a “new surface invasion” into the HDMI by “tapping” into the CEC vulnerabilities (Rondon et al., 2021). Some issues are malicious analysis of devices, eavesdropping, denial-of-service attacks, and targeted device attacks (Rondon et al., 2021).

Android Boxes

An Android TV box is a machine that runs on the Android operating system and connects to a smart TV. It can access streaming devices, applications, and the web, hence it is popular for users. In a recent article, it was mentioned that thousands of Android TV boxes were infected with the dangerous Triada-based malware linked to fraud (Tom’s Guide, Oct 2023). In the same article, Human Security, a Cyber security firm claimed that they found several models of those boxes that were infected with dangerous backdoors which are challenging to detect or remove.

Alexa and Google

An article by the German Security Research Lab found that home users were subjected to eavesdropping by the Amazon Alexa and Google Home apps. The security flaws in those apps can be exploited by the users’ voice commands: malicious users can eavesdrop on users, open backdoors, and do other harmful activities (Bräunlein, & Frerichs, 2019). In a similar study, Kumar et al. carried out research at the University of Illinois. They found a new security attack called “skill squatting,” where the hackers can direct users to the malicious application without their knowledge by leveraging the systematic errors found in Amazon Alexa (Kumar et al., 2018).

Smart TV Landscape

Smart TV are devices connected to the internet, and once this takes place, data is exchanged (Whittaker, 2019), a reality which may be unknown to many users. People are purchasing them to get additional functionalities and interacting experience, but they are unaware of the fact that the so-called “smart devices” are opening doors for hackers to use their TVs for malicious purposes. While technology is making our life more convenient, it also “provides new opportunities for abusers to control, harass and stalk their victims” (Riley, 2020). The smart TV threat landscape continues to evolve, and hackers are becoming more intelligent and innovative. These threats target all consumers.

The smart TV landscape has shifted from regular TVs to ones with integrated internet usage. It has changed drastically in the past years; it has increased in sophistication and is quite intricate (Alam et al., 2017). Smart TVs are heterogeneous platforms with divergent characteristics and different operating systems. The two top smart TV operating systems are Tizen and WebOS (Statista, 2020).

Some of the smart TVs’ popular functionalities (Silva, 2022):

- Availability of many channels
- Streaming Videos/Music
- Media Player
- Browse online, Web Browsing
- Search Capabilities
- Screen Sharing/interactive gaming
- Skype and Transfer Smartphone content to other smart devices

In a recent 2021 study, Liu et al. studied 3163 smart TV Android applications to investigate their security issues. The researchers investigated the security flaws in those apps by using dynamic and static analysis and machine learning. Experimental results showed that those Android apps have various security flaws and may contain malicious code leading to leakage of users' confidential information (Liu et al., 2021). The researchers used the Andro Bugs framework, which scanned the application for vulnerabilities and reported at least fifty vulnerabilities per Android app. A total of 2997 Android apps contained critical security bugs (Liu et al., 2021). The researchers mentioned that not much research is done in that area, and further studies are needed.

Vulnerabilities and Surface Attack Vectors

Figure 1 lists some existing vulnerabilities and security risks that are prevalent in the smart TV ecosystem (Hammi et al., 2022). Gai et al. found more than eleven vulnerabilities and fifteen attack surfaces in research on seven IoT home devices, including smart TVs. Some of their findings on the smart TVs are:

1. Unencrypted services: data sent between the smart TVs and devices are not encrypted, so malicious attackers can easily intercept this.
2. Weak passwords: weak passwords were used.
3. Lack of two-factor authentication: There was no use of tokens between devices while connecting to the network. (Gai et al., 2018).

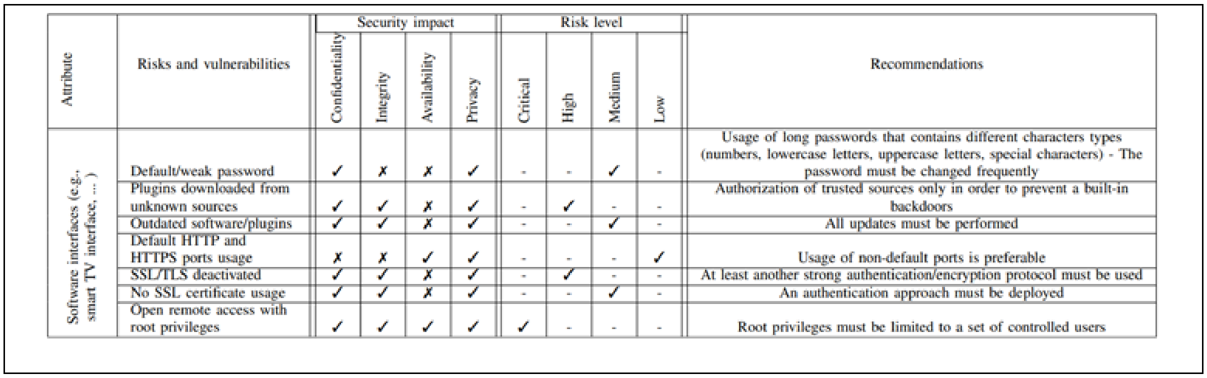
Some of the attack vectors that were found in the smart TVs are: (Gai et al. 2018)

1. Open network ports: can be easily exploited and subjected to different attacks such as denial of service, replay, and injection attacks.
2. Data storage: data stored in the device should be encrypted, which is not the case.

3. Authentication or authorization: devices lack 2-factor authentication, leading to unauthorized access because of weak passwords.
4. Device firmware: storing information, and consequently can leak sensitive information such as credentials and history.
5. Device web interface: device accesses a web interface that has many vulnerabilities, such as SQL injection, phishing, and cross-site scripting (Gai et al., 2018).

According to Consumer Reports, malicious users can control and effortlessly exploit millions of smart TVs because of quickly found security flaws in the devices. These can occur with Samsung TVs, some TCL, and others using the Roku TV platform and the Roku Ultra streaming device (Consumer Reports, 2018). In Japan, more than three hundred ransom attacks took place on smart TVs, where the affected smart TVs were locked, and owners were asked to pay around $100 within 72 hours (InfoSecurity, 2017).

In 2018, Bitdefender studied Romania and found that cybercriminals controlled many smart TVs simultaneously to cause DDoS attacks on accessed websites. The hackers would then demand money from the website owners to release the sites (Bitdefender, 2018). The same study found that 46% of Romanians were concerned that malicious users may take control of their smart TVs.



Attribute	Risks and vulnerabilities	Security impact				Risk level				Recommendations
		Confidentiality	Integrity	Availability	Privacy	Critical	High	Medium	Low	
Software interfaces (e.g., smart TV interface, ...)	Default/weak password	✓	✗	✗	✓	-	-	✓	-	Usage of long passwords that contains different characters types (numbers, lowercase letters, uppercase letters, special characters) - The password must be changed frequently
	Plugins downloaded from unknown sources	✓	✓	✗	✓	-	✓	-	-	Authorization of trusted sources only in order to prevent a built-in backdoors
	Outdated software/plugins	✓	✓	✗	✓	-	-	✓	-	All updates must be performed
	Default HTTP and HTTPS ports usage	✗	✗	✓	✓	-	-	-	✓	Usage of non-default ports is preferable
	SSL/TLS deactivated	✓	✓	✗	✓	-	✓	-	-	At least another strong authentication/encryption protocol must be used
	No SSL certificate usage	✓	✓	✗	✓	-	-	✓	-	An authentication approach must be deployed
	Open remote access with root privileges	✓	✓	✓	✓	✓	-	-	-	Root privileges must be limited to a set of controlled users

Figure 1. Some Smart TV Security Risks (Hammi et al., 2022)

Forbes stated that the CIA, along with M15, created a TV malware called “Weeping Angel” which hacked the Samsung smart TV (Hall et al., 2020). This malware runs like a TV app in the background, captures audio, recovers Wi-Fi keys, and keeps recording even if shut down (Brewster T. 2017). Wikileaks added that the Samsung TVs were hacked to spy on users using the microphones as listening devices (CBC News, 2017). Per Hall et al., the “Weeping Angel” was a significant breach of users’ privacy (Hall et al., 2020).

One alarming attack vector is botnets. Botnets can cause significant national and global damage by sabotaging electric and power grids (Ornes, 2019). Since smart TVs connect to the internet, and their default passwords are extremely easy to recognize, botnets can “sneak” into the connection undetected and then prepare the environment for future cybercrimes (Ornes, 2019).

Previous Research

The smart TV ecosystem is intricate, complex, and shifting. Moreover, it is full of trackers. There are various existing vulnerabilities and security risks oblivious to homeowners. In 2018, Malkin et al. conducted a study on 591 US users to investigate their expectations of how smart TVs collect and use their data. The researchers got various answers, and there was uncertainty regarding what was collected and how it was used (Malkin et al., 2018). However, all participants agreed that it was unacceptable for data to be shared (Malkin et al., 2018). The researchers hoped their findings would prompt lawmakers and IoT device manufacturers to improve users' privacy (Malkin et al., 2018).

In a similar study, Ghiglieri et al. carried out three studies using online surveys of 524 participants in Germany to investigate their smart TV privacy awareness. The first study checked two hundred participants’ awareness of smart TV privacy risks (Ghiglieri et al., 2017). The response was that these users had minimal awareness. Then, the researchers tried to develop awareness-raising messages in the second study and tested 155 participants. The dominant discovery was that the participants valued their “smart TV's Internet functionality more than their privacy” (Ghiglieri et al., 2017). Then they tried to raise the awareness of a subgroup of 169 users in a third study but concluded that raising consumers' awareness was insufficient. The researchers mentioned that making “participants aware of potential misuse is more effective than only making them aware that data is collected and analyzed by vendors whom they may trust” (Ghiglieri et al., 2017). They claimed that what is needed is more research into the “development of usable privacy-enhancing technologies (PET), providing an improved level of privacy preservation while retaining functionality” (Ghiglieri et al., 2017).

Nevertheless, in another research project, Aleisa et al. conducted a study in Saudi Arabia with 236 participants (Aleisa et al., 2017). They found out that although some participants were concerned about privacy “invasions," they were more concerned about the convenience of having smart TVs. Even though Saudi Arabia was big on technology, the researchers concluded that there was a low privacy awareness among the participants (Aleisa et al., 2017). However, more than two-thirds of the participants were females, and 250 users refused to participate. The authors predicted that there would be tighter security rules, secure IoT devices, and complete privacy disclosures (Aleisa et al., 2017).

Alqarni studied 301 students' responses at Midwestern University to investigate factors that impact students’ adoption of computer security practices. Her finding was that university administrations need to educate students about the benefits and ease of adopting security practices by organizing workshops for them (Alqarni, 2017). She added that when students feel threatened and vulnerable, they feel the need to embrace protective security measures. According to Alqarni, students can change their security attitude if shown and taught that this is not difficult to adopt and will protect them from security threats.

Chapter Summary

Users are heading towards having smart homes and TVs without the knowledge of how to protect their privacy nor having any safeguards in the smart TVs, which is a concern. There were some efforts towards educating users and homeowners more about their smart TVs, however, it seems from previous literature that the effort did not pay off. According to several articles, most users were not ready to do anything about it. Homeowners need to be educated to protect themselves and their data. This study wanted to build on previous studies and investigate claims that even if users are educated about the vulnerabilities, they would still choose smart TV's functionality over protecting their privacy.

CHAPTER 3

RESEARCH METHODOLOGY

The research aims to investigate a small mid-western public institution of higher education undergraduate students' attitudes and practices while using a smart TV. Moreover, the purpose is to compare the STEM versus the non-STEM students' security awareness and mindset. One main goal is to seek whether proper security exposure would make a difference to students' privacy and security awareness while dealing with smart TVs. Another aim is to understand students better and assess if the majors impact students' security awareness mindset. This study expected that students in security majors be more aware of the vulnerabilities of smart TVs and care to protect their privacy.

This chapter outlines the research design, data collection, and methods to analyze the data used by the researcher. Moreover, it discusses the survey population and sample size.

Research Method

Creswell defined quantitative methodology as “explaining phenomena by collecting numerical data that are analyzed using mathematically based methods (in particular statistics)” (Sukamolson, 2007). The research chosen for this study is the cross-sectional descriptive quantitative method. Some advantages of using this research methodology are collecting information quickly and reaching a high sample rate (Miller, 2020).

A descriptive study is where data is collected without affecting the environment or one where the primary objective is estimating a parameter of interest (SDSU, 2020). It is one of the best methods to collect information and show relationships and is also known as “correlational” or “observational” studies (SDSU, 2020). The survey aims to describe a numeric parameter of interest (security and privacy awareness) from the population by studying a sample of the population, in this case, undergraduate students. This is in line with the purpose of the research survey.

Using an online web tool to conduct the survey and collect the needed data from the students is very efficient for this study since it is constructive for both students and the researcher. Students can participate in the study without volunteering personal data, do it at their chosen time, and stop completing it, should they choose to do so. The advantage for the researcher is that a single link is shared with all participants by their professors, and all responses are stored in one location. Moreover, the participants would be screened if they fit the criteria: those who never used smart TVs or were below 18 would exit the survey. Only those who fit the criteria are selected.

Data Collection Tool

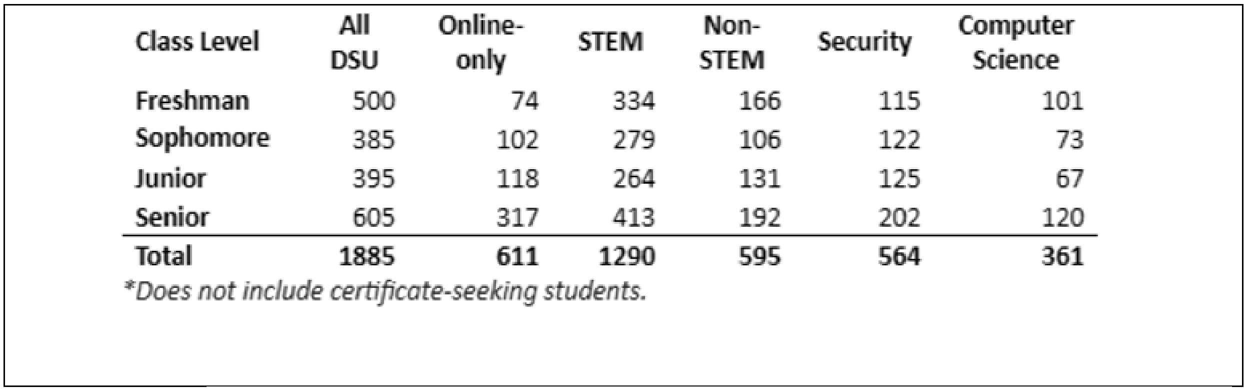
The researcher chose the paid version of Survey Monkey. It is a web-based surveying tool which is suitable for in-depth survey collection. Moreover, there was a privacy setting in the tool that would protect the privacy of all participants. Consequently, Survey Monkey became the chosen tool for building the survey for the research and assisting with survey distribution via the professors of the different departments. Finally, the number of participants who could take the survey was unlimited.

Since the survey was opened in the Fall 2022 and Spring 2023 semesters, there were concerns about duplicate entries, which was the case. Upon exporting the data from Survey Monkey, the IP addresses were included. The researcher discovered that a small proportion of students retook the survey. The earlier entries were deleted, and the most current records were kept for analysis.

The target population was undergraduate students across majors, departments, and programs. The researcher shared the survey link with her chair who then emailed it to the different department heads and professors. The survey was circulated to diverse undergraduate students from different departments and colleges. There was no interaction between the researcher and the students.

Survey Population and Sample Size

Due to limited time and resources, a small sample from the population of a small mid-western public institution of higher education will be used.



Class Level	All DSU	Online-only	STEM	Non-STEM	Security	Computer Science
Freshman	500	74	334	166	115	101
Sophomore	385	102	279	106	122	73
Junior	395	118	264	131	125	67
Senior	605	317	413	192	202	120
Total	**1885**	**611**	**1290**	**595**	**564**	**361**

**Does not include certificate-seeking students.*

Table 1. Undergraduate Fall 2022 Enrollment

The survey's sampling frame is students 18 years or older who have used or are using smart TVs, even via external devices. For the Fall 2022, the small mid-western public university had a student population of 1885 undergraduate students, with 611 being online (that number was provided by the university research office). The population size is 1885, as presented in Table 1, for Fall 2022 undergraduate students' enrollment. The number of students was determined by an on-line sample calculator: https://www.surveymonkey.com/mp/sample-size-calculator/ . The target number of students required for this research is 320, so this is the target sample size for this research to get the desired results. A sample size of 320 which is adequate to estimate the assumed 95% confidence interval with a 5% margin of error. This means 320 or more students are needed to have a confidence level of 95% that the true parameter is within ±5% of the measured/surveyed value.

Survey Administration

Survey Monkey was used for the online survey, and it was easy to use and implement. Additionally, it looked more suitable for in-depth survey design, distribution, and analysis than Google Forms. Moreover, there were some filtering options to extract distinct categories of students, and the results could be split into Excel and PDF files. Survey Monkey allowed for easy screening of the participants and their answers. In addition, the results could be customized in nice pie charts. Finally, there was no limit on the number of participants who could take the survey and the researcher could create different filters to slice and dice the data.

The researcher used a web-based survey tool, to facilitate students' ease of usage and gather their responses. There was no plan to offer any incentives to the participants willing to take the survey. Although this may have resulted in fewer participants, one reason to take that route is to protect the participants' privacy. If incentives were offered, then the emails would have to be collected. Since Survey Monkey is a third-party tool that stores the collected data in the cloud, the researcher wanted to keep information about the participants private from Survey Monkey.

The online survey collected the answers to the questions from the participants willing to participate in this research. The survey participants were students from different academic groups. No PII information was collected. The survey went live in the Fall of 2022, and data collection took seven weeks between October 17 and December 2, 2022. Since more data was needed, the survey opened again From January 18- February 11, 2023, for almost four weeks**.**

For freshmen students, the survey was offered via a freshmen course: CSC 105 course, where the students took the survey on tablets during the class. Consequently, there was a higher number of freshmen students than in the other categories.

Survey Participation

IRB approval was obtained prior to participation in the research (Appendix A). All students from any major could participate in the survey if they were above eighteen years old and used smart TVs. The researcher provided detailed information to the participants in the survey, so things were clear to them before they began the survey. The survey introduction stated that there are no participation costs, the participation is voluntary, and the participants can stop the survey at any time. Moreover, the researcher and Institutional Review Board (IRB) contact email information was displayed should the participants have any questions. Additionally, the following were covered in the survey introduction:

- Purpose of the study
- How do students participate in the survey
- Any anticipated risks for participation
- The benefits of participating
- How long and how will the information be kept?
- Statement of Consent

Survey Research and Design

The research questions were prepared, developed, and then refined by the researcher. The survey questions were modified over the period of several months, before administering it to the students, to better fit the goal of the study. The modified survey was reviewed and validated by a specific committee member who graciously offered help. This was to ensure that the survey questions addressed the research questions accurately.

The research survey's aim, as previously stated, is to examine students' security awareness while using smart TVs. In addition, a comparison between the different groups would be carried out to see if majors have an impact on students' security perceptions. Moreover, the researcher wanted to examine if being exposed to some security courses would change students' security attitudes. All the data analysis was conducted in R-Studio.

Survey Questions

There were 17 5-Lickert scale questions with responses: strongly agree/likely, agree/likely, unsure/maybe, disagree/unlikely, strongly disagree/unlikely. The survey questions were divided into three categories: knowledge, awareness, and attitude targeted to answer the two research questions. The questions are listed in Appendix C.

Data Analysis

The collected data from the Survey Monkey survey was analyzed in R-Studio to answer this research questions. There were seventeen variables of interest (outcomes), which are the seventeen survey questions. These were tested against both STEM and non-STEM students.

The researcher used the Chi-square statistic to test for the independence between outcomes (knowledge, attitude, and awareness) and research questions. Several of the outcomes had very small numbers of students' responses and had warnings for the Chi-square tests because the expected frequencies in the cells were less than five and thus the Chi-square tests were not valid. Therefore, these responses from the 17 questions were collapsed for the Chi-square test to become valid/ Answers to questions in the "Extremely Likely" (or

Extremely Agree) or “Likely” (or Agree) were combined into one category (Extremely Likely/likely or Extremely Agree/Agree). On the other hand, Extremely Unlikely and Unlikely or Extremely Disagree and Disagree values were combined into another category (Extremely unlikely/unlikely). The Unsure or maybe answers were combined into a new category: Maybe. The output from all the Chi-square tests is listed in Appendix D.

The threshold for statistical analysis was a two-sided p-value < 0.05. All reported p values are based on two sided tests. The p-value is a measure of the probability of observing a test statistic as extreme as the one computed from the sample data, assuming that the null hypothesis is true. In other words, it indicates the level of significance of the test. If the two-sided p-value is less than or equal to 0.05, then the null hypothesis is rejected, and one can conclude that there is a statistically significant difference between the outcomes and the predictors.

Logistic Regression Analysis

Logistic regression was utilized to identify predictors that played an important role in affecting students' awareness, knowledge, and attitudes. Logistic regression models were created for the outcomes that were statistically associated with STEM status and credits status. Per Edgar and Manz (2017) “logistic regression is a process of modeling the probability of a discrete outcome given an input variable. IBM defined logistic regression as a “statistical approach that is used to analyze the relationship between a dependent variable and one or more predictors. It is a regression model that is used when we want to predict the probability of an event occurring based on some predictor variables.”

The different survey questions' values were changed to binary (0 or 1) to perform the logistic regression analyses, where 1 represents the response of strongly agree/disagree and 0 is otherwise. Models were created for the different survey questions in R using the glm (generalized linear model) function. The threshold for statistical significance was considered as 0.05. The list of all the models and the output from R are presented in Appendix E. The predictors that were considered were: age group (AGeGRoup) credits (creditlb), STEM status (major), and security courses (SecCourses).

AgeGRoup is the age range of the participating students. This was collected as a categorical variable in the survey.

- AGeGRoupC 1: were students in the 18-21 age group and were assigned a value 1.
- AGeGRoupC 2: were students in the 22-25 age group and were assigned a value of 2.
- AGeGRoupC 3: were students in the 26-30 age group have a value of 3.
- AGeGRoupC 4: were students in the 31-34 age group and were assigned a value of 4.
- AGeGRoupC 5: were students in 35+ age group and were assigned a value 5.

Note. AGeGRoupC 1 was the referent and AGeGRoupC 2-5 were combined later for better results as the glm model was not converging appropriately.

Creditlb is the number of credits students have taken at the time of the survey. Freshmen and sophomore categories were combined into one group and were assigned the value of zero (referent) whereas junior and senior students were combined into another category and were assigned the value of one.

STEM is the STEM status, where STEM students in any of the various majors in Beacom College, Mathematics or Science. Non-STEM students are all the students who are in the other majors and their binary value is zero (referent). The binary value for STEM Students is one in the model.

SecCourses: is the number of security courses that the participating students took:

- SecCourses 0: students took zero security courses.
- SecCourses 1: students took one security course.
- SecCourses 2: students took two security courses.
- SecCourses 3: students took three security courses.
- SecCourses 4: students took four or more security courses.

The number of courses was categorized as a binary predictor due to converging issues in the glm function and category 0 was the referent.

Chapter Summary

In this chapter, the methodology chosen for this research and the survey platform were discussed, along with the sample size needed for this research. The aim of the study was to investigate two groups of students' behavior at a small mid-western public institution of higher education while using smart TVs. Those groups are STEM versus non-STEM and junior/seniors versus freshmen/sophomore. The survey asked in-depth questions to examine if students were affected in their security awareness knowledge, behavior, and attitude due to being enrolled in STEM programs or being in higher classes. In the next chapter, the results of the survey questions will be presented.

CHAPTER 4

RESEARCH ANALYSIS AND RESULTS

This quantitative research examined the security and privacy awareness of a small mid-western public university where the survey participants were undergraduate students who dealt or are dealing with smart TVs. A survey was performed on the undergraduate student population across majors. The survey questions were targeted to answer the research questions and to examine the security behavior and mindset of the participants.

In this chapter, the researcher discusses the survey population. Moreover, the findings of the study will be presented.

Survey Population

For the Fall of 2022, the university had a student population of 1885 undergraduate students, including 611 online students. However, the survey did not capture if students were online or attending campus.

For STEM, there were a total of 1290 undergraduate enrolled students for the Fall 2022 which constituted 68% of total undergraduate enrollment. For Non-STEM there were a total of 595 students which constitute 32% of total undergraduate enrollment, (Table 1, Chapter 3).

258 STEM students participated in the survey which was 20% of the total STEM student population (Table 2). 122 non-STEM students participated in the survey which was 21% of the total non-STEM student population. Although STEM student’s enrollment for Fall

2022 was double that of non-STEM, the participants from the two groups: STEM and Non-STEM were comparable: 20% versus 21%.

On the other hand, of the 1290 STEM enrolled students, 613 freshmen and sophomores versus 677 junior and senior students. Computer Science and Security constitute around 72% of the total enrolled STEM students. Of the 595 non-STEM students, 272 were freshmen and sophomores versus 323 junior and senior students, Chapter 3, Table 1.

Survey Details

The details of the survey were such:

- For the Fall semester 2022 the survey was opened from: 10/19/2022- 12/04/2022, 335 participants started the survey, with 204 STEM (31 did not complete it) and 131 non-STEMS (16 did not complete it).
- For the Spring semester of 2023 the survey was opened in this time interval: Spring: 1/19/2023-2/12/2023: 120 participants started the survey, with 107 STEM and 13 non-STEM.
- 312 STEM students started the survey, and 258 completed it.
- 143 non-STEM students started the survey, and 122 completed it.
- A total of 380 students completed the survey, the sample size is 320.

Survey information

- 455 started the survey, but 380 completed it. Incomplete responses were discarded and not included in the data analysis.
- Completion rate was 84%, time to take the survey was 6 minutes and 2 seconds, Figure 3

- Seventy-five participants did not complete the survey. The breakdown of those students was. as follows:
  a. Forty participants did not complete the questions; hence these records were removed from the data analysis.
  b. Twenty-six students have not used Smart TVs, even through external devices, so they exited the survey.
  c. Two students were under eighteen, so they exited automatically.
  d. Seven students retook the survey in Spring 2023; the older records of Fall 2022 were deleted and the most recent was kept, which was apparent by the IP address that was captured by Survey Monkey.

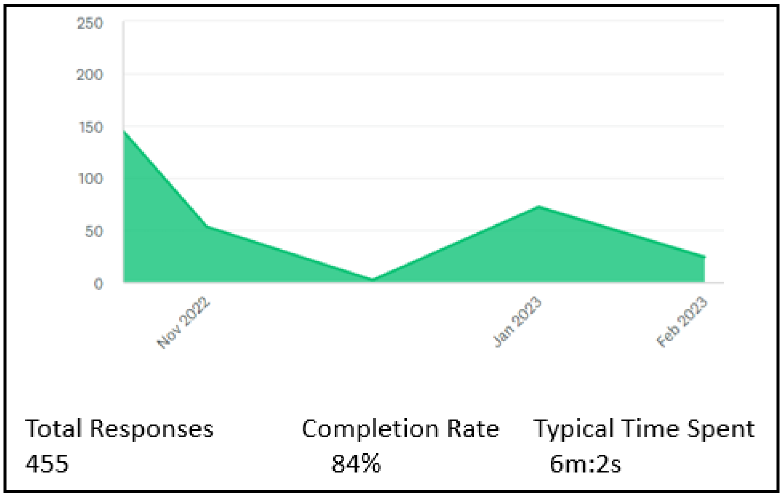


Figure 2. Survey Statistics

Survey Demographics

Participants Age

Age was collected as a categorical variable. The distribution of participants by a groups is presented in Figure 3. The breakdown of the age participants was as such:

- 324 participants in the 18-21 age group started the survey, but only 274 (72%) participants completed the survey.
- 63 participants in the 22-25 age group started the survey, of which 53 (14%) completed it.
- 20 participants in the 26-30 age group started the survey, of which 19 (5%) completed it.
- 19 participants in the 35 age group started the survey, of which 19 (5%) completed it.
- 27 participants in the 31-34 age group started the survey, of which 15 (4%) completed it.

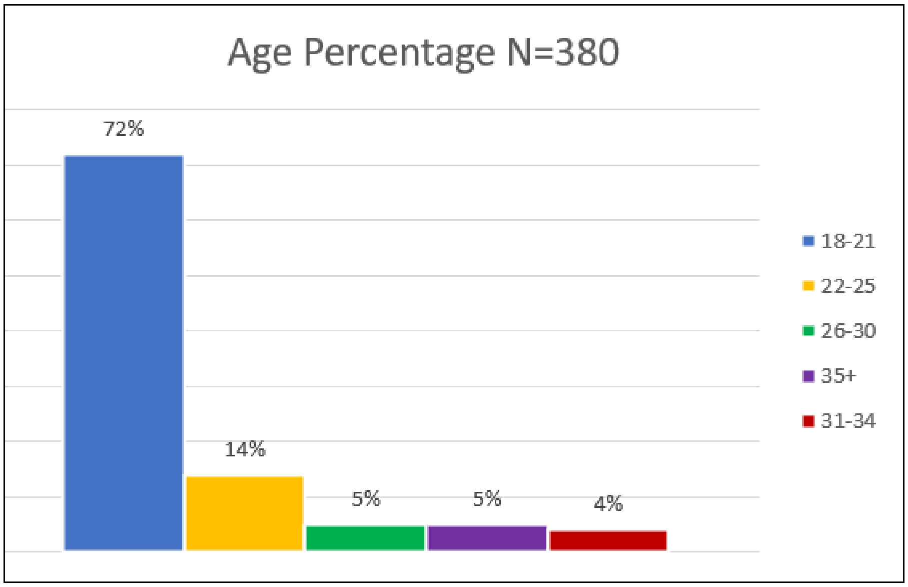


Figure 3. Participants' Age

Participants Majors

Survey participants were asked to choose their major. The results did not lead to a fair distribution among all majors. The four highest ranking majors reported are shown in Figure 4. : Forty percent were computer science majors, twenty-five percent were security, eleven percent were business and around eight percent (30 participants) were education majors.

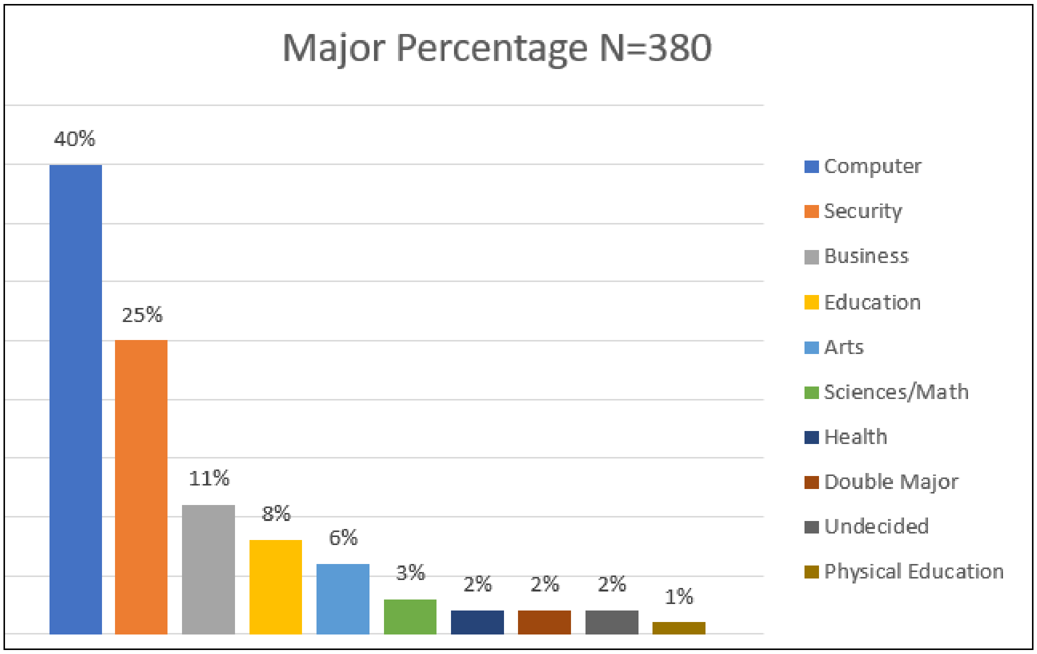


Figure 4. Participants' Major

Participants STEM Non-STEM

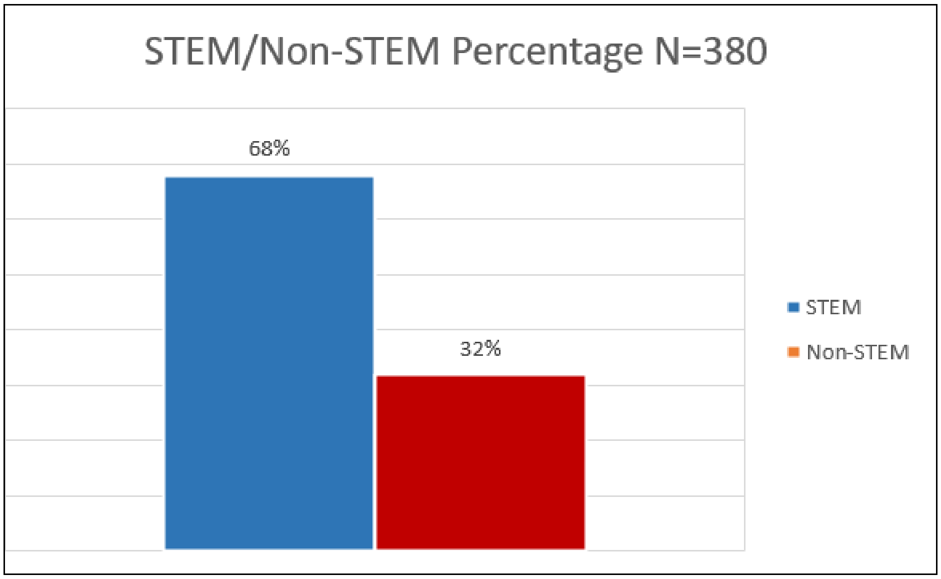


Figure 5. Participants' STEM/Non-STEM

The bar plot in Figure 5 presents the percent distribution of students by STEM status. Sixty-eight percent (258) were STEM, versus thirty-two percent (122) non-STEM students.

Participants Credit Hours

The percentage breakdown of each category is shown in Figure 6. The largest category was freshmen students, which was expected since the survey was offered to freshmen students in their first-year course: via a GS 100 course. Per the university's catalog this course involves students in group discussions so that they "develop critical thinking and social interaction skills to prepare them for the academic environment."

A total of 38% (144) freshmen students completed the survey followed by 28% (106) seniors, then 22% (84) juniors, and 12% (46) sophomores. Combining the freshmen with sophomores (190 in total, 50%), and juniors with seniors (190, 50%), ended in a fair split among participants' credit hours.

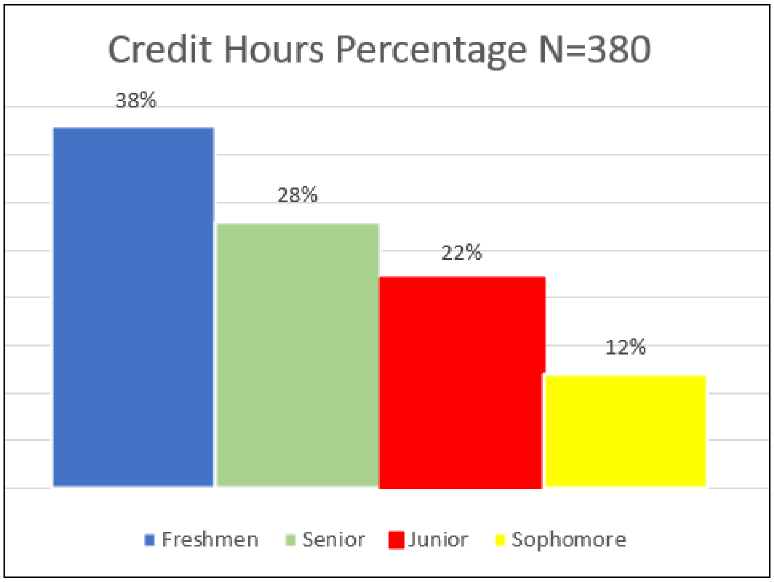


Figure 6. Participants' Credit Hours

Participants' Security/Privacy Courses

The breakdown of the question was as follows, Figure 7:

1. 148(30%) of the participants did not take any security or privacy courses, which was expected since a lot of freshmen students took the survey.
    a. 31% of STEM students did not take any security or privacy courses
2. 72 students (19%) took one course
3. 57 students (15%) took two courses
4. 31 students (8%) took three courses
5. 72 students (19%) took four or more courses

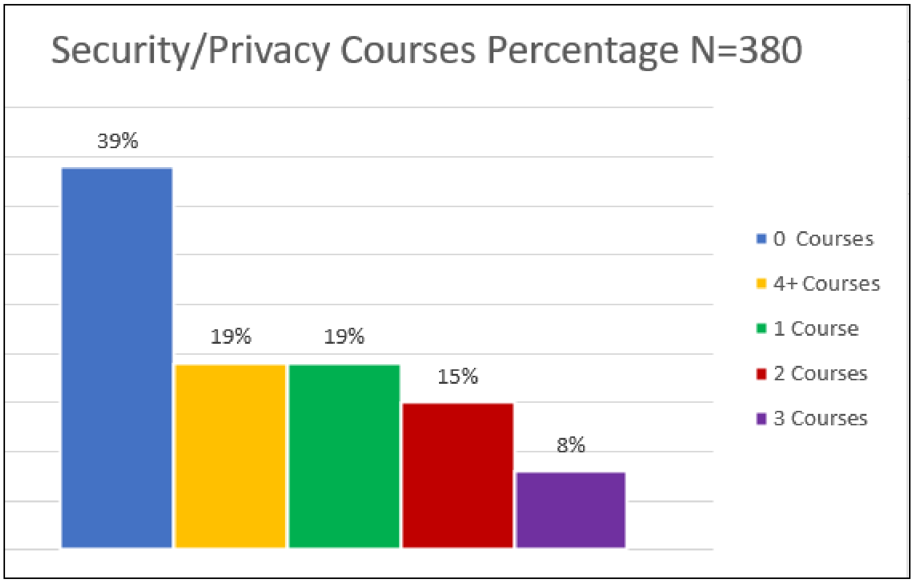
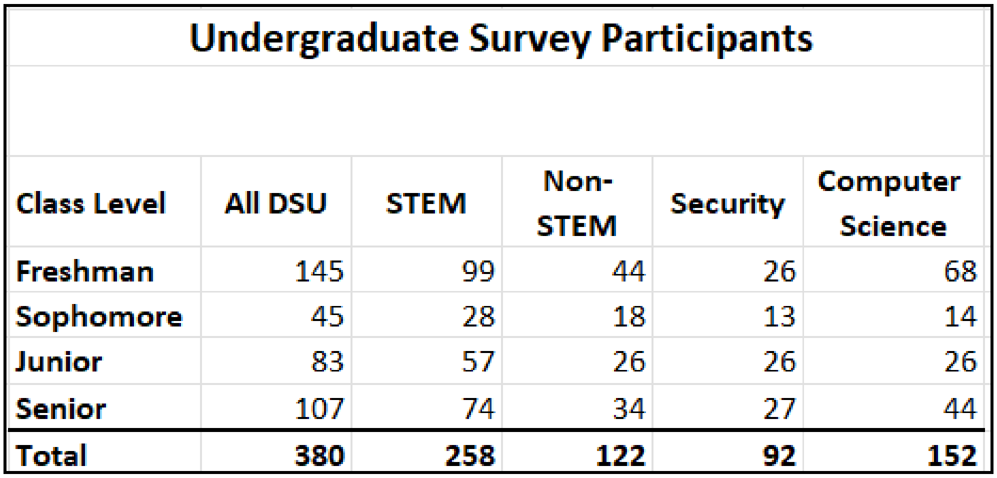


Figure 7. Participants' Security/Privacy Courses

Out of 258 STEM Students, 31% (80) students did not take any security/privacy courses and 69% (178) students took one or more security or privacy courses. Of the 178 (69%) STEM students, 92 (36%) were security majors and 152 (59%) were computer majors, Table 2. Almost 50% of the 92 security students took four or more security courses. The breakdown was as follows:



Undergraduate Survey Participants

Class Level	All DSU	STEM	Non-STEM	Security	Computer Science
Freshman	145	99	44	26	68
Sophomore	45	28	18	13	14
Junior	83	57	26	26	26
Senior	107	74	34	27	44
Total	**380**	**258**	**122**	**92**	**152**

Table 2. Undergraduate Survey Participants

- Security Total: 92 (Table 2)

  - Freshmen/sophomores: 39 students
  - Junior/senior: 53 students
  - 42 (46%) students took 4 courses or more
- Computers Total: 152
  - Freshmen/sophomores: 82 students
  - Junior/Senior: 70 students
  - 19 (13%) students took one sec/privacy class
- Sciences/Math Total: 14
  - Freshmen/sophomore: 7 students
  - Junior/Senior: 7 students

Non-STEM Participants

122 (32% of 380 participants) non-STEM students completed the survey, (Table 2). The breakdown was as follows:

- Business: 40 students.
  - Freshmen/sophomores: 11 students
  - Junior/senior: 19 students
- Education: 30 students.
  - Freshmen/sophomores: 17 students
  - Junior/senior: 13 students
- Arts: 23 students.
  - Freshmen/sophomores: 18 students
  - Junior/senior: 5 students
- Other Majors*: 29 students.

- Freshmen/sophomores: 16 students
- Junior/senior: 13 students

* General, Health, Physical Education, Undecided, Double Major

For the 122 non-STEM students, 53 (43% of 122) students took security/privacy courses. Of the 53 students, 18 students were freshmen/sophomore and 35 were junior/senior.

- 26 students took 1 course, 10 students were business major
- 14 students took 2 courses, half of these were business majors as well
- 7 students took 3 courses, 3 of which were business major
- 6 students took 4 courses, 3 of these were double major

Percent Responded Strongly Agree/Agree by Questions

In this section the percent distribution of students who responded strongly agree/agree on their outcomes are presented by knowledge, awareness and attitude.

Knowledge Questions

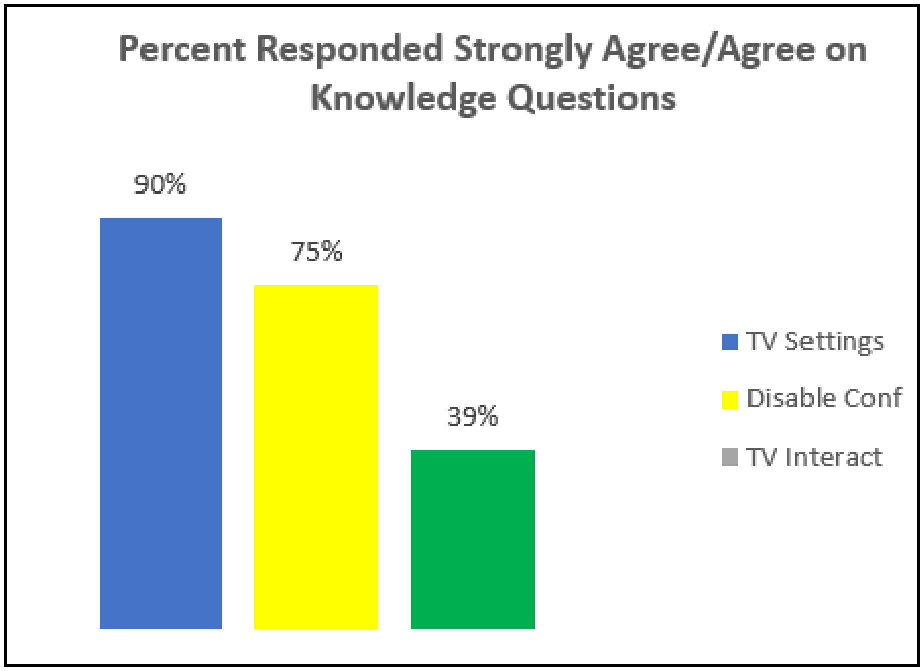


Figure 8. Percent Responded Strongly Agree/Agree on Knowledge Questions

As shown in Figure 8, 90% and 75% of students responded strongly agree/agree on 2 out of 3 knowledge questions. This shows that overall students had high levels of knowledge about smart TV settings and how to change them.

Awareness Questions

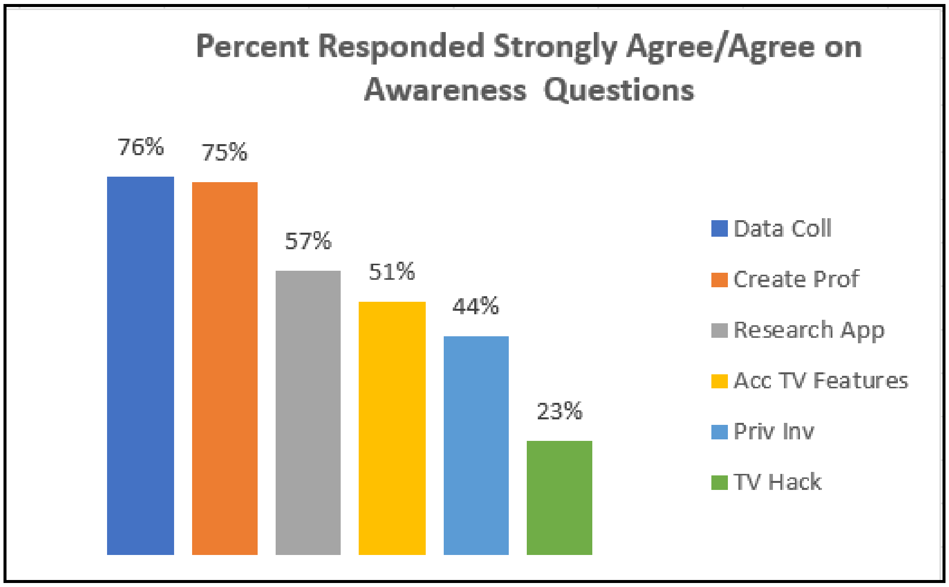


Figure 9. Percent Responded Strongly Agree/Agree on Awareness Questions

In general, at least 50% students reported strongly agree/agreed on 4 out of the 6 on the awareness questions (Figure 9).

Attitude Questions

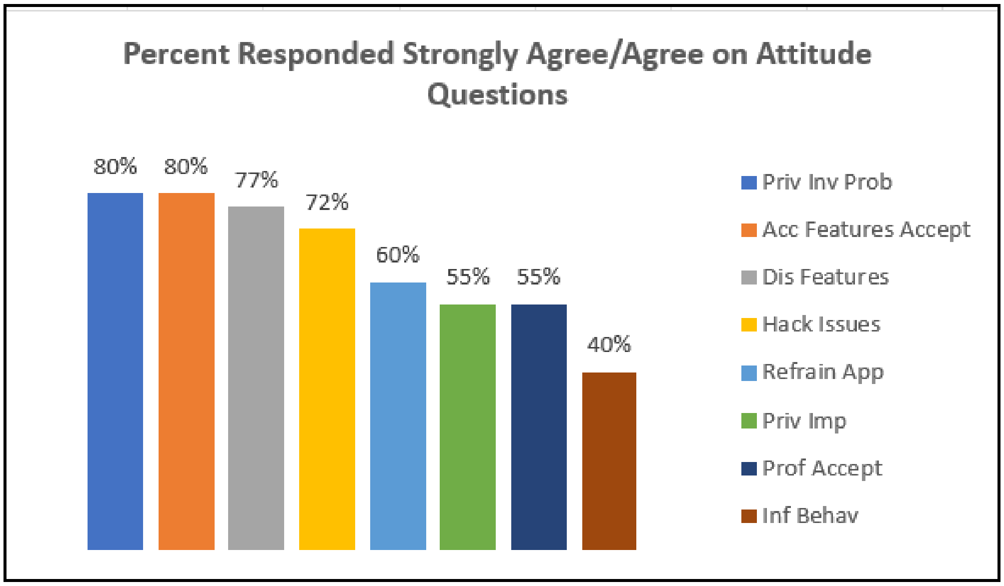


Figure 10. Percent Responded Strongly Agree/Agree on Attitude Questions

In general, at least 55% of students responded strongly agree/agree for 7 out of the 8 attitude questions (Figure 10). The only question that had a low proportion is expected since it questioned the participants if the security or privacy courses that they took influenced their behavior and most non-Stem and some freshmen STEM would have answered not applicable.

Research Questions 1 Results and Analysis

RQ1: Does security awareness (STEM programs) positively influence students' likelihood of adopting security best practices (knowledge, attitude, awareness) while using smart TVs?

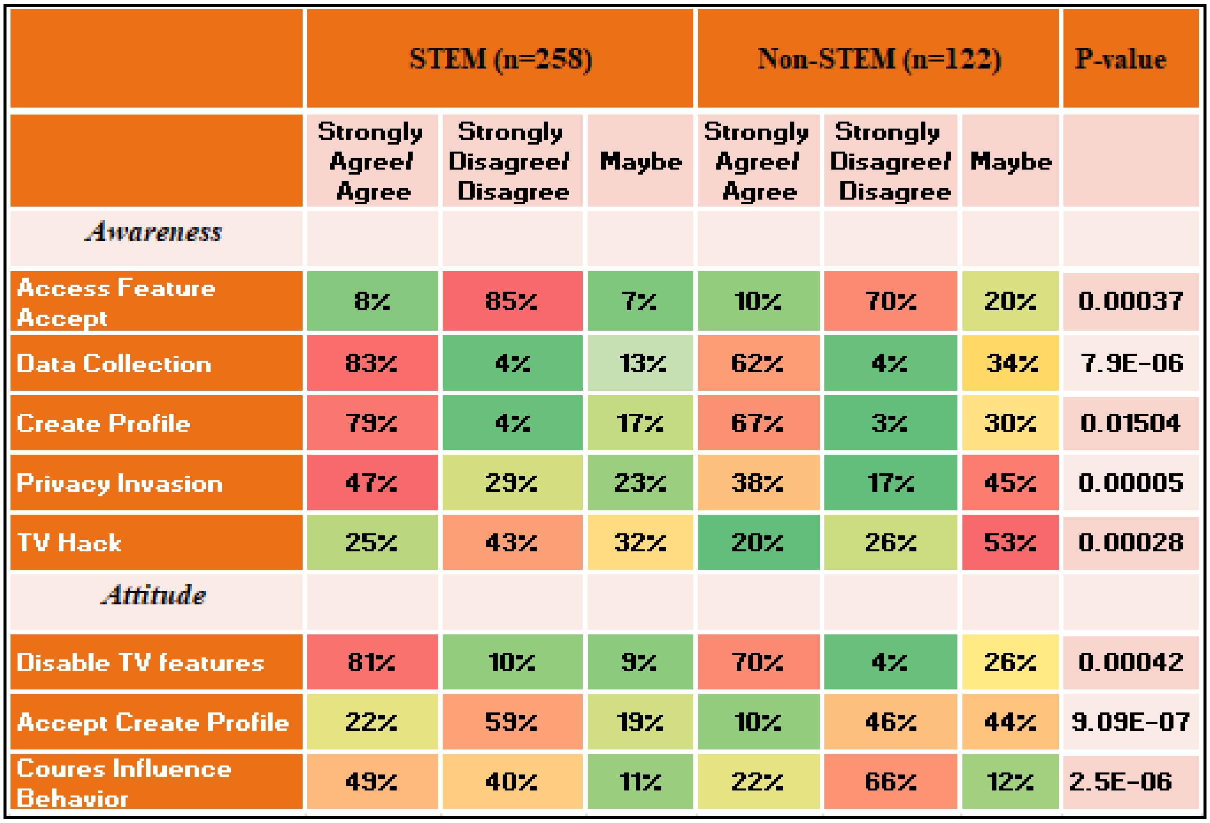
The analysis is based on 380 participants of which 122 were non-STEM (32%) and 258 (68%) were STEM students. Those two categories were not balanced, the STEM category was double that of the non-STEM.

STEM student status for research question one was tested for the 17 survey questions. Eight of the survey questions showed that there was an association between the question (outcome) and STEM status. The following was observed:

The percentage was higher for the STEM students which showed that the knowledge and awareness of STEM students are higher than those of non-STEM students because they took security and privacy courses (Table 3). However, when participants were asked about their privacy, STEM and non-STEM students claimed that they care about their privacy, and it would be “problematic for their privacy to be invaded” which echoes what is there is previous work. When further asked if they were willing to disable the camera and audio features of their smart TVs to protect their privacy, the percentage were close for STEM and non-STEM students.

When asked if they research third-party apps and refrain from installing third-party applications on their smart TVs, STEM students (62%) were 12% ahead of non-STEM students (50%). What was interesting to note was when students were asked if protecting their privacy was more important than using smart TV features; there was a drop in percentage for both STEM and non-STEM students by almost 30%. There was a visible disconnect between caring about privacy and protecting it for both STEM and non-STEM students. There is no tangible agreement between knowing and being aware of smart TV security issues and privacy attitudes. This is known as the Privacy Paradox which was noted in some literature. In a study by Ghiglieri et al. (2017), the researchers claimed that even by raising users’ awareness of smart TV dangers, users cared more for TV functionality than protecting their privacy. Yet in another research by Aleisa et al. (2017), users were concerned about their privacy “invasions," but cared more for smart TVs. However, in her dissertation, Alqarni

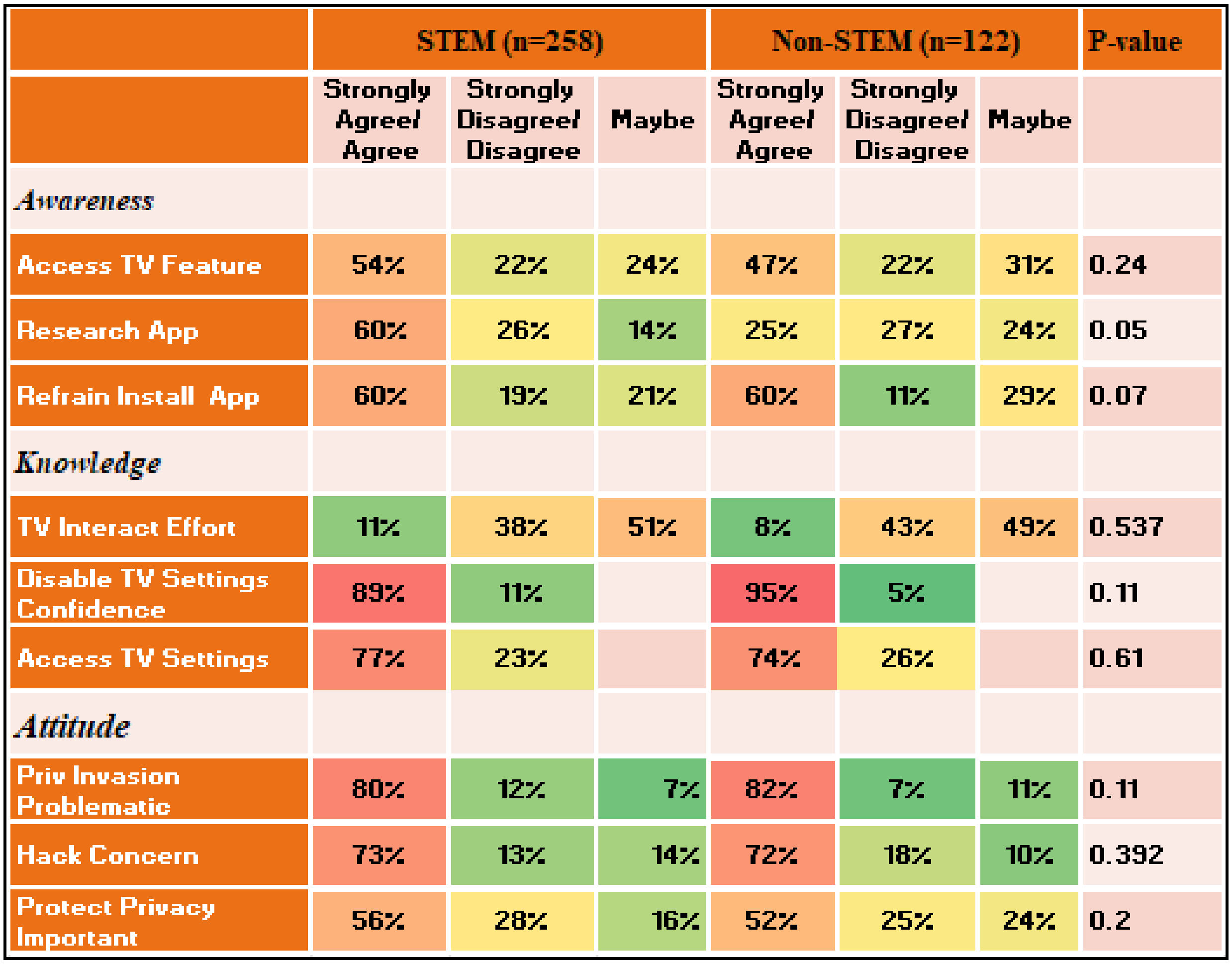
(2017), indicated that when students feel threatened, they will take protective measures to secure their privacy. Furthermore, she explained that it is up to the university administration to develop easy methods to teach students how to protect themselves from security threats.



	STEM (n=258)			Non-STEM (n=122)			P-value
	Strongly Agree/ Agree	Strongly Disagree/ Disagree	Maybe	Strongly Agree/ Agree	Strongly Disagree/ Disagree	Maybe	
Awareness							
Access Feature Accept	8%	85%	7%	10%	70%	20%	0.00037
Data Collection	83%	4%	13%	62%	4%	34%	7.9E-06
Create Profile	79%	4%	17%	67%	3%	30%	0.01504
Privacy Invasion	47%	29%	23%	38%	17%	45%	0.00005
TV Hack	25%	43%	32%	20%	26%	53%	0.00028
Attitude							
Disable TV features	81%	10%	9%	70%	4%	26%	0.00042
Accept Create Profile	22%	59%	19%	10%	46%	44%	9.09E-07
Coures Influence Behavior	49%	40%	11%	22%	66%	12%	2.5E-06

Table 3. Research Question 1 Statistically Significant Outcomes by STEM Status

Table 3 presents, the statistically significant results for the eight survey questions (two-sided p-value < 0.05) by STEM status, which implies there was an association between those survey questions and STEM status (being a STEM student). In general, there was a positive trend where STEM students have higher awareness and attitude than non-STEM students.

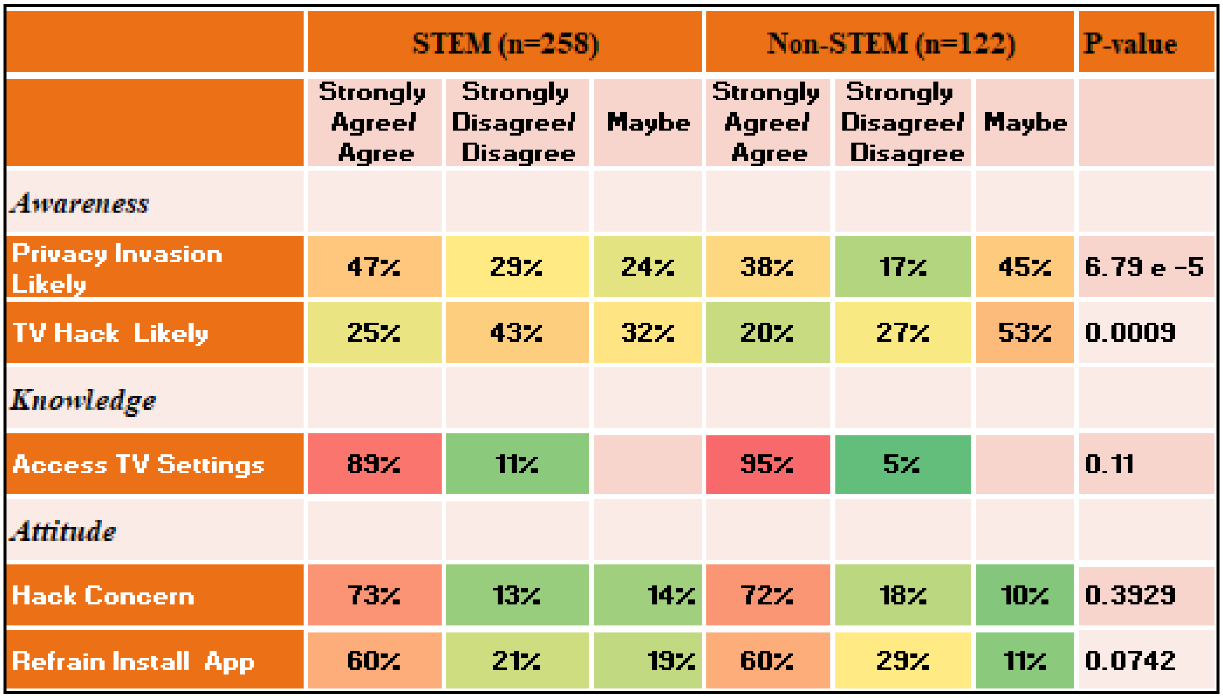


	STEM (n=258)			Non-STEM (n=122)			P-value
	Strongly Agree/ Agree	Strongly Disagree/ Disagree	Maybe	Strongly Agree/ Agree	Strongly Disagree/ Disagree	Maybe	
Awareness							
Access TV Feature	54%	22%	24%	47%	22%	31%	0.24
Research App	60%	26%	14%	25%	27%	24%	0.05
Refrain Install App	60%	19%	21%	60%	11%	29%	0.07
Knowledge							
TV Interact Effort	11%	38%	51%	8%	43%	49%	0.537
Disable TV Settings Confidence	89%	11%		95%	5%		0.11
Access TV Settings	77%	23%		74%	26%		0.61
Attitude							
Priv Invasion Problematic	80%	12%	7%	82%	7%	11%	0.11
Hack Concern	73%	13%	14%	72%	18%	10%	0.392
Protect Privacy Important	56%	28%	16%	52%	25%	24%	0.2

Table 4. Research Question 1 Statistically Non-Significant Outcomes by STEM Status

Table 4 presents the remaining nine questions which were not statistically significant (two-sided p-value > 0.05), which implies there was no association between those questions and being a STEM student.

However, there were some unexpected results by STEM status, where the values Strongly Agree/Agree for STEM students were close to non-STEM or even less than the non-STEM students. This is evident in Table 5.



	STEM (n=258)			Non-STEM (n=122)			P-value
	Strongly Agree/ Agree	Strongly Disagree/ Disagree	Maybe	Strongly Agree/ Agree	Strongly Disagree/ Disagree	Maybe	
Awareness							
Privacy Invasion Likely	47%	29%	24%	38%	17%	45%	6.79 e -5
TV Hack Likely	25%	43%	32%	20%	27%	53%	0.0009
Knowledge							
Access TV Settings	89%	11%		95%	5%		0.11
Attitude							
Hack Concern	73%	13%	14%	72%	18%	10%	0.3929
Refrain Install App	60%	21%	19%	60%	29%	11%	0.0742

Table 5. Unexpected Results for Outcomes by STEM Status

Research Questions 2 Results and Analysis

RQ2: Do the two groups junior/senior and freshmen/sophomore students differ considerably in their security awareness, attitude, and knowledge?

This question's hypothesis states that junior/senior students are more advanced than freshmen/sophomore students in their security awareness, attitude, and knowledge due to the first groups' exposure to security courses.

Of the 380 participants students, 38% were freshmen, 12% were sophomores, 22% were juniors and 28% were seniors. Juniors and seniors were grouped into one category. On the other hand, freshmen and sophomore students were combined into another one, as the assumption is that these students may not be exposed to security and privacy courses, unlike the juniors and seniors. Each category included 190 students. Similar to research question one, the Chi-square was used to test for the independence between the main outcomes of interest (17 questions in knowledge, awareness, and attitude) and freshmen/ sophomore and juniors/senior. Eleven out of 17 survey questions showed that there was a statistically significant association between the research question and the Credits student status, (Table 5).

Knowledge and Awareness

When participants were asked if their privacy would be invaded, 54% of juniors/seniors reported strongly agree/agree versus 36% of freshmen/sophomores. Moreover, 20% of juniors/seniors answered "maybe," while freshmen/sophomores answer was double that of them. Furthermore, when they questioned whether their TV would be hacked, that percentage dropped: the answers to strongly agree/agree were 28% for juniors/seniors, and 19% for freshmen/sophomores. This decline in percentage may be because the junior/senior students are exposed to security and privacy classes and know how to protect their smart TVs, while freshmen/sophomore students were not exposed to that.

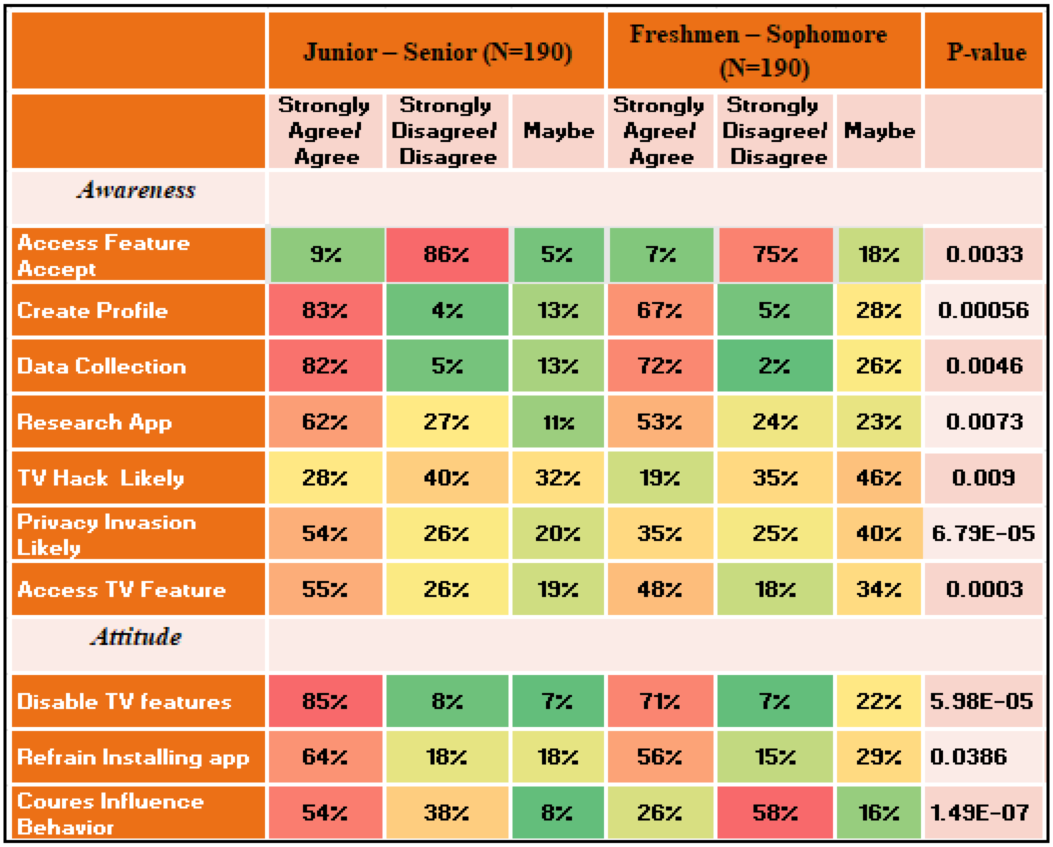
When students were asked about smart TV features and whether others could access them, 55% percent of juniors/seniors students indicated strongly agree/agree vs. 48% of freshmen/sophomores, and 19% and 34% answered "maybe" for juniors/seniors and freshmen/sophomores, respectively.

Furthermore, when asked if TV manufacturers will collect data from their home IoT devices and then create detailed profiles of their habits, 82% and 83% for junior/senior, 72% and 67% responded strongly agree/agree for freshmen/sophomores. Further research is needed to investigate if this difference is due only to the fact that those students in juniors/seniors did take security or privacy classes.

Attitude

When asked if they would consider disabling TV features to protect their safety, 85% of juniors/seniors confirmed that they would do it versus 71% of freshmen/sophomore. When further asked if they would research the safety of third-party apps before installing them, 62% answered " strongly agree/agree" and 11% "maybe" for juniors/seniors , while the percentages for freshmen/sophomores were 53% and 23%, respectively. When asked about their abstaining from using third-party applications on their smart TV, 64% answered " strongly agree/agree" and 18% "maybe" for juniors/seniors , while the percentages for freshmen/sophomore were 56% and 29%.

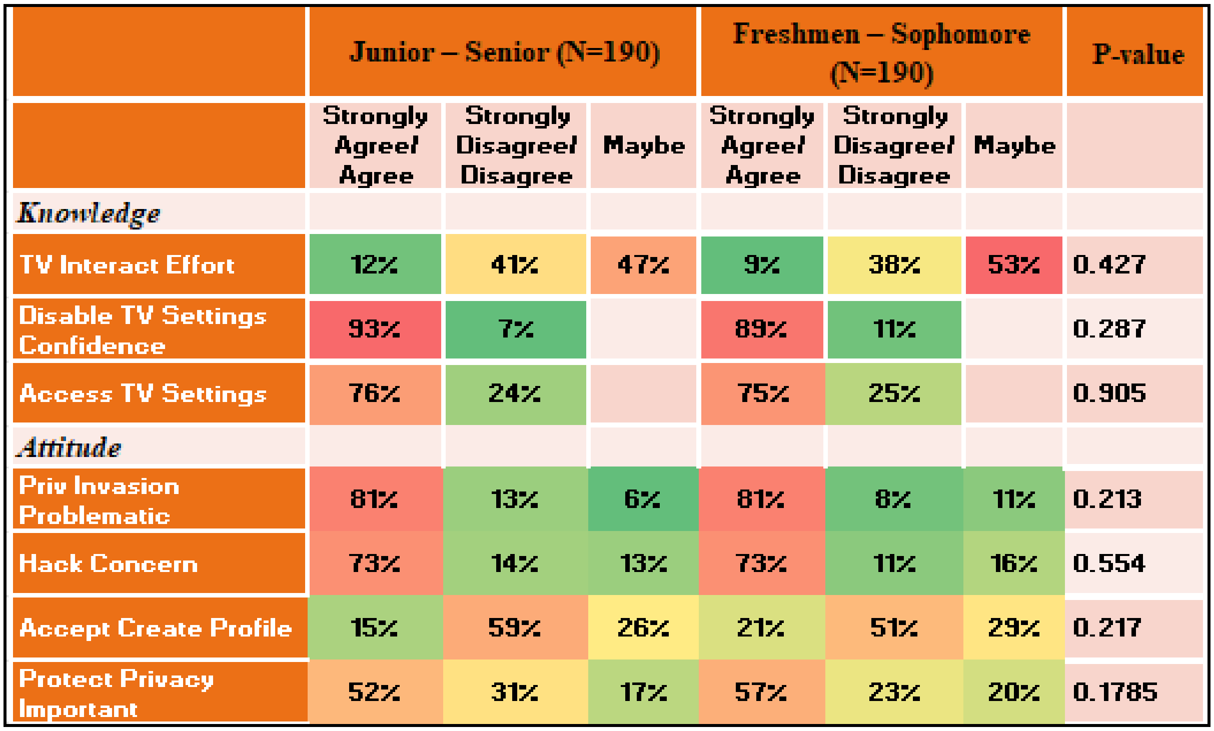
Overall, the percentages were higher for juniors/seniors students, which showed that the knowledge and awareness of these students were higher than those of freshmen/sophomore because it indicates how many security courses they took. Similar results were observed with STEM and non-STEM.



	Junior – Senior (N=190)			Freshmen – Sophomore (N=190)			P-value
	Strongly Agree/ Agree	Strongly Disagree/ Disagree	Maybe	Strongly Agree/ Agree	Strongly Disagree/ Disagree	Maybe	
Awareness							
Access Feature Accept	9%	86%	5%	7%	75%	18%	0.0033
Create Profile	83%	4%	13%	67%	5%	28%	0.00056
Data Collection	82%	5%	13%	72%	2%	26%	0.0046
Research App	62%	27%	11%	53%	24%	23%	0.0073
TV Hack Likely	28%	40%	32%	19%	35%	46%	0.009
Privacy Invasion Likely	54%	26%	20%	35%	25%	40%	6.79E-05
Access TV Feature	55%	26%	19%	48%	18%	34%	0.0003
Attitude							
Disable TV features	85%	8%	7%	71%	7%	22%	5.98E-05
Refrain Installing app	64%	18%	18%	56%	15%	29%	0.0386
Coures Influence Behavior	54%	38%	8%	26%	58%	16%	1.49E-07

Table 6. Research Question 2 Statistically Significant Outcomes by Credits

Table 6 presents the ten questions which were statistically significant by credit status (two-sided p-value < 0.05). This implies there was an association between those ten questions and credits status.



	Junior – Senior (N=190)			Freshmen – Sophomore (N=190)			P-value
	Strongly Agree/ Agree	Strongly Disagree/ Disagree	Maybe	Strongly Agree/ Agree	Strongly Disagree/ Disagree	Maybe	
Knowledge							
TV Interact Effort	12%	41%	47%	9%	38%	53%	0.427
Disable TV Settings Confidence	93%	7%		89%	11%		0.287
Access TV Settings	76%	24%		75%	25%		0.905
Attitude							
Priv Invasion Problematic	81%	13%	6%	81%	8%	11%	0.213
Hack Concern	73%	14%	13%	73%	11%	16%	0.554
Accept Create Profile	15%	59%	26%	21%	51%	29%	0.217
Protect Privacy Important	52%	31%	17%	57%	23%	20%	0.1785

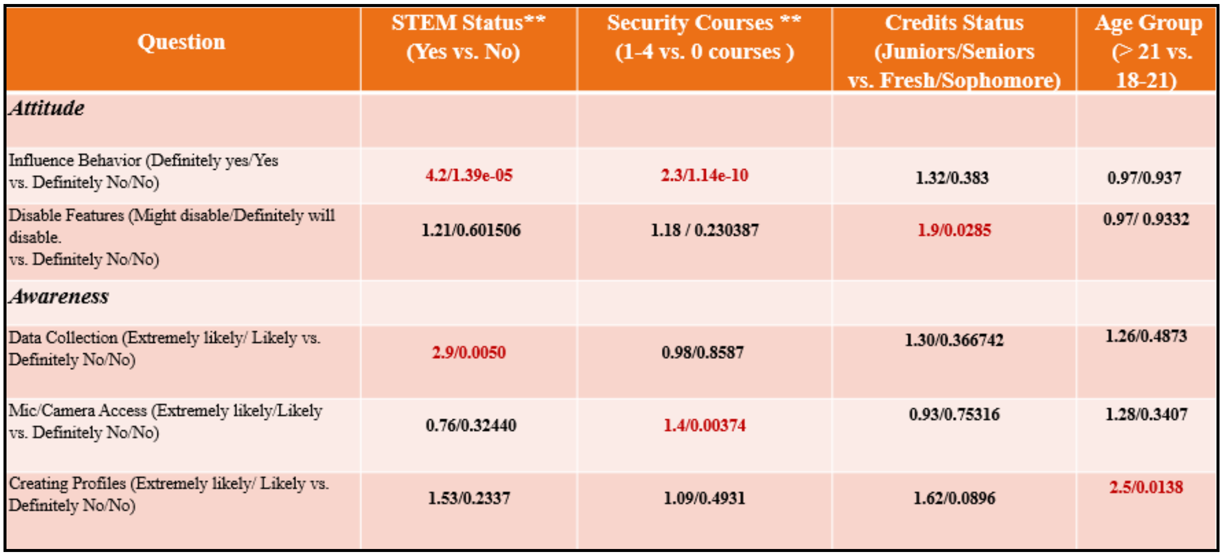
Table 7. Research Question 2 Statistically Non-Significant Outcomes by Credits

Table 7 presents the remaining seven questions that were not significant two-sided (p-value > 0.05) which mean there was no association between those questions and credits status.

Logistic Regression Results and Analysis

The previous analyses described the differences between STEM and credits (research questions 1 & 2) for each of the 17 questions. The logistic regression was used to assess the relationship between the outcomes (awareness, knowledge, and attitudes) and the independent predictors (STEM status, credits, security courses, and age). As previously mentioned, the logistic regression is a statistical model that is used with several variables (predictors) that predict the probability of an event occurring based on a given dataset of independent variables.

Here the researcher reports the results from the logistic regression analyses for the statistically significant predictors of the awareness, knowledge, and attitudes questions. Five logistic regression models had at least one statistically significant predictor of outcomes.



Question	STEM Status** (Yes vs. No)	Security Courses ** (1-4 vs. 0 courses)	Credits Status (Juniors/Seniors vs. Fresh/Sophomore)	Age Group (> 21 vs. 18-21)
Attitude				
Influence Behavior (Definitely yes/Yes vs. Definitely No/No)	4.2/1.39e-05	2.3/1.14e-10	1.32/0.383	0.97/0.937
Disable Features (Might disable/Definitely will disable. vs. Definitely No/No)	1.21/0.601506	1.18 / 0.230387	1.9/0.0285	0.97/ 0.9332
Awareness				
Data Collection (Extremely likely/ Likely vs. Definitely No/No)	2.9/0.0050	0.98/0.8587	1.30/0.366742	1.26/0.4873
Mic/Camera Access (Extremely likely/Likely vs. Definitely No/No)	0.76/0.32440	1.4/0.00374	0.93/0.75316	1.28/0.3407
Creating Profiles (Extremely likely/ Likely vs. Definitely No/No)	1.53/0.2337	1.09/0.4931	1.62/0.0896	2.5/0.0138

Table 8. Odds Ratios/P-values from Statistically Significant Predictors from Logistic ***Regression Analysis***

The result for the statistically significant logistic regression is as follows:

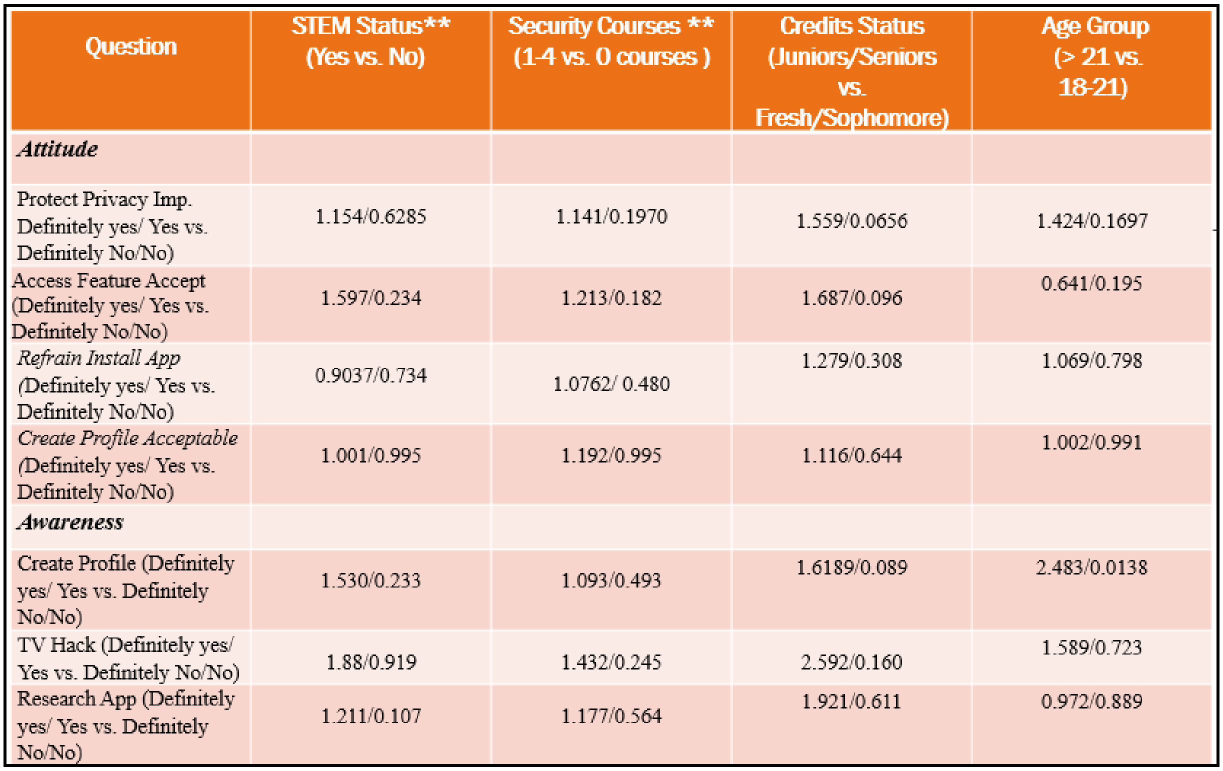
In a multivariable logistic regression model where the question is : did the security/privacy course(s) that you took influence you to have a more proactive security behavior to protect your privacy, both STEM status and security course were statistically significant predictors of this outcome (Table 8). STEM students were 4.2 (3rd row 2nd column) times more likely than non-STEM students to report strongly agree/agree that the courses they took definitely yes/yes influenced their behavior proactively to protect their privacy. Students who took 1-4 security classes were 2.3 (3rd row, 3rd column) more likely than students who did not take any security classes to indicate that the courses they took definitely yes/yes influenced their behavior. Age and credits status did not impact this outcome.

In a second logistic regression model where the outcome is disabling TV features to protect their safety, seniors/junior students were 1.9 (4th row, 4th column) times more likely than freshmen and sophomores to report that the courses they took influenced their behavior to protect their privacy to report that they might disable/will definitely disable the TV feature (Table 8). However, STEM status, security courses and age did not impact this outcome.

In third logistic regression model where the outcome is TV manufacturers will collect data from their home devices, STEM students were 2.9 (6th row, 2nd column) more likely than non-STEM students to respond extremely likely/likely (Table 8). However, credit status, security courses and age did not impact this outcome.

In the fourth logistic regression model where the outcome is microphone/camera, students who took 1-4 security classes were 1.4 (7th row, 3rd column) more likely than students who did not take any security classes to respond extremely likely/likely (Table 8). However, STEM status, credit status, and age, did not impact this outcome.

In the logistic regression model where the outcome is TV manufacturers will create profiles, students older than 21 were 2.5 (8th row, 5th column) more likely than <21 years students to respond extremely likely/likely (Table 8). However, STEM status, credits status, and security courses did not impact this outcome.



Question	STEM Status** (Yes vs. No)	Security Courses ** (1-4 vs. 0 courses)	Credits Status (Juniors/Seniors vs. Fresh/Sophomore)	Age Group (> 21 vs. 18-21)
Attitude				
Protect Privacy Imp. Definitely yes/ Yes vs. Definitely No/No)	1.154/0.6285	1.141/0.1970	1.559/0.0656	1.424/0.1697
Access Feature Accept (Definitely yes/ Yes vs. Definitely No/No)	1.597/0.234	1.213/0.182	1.687/0.096	0.641/0.195
Refrain Install App (Definitely yes/ Yes vs. Definitely No/No)	0.9037/0.734	1.0762/ 0.480	1.279/0.308	1.069/0.798
Create Profile Acceptable (Definitely yes/ Yes vs. Definitely No/No)	1.001/0.995	1.192/0.995	1.116/0.644	1.002/0.991
Awareness				
Create Profile (Definitely yes/ Yes vs. Definitely No/No)	1.530/0.233	1.093/0.493	1.6189/0.089	2.483/0.0138
TV Hack (Definitely yes/ Yes vs. Definitely No/No)	1.88/0.919	1.432/0.245	2.592/0.160	1.589/0.723
Research App (Definitely yes/ Yes vs. Definitely No/No)	1.211/0.107	1.177/0.564	1.921/0.611	0.972/0.889

Table 9. Odds Ratios/P-values from Statistically Non-Significant Predictors from Logistic Regression

Table 9 presents the odds ratios that were not statistically significant of the seven outcomes.

There was a visible disconnect between caring about privacy and protecting it for both STEM and non-STEM students. There is no tangible agreement between knowing and being aware of smart TV security issues and privacy attitudes. This is known as the Privacy Paradox which was noted in some literature. In a study by Ghiglieri et al. (2017), the researchers claimed that even by raising users' awareness of smart TV dangers, users cared more for TV functionality than protecting their privacy. Yet in another research by Aleisa et al. (2017), users were concerned about their privacy "invasions," but cared more for smart TVs. However, in her dissertation, Alqarni (2017), mentioned that when students feel threatened, they will take protective measures to secure their privacy. She mentioned that it is up to the university administration to develop easy methods to teach students how to protect themselves from security threats.

Chapter Summary

In this chapter, the survey results were presented. The majority of the participants agreed that privacy is significant while dealing with smart TVs, no matter what major, STEM or class/credits. However, an essential issue is the willingness to change attitudes and protect their privacy while dealing with their smart TV devices. STEM students were ahead of non-STEM students for most of the significant questions regarding awareness and attitude questions. They were willing to change attitudes and protect their security and privacy. This means that the non-STEM students, either were not exposed to enough knowledge, because they did not take security courses and were not enrolled in STEM programs, or did not have enough skills to modify their attituue and defend their privacy.

In chapter five, the conclusion of the research study is discussed. Moreover, the strength of the survey and its potential limitations are provided. In addition, recommendations based on the results are addressed and future research is suggested.

CHAPTER 5

CONCLUSION

Internet of things (IoT) compromise currently of billions of connected objects in homes and workplaces. They are cheaply made without taking into consideration security or privacy. The scale of IoT is enormous; it is expected to have more than 20 billion IoT-connected devices in 2025, which may generate around eighty zettabytes of data (Nassar, 2020). In another article, this number is expected to go to 125 billion by 2020 (Riley 2020).

These IoT devices transmit, access, collect, and analyze personal and sensitive users' data (Stevens, 2018). Hackers keep track of the network traffic and access that transmitted data, sometimes even without it being encrypted. Distributed denial-of-service and man-in-the-middle attacks, botnet attacks, data leakage, and malware injections are some security threats that IoT-connected devices may face (Nassar, 2020).

Unencrypted services, weak passwords, denial of service, and lack of two-factor authentication are common vulnerabilities in smart home devices, including smart TVs. Smart TVs are one such insecure IoT device. They can be used to spy, collect, and steal users' sensitive data and harass them (Manwaring & Clarke, 2020). Users must be aware of the dangers of smart TV devices before purchasing them (Gai et al., 2018).

Smart TVs are not "smart" regarding security (Ornes, 2019). Privitera et al. discussed that although smart TVs are costly, there are no adequate safeguards against malware and security attacks in those devices (Privitera et al., 2018). They suggested that protectors can be added to the smart TV device, ensuring protection against attacks at a low cost (Privitera et al., 2018).

Previous research claimed that users do not want their data to be leaked and used, have minimal privacy awareness, and even if told of the security and privacy issues about smart TVs, they choose functionality over privacy (Malkin et al., 2018, Aleisa et al., & Ghiglieri et al., 2017). On the other hand, Alqarni (2017) claimed that students may change their attitude if they feel threatened. This study extended previous research and investigated claims that users will keep their attitude and mindset toward their smart TV devices even if told of their dangers and vulnerabilities.

This research examined several groups of undergraduate college students at a mid-size university. Different school groups were tested: STEM versus non-STEM, then Junior/Senior versus freshmen/sophomore. All group's results were analyzed to see which group had more security knowledge, awareness, and attitude. The researcher’s aim was to investigate whether, with proper training, STEM students were willing to change their behavior and select to protect their privacy while using smart TVs.

There were some unexpected results for the STEM Chi-square testing as shown in Table 5. These questions are:

- Awareness question “Would you expect your smart TV to be hacked?” The answers were very low for both STEM (25%) and non-STEM (20%), which was unexpected.
- Knowledge question “Do you feel confident about checking and disabling TV settings?” The responses were unanticipated: non-STEM students responded agree by 95% versus 89% for STEM students. A drop for STEM students.

- Attitude question "Would you refrain from installing third party apps on your smart TV to protect yourself?" Both STEM and non-STEM students responded "agreed" by 60% each.

In summary, STEM students have higher knowledge and attitudes than non-STEM students underscoring the importance of training. Although differences were observed between the two groups, some results were inconsistent. Based on the findings, it is recommended that STEM students take more real-life courses. It is suggested that all non-STEM students, regardless of their major might benefit from having access to introductory privacy and security courses. Additional research is needed in this area to determine how to influence users and students alike in taking so that they modify their behaviors to proactively protect their privacy.

Overall, there is high knowledge for the participating students who completed the survey with respect to several questions and the findings do support the researcher's hypotheses. The findings did support the hypothesis that STEM students are positively influenced to adopt security practices (attitude, awareness) while using smart TVs, due to their programs. If they perceive that there are problems, they are willing to take actions such as researching third-party applications before using them, refraining from installing third-party application on their smart TVs, and disabling the smart TV features that can be used for spying like camera and audio features.

Finally, the results that were presented in Chapter 4 show that STEM students were indeed influenced by their programs, and this is more in line with what Alqarni found (2017) where she mentioned . This suggests that previous claims of some researchers (Malkin et al., 2018, Aleisa et al., & Ghiglieri et al., 2017) that users will not change their attitude even if they know about the smart TV security and privacy issues are not accurate, but they investigated homeowners and not students. More in-depth and current research and investigations are needed in that area to address previous researchers' claims. It would be beneficial to expand research to include homeowners in addition to college students.

Research Strengths and Limitations

There are several strengths to this research. First the sample size was large: 380 out of 1885 enrolled undergraduate students in Fall 2022, which was 20% of enrolled undergraduate students. Another strength was that there were high response and completion rates. In addition, data collected on 17 questions (outcomes) on knowledge, awareness**,** and attitude. Lastly the sample was representative of the undergraduate students. Undergraduate STEM students were 68% and non-STEM were 32% and these were the same percentages for STEM and non-STEM students enrolled were 68% and 32% and these were the same percentages for STEM and non-STEM survey participants. For enrolled freshmen and sophomore Fall 2022 enrollment, the percentage was 47% versus 50% of sampled (participants). For the 18-21 age group, it was 68% for Fall enrollment versus 72% of sampled participants.

There are a few limitations. One main limitation is that 31% (80 students) of STEM students did not take any security/privacy courses, which may have affected the responses to several survey questions. But this may be because security and privacy courses were not offered at freshmen and sophomore levels. Another limitation is that the types of security and privacy courses that STEM students took were not captured. This would have given some insight into what affected students in their attitudes. In addition, the sample was biased toward a specific demographic, and the groups were unbalanced. The sample size of STEM students was almost double that of non-STEM students. Freshmen students accounted for almost 40%

of the total population. The survey did not capture if students were online or attending campus which is another limitation. Yet another limitation is that all the data was collected from one school, representing a small percentage of students nationwide. Since there were no participants from other schools or universities, conclusions from other college students cannot be made, although there may be some inferences made.

Recommendations

This research targeted undergraduate students' knowledge, awareness, and attitude while using a specific IoT device, a smart TV. Recommendations for university training and education outreach are presented below.

University Training

One solution to alleviate this knowledge gap in college students is to incorporate hands-on labs showing smart TV devices' dangers to all students: freshman to senior levels for STEM and non-STEM. For example: show how personal data can be collected from smart TVs and used to create profiles and how hackers can take charge of their devices and use them for botnet attacks or open back doors and execute malicious codes. Another recommendation would be to have smart TV workshops and seminars carried out in the university throughout the year. Another solution is to prepare short videos that professors and instructors can show in classrooms to warn students about the dangers of smart TV devices and ways to protect themselves, starting from the freshman level. A good approach is to incorporate all the suggested solutions so that students are more exposed to them and are motivated to do something about their privacy and protect it. The crucial thing is to have constant reminders and keep workshops, seminars, hands-on, labs, ongoing and continuous and keep students engaged, motivated, and interested.

Education Outreach

It is crucial to engage middle school and high school students early on and have them exposed to smart TV security and privacy vulnerabilities and issues through several channels. University workshops can be offered throughout the year including some smart TV conferences. Summer camps can be held for high school students to prepare them for what is out there on smart TV. In addition, university smart TV internships can be offered to students to get them more involved. Finally, it would be invaluable to reach out to the community and offer parents/children smart TV seminars in libraries, schools, and universities. In addition, smart TV summer camps can be offered to the community to educate them on what is out there and teach them how to protect their privacy while dealing with smart TVs.

Future Research

There is a considerable amount of work that still needs to be examined in this area. Participants from other universities would be insightful. Additional schools can be surveyed, and different groups of students nationwide could be investigated for a more comprehensive study. Moreover, this study can be expanded to graduate, and K-12 grade students. This would allow for further explorations of age ranges, credit hours, and majors. Moreover, students could be surveyed from freshmen until graduation, and changes over the years could be observed, recorded, and analyzed. This will allow for evaluating the impact of training on students' knowledge attitude and awareness and capture changes observed over time. Implementation of smart TV security and privacy courses that can affect student attitudes while using them could be explored to see how it can affect their security habits, awareness, and behavior.

It is very beneficial to engage key smart TV industry stakeholders with the school for advanced innovative safe smart TVs. Finally, it is of the utmost importance to involve news channels in spreading the knowledge: knowing about smart TV incidents will increase people’s awareness while dealing with their smart TVs.

REFERENCES

1. Abdugani, A. 2020, Privacy Analysis of Smart TV Communication, https://www.duo.uio.no/handle/10852/84344

2. Abomhara, A., & Køien, G. 2015, Cyber Security, and the Internet of Things: Vulnerabilities, Threats Intruders and Attacks, https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_414.pdf

3. AboneLaw, 2020, These Everyday Devices are Susceptible to Hacking, https://abonelaw.com/2020/01/21/these-everyday-devices-are-susceptible-to-hacking/

4. Ahn, M. 2020, Calculating the Minimum Size for Sample Testing, https://maxahn.com/calculating-the-minimum-size-for-sample-testing/

5. Alam, I. Khusro, S. Naeem, M. 2017, A Review of Smart TV Past Present and Future, 2017 International Conference on Open-Source Systems and Technologies (ICOSST)

6. Aleisa, N. & Renaud, K., 2017, Yes, I know this IoT Device Might Invade my Privacy, but I Love it Anyway! A Study of Saudi Arabian Perceptions, Proceedings of the 2nd International Conference on Internet of Things, Big Data, and Security

7. Alharbi, R. Aspinall, D. (2018) An IoT analysis framework: An investigation of IoT smart cameras' vulnerabilities, https://ieeexplore.ieee.org/document/8379734

8. Alqarni, A. 2017, Exploring factors that affect adoption of computer. security practices among college students, [Doctoral dissertation, Eastern Michigan University]

9. Anthony, R. 2016, Internet of Things: Is the Future Susceptible to Hacking? http://www.inquisitr.com/3712810/internet-of-thingsis-the-future-susceptible-to-hacking/

10. Assiri, A. Almagwashi, H. (2018), IoT Security and Privacy Issues, 1st International Conference on Computer Applications & Information Security (ICCAIS), IEEE

11. Australian Government, 2020, Draft Code of Practice: Securing the Internet of Things for Consumers, https://www.homeaffairs.gov.au/reports-and-pubs/files/consultation-summary.pdf

12. Bachy, Y. Nicomette, V. Kaâniche, M & Alata, E. 2019, Smart-TV security: risk analysis and experiments on Smart-TV communication channels, Journal of Computer Virology and Hacking Techniques volume 15, pages 61–76 (2019)

13. Barth, S. De Jong, M. D. T. 2017, The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telematics and Informatics, *34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

14. BCG, 2015, The Mobile Revolution: How Mobile Technologies Drive a Trillion-Dollar Impact, https://www.bcg.com/publications/2015/telecommunications-technology-industries-the-mobile-revolution

15. Berkman Centre for Internet and Society (BCIS), 2016 Don't Panic. Making Progress on the "Going Dark*,"* https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

16. Bevans, R., 2020 Understanding P-values, https://www.scribbr.com/statistics/p-value/

17. Bergenstock, J. 2017, Internet of Things: Ease of life vs. demolition of personal privacy. ProQuest Dissertations Publishing, 10686190. https://search.proquest.com/openview/3a553ae219295ca3c0d858475dc7c741/

18. Bitdefender, 2018, Bitdefender study: One in four urban homes is smart. Smart TVs, the most used, https://www.bitdefender.ro/news/studiu-bitdefender:-una-din-patru-locuinte-din-mediul-urban-este-smart-televizoarele-inteligente-cele-mai-folosite-3495.html (In Romanian, Translated it)

19. Bjelica, M. Z., 2018, How Much Smart Is Too Much? Exploring the slow adoption of new consumer technology, IEEE Consumer Electronics Magazine

20. BUMC (Boston University Medical Campus), 2019, The Theory of Planned Behavior, https://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories3.html

21. Boztas, A. Riethoven, A.R.J. Roeloffs, M., 2015, Smart TV forensics: Digital Traces on Televisions, Science Digest, DFRWS 2015 Europe

22. Bräunlein, F. Frerichs, L. 2019, Smart spies: Alexa and Google Home Expose Users to Vishing and Eavesdropping, Security Research Labs, https://www.srlabs.de/

23. Brewster, T. 2017, Here's How The CIA Allegedly Hacked Samsung Smart TVs -- And How To Protect Yourself, https://www.forbes.com/sites/thomasbrewster/2017/03/07/cia-wikileaks-samsung-smart-tv-hack-security/?sh=453620414bcd

24. CBCNews, WikiLeaks says CIA hacked Samsung smart TVs, 2017, https://www.cbsnews.com/news/cia-hacked-samsung-smart-tvs-wikileaks-vault-7/

25. Chernyshev, M. Hannay, P. 2015, Security Assessment of IoT Devices: The Case of Two Smart TVs Conference: 13th Australian Digital Forensics Conference

26. CNet. 2018, California Governor Signs Country's First IoT Security Law: https://www.cnet.com/news/california-governor-signs-countrys-first-iot-security-law/

27. Constantin, L. 2017, Ransomware on smart TVs is here and removing it can be a pain, https://www.pcworld.com/article/411486/ransomware-on-smart-tvs-is-here-and-removing-it-can-be-a-pain.html

28. Consumer Reports, 2018, Samsung and Roku smart TVs could be controlled by 'a relatively unsophisticated hacker,' https://www.businessinsider.com/samsung-and-roku-smart-tvs-security-flaws-2018-2?IR=T

29. Consumer Reports, Consumer reports TV buying guide: Getting the right TV, 2021, https://www.consumerreports.org/cro/tvs/buying-guide/index.htm

30. Crossler, R.E., 2009, Protection Motivation Theory: Understanding the Determinants of Individual Security Behavior [Doctoral dissertation, Virginia Polytechnic Institute and State University].

31. Dark Reading, 2019, Nest Hack Leaves Homeowner Sleepless in Chicago, https://www.darkreading.com/attacks-breaches/nest-hack-leaves-homeowner-sleepless-in-chicago

32. D.D. Furszyfer Del Rio, 2021, Smart but unfriendly: Connected home products as enablers of conflict, https://doi.org/10.1016/j.techsoc.2021.101808

33. Dell, 2012 Mobility and the Network, https://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/ESG-Mobility-and-the-Network-White-Paper.pdf

34. Deloitte, 2018, The future of the TV and video landscape by 2030, 2018, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/de-future-tv-and-video.pdf

35. DiGiacomo, J., 2017, Is Your Smart TV at Risk of a Ransomware Cyberattack? https://revisionlegal.com/internet-law/data-breach/smart-tv-ransomware-risk/

36. Digital Hub, 2020, The 'Security of Things' – Government releases Voluntary IoT Code of Practice, https://www.gtlaw.com.au/insights/security-things-government-releases-voluntary-iot-code-practice

37. Dinham, P. 2020, Smartphones dominate the 'digital experience' research reveals Featured, https://www.itwire.com/market/smartphones-dominate-the-%E2%80%98digital-experience%E2%80%99-research-reveals.html

38. Dumont, C., 2015, NIST 800-53 Family Reports, https://www.tenable.com/sc-report-templates/nist-800-53-family-reports

39. Eddy, N. 2015, 21 Billion IoT Devices to Invade By 2020, https://www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081

40. Edgar, T. W. Manz, D. O. 2017, Logistic Regression Exploratory Study in Research Methods for Cyber Security, 2017 https://www.sciencedirect.com/topics/computer-science/logistic-regression

41. Fung, C. Motti, V. Zhang, K. and. Qian, Y, 2022, A Study of User Concerns about Smartphone Privacy,2022 6th Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 2022, pp. 1-8, doi: 10.1109/CSNet56116.2022.9955623.

42. Furnell, S. Tsaganidi, V. Phippen, A. 2008, Security beliefs and barriers for novice Internet users Computers & Security Volume 27, Issues 7–8, December 2008, Pages 235-240

43. Gai, A. Azam, S. Shanmugam, B. Jonkman, M. De Boe, F. 2018, Categorization of security threats for smart home appliances, 2018 International Conference on Computer Communication and Informatics (ICCCI -2018)

44. Ghiglieri, M. Volkamer, M. and Renaud, K. 2017, Exploring Consumers' Attitudes of Smart TV Related Privacy Risks

45. Ghosh, I. 2021, 4 key areas where AI and IoT are being combined, https://www.weforum.org/agenda/2021/03/ai-is-fusing-with-the-internet-of-things-to-create-new-technology-innovations/

46. Good Home Automation, 2021, {Smart Home} Technology Made Easy, https://goodhomeautomation.com/what-year-did-the-smart-tv-come-out/

47. Goodin, D. 2017, Smart TV hack embeds attack code into broadcast signal—no access required, https://arstechnica.com/information-technology/2017/03/smart-tv-hack-embeds-attack-code-into-broadcast-signal-no-access-required/

48. Goriawala, S. 2013, Are Security and Privacy the same thing? Quora, https://www.quora.com/Are-Security-and-Privacy-the-same-thing

49. Grand Review Research, Smart TV Market Size, Share & Trends Analysis Report by Resolution, 2021, https://www.grandviewresearch.com/industry-analysis/smart-tv-industry

50. Gupta, A. 2019, The IoT Hackers Handbook, Apress, https//doi.org/10.1007/978-1-4842-4300-8

51. Hackers-arise, 2017, Browser Exploitation Framework (BeEF), Part 1 https://www.hackers-arise.com/post/2017/05/22/browser-exploitation-framework-beef-part-1

52. Hall, F. Maglaras, L. Aivaliotis, T. Xagoraris, L. and Kantzavelou, I. 2020, Smart Homes: Security Challenges and Privacy Concerns

53. Hammi, B. Zeadally, S. Khatoun, R. Nebhen, J. Survey on smart homes: Vulnerabilities, risks, and countermeasures, 2022, Computers & Security, Volume 117, https://doi.org/10.1016/j.cose.2022.102677

54. HI Tech, 2021, Your smart TV can be hacked! Here's how to protect it from malware. https://tech.hindustantimes.com/how-to/your-smart-tv-can-be-hacked-here-s-how-to-protect-it-from-malware-71632320500723.html

55. Hospitality Technology, 2016, Security Must Be Built into the Design of IoT Devices, https://hospitalitytech.com/security-must-be-built-design-iot-devices

56. IBM, 2019, Identify and fix IoT security vulnerabilities during design and beyond, https://www.ibm.com/security/services/iot-testing

57. IBM, What is logistic regression? https://www.ibm.com/topics/logistic-regression

58. InfoSecurity, 2017, Japan Sees a Spike in Smart TVs Held Hostage, https://www.infosecurity-magazine.com/news/japan-sees-a-spike-in-smart-tvs/

59. Ipsos, 2014, The Changing Landscape of TV, https://www.ipsos.com/en-us/knowledge/media-brand-communication/changing-landscape-tv

60. Jongho Lee, Mingeun Kim, Seungjoo Kim, 2017, Are You Watching TV Now? Is It Real? Hacking of Smart TV with 0-day, Korea University

61. Johnson-Lynn, G, 2019, Hooking a Browser with the Browser Exploitation Framework (BeEF), A Quick Guide to Starting BeEF and Running Commands Against a Hooked Browser, https://www.gavinjl.me/getting-started-with-beef/

62. Jovanović, B. 2021, Internet of Things statistics for 2021 – Taking Things Apart https://dataprot.net/statistics/iot-statistics/

63. Kaur, J. 2019, TV becomes essential part of life, it acts like companion 103. https://onlinepte.com/tv-essential-part-life-acts-companion/

64. Kovacs, N. 2021, What is a smart TV and the privacy risks of a smart TV, https://us.norton.com/internetsecurity-iot-smart-tvs-and-risk.html

65. Kumar, D. Paccagnella, R. Murley, P. Hennenfent, E. Mason, J. Bates, A. & Bailey, M. 2018, Skill Squatting Attacks on Amazon Alexa, Proceedings of the 27th USENIX Security Symposium

66. Lai. PC. 2017, The Literature Review of Technology Adoption Models and Theories for the Novelty Technology PC, JISTEM - Journal of Information Systems and Technology Management, Vol. 14, No. 1, Jan/Apr. 2017 pp. 21-38

67. Lee, S.J, Kim, S. 2013, Hacking, Surveilling, and Deceiving Victims on Smart TV, Korea University, Black Hat USA 2013

68. Lit, Y. Kim, S. Sy, E. 2021, A Survey on Amazon Alexa Attack Surfaces, IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)

69. Liu, Y. Li, L. Kong, P. Sun, X. Tegawend´e F. Bissyand´e, 2021, A First Look at Security Risks of Android TV Apps, 2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW)

70. Malkin, N. Berndy, J. Johnsony, M. and Egelman, S. 2018, Privacy Expectations about Smart TVs in the U.S., European Workshop on Usable Security (EuroUSEC) 2018

71. Manwaring, K. & Clarke, R. 2020, Are your devices spying on you? Australia’s very small step to make the Internet of Things safer, https://theconversation.com/are-your-devices-spying-on-you-australias-very-small-step-to-make-the-internet-of-things-safer-145554

72. Mazhar, M. H. & Shafiq, Z. 2020, Characterizing Smart Home IoT Traffic in the Wild, 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI*)*, pp. 203-215, doi: 10.1109/IoTDI49375.2020.00027

73. Michéle, B. Karpow, A., 2014, Using Malicious Media Files to Compromise the Security and Privacy of Smart TVs, The 11th Annual IEEE Consumer Communications and Networking Conference - 2014

74. Milley, P. 2017, Privacy and the Internet of Things, SANS, https://www.sans.org/reading-room/whitepapers/internet/privacy-internet-things-38105

75. Moghaddam, H.M. Acar, G. Burgess, B. Mathur, A. Danny, D.Y. Feamster, N. Felten, E. W. Mittal, P. Narayanan, A., 2019 Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices, CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, Pages 131–147, https://doi.org/10.1145/3319535.3354198

76. mTab, Validating a Survey: What It Means, how to do It. https://www.mtab.com/blog/validating-a-survey-what-it-means-how-to-do-it

77. Nassar, S., 2020, Requirements for the New Era of IoT Security, https://www.iotevolutionworld.com/iot/articles/447200-requirements-the-new-era-iot-security.htm

78. NGIoT, EU-IoT project kicks off, 2020, https://www.ngiot.eu/eu-iot-project-kicks-off/

79. Ornes, S. 2019, Rise of the botnets, Science News for students https://www.sciencenewsforstudents.org/article/botnets-malware-cyberattack-increase

80. Palenchar, J. 2016, Smart TVs Turn into The Hub of a Smart House, https://www.twice.com/news/smart-tvs-turn-hub-smart-house-60462

81. Panda, 2017, Your Smart TV Has Been Hijacked. To Continue, Please Pay Ransom, https://www.pandasecurity.com/en/mediacenter/security/smart-tvs-ransomware/

82. Popescul, D. 2018, Smart TVs: What Do They Know (and tell) about Us? IACSS 2018-IACLPM 2018 Joint Conference Proceedings

83. Privitera, D. Shahriar, H, 2018, Design and Development of Smart TV Protector, 2018 National Cyber Summit Research Track

84. Richards, D. 2018, Hisense, TCL, Sony & Samsung TV’s Can Be Easily Hacked Claim Consumer Group, https://www.channelnews.com.au/hisense-tcl-sony-samsung-tvs-can-be-easily-hacked-claim-consumer-group/

85. Riley, A. 2020, How your smart home devices can be turned against you, https://www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse

86. Rondon L.P., Babun, L. Akkaya, K. Uluagac, A.S. 2021, HDMI-Watch: Smart Intrusion Detection System Against HDMI Attack, IEEE Transactions on Network Science and Engineering, Vol. 8, NO. 3, July-September 2021

87. Ross, R. Pillitteri, V. Dempsey, K. Riddle, M. Guissani, G. Protecting Controlled Unclassified Information in Nonfederal Systems, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

88. SDSU (San Diego State University), 2020, Descriptive Studies, https://ori.hhs.gov/education/products/sdsu/res_des1.htm

89. Salloum, S. Al-Hamad, A.Q.M., Al-Emran, M. Monem, A.A. Shaalan, K. 2019, Exploring Students' Acceptance of E-Learning Through the Development of a Comprehensive Technology Acceptance Model IEEE Access

90. Sharif, K. Tenbergen, B. 2020, Smart Home Voice Assistants: A Literature Survey of User Privacy and Security Vulnerabilities, State University of New York at Osweg, Complex Systems Informatics and Modeling Quarterly (CSIMQ)

91. Silva, R. 2022, Smart TVs: What You Need to Know
If You're Thinking of Streaming - or Already Do - a Smart TV Could be For You. Life Wire, https://www.lifewire.com/what-is-a-smart-tv-4140172

92. Singh, G. Mehta, K., Singla, H. 2020, Security Concerns of Smart Homes and its Solutions, Advances and Applications in Mathematical Sciences Volume 19, Issue 6, April 2020, Pages 543-549

93. Solove, D.J. 89 Geo. Wash. L. Rev. 1, The George Washingot Law Review, https://www.gwlr.org/the-myth-of-the-privacy-paradox/

94. Statista, 2018. Internet of Things Connected Installed Devices from 2015 to 2025, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

95. Sriram S, Yimin Dai, Sean Rui Xiang Tan, Nirupam Roy, Jun Han, 2020, Spying With Your Robot Vacuum Cleaner: Eavesdropping via Lidar Sensors, https://dl.acm.org/doi/abs/10.1145/3384419.3430781

96. Steve, 2021, Basic Home Network Hardware Components, Devices and Services https://stevessmarthomeguide.com/networking-components/

97. Stevens. T. 2018, Internet of Things: when objects threaten national security, https://theconversation.com/internet-of-things-when-objects-threaten-national-security-96962

98. Sukamolson, 2007, S. Fundamentals of quantitative research, https://www.iicseonline.org/Quantitative_MethodsII.pdf

99. Sun, D. 2020, Singapore home cams hacked, and stolen footage sold on pornographic sites, https://tnp.straitstimes.com/news/singapore/hackers-hawk-explicit-videos-taken-spore-home-cams

First, click on the numbers in front of the references so they're all highlighted. Then, go to the search bar and type "define new number format" and change the alignment from left to centered. This seems to fix it.

100. Surendran, P. 2012, Technology Acceptance Model: A Survey of Literature, International Journal of Business and Social Research, MIR Center for Socio-Economic Research, vol. 2(4), pages 175-178

101. Taherdoost, H. 2016, Sampling Method in Research Methodology How to Choose a Sampling Technique for Research, International Journal of Academic Research in Management (IJAR

102. Techresider, 2019, How technology has changed human life in the last decade, https://techresider.com/technology/how-technology-has-changed-human-life-in-the-last-decade/

103. TechieGuy, 2020, Stop your Smart TV from spying on you! https://www.youtube.com/watch?v=1-vIiEpUqI0

104. TMJ4 News, 2020, How hackers get into your smart TV https://www.youtube.com/watch?v=I7cPDl-1_Rg

105. TPVision, TP Vision, Welcome to Philips Smart TV, 2018. http://www.tpvision.com/policy/Privacy_Policy_english.pdf

106. Turow, J. Hennessy, M. & Draper, N. 2016, The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060

107. Vargas-Morales, "Privacy Concerns about Common IoT devices: First Approach in Costa Rica," 2019 IV Jornadas Costarricenses de Investigación en Computación e Informática (JoCICI), San Pedro, Costa Rica, 2019, pp. 1-5, doi: 10.1109/JoCICI48395.2019.9105189.

108. Varmarken, J. Le, H. Shuba, A. Markopoulou, A. and Shafiq, Z. 2020, The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking, Proceedings on Privacy Enhancing Technologies; 2020 (2):129–154. https://par.nsf.gov/servlets/purl/10205759

109. Vijayan, J. 2020, Most IoT Hardware Dangerously Easy to Crack, https://www.darkreading.com/iot/most-iot-hardware-dangerously-easy-to-crack-/d/d-id/1338828

110. Vuleta, B. 2021, From College Student Statistics: Mental Health and Loans, https://seedscientific.com/college-student-statistics/

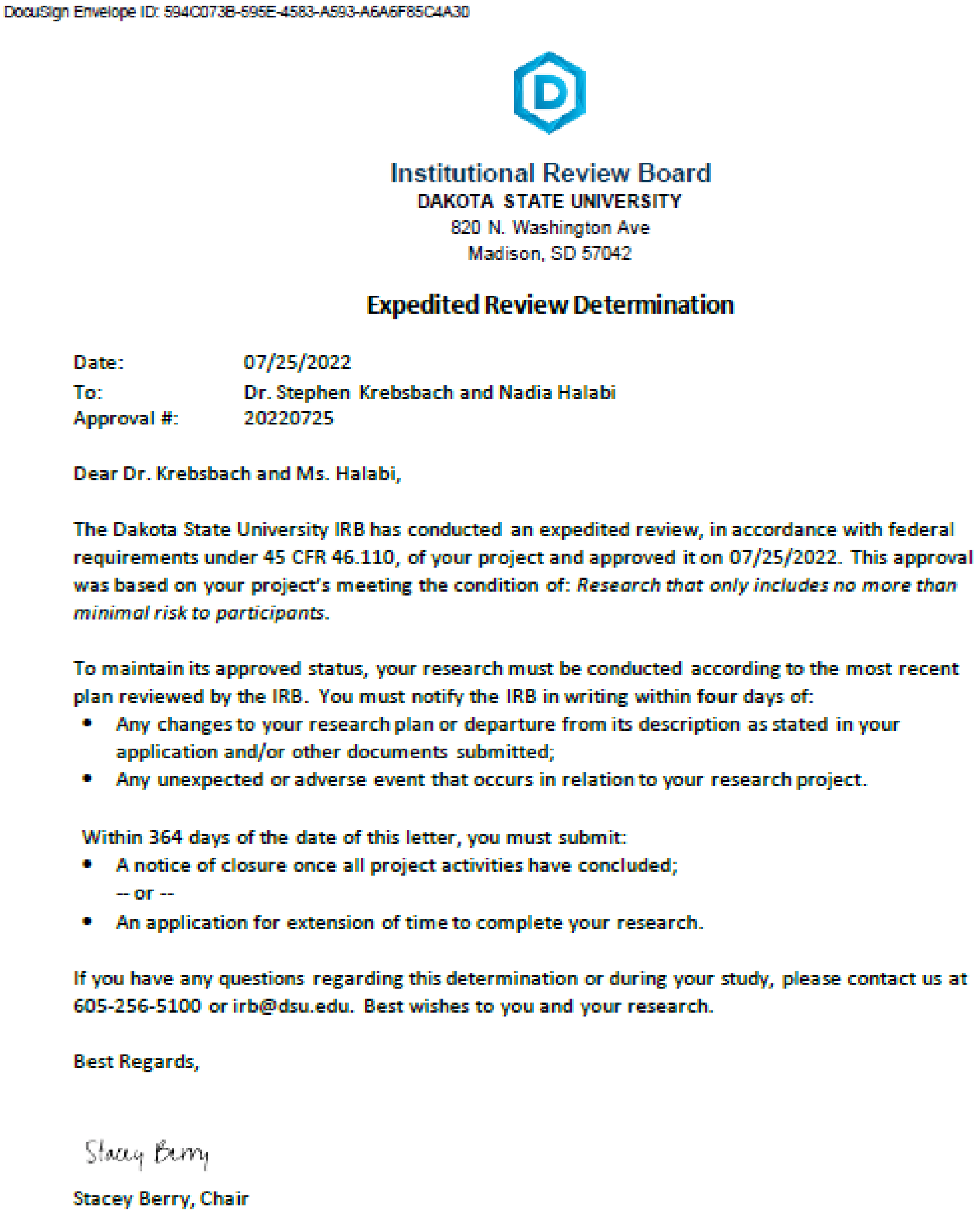
111. Wang, X. Cheng, Z. 2020, Cross-Sectional Studies Strengths, Weaknesses, and

Recommendations, CHESS Journal, Volume 158, ISSUE 1, SUPPLEMENT, S65-S71, July 01, 2020

112. Whittaker, Z. 2019, Now even the FBI is warning about your smart TV's security https://techcrunch.com/2019/12/01/fbi-smart-tv-security/

113. Willcox, J. K., 2019, Pros and Cons of Smart TV Systems, before you shop, find out whether Amazon Fire TV Edition, Android TV, Roku TV, Smart Cast, Tizen, or webOS is right for you, https://www.consumerreports.org/tvs/smart-tv-systems-pros-cons/

APPENDIX A. IRB APPROVAL



DocuSign Envelope ID: 594C073B-595E-4583-A593-A6A6F85C4A30

Institutional Review Board
DAKOTA STATE UNIVERSITY
820 N. Washington Ave
Madison, SD 57042

Expedited Review Determination

Date:	07/25/2022
To:	Dr. Stephen Krebsbach and Nadia Halabi
Approval #:	20220725

Dear Dr. Krebsbach and Ms. Halabi,

The Dakota State University IRB has conducted an expedited review, in accordance with federal requirements under 45 CFR 46.110, of your project and approved it on 07/25/2022. This approval was based on your project's meeting the condition of: *Research that only includes no more than minimal risk to participants.*

To maintain its approved status, your research must be conducted according to the most recent plan reviewed by the IRB. You must notify the IRB in writing within four days of:

- Any changes to your research plan or departure from its description as stated in your application and/or other documents submitted;
- Any unexpected or adverse event that occurs in relation to your research project.

Within 364 days of the date of this letter, you must submit:

- A notice of closure once all project activities have concluded;
  -- or --
- An application for extension of time to complete your research.

If you have any questions regarding this determination or during your study, please contact us at 605-256-5100 or irb@dsu.edu. Best wishes to you and your research.

Best Regards,

Stacey Berry

Stacey Berry, Chair

APPENDIX B.

CONSENT FORM

Students' Smart TV

This survey is intended for Undergrad students who have previously used or are using a smart TV.

The person in charge of this study is Nadia Halabi, a cyber operations doctoral student at DSU. She very much appreciates your participation in this study. The researcher's faculty adviser and project principal investigator are Professor Stephen Krebsbach.

Purpose of the study

This study aims to investigate several groups of university students: STEM and non-STEM freshmen/sophomores and juniors/seniors.

This research project will examine the security behavior of students, especially the STEM senior students who had in-depth security training. In addition, it will investigate if students with in-depth training will be positively influenced to become more vigilant about protecting their privacy and security when using IoT devices, especially smart TVs.

How do I participate in this survey?

Participation in this study involves completing a survey on SurveyMonkey.

What are the anticipated risks for participation?

There are no anticipated risks associated with participating in this study.

Are there any benefits to participating?

There are no direct benefits to the students in participating in this research. However, this study will contribute to the knowledge regarding the practice of privacy and security. Furthermore, the results of this research will contribute to protecting users' privacy and help the direction of future research efforts in this area.

How will my information be kept?
Except for age and major, no personal information (PII) will be collected nor analyzed.

Storing study information for future use
The collected information will be stored for three years after the publication of the results of this study. Moreover, the information will not be shared with third parties or marketing agencies.

Are there any participation costs?
There are no costs associated with taking part in the study.

Will I be paid for participation?
There will be no compensation for participating in the study.

Study contact information
If you have any questions about the research, please feel free to contact Nadia Halabi at **nhalabi@pluto.dsu.edu** before or after taking the survey.

For questions about your rights as a research subject, you may contact the DSU IRB at: **irb@dsu.edu**

Voluntary participation
Participation in this research study is completely voluntary. You may choose to stop taking the survey at any time, in that case, your answers will not be counted in the study.

Statement of Consent
I have read this consent form. I give my consent to participate in this research study.

Important:

PLEASE Note, you need to complete **ALL** questions, otherwise, your answers will not be counted in the research. If you want, you can skip the last question only, Question Number 27. The survey would take around 6 minutes. I appreciate your cooperation.

Note:
By clicking the **Next** button and completing this survey, students will be considered as consenting to participate in this study.

APPENDIX C

SURVEY QUESTIONS

DEMOGRAPHICS

1-Please indicate your age.

a. Under 18 (You will exit the survey)
b. 18-21
c. 22-25
d. 26-30
e. 31-34
f. 35+

2- What is your major, select one of the below groups?

a. Sciences (Biology, Chemistry, Physics)
b. Mathematics
c. Computers (Computer Science, Information Systems, Artificial Intelligence, Graphics, Software Engineer, Data Analytics, Web Development, Game Design, Web Design)
d. Business (Accounting, Administration, Business Technology, Management, Marketing, Finance, Technology)
e. Security (Mathematics Cryptography, Network and Security Administration, Cyber Leadership & Intelligence: Digital, Cyber Operations)
f. Education
g. Health (Information Administration)
h. Arts (Digital Arts & Design)
i. General Studies
j. Physical Education
k. Double Major
l. Undecided

3- How many college credits have you earned as of Fall 2022?

a. 0-30
b. 31-60
c. 61-90
d. 90

4. How many security/privacy courses did you take in the past?

a. 0

b. 1
c. 2
d. 3
e. 4+

SMART TV INFO (STV)

A Smart TV is a television that is connected to the Internet. This allows users to view content from Internet-based providers,

However, some users may not have smart TVs or may opt out of using them and choose instead to use external devices to get the smart TV features: streaming channels.

TV Streaming is a process that allows users to watch TV via external devices which are connected to the internet, such as smart TVs, laptops, smartphones, monitors, and gaming consoles.

1. Are you using, or have you used a smart TV in the past?
Participants who use smart TVs please select option b
For Participants who user smart TV features via external devices please select option c
a. No (You will exit the survey)
b. Yes
c. Via external devices

2. What brand?
a. LG
b. Samsung
c. Sony
d. Vizio
e. Tizen
f. Not applicable
g. Other

3.What streaming services are you using? (Select all the apply)
a. Netflix
b. Sling

c. Disney +
d. Hulu
e. Amazon Prime
f. Apple TV +
g. HBO Max
h. DIRECT TV
i. Paramount +
j. Philo
k. Peacock
l. Fubo
m. Not applicable
n. Other

PERCEIVED EASE OF USE (PEU)

Perceived ease of use reflects the extent to which a person believes it is easy to use a particular system in this case a smart TV.

"The degree to which a person believes that using a system would be free of effort."

1- Does Smart TV interaction require mental effort?

a. No
b. Yes
c. Somewhat

COMPUTER SELF-EFFICACY (CSE)

Computer self-efficacy is the ability to study computers. Self-efficacy refers to the self-confidence of students that they can use computers easily, or in this case smart TVs.

1- Do you feel confident about checking and using the Smart TV settings?

a. No
b. Yes
c. I can look for instructions on YouTube or on the web.

2- Do you feel confident about disabling some features that are not needed on the Smart TV?

a. No
b. Yes
c. I can look for instructions on YouTube or on the web.

3- Since the smart TV is connected to the home Router (the entry point to the home environment), do you feel confident about changing the home router's password?

a. No
b. Yes
c. I can look for instructions on YouTube or on the web.

4-How comfortable are you looking for instructions related to smart TV changing settings, disabling features, etc. on YouTube or the web?

a. Extremely Comfortable
b. Comfortable
c. Not sure
d. Uncomfortable
e. Extremely uncomfortable

PERCEIVED THREAT VULNERABILITY (PTV)

The degree to which respondents believe "they are vulnerable to computer security threats posed during their home use."

Smart TVs present both privacy and security risks. Privacy issues include your personal data and habits being monitored and sold, while security concerns involve viruses and hackers.

Privacy issues are violations of users' private information. Some examples of privacy violations are:

- Accessing someone's smart TV login credentials, browsing history, search viewing habits
- Listening to users' private conversations via the smart TV audio
- Watching users' area, taking their pictures via the smart TV camera, if applicable
- Collecting personal information of users, and sharing or selling it to another party
- Leaking sensitive information about users' and their families

Some security violations would be using smart TVs to:

- Inject some malware code to cause harm.

· Open back doors for some malicious activity, especially if users download unsafe apps on their devices

· Keep track of the users' internet activity

1-What are the chances of your privacy being invaded?

a. It is definite.
b. It is likely.
c. Unsure
d. It is not likely.
e. It is not possible.

2. What are the chances of your smart TV being hacked?

a. It is definite.
b. It is likely.
c. Unsure
d. It is not likely.
e. It is not possible.

PERCEIVED THREAT SEVERITY (PTS)

"The degree to which respondents' are concerned with the severity of computer security threats posed during their home use."

Smart TVs present both privacy and security risks. Privacy issues include your personal data and habits being monitored and sold, while security concerns involve viruses and hackers.

1- It would be a severe problem if my privacy was invaded while using my smart TV

a. Strongly Agree
b. Agree
c. Unsure
d. Disagree
e. Strongly Disagree

2. It would be problematic if my smart TV was hacked

a. Strongly Agree
b. Agree
c. Unsure

d. Disagree
e. Strongly Disagree

VOICE RECOGNITION/CAMERA (VRC)

Some smart TV features are:
- Voice recognition
- Gesture/facial recognition
- Cameras
- Microphone

Voice recognition allows the user to speak various commands instead of using a remote control. For example, changing channels, searching for content, or even turning the Smart TV on or off.

Gesture recognition technology is the ability to communicate with machines utilizing human bodily forms of motion which commonly originates from the face or hand.

A voice command starts the smart TV, a smart TV camera recommends a show based on facial recognition if available. This type of interconnectivity has privacy implications and could be a backdoor for malicious attackers.

Smart TVs can keep track of users in three ways:
ACR technology: collecting data about users' viewing habits.
Smart TV camera: watching users.
Smart TV microphone: listening to users.

1. How likely is it that in-home audio, recorded for voice recognition purposes, or your smart TV camera and microphone will be accessed by third parties such as: TV/Streaming Providers?

a. Extremely likely
b. Likely
c. Not sure

d. Unlikely
e. Extremely unlikely

2. How acceptable would it be if your in-home audio, recorded for voice recognition purposes, was accessed by third parties or your smart TV camera and microphone were used to watch and listen to you?

a. Completely acceptable
b. Somewhat acceptable
c. Not sure
d. Unacceptable
e. Completely unacceptable

3. To have a more secure home environment and prevent other parties to misuse voice recognition feature, or use smart TV camera and microphone to watch and listen to you, will you consider disabling those features?

a. Definitely would not
b. Might not disable.
c. Unsure
d. Might disable.
e. Definitely will disable.

THIRD-PARTY APPS (TPA)

Third-party apps are software applications that are developed by software developers and not by the device manufacturer.

Smart TV applications (apps) are software apps that deal with smart TV devices to add more functionality and features. Despite its importance, too little attention has been paid to testing these kinds of apps. Third-party apps can be installed on the smart TV which was not developed by the smart TV manufacturers. Some third-party tv app types are streaming, videos, digital music, online news, online games, and so forth.

Some examples of streaming apps such as YouTube, Hulu, Sling, Disney +, DIRECTTV Stream, Apple TV, Amazon Prime, and some free services.

1- If you want to install third-party apps, would you research the app to see how safe it is before you install it on your smart TV?

a. Definitely yes

b. Yes
c. Unsure
d. No
e. Definitely not

2- By allowing new software to be installed on your Smart TV to enable third-party apps, your TV may become vulnerable to malicious software being installed. Would you consider refraining from installing third-party apps on your smart TV?

a. Definitely yes
b. Yes
c. Unsure
d. No
e. Definitely not

SECURITY/PRIVACY AWARENESS (SPA)

Many Smart TVs feature a technology called Automatic Content Recognition (ACR), which tracks what users watch and then sells that data to advertisers.

In 2017, the Federal Trade Commission fined Vizio 2.2 million dollars, because they were tracking their customers' viewing habits and then sold that information to a third party (Hall et al, 2020).

1. What is the likelihood of your smart TV manufacturer collecting data including your viewing history and search patterns from your home environment?

a. Extremely likely
b. Likely
c. Unsure
d. Unlikely
e. Extremely Unlikely

2. How likely will data collected from your Smart TV (including viewing history/search patterns) be combined with data collected from your other IoT devices (smartphone, tablet, laptop) to create a detailed profile of your habits and interests?

a. Extremely likely
b. Likely
c. Unsure
d. Unlikely
e. Extremely Unlikely

3. Is collecting data from several sources to create a detailed profile of you acceptable?

   a. Extremely acceptable.
   b. Acceptable.
   c. Not sure
   d. Unacceptable.
   e. Extremely unacceptable.

5- Is protecting your privacy more important than using smart TV features?

   a. Protecting my privacy comes first.
   b. Using smart TV features is more important.
   c. They are equally important.
   d. Unsure

6- How many security/privacy courses did you take in the past?

   a. 0
   b. 1
   c. 2
   d. 3
   e. 4+

7- Did the security/privacy course(s) that you took influence you to have a more proactive security behavior to protect your privacy?

   a. Definitely yes
   b. Yes
   c. Unsure
   d. Definitely not
   e. Not applicable

END OF SURVEY

Thank you for taking the survey. The researchers very much appreciate you taking the time to participate in this research.

Did this survey change your attitude towards the dangers of smart TV?

   a. Yes
   b. No
   c. Not Applicable (For branching logic)

If your answer was Yes or No in the previous question, explain why.

APPENDIX D.

Chi-Test Square Test in R

RESEARCH QUESTION 1: STEM/NON-STEM

2023-08-06

install.packages("dplyr") library(dplyr) library(gmoldes) library(forcats) library(dplyr) library(magrittr) ## Libraries library(tidyr) library(tidyverse) library(haven) library(readxl) library(table1) library(xtable) library(dplyr) library(kableExtra) library(devEMF) library(forcats) library(datasets) library(ggplot2) library(readxl) library(tidyr)

```
testa=read.csv("C:/Spring2023/Participants/Survey.csv", header=TRUE,
sep=",")

#head(testa) # description of data variables in the data

dim(testa)

## [1] 380  24

test_frame <-data.frame(testa)


str(test_frame)

## 'data.frame':    380 obs. of  24 variables:

##  $ IP                  : chr  "174.235.211.163" "138.247.98.46"
"138.247.100.51" "138.247.110.184" ...

##  $ AgeGroup            : chr  "18-21" "18-21" "22-25" "18-21" ...

##  $ Major               : chr  "Arts" "Security" "Arts" "Computers" ...

##  $ Stem                : int  0 1 0 1 1 1 1 1 1 1 ...

##  $ Credits             : chr  "31-60" "90" "31-60" "31-60" ...

##  $ Effort              : chr  "Somewhat" "Somewhat" "No" "No" ...

##  $ Confident           : chr  "Yes" "Yes" "Yes" "Yes" ...

##  $ DisablingFeatures   : chr  "Yes" "No" "Yes" "Yes" ...

##  $ PrivInvasion        : chr  "It is definite" "It is likely" "It is
definite" "It is not likely" ...

##  $ HackedIssue         : chr  "It is likely" "Unsure" "It is not likely"
"It is not likely" ...
```

```
## $ ProblematicPriv    : chr  "Agree" "Agree" "Agree" "Disagree" ...
## $ HackedTV           : chr  "Agree" "Agree" "Agree" "Agree" ...
## $ CameraMicAccess    : chr  "Extremely likely" "Extremely likely"
"Extremely likely" "Extremely likely" ...
## $ AccessAcceptable   : chr  "Completely unacceptable" "Somewhat
acceptable" "Completely unacceptable" "Unacceptable" ...
## $ DisablingCamMic    : chr  "Definitely will disable" "Definitely will
disable" "Definitely will disable" "Definitely will disable" ...
## $ ResearchApps       : chr  "Unsure" "Yes" "Definitely yes" "No" ...
## $ NoApps             : chr  "No" "Yes" "Definitely yes" "No" ...
## $ DataCollection     : chr  "Extremely likely" "Extremely likely"
"Extremely likely" "Extremely likely" ...
## $ CreateProfileHabits: chr  "Extremely likely" "Extremely likely"
"Extremely likely" "Extremely likely" ...
## $ ProfileAcceptable  : chr  "Extremely unacceptable" "Acceptable" "Not
sure" "Unacceptable" ...
## $ Privacy            : chr  "Protecting my privacy comes first" "They
are equally important" "Protecting my privacy comes first" "They are
equally important" ...
## $ SecCourses         : int  0 2 0 0 4 2 4 0 0 4 ...
## $ InfluenceBehavior  : chr  "Not applicable" "Yes" "Not applicable"
"Not applicable" ...
## $ Stem.1             : logi  NA NA NA NA NA NA ...
```

```r
data1 <-data.frame(testa)


library(forcats)
```

```
## Warning: package 'forcats' was built under R version 4.2.3
```

```r
library(dplyr)
```

```
## Warning: package 'dplyr' was built under R version 4.2.3
##
## Attaching package: 'dplyr'
## The following objects are masked from 'package:stats':
##
##     filter, lag
## The following objects are masked from 'package:base':
##
##     intersect, setdiff, setequal, union
```

```r
library(magrittr)
```

```
## Warning: package 'magrittr' was built under R version 4.2.3
```

```
tab00 = table(data1$Stem)
print (tab00)
```

```
##
##   0   1
## 122 258
```

```
tab0 = table(data1$Effort)
print (tab0)
```

```
##
##       No Somewhat      Yes
##      150      191       39
```

```
chisq.test(tab0)
```

```
##
##  Chi-squared test for given probabilities
##
## data:  tab0
## X-squared = 97.647, df = 2, p-value < 2.2e-16
```

```
#Stem, Effort
tab1 = table(data1$Stem, data1$Effort )
tab12=round(prop.table(tab1*100,1),digits=2)
print(tab12)
```

```
##
##       No Somewhat  Yes
##   0 0.43     0.49 0.08
##   1 0.38     0.51 0.11
```

```
chisq.test(tab1)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab1
## X-squared = 1.241, df = 2, p-value = 0.5377
```

```
#Stem, Settings Confidence
tab11 = table(data1$Stem, data1$Confident )
tab112=round(prop.table(tab11*100,1),digits=2)
```

```
print(tab112)
##
##       No  Yes
##   0 0.05 0.95
##   1 0.11 0.89
chisq.test(tab11)
##
##  Pearson's Chi-squared test with Yates' continuity correction
##
## data:  tab11
## X-squared = 2.8896, df = 1, p-value = 0.08915
#Stem, Confidence DisablingFeatures
tab21 = table(data1$Stem,data1$DisablingFeatures)
tab22=round(prop.table(tab21*100,1),digits=2)
print(tab22)
##
##       No  Yes
##   0 0.26 0.74
##   1 0.23 0.77
chisq.test(tab22)
## Warning in chisq.test(tab22): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test with Yates' continuity correction
##
## data:  tab22
## X-squared = 5.1851e-33, df = 1, p-value = 1
chisq.test(tab00)
##
##  Chi-squared test for given probabilities
##
## data:  tab00
## X-squared = 48.674, df = 1, p-value = 3.023e-12
#collapse PrivInvasion 5 var into 3
newd1 <- fct_collapse(data1$PrivInvasion,
           "disagree" = c("It is not possible", "It is not likely"),
            "agree" = c("It is likely", "It is definite"),
            "maybe" = "Unsure")

# Stem, PrivInvasion
tab32 = table(data1$Stem, newd1  )
tab321=round(prop.table(tab32*100,1),digits=2)
print(tab321)
```

```
##    newd1
##     agree disagree maybe
##   0  0.38     0.17  0.45
##   1  0.47     0.29  0.23
```

```
chisq.test(tab32)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab32
## X-squared = 19.624, df = 2, p-value = 5.48e-05
```

```
tab00 = table(data1$HackedIssue)
print (tab00)
```

```
##
##     It is definite       It is likely   It is not likely It is not
possible
##                  5                 84                138
5
##             Unsure
##                148
```

```
chisq.test(tab00)
```

```
##
##  Chi-squared test for given probabilities
##
## data:  tab00
## X-squared = 252.29, df = 4, p-value < 2.2e-16
```

```
tab40 = table(testa$Stem, data1$HackedIssue )
print (tab40)
```

```
##
##      It is definite It is likely It is not likely It is not possible
Unsure
##    0              0           25               30                 2
65
##    1              5           59              108                 3
83
#chisq.test(tab40, simulate.p.value = TRUE)
chisq.test(tab40)
## Warning in chisq.test(tab40): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab40
## X-squared = 18.998, df = 4, p-value = 0.0007867
#simulate.p.value=TRUE

#collapse HackedIssue 5 var into 3
newd2 <- fct_collapse(data1$HackedIssue,
         "disagree" = c("It is not possible", "It is not likely"),
          "agree" = c("It is likely", "It is definite"),
          "maybe" = "Unsure")

tab4 = table(testa$Stem, newd2 )
tab41=round(prop.table(tab4*100,1),digits=2)
print(tab41)
##     newd2
##      agree disagree maybe
##    0  0.20     0.26  0.53
##    1  0.25     0.43  0.32
chisq.test(tab4)
##
##  Pearson's Chi-squared test
##
## data:  tab4
## X-squared = 16.342, df = 2, p-value = 0.0002827
#collapse ProblematicPriv 5 var into 3
newd3 <- fct_collapse(data1$ProblematicPriv,
         "disagree" = c("Strongly Disagree", "Disagree"),
          "agree" = c("Strongly Agree", "Agree"),
          "maybe" = "Unsure")

tab5= table(testa$Stem, newd3)
tab51=round(prop.table(tab5*100,1),digits=2)
print(tab51)
##    newd3
##     agree disagree maybe
##   0  0.82     0.07  0.11
##   1  0.80     0.12  0.07
chisq.test(tab5)
##
##  Pearson's Chi-squared test
##
## data:  tab5
## X-squared = 4.3319, df = 2, p-value = 0.1146
tab6= table(testa$Stem, testa$HackedTV)
tab61=round(prop.table(tab6*100,1),digits=2)
print(tab61)
##
##     Agree Disagree Strongly Agree Strongly Disagree  Unsure
##   0  0.41     0.09           0.31              0.01   0.18
##   1  0.36     0.11           0.37              0.03   0.13
chisq.test(tab6)
## Warning in chisq.test(tab6): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab6
## X-squared = 4.2218, df = 4, p-value = 0.3768
```

```
#collapse HackedTV Issue 5 var into 3
newd4 <- fct_collapse(data1$HackedTV,
         "disagree" = c("Strongly Disagree", "Disagree"),
          "agree" = c("Strongly Agree", "Agree"),
          "maybe" = "Unsure")

tab6= table(testa$Stem, newd4)
tab61=round(prop.table(tab6*100,1),digits=2)
print(tab61)
```

```
##    newd4
##     agree disagree maybe
##   0  0.72     0.10  0.18
##   1  0.73     0.14  0.13
```

```
chisq.test(tab6)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab6
## X-squared = 2.2706, df = 2, p-value = 0.3213
```

```
# Stem, CameraMicAccess
tab7 = table(testa$Stem, testa$CameraMicAccess )
tab71=round(prop.table(tab7*100,1),digits=2)
print(tab71)
```

```
##
##     Extremely likely Extremely Unlikely Likely Not sure Unlikely
##   0             0.13               0.09   0.34     0.31     0.12
##   1             0.22               0.08   0.32     0.24     0.14
```

```
chisq.test(tab7)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab7
## X-squared = 5.4925, df = 4, p-value = 0.2404
```

```
# Stem, AccessAcceptable
```

```
tab8 = table(testa$Stem, testa$AccessAcceptable )
tab81=round(prop.table(tab8*100,1),digits=2)
print(tab81)
```

```
##
##     Completely acceptable Completely unacceptable Not sure Somewhat
acceptable
##   0                  0.02                    0.46     0.20
0.07
##   1                  0.02                    0.55     0.07
0.06
##
##     Unacceptable
##   0         0.25
##   1         0.30
```

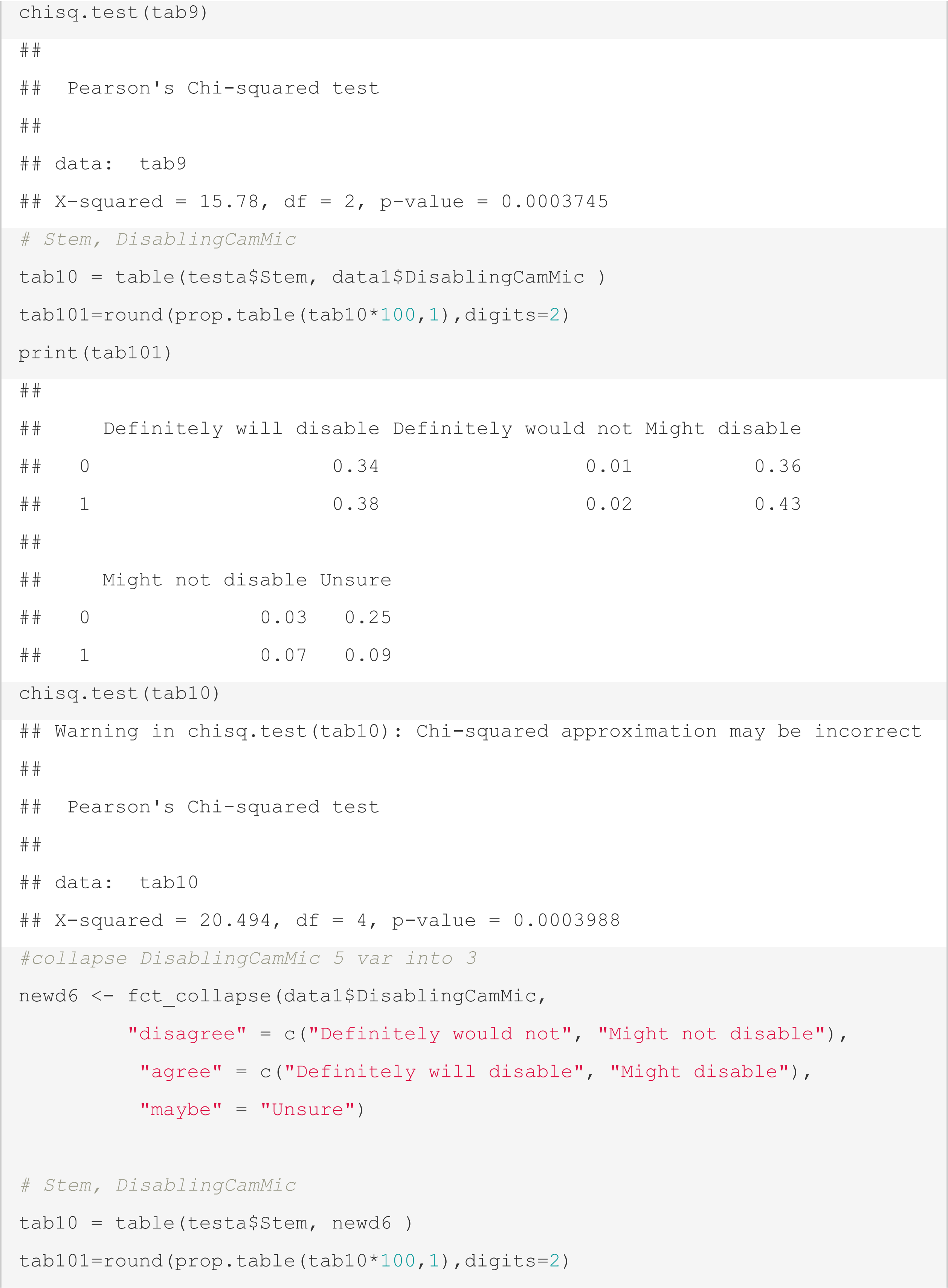
```
chisq.test(tab8)
```

```
## Warning in chisq.test(tab8): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab8
## X-squared = 15.8, df = 4, p-value = 0.003299
```

```
#collapse AccessAcceptable 5 var into 3
newd5 <- fct_collapse(data1$AccessAcceptable,
         "disagree" = c("Completely unacceptable", "Unacceptable"),
          "agree" = c("Completely acceptable", "Somewhat acceptable"),
          "maybe" = "Not sure")

# Stem, AccessAcceptable
tab9 = table(testa$Stem, newd5 )
tab91=round(prop.table(tab9*100,1),digits=2)
print(tab91)
```

```
##    newd5
##     agree disagree maybe
##   0  0.09     0.70  0.20
##   1  0.08     0.85  0.07
```



```
chisq.test(tab9)
##
##  Pearson's Chi-squared test
##
## data:  tab9
## X-squared = 15.78, df = 2, p-value = 0.0003745
# Stem, DisablingCamMic
tab10 = table(testa$Stem, data1$DisablingCamMic )
tab101=round(prop.table(tab10*100,1),digits=2)
print(tab101)
##
##     Definitely will disable Definitely would not Might disable
##   0                    0.34                 0.01          0.36
##   1                    0.38                 0.02          0.43
##
##     Might not disable Unsure
##   0              0.03   0.25
##   1              0.07   0.09
chisq.test(tab10)
## Warning in chisq.test(tab10): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab10
## X-squared = 20.494, df = 4, p-value = 0.0003988
#collapse DisablingCamMic 5 var into 3
newd6 <- fct_collapse(data1$DisablingCamMic,
         "disagree" = c("Definitely would not", "Might not disable"),
          "agree" = c("Definitely will disable", "Might disable"),
          "maybe" = "Unsure")

# Stem, DisablingCamMic
tab10 = table(testa$Stem, newd6 )
tab101=round(prop.table(tab10*100,1),digits=2)
```

```
print(tab101)
##    newd6
##     agree disagree maybe
##   0  0.70     0.04  0.25
##   1  0.81     0.10  0.09
chisq.test(tab10)
##
##  Pearson's Chi-squared test
##
## data:  tab10
## X-squared = 20.404, df = 2, p-value = 3.709e-05
# Stem, ResearchApps
tab11 = table(testa$Stem, data1$ResearchApps )
tab111=round(prop.table(tab11*100,1),digits=2)
print(tab111)
##
##     Definitely not Definitely yes    No Unsure   Yes
##   0           0.01           0.19 0.24   0.24 0.33
##   1           0.04           0.25 0.22   0.14 0.35
chisq.test(tab11)
## Warning in chisq.test(tab11): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab11
## X-squared = 9.4805, df = 4, p-value = 0.05015
#collapse ResearchApp 5 var into 3
newd7 <- fct_collapse(data1$ResearchApps,
          "disagree" = c("Definitely not", "No"),
          "agree" = c("Definitely yes", "Yes"),
          "maybe" = "Unsure")

# Stem, ResearchApps
tab12= table(testa$Stem, newd7 )
```

```
tab121=round(prop.table(tab12*100,1),digits=2)
print(tab121)
```

```
##     newd7
##      disagree agree maybe
##    0     0.25  0.52  0.24
##    1     0.26  0.60  0.14
```

```
chisq.test(tab12)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab12
## X-squared = 5.7566, df = 2, p-value = 0.05623
```

```
# Stem, refrain from installing Apps
tab15 = table(testa$Stem, testa$NoApps )
tab151=round(prop.table(tab15*100,1),digits=2)
print(tab151)
```

```
##
##      Definitely not Definitely yes   No Unsure  Yes
##    0           0.02           0.17 0.10   0.29 0.43
##    1           0.05           0.21 0.15   0.21 0.38
```

```
chisq.test(tab15)
```

```
## Warning in chisq.test(tab15): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab15
## X-squared = 6.7496, df = 4, p-value = 0.1497
```

```
#collapse NoApp 5 var into 3
newd16  <- fct_collapse(data1$NoApps,
          "disagree" = c("Definitely not", "No"),
          "agree" = c("Definitely yes", "Yes"),
          "maybe" = "Unsure")


# Stem, refrain from installing Apps
```

```
tab15 = table(testa$Stem, newd16  )
tab151=round(prop.table(tab15*100,1),digits=2)
print(tab151)
```

```
##    newd16
##     disagree agree maybe
##   0      0.11  0.60  0.29
##   1      0.19  0.60  0.21
```

```
chisq.test(tab15)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab15
## X-squared = 5.2019, df = 2, p-value = 0.0742
```

```
# Stem, DataCollection
tab10 = table(testa$Stem, testa$DataCollection )
tab101=round(prop.table(tab10*100,1),digits=2)
print(tab101)
```

```
##
##     Extremely likely Extremely Unlikely Likely Unlikely Unsure
##   0             0.28               0.00   0.34     0.03   0.34
##   1             0.47               0.01   0.36     0.03   0.13
```

```
chisq.test(tab10)
```

```
## Warning in chisq.test(tab10): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab10
## X-squared = 27.405, df = 4, p-value = 1.647e-05
```

```
#collapse DataCollection 5 var into 2
newd7  <- fct_collapse(data1$DataCollection,
          "disagree" = c("Extremely Unlikely", "Unlikely"),
          "agree" = c("Extremely likely", "Likely"),
          "maybe" =  "Unsure" )
```

```
# Stem, DataCollection
tab11 = table(testa$Stem, newd7)
tab110 =round(prop.table(tab11*100,1),digits=2)
print(tab110)
```

```
##    newd7
##     agree disagree maybe
##   0  0.62     0.03  0.34
##   1  0.83     0.03  0.13
```

```
chisq.test(tab11)
```

```
## Warning in chisq.test(tab11): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab11
## X-squared = 23.496, df = 2, p-value = 7.904e-06
```

```
#collapse CreateProfileHabits 5 var into 3
newd8  <- fct_collapse(data1$CreateProfileHabits,
          "disagree" = c("Extremely Unlikely", "Unlikely" ),
          "agree" = c("Extremely likely", "Likely"),
          "maybe" =  "Unsure" )

# Stem, CreateProfileHabits
tab12 = table(testa$Stem, newd8 )
tab121=round(prop.table(tab12*100,1),digits=2)
print(tab121)
```

```
##    newd8
##     agree disagree maybe
##   0  0.67     0.03  0.30
##   1  0.79     0.05  0.17
```

```
chisq.test(tab12)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab12
## X-squared = 8.3936, df = 2, p-value = 0.01504
```

```
# Stem, ProfileAcceptable
tab12 = table(testa$Stem, testa$ProfileAcceptable )
tab121=round(prop.table(tab12*100,1),digits=2)
print(tab121)
```

```
##
##     Acceptable Extremely acceptable Extremely unacceptable Not sure
##   0       0.09                 0.01                   0.18     0.44
##   1       0.21                 0.01                   0.22     0.19
##
##     Unacceptable
##   0         0.28
##   1         0.37
```

```
chisq.test(tab12)
```

```
## Warning in chisq.test(tab12): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab12
## X-squared = 28.271, df = 4, p-value = 1.099e-05
```

```
#collapse ProfileAcceptable 5 var into 3
newd9  <- fct_collapse(data1$ProfileAcceptable,
          "disagree" = c("Extremely unacceptable", "Unacceptable"),
          "agree" = c("Extremely acceptable", "Acceptable"),
          "maybe" = "Unsure")
```

```
## Warning: Unknown levels in `f`: Unsure
```

```
# Stem, ProfileAcceptable
tab13 = table(testa$Stem, newd9 )
tab131=round(prop.table(tab13*100,1),digits=2)
print(tab131)
```

```
##    newd9
##     agree disagree Not sure
##   0  0.10     0.46     0.44
##   1  0.22     0.59     0.19
```

```
chisq.test(tab13)
##
##  Pearson's Chi-squared test
##
## data:  tab13
## X-squared = 27.822, df = 2, p-value = 9.089e-07
# Stem, Privacy
tab13 = table(testa$Stem, testa$Privacy )
tab131=round(prop.table(tab13*100,1),digits=2)
print(tab131)
##
##     Do not care Protecting my privacy comes first They are equally
important
##   0        0.07                              0.52
0.22
##   1        0.08                              0.56
0.25
##
##     Unsure Using the smart TV features is more important
##   0   0.16                                          0.02
##   1   0.09                                          0.03
chisq.test(tab13)
## Warning in chisq.test(tab13): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab13
## X-squared = 5.2589, df = 4, p-value = 0.2618
#collapse Protecting Privacy 5 var into 3
newd10  <- fct_collapse(data1$Privacy,
          "disagree" = c("They are equally important", "Using the smart TV
features is more important"),
          "agree" = "Protecting my privacy comes first",
          "maybe" =  c("Unsure", "Do not care"))


# Stem, Protecting  Privacy
```

```
tab131 = table(testa$Stem, newd10 )
tab1312=round(prop.table(tab131*100,1),digits=2)
print(tab1312)
##    newd10
##     maybe agree disagree
##   0  0.24  0.52     0.25
##   1  0.16  0.56     0.28
chisq.test(tab131)
##
##  Pearson's Chi-squared test
##
## data:  tab131
## X-squared = 3.0925, df = 2, p-value = 0.213
#collapse Influence Behavior 5 var into 3
newd10  <- fct_collapse(data1$InfluenceBehavior,
          "disagree" = c("No", "Not applicable"),
          "agree" = c("Definitely yes", "Yes"),
          "maybe" =  "Unsure")

# Stem, Security Courses’ Influence Behavior
tab14 = table(testa$Stem, newd10 )
tab141=round(prop.table(tab14*100,1),digits=2)
print(tab141)
##    newd10
##     agree disagree maybe
##   0  0.22     0.66  0.12
##   1  0.49     0.40  0.11
chisq.test(tab14)
##
##  Pearson's Chi-squared test
##
## data:  tab14
## X-squared = 25.743, df = 2, p-value = 2.57e-06
# Stem, SecCourses
```

```
tab15 = table(testa$Stem, testa$SecCourses)

tab151=round(prop.table(tab15*100,1),digits=2)

print(tab151)
```

```
##

##         0    1    2    3    4

##   0 0.57 0.21 0.11 0.06 0.05

##   1 0.31 0.19 0.16 0.09 0.26
```

```
chisq.test(tab151)
```

```
## Warning in chisq.test(tab151): Chi-squared approximation may be
incorrect

##

##  Pearson's Chi-squared test

##

## data:  tab151

## X-squared = 0.23529, df = 4, p-value = 0.9936
```

RESEARCH QUESTION 2: CREDITS: FRESHMAN-SOPHOMORE VS. JUNIOR-SENIOR

2023-08-07

install.packages("dplyr") library(dplyr) library(gmoldes) library(forcats) library(dplyr) library(magrittr) ## Libraries library(tidyr) library(tidyverse) library(haven) library(readxl) library(table1) library(xtable) library(dplyr) library(kableExtra) library(devEMF) library(forcats) library(datasets) library(ggplot2) library(readxl) library(tidyr)

```
testa=read.csv("C:/Spring2023/Participants/Credits.csv", header=TRUE,
sep=",")

#head(testa) # description of data variables in the data

dim(testa)

## [1] 380  23

test_frame <-data.frame(testa)


str(test_frame)

## 'data.frame':    380 obs. of  23 variables:

##  $ Age                : chr  "18-21" "18-21" "35" "18-21" ...

##  $ Major              : chr  "Arts" "Business" "Security" "Business" ...

##  $ Credits            : chr  "31-60" "31-60" "90" "90" ...

##  $ Cr                 : int  0 0 1 1 1 0 1 1 0 0 ...

##  $ Effort             : chr  "Somewhat" "Somewhat" "No" "No" ...

##  $ Confident          : chr  "Yes" "Yes" "Yes" "Yes" ...

##  $ DisablingFeatures  : chr  "Yes" "No" "Yes" "No" ...

##  $ PrivInvasion       : chr  "It is definite" "It is likely" "It is
definite" "It is definite" ...

##  $ HackedIssue        : chr  "It is likely" "It is likely" "It is
likely" "It is likely" ...

##  $ ProblematicPriv    : chr  "Agree" "Agree" "Agree" "Agree" ...

##  $ HackedTV           : chr  "Agree" "Agree" "Agree" "Agree" ...

##  $ CameraMicAccess    : chr  "Extremely likely" "Likely" "Likely"
"Unlikely" ...

##  $ AccessAcceptable   : chr  "Completely unacceptable" "Completely
unacceptable" "Unacceptable" "Completely unacceptable" ...
```

```
##  $ DisablingCamMic    : chr  "Definitely will disable" "Definitely will
disable" "Definitely will disable" "Definitely will disable" ...

##  $ ResearchApps       : chr  "Unsure" "Yes" "Definitely yes" "No" ...

##  $ NoApps             : chr  "No" "Definitely yes" "Definitely not"
"Definitely yes" ...

##  $ DataCollection     : chr  "Extremely likely" "Extremely likely"
"Extremely likely" "Extremely likely" ...

##  $ CreateProfileHabits: chr  "Extremely likely" "Extremely likely"
"Extremely likely" "Extremely likely" ...

##  $ ProfileAcceptable  : chr  "Extremely unacceptable" "Unacceptable"
"Extremely unacceptable" "Unacceptable" ...

##  $ Privacy            : chr  "Protecting my privacy comes first"
"Protecting my privacy comes first" "Protecting my privacy comes first"
"Protecting my privacy comes first" ...

##  $ SecCourses         : int  0 1 4 1 4 4 1 4 0 2 ...

##  $ InfluenceBehavior  : chr  "Not applicable" "No" "Yes" "Unsure" ...

##  $ Stem               : logi  NA NA NA NA NA NA ...
```

```
data1 <-data.frame(testa)


 library(forcats)
```

```
## Warning: package 'forcats' was built under R version 4.2.3
```

```
library(dplyr)
```

```
## Warning: package 'dplyr' was built under R version 4.2.3

##

## Attaching package: 'dplyr'

## The following objects are masked from 'package:stats':

##

##     filter, lag

## The following objects are masked from 'package:base':

##

##     intersect, setdiff, setequal, union
```

```
library(magrittr)
```

```
## Warning: package 'magrittr' was built under R version 4.2.3
```

```
tab00 = table(data1$Cr)

print (tab00)
```

```
##

##   0   1
## 190 190
# Cr, Effort
tab1 = table(data1$Cr, data1$Effort )
tab12=round(prop.table(tab1*100,1),digits=2)
print(tab12)
##
##        No Somewhat  Yes
##    0 0.38     0.53 0.09
##    1 0.41     0.47 0.12
chisq.test(tab1)
##
##  Pearson's Chi-squared test
##
## data:  tab1
## X-squared = 1.7013, df = 2, p-value = 0.4271
#Age, Settings
tab11 = table(data1$Cr, data1$Confident )
tab112=round(prop.table(tab11*100,1),digits=2)
print(tab112)
##
##        No  Yes
##    0 0.11 0.89
##    1 0.07 0.93
chisq.test(tab11)
##
##  Pearson's Chi-squared test with Yates' continuity correction
##
## data:  tab11
## X-squared = 1.1329, df = 1, p-value = 0.2872
tab21 = table(data1$DisablingFeatures)
print (tab21)
##
##  No Yes
##  92 288
```

```
# Cr,   ChangeSettings
tab2 = table(testa$Cr, testa$DisablingFeatures )
tab21=round(prop.table(tab2*100,1),digits=2)
print(tab21)
##
##        No  Yes
##    0 0.25 0.75
##    1 0.24 0.76
chisq.test(tab2)
##
##  Pearson's Chi-squared test with Yates' continuity correction
##
## data:  tab2
## X-squared = 0.014342, df = 1, p-value = 0.9047
tab3 = table(testa$Cr, testa$PrivInvasion )
#prop.table(tab6*100,1)
tab31=round(prop.table(tab3*100,1),digits=2)
print(tab31)
##
##      It is definite It is likely It is not likely It is not possible
Unsure
##    0           0.08         0.27             0.24               0.01
0.40
##    1           0.12         0.42             0.25               0.01
0.21
chisq.test(tab3)
## Warning in chisq.test(tab3): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab3
## X-squared = 19.622, df = 4, p-value = 0.000593
#collapse PrivInvasion 5 var into 3
newd1 <- fct_collapse(data1$PrivInvasion,
         "disagree" = c("It is not possible", "It is not likely"),
          "agree" = c("It is likely", "It is definite"),
          "maybe" = "Unsure")

tab3 = table(testa$Cr, newd1)
#prop.table(tab6*100,1)
tab31=round(prop.table(tab3*100,1),digits=2)
print(tab31)
```

```
##    newd1
##     agree disagree maybe
##   0  0.35     0.25  0.40
##   1  0.54     0.26  0.21
```

```
chisq.test(tab3)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab3
## X-squared = 19.195, df = 2, p-value = 6.791e-05
```

```
#collapse HackedIssue 5 var into 3
newd2 <- fct_collapse(data1$HackedIssue,
         "disagree" = c("It is not possible", "It is not likely"),
          "agree" = c("It is likely", "It is definite"),
          "maybe" = "Unsure")

tab4 = table(testa$Cr, newd2 )
tab41=round(prop.table(tab4*100,1),digits=2)
print(tab41)
```

```
##    newd2
##     agree disagree maybe
##   0  0.19     0.35  0.46
##   1  0.28     0.41  0.32
```

```
chisq.test(tab4)
```

```
##
##  Pearson's Chi-squared test
##
```

```
## data:  tab4
## X-squared = 9.3906, df = 2, p-value = 0.009138
#collapse ProblematicPriv 5 var into 3
newd3 <- fct_collapse(data1$ProblematicPriv,
         "disagree" = c("Strongly Disagree", "Disagree"),
          "agree" = c("Strongly Agree", "Agree"),
          "maybe" = "Unsure")

tab5= table(testa$Cr, newd3)
tab51=round(prop.table(tab5*100,1),digits=2)
print(tab51)
##    newd3
##     agree disagree maybe
##   0  0.81     0.08  0.11
##   1  0.81     0.13  0.07
chisq.test(tab5)
##
##  Pearson's Chi-squared test
##
## data:  tab5
## X-squared = 3.0881, df = 2, p-value = 0.2135
tab6= table(testa$Cr, testa$HackedTV)
tab61=round(prop.table(tab6*100,1),digits=2)
print(tab61)
##
##     Agree Disagree Strongly Agree Strongly Disagree Unsure
##   0  0.39     0.10           0.33              0.01   0.16
##   1  0.36     0.11           0.37              0.03   0.13
chisq.test(tab6)
## Warning in chisq.test(tab6): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab6
## X-squared = 3.2869, df = 4, p-value = 0.511
```

```r
#collapse HackedTV 5 var into 3
newd4 <- fct_collapse(data1$HackedTV,
         "disagree" = c("Strongly Disagree", "Disagree"),
          "agree" = c("Strongly Agree", "Agree"),
           "maybe" = "Not sure")
```

```
## Warning: Unknown levels in `f`: Not sure
```

```r
tab6= table(testa$Cr, newd4)
tab61=round(prop.table(tab6*100,1),digits=2)
print(tab61)
```

```
##    newd4
##     agree disagree Unsure
##   0  0.73     0.11   0.16
##   1  0.73     0.14   0.13
```

```r
chisq.test(tab6)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab6
## X-squared = 1.1784, df = 2, p-value = 0.5548
```

```r
#collapse CameraMicAccess 5 var into 3
newd4 <- fct_collapse(data1$CameraMicAccess,
         "disagree" = c("Extremely Unlikely", "Unlikely"),
          "agree" = c("Extremely likely", "Likely"),
          "maybe" = "Not sure")

#  Cr,CameraMicAccess
tab7 = table(testa$Cr, newd4 )
tab71=round(prop.table(tab7*100,1),digits=2)
print(tab71)
```

```
##    newd4
##     agree disagree maybe
##   0  0.48     0.18  0.34
##   1  0.55     0.26  0.19
```

```
chisq.test(tab7)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab7
## X-squared = 11.409, df = 2, p-value = 0.003331
```

```
# Age, AccessAcceptable
tab8 = table(testa$Cr, testa$AccessAcceptable )
tab81=round(prop.table(tab8*100,1),digits=2)
print(tab81)
```

```
##
##     Completely acceptable Completely unacceptable Not sure Somewhat
acceptable
##   0                  0.03                    0.44     0.17
0.04
##   1                  0.01                    0.61     0.05
0.08
##
##     Unacceptable
##   0         0.32
##   1         0.25
```

```
chisq.test(tab8)
```

```
## Warning in chisq.test(tab8): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab8
## X-squared = 23.485, df = 4, p-value = 0.0001013
```

```
#collapse AccessAcceptable 5 var into 3
newd5 <- fct_collapse(data1$AccessAcceptable,
         "disagree" = c("Completely unacceptable", "Unacceptable"),
          "agree" = c("Completely acceptable", "Somewhat acceptable"),
          "maybe" = "Not sure")


#  Cr, AccessAcceptable
```

```
tab9 = table(testa$Cr, newd5 )
tab91=round(prop.table(tab9*100,1),digits=2)
print(tab91)
##    newd5
##     agree disagree maybe
##   0  0.07     0.75  0.17
##   1  0.09     0.86  0.05
chisq.test(tab9)
## 
##  Pearson's Chi-squared test
## 
## data:  tab9
## X-squared = 13.9, df = 2, p-value = 0.0009587
#collapse DisablingCamMic 5 var into 3
newd6 <- fct_collapse(data1$DisablingCamMic,
         "disagree" = c("Might not disable", "Definitely would not"),
          "agree" = c("Definitely will disable", "Might disable"),
          "maybe" = "Not sure")
## Warning: Unknown levels in `f`: Not sure
#  Cr,DisablingCamMic
tab10 = table(testa$Cr, data1$DisablingCamMic )
tab101=round(prop.table(tab10*100,1),digits=2)
print(tab101)
##    
##     Definitely will disable Definitely would not Might disable
##   0                    0.33                 0.02          0.38
##   1                    0.41                 0.02          0.44
##    
##     Might not disable Unsure
##   0              0.06   0.22
##   1              0.06   0.06
chisq.test(tab10)
## Warning in chisq.test(tab10): Chi-squared approximation may be incorrect
## 
```

```
##  Pearson's Chi-squared test
##
## data:  tab10
## X-squared = 19.605, df = 4, p-value = 0.0005976
#  Cr,  DisablingCamMic
tab10 = table(testa$Cr, newd6 )
tab101=round(prop.table(tab10*100,1),digits=2)
print(tab101)
##    newd6
##     agree disagree Unsure
##   0  0.71     0.07   0.22
##   1  0.85     0.08   0.06
chisq.test(tab10)
##
##  Pearson's Chi-squared test
##
## data:  tab10
## X-squared = 19.449, df = 2, p-value = 5.981e-05
#  Cr,  ResearchApps
tab11 = table(testa$Cr, data1$ResearchApps )
tab111=round(prop.table(tab11*100,1),digits=2)
print(tab111)
##
##     Definitely not Definitely yes   No Unsure   Yes
##   0           0.02           0.20 0.22   0.23 0.33
##   1           0.05           0.26 0.23   0.11 0.35
chisq.test(tab11)
##
##  Pearson's Chi-squared test
##
## data:  tab11
## X-squared = 12.91, df = 4, p-value = 0.01173
#collapse ResearchApp 5 var into 3
newd7 <- fct_collapse(data1$ResearchApps,
          "disagree" = c("Definitely not", "No"),
          "agree" = c("Definitely yes", "Yes"),
          "maybe" = "Unsure")

#  Cr,  ResearchApps
tab12= table(testa$Cr, newd7 )
tab121=round(prop.table(tab12*100,1),digits=2)
print(tab121)
```

```
##    newd7
##     disagree agree maybe
##   0     0.24  0.53  0.23
##   1     0.27  0.62  0.11
```

```
chisq.test(tab12)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab12
## X-squared = 9.8179, df = 2, p-value = 0.00738
```

```
# Age,  refrain from installing Apps
tab15 = table(testa$Cr, testa$NoApps )
tab151=round(prop.table(tab15*100,1),digits=2)
print(tab151)
```

```
##
##     Definitely not Definitely yes    No Unsure  Yes
##   0           0.02           0.17 0.13   0.29 0.38
##   1           0.05           0.23 0.13   0.18 0.41
```

```
chisq.test(tab15)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab15
## X-squared = 9.0078, df = 4, p-value = 0.0609
```

```
#collapse NoApp 5 var into 3
newd16 <- fct_collapse(testa$NoApps,
          "disagree" = c("Definitely not", "No"),
          "agree" = c("Definitely yes", "Yes"),
          "maybe" = "Unsure")

# Cr,   refrain from installing Apps
tab15 = table(testa$Cr, newd16  )
tab151=round(prop.table(tab15*100,1),digits=2)
print(tab151)
##    newd16
##     disagree agree maybe
##   0     0.15  0.56  0.29
##   1     0.18  0.64  0.18
chisq.test(tab15)
##
##  Pearson's Chi-squared test
##
## data:  tab15
## X-squared = 6.5087, df = 2, p-value = 0.03861
#Cr,    DataCollection
tab10 = table(testa$Cr, testa$DataCollection )
tab101=round(prop.table(tab10*100,1),digits=2)
print(tab101)
##
##     Extremely likely Extremely Unlikely Likely Unlikely Unsure
##   0             0.36               0.01   0.35     0.02   0.26
##   1             0.45               0.01   0.36     0.04   0.14
chisq.test(tab10)
## Warning in chisq.test(tab10): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab10
## X-squared = 11.746, df = 4, p-value = 0.01935
#collapse DataCollection 5 var into 3
```

```
newd7  <- fct_collapse(data1$DataCollection,
          "disagree" = c("Extremely Unlikely", "Unlikely"),
          "agree" = c("Extremely likely", "Likely"),
          "maybe" = "Unsure")

# Cr,   DataCollection
tab11 = table(testa$Cr, newd7)
tab110 =round(prop.table(tab11*100,1),digits=2)
print(tab110)
```

```
##    newd7
##     agree disagree maybe
##   0  0.72     0.02  0.26
##   1  0.82     0.05  0.14
```

```
chisq.test(tab11)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab11
## X-squared = 10.743, df = 2, p-value = 0.004648
```

```
# Cr,   CreateProfileHabits
tab12 = table(testa$Cr, testa$CreateProfileHabits )
tab121=round(prop.table(tab12*100,1),digits=2)
print(tab121)
```

```
##
##     Extremely likely Extremely Unlikely Likely Unlikely Unsure
##   0             0.33               0.01   0.34     0.04   0.28
##   1             0.45               0.00   0.38     0.04   0.13
```

```
chisq.test(tab12)
```

```
## Warning in chisq.test(tab12): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab12
## X-squared = 16.788, df = 4, p-value = 0.002125
```

```
#collapse CreateProfileHabits 5 var into 3
newd8  <- fct_collapse(data1$CreateProfileHabits,
          "disagree" = c("Extremely Unlikely", "Unlikely"),
          "agree" = c("Extremely likely", "Likely"),
          "maybe" = "Unsure")



# Cr,   CreateProfileHabits
tab12 = table(testa$Cr, newd8 )
tab121=round(prop.table(tab12*100,1),digits=2)
print(tab121)
```

```
##    newd8
##     agree disagree maybe
##   0  0.67     0.05  0.28
##   1  0.83     0.04  0.13
```

```
chisq.test(tab12)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab12
## X-squared = 14.969, df = 2, p-value = 0.0005617
```

```
# Cr,   ProfileAcceptable
tab12 = table(testa$Cr, testa$ProfileAcceptable )
tab121=round(prop.table(tab12*100,1),digits=2)
print(tab121)
```

```
##
##     Acceptable Extremely acceptable Extremely unacceptable Not sure
##   0       0.20                 0.01                   0.16     0.29
##   1       0.14                 0.01                   0.25     0.26
##
##     Unacceptable
##   0         0.35
##   1         0.34
```

```
chisq.test(tab12)
```

```
## Warning in chisq.test(tab12): Chi-squared approximation may be incorrect
##
##  Pearson's Chi-squared test
##
## data:  tab12
## X-squared = 6.7256, df = 4, p-value = 0.1511
```

```
#collapse   ProfileAcceptable 5 var into 3
newd9  <- fct_collapse(data1$ProfileAcceptable,
          "disagree" = c("Extremely unacceptable", "Unacceptable"),
          "agree" = c("Extremely acceptable", "Acceptable"),
          "maybe" = "Unsure")
```

```
## Warning: Unknown levels in `f`: Unsure
```

```
# Cr,   ProfileAcceptable
tab13 = table(testa$Cr, newd9 )
tab131=round(prop.table(tab13*100,1),digits=2)
print(tab131)
```

```
##    newd9
##     agree disagree Not sure
##   0  0.21     0.51     0.29
##   1  0.15     0.59     0.26
```

```
chisq.test(tab13)
```

```
##
##  Pearson's Chi-squared test
##
## data:  tab13
## X-squared = 3.0475, df = 2, p-value = 0.2179
```

```
# Cr, Privacy More imp
tab13 = table(testa$Cr, testa$Privacy )
tab131=round(prop.table(tab13*100,1),digits=2)
print(tab131)
```

```
##
##     Do not care Protecting my privacy comes first They are equally
important
##   0        0.06                              0.57
0.19
```

```
##   1        0.09                              0.52
0.29
##
##      Unsure Using the smart TV features is more important
##   0   0.14                                              0.04
##   1   0.08                                              0.02
chisq.test(tab13)
##
##  Pearson's Chi-squared test
##
## data:  tab13
## X-squared = 9.7754, df = 4, p-value = 0.04439
#collapse Privacy 5 var into 3
newd11 <- fct_collapse(data1$Privacy,
          "disagree" = c("Using the smart TV features is more important",
"They are equally important"),
          "agree" = "Protecting my privacy comes first",
           "maybe" =  c("Do not care", "Unsure"))



# Cr,   Privacy More imp
tab131 = table(testa$Cr, newd11 )
tab1312=round(prop.table(tab131*100,1),digits=2)
print(tab1312)
##     newd11
##      maybe agree disagree
##   0  0.20  0.57     0.23
##   1  0.17  0.52     0.31
chisq.test(tab131)
##
##  Pearson's Chi-squared test
##
## data:  tab131
## X-squared = 3.4465, df = 2, p-value = 0.1785
#collapse InfluenceBehavior 5 var into 3
```

```
newd10  <- fct_collapse(data1$InfluenceBehavior,
          "disagree" = c("No", "Not applicable"),
          "agree" = c("Yes", "Definitely yes"),
           "maybe" =  "Unsure")

#   Cr, InfluenceBehavior
tab14 = table(testa$Cr, newd10 )
tab141=round(prop.table(tab14*100,1),digits=2)
print(tab141)
##     newd10
##      agree disagree maybe
##    0  0.26     0.58  0.15
##    1  0.54     0.38  0.07
chisq.test(tab14)
##
##  Pearson's Chi-squared test
##
## data:  tab14
## X-squared = 31.44, df = 2, p-value = 1.489e-07
# Cr,   SecCourses
tab14 = table(testa$Cr, testa$SecCourses)
tab141=round(prop.table(tab14*100,1),digits=2)
print(tab141)
##
##         0    1    2    3    4
##    0 0.54 0.22 0.13 0.06 0.06
##    1 0.24 0.17 0.17 0.10 0.32
```

APPENDIX E.

LOGISTIC REGRESSION

2023-09-01

install.packages(“dplyr”) library(dplyr) library(gmoldes) library(forcats) library(dplyr) library(magrittr) ## Libraries library(tidyr) library(tidyverse) library(haven) library(readxl) library(table1) library(xtable) library(dplyr) library(kableExtra) library(devEMF) library(forcats) library(datasets) library(ggplot2) library(readxl) library(tidyr)

```
testa=read.csv("C:/Fall_2023/News1.csv", header=TRUE, sep=",")
head(testa) # description of data variables in the data
```

```
##   AGeGRoupC     Major SecCourses Stem Credits creditb     PrivInvasion
privqc
## 1         0 Computers          3    1      90       1 It is not likely
0
## 2         0  Security          4    1      90       1     It is likely
1
## 3         0  Security          4    1      90       1     It is likely
1
## 4         0 Computers          4    1      90       1     It is likely
1
## 5         0  Security          4    1      90       1     It is likely
1
## 6         0  Security          4    1      90       1   It is definite
1
##         HackedIssue Hackqc  CameraMicAccess camerac
AccessAcceptable
## 1 It is not likely      0 Extremely likely       1
Unacceptable
## 2 It is not likely      0           Likely       1
Unacceptable
## 3           Unsure      0           Likely       1
Unacceptable
## 4 It is not likely      0         Not sure       0 Completely
unacceptable
## 5     It is likely      1         Unlikely       0 Completely
unacceptable
```

```
## 6 It is not likely      0        Unlikely       0 Completely
unacceptable
##   accessc       X_DisablingCamMic disablec   ResearchApps rappsc
NoApps
## 1       1           Might disable        1             No      0
No
## 2       1 Definitely will disable        1            Yes      1
Yes
## 3       1           Might disable        1            Yes      1
Unsure
## 4       1           Might disable        1 Definitely yes      1
Yes
## 5       1           Might disable        1 Definitely yes      1
No
## 6       1 Definitely will disable        1 Definitely yes      1
Definitely yes
##   NoAppsc   DataCollection DataCollb CreateProfileHabits creatpc
## 1       0 Extremely likely         1    Extremely likely       1
## 2       1           Likely         1              Likely       1
## 3       0           Likely         1    Extremely likely       1
## 4       1           Likely         1              Likely       1
## 5       0 Extremely likely         1    Extremely likely       1
## 6       1 Extremely likely         1              Likely       1
##         ProfileAcceptable profc InfluenceBehavior inflc
## 1            Unacceptable     1    Definitely yes     1
## 2            Unacceptable     1    Definitely yes     1
## 3            Unacceptable     1    Definitely yes     1
## 4              Acceptable     0    Definitely yes     1
## 5            Unacceptable     1    Definitely yes     1
## 6 Extremely unacceptable      1    Definitely yes     1
```

```
test_frame <-data.frame(testa)


data1 <-data.frame(testa)


#library(glm)
library(forcats)
```

```
## Warning: package 'forcats' was built under R version 4.2.3
```

```
library(dplyr)
## Warning: package 'dplyr' was built under R version 4.2.3
##
## Attaching package: 'dplyr'
## The following objects are masked from 'package:stats':
##
##     filter, lag
## The following objects are masked from 'package:base':
##
##     intersect, setdiff, setequal, union
library(magrittr)
## Warning: package 'magrittr' was built under R version 4.2.3
#for Privacy
model = glm(privqc~AGeGRoupC+creditb+Stem+SecCourses, family="binomial",
data=test_frame )


summary(model)
##
## Call:
## glm(formula = privqc ~ AGeGRoupC + creditb + Stem + SecCourses,
##     family = "binomial", data = test_frame)
##
## Deviance Residuals:
##     Min       1Q   Median       3Q      Max
## -1.4626  -1.0220  -0.8537   1.1691   1.5402
##
## Coefficients:
##             Estimate Std. Error z value Pr(>|z|)
## (Intercept)  -0.8217     0.1753  -4.688 2.76e-06 ***
## AGeGRoupC     0.3540     0.2578   1.373   0.1697
## creditb       0.4446     0.2414   1.841   0.0656 .
## Stem          0.1435     0.2965   0.484   0.6285
## SecCourses    0.1322     0.1025   1.290   0.1970
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
##
## (Dispersion parameter for binomial family taken to be 1)
##
##     Null deviance: 521.69  on 379  degrees of freedom
## Residual deviance: 500.94  on 375  degrees of freedom
## AIC: 510.94
##
## Number of Fisher Scoring iterations: 4
```

```
exp(cbind(Odds_Ratio = coef(model), confint(model)))
```

```
## Waiting for profiling to be done...
##              Odds_Ratio     2.5 %    97.5 %
## (Intercept)  0.4396848 0.3097797 0.6166475
## AGeGRoupC    1.4247854 0.8592286 2.3652266
## creditb      1.5598365 0.9711493 2.5061982
## Stem         1.1542651 0.6434914 2.0643100
## SecCourses   1.1413875 0.9333810 1.3964418
```

```
# for Hack
model2 = glm(Hackqc~AGeGRoupC+creditb+Stem+SecCourses, family="binomial",
data=test_frame )


summary(model2)
```

```
##
## Call:
## glm(formula = Hackqc ~ AGeGRoupC + creditb + Stem + SecCourses,
##     family = "binomial", data = test_frame)
##
## Deviance Residuals:
##     Min       1Q   Median       3Q      Max
## -0.9114  -0.7695  -0.6458  -0.6170   1.8716
##
## Coefficients:
##              Estimate Std. Error z value Pr(>|z|)
## (Intercept)  -1.5610     0.2105  -7.417  1.2e-13 ***
## AGeGRoupC    -0.1040     0.2934  -0.354    0.723
## creditb       0.3962     0.2823   1.404    0.160
## Stem         -0.0346     0.3423  -0.101    0.919
## SecCourses    0.1339     0.1153   1.161    0.245
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
##
## (Dispersion parameter for binomial family taken to be 1)
##
##     Null deviance: 413.68  on 379  degrees of freedom
## Residual deviance: 406.96  on 375  degrees of freedom
## AIC: 416.96
##
## Number of Fisher Scoring iterations: 4
```

```
#exp(coef(model))


exp(cbind(Odds_Ratio = coef(model2), confint(model2)))
```

```
## Waiting for profiling to be done...
##             Odds_Ratio     2.5 %    97.5 %
## (Intercept)  0.2099373 0.1367648 0.3127799
## AGeGRoupC    0.9012371 0.5017649 1.5899190
## creditb      1.4862445 0.8550671 2.5924618
## Stem         0.9659890 0.4912853 1.8877933
## SecCourses   1.1432358 0.9108058 1.4329657
```

```
#for Camera Access
model3 = glm(camerac~AGeGRoupC+creditb+Stem+SecCourses, family="binomial",
data=test_frame )


summary(model3)
```

```
##
## Call:
## glm(formula = camerac ~ AGeGRoupC + creditb + Stem + SecCourses,
##     family = "binomial", data = test_frame)
##
```

```
## Deviance Residuals:
##     Min       1Q   Median       3Q      Max
## -1.5815  -1.0746   0.8481   1.1813   1.3219
##
## Coefficients:
##             Estimate Std. Error z value Pr(>|z|)
## (Intercept) -0.25758    0.16620  -1.550  0.12118
## AGeGRoupC    0.24846    0.26081   0.953  0.34077
## creditb     -0.07587    0.24126  -0.314  0.75316
## Stem        -0.29307    0.29740  -0.985  0.32440
## SecCourses   0.30386    0.10480   2.899  0.00374 **
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
##
## (Dispersion parameter for binomial family taken to be 1)
##
##     Null deviance: 526.28  on 379  degrees of freedom
## Residual deviance: 511.84  on 375  degrees of freedom
## AIC: 521.84
##
## Number of Fisher Scoring iterations: 4
```

```
exp(cbind(Odds_Ratio = coef(model3), confint(model3)))
```

```
## Waiting for profiling to be done...
##             Odds_Ratio     2.5 %   97.5 %
## (Intercept)  0.7729186 0.5568494 1.069495
## AGeGRoupC    1.2820478 0.7696325 2.144239
## creditb      0.9269348 0.5756562 1.484588
## Stem         0.7459679 0.4133568 1.330220
## SecCourses   1.3550831 1.1061458 1.669876
```

```
#for Access

model4 = glm(accessc~AGeGRoupC+creditb+Stem+SecCourses, family="binomial",
data=test_frame )


summary(model4)
```

```
##
## Call:
## glm(formula = accessc ~ AGeGRoupC + creditb + Stem + SecCourses,
##     family = "binomial", data = test_frame)
##
## Deviance Residuals:
##     Min       1Q   Median       3Q      Max
## -2.3277   0.3712   0.5571   0.7686   1.0008
##
## Coefficients:
##             Estimate Std. Error z value Pr(>|z|)
## (Intercept)   0.8748     0.1888   4.634 3.58e-06 ***
## AGeGRoupC    -0.4440     0.3431  -1.294   0.1957
## creditb       0.5230     0.3148   1.662   0.0966 .
## Stem          0.4687     0.3938   1.190   0.2341
## SecCourses    0.1935     0.1453   1.332   0.1829
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
##
## (Dispersion parameter for binomial family taken to be 1)
##
##     Null deviance: 374.69  on 379  degrees of freedom
## Residual deviance: 356.66  on 375  degrees of freedom
## AIC: 366.66
##
## Number of Fisher Scoring iterations: 4
```

```
exp(cbind(Odds_Ratio = coef(model4), confint(model4)))
```

```
## Waiting for profiling to be done...
##             Odds_Ratio     2.5 %   97.5 %
## (Intercept)  2.3983558 1.6686575 3.503508
## AGeGRoupC    0.6414957 0.3278163 1.267367
## creditb      1.6871604 0.9178345 3.166045
## Stem         1.5978516 0.7426742 3.493405
## SecCourses   1.2134312 0.9196308 1.629972
```

```
#for Disable Features
model5 = glm(disablec~AGeGRoupC+creditb+Stem+SecCourses, family="binomial",
data=test_frame )


summary(model5)
```

```
##
## Call:
## glm(formula = disablec ~ AGeGRoupC + creditb + Stem + SecCourses,
##     family = "binomial", data = test_frame)
##
## Deviance Residuals:
##     Min       1Q   Median       3Q      Max
## -2.1419   0.4612   0.5875   0.7764   0.9124
##
## Coefficients:
##             Estimate Std. Error z value Pr(>|z|)
## (Intercept)  0.68935    0.18160   3.796 0.000147 ***
## AGeGRoupC   -0.02826    0.33734  -0.084 0.933232
## creditb      0.65308    0.29822   2.190 0.028531 *
## Stem         0.19213    0.36791   0.522 0.601506
## SecCourses   0.16323    0.13610   1.199 0.230387
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
##
## (Dispersion parameter for binomial family taken to be 1)
##
##     Null deviance: 401.46  on 379  degrees of freedom
## Residual deviance: 384.58  on 375  degrees of freedom
## AIC: 394.58
##
## Number of Fisher Scoring iterations: 4
```

```
exp(cbind(Odds_Ratio = coef(model5), confint(model5)))
```

```
## Waiting for profiling to be done...
##             Odds_Ratio     2.5 %   97.5 %
## (Intercept)  1.9924170 1.4031229 2.863888
## AGeGRoupC    0.9721337 0.5060419 1.913391
## creditb      1.9214476 1.0792322 3.486400
## Stem         1.2118327 0.5900898 2.505383
## SecCourses   1.1773084 0.9066199 1.549474
```

```
#for Research Apps
model6 = glm(rappsc~AGeGRoupC+creditb+Stem+SecCourses, family="binomial",
data=test_frame )


summary(model6)
```

```
##
## Call:
## glm(formula = rappsc ~ AGeGRoupC + creditb + Stem + SecCourses,
##     family = "binomial", data = test_frame)
##
## Deviance Residuals:
##     Min       1Q   Median       3Q      Max
## -1.5298  -1.1955   0.8753   1.0940   1.2119
##
## Coefficients:
##             Estimate Std. Error z value Pr(>|z|)
## (Intercept) -0.08086    0.16542  -0.489    0.625
## AGeGRoupC    0.03674    0.26288   0.140    0.889
## creditb      0.12326    0.24233   0.509    0.611
## Stem         0.47891    0.29746   1.610    0.107
## SecCourses   0.06016    0.10418   0.577    0.564
##
## (Dispersion parameter for binomial family taken to be 1)
##
##     Null deviance: 518.51  on 379  degrees of freedom
## Residual deviance: 508.03  on 375  degrees of freedom
## AIC: 518.03
##
## Number of Fisher Scoring iterations: 4
```

```
exp(cbind(Odds_Ratio = coef(model5), confint(model6)))
## Waiting for profiling to be done...
##             Odds_Ratio     2.5 %   97.5 %
## (Intercept)  1.9924170 0.6662380 1.275704
## AGeGRoupC    0.9721337 0.6200940 1.741858
## creditb      1.9214476 0.7027193 1.820022
## Stem         1.2118327 0.9027373 2.906919
## SecCourses   1.1773084 0.8657555 1.304059
#for No Apps
model7 = glm(NoAppsc~AGeGRoupC+creditb+Stem+SecCourses, family="binomial",
data=test_frame )


summary(model7)
##
## Call:
## glm(formula = NoAppsc ~ AGeGRoupC + creditb + Stem + SecCourses,
##     family = "binomial", data = test_frame)
##
## Deviance Residuals:
##     Min       1Q   Median       3Q      Max
## -1.5276  -1.2573   0.9258   1.0266   1.1110
##
## Coefficients:
##             Estimate Std. Error z value Pr(>|z|)
## (Intercept)  0.18582    0.16587   1.120    0.263
## AGeGRoupC    0.06714    0.26254   0.256    0.798
## creditb      0.24678    0.24196   1.020    0.308
## Stem        -0.10117    0.29780  -0.340    0.734
## SecCourses   0.07352    0.10415   0.706    0.480
##
## (Dispersion parameter for binomial family taken to be 1)
##
##     Null deviance: 513.07  on 379  degrees of freedom
## Residual deviance: 509.89  on 375  degrees of freedom
## AIC: 519.89
##
## Number of Fisher Scoring iterations: 4
```

```
exp(cbind(Odds_Ratio = coef(model7), confint(model7)))
```

```
## Waiting for profiling to be done...
##              Odds_Ratio     2.5 %   97.5 %
## (Intercept)  1.2042099 0.8707576 1.670263
## AGeGRoupC    1.0694492 0.6401852 1.796029
## creditb      1.2798949 0.7969845 2.061122
## Stem         0.9037809 0.5026297 1.620206
## SecCourses   1.0762951 0.8781984 1.322487
```

```
# Data Collection
model8 = glm(DataCollb~AGeGRoupC+creditb+Stem+SecCourses,
family="binomial", data=test_frame )


summary(model8)
```

```
##
## Call:
## glm(formula = DataCollb ~ AGeGRoupC + creditb + Stem + SecCourses,
##     family = "binomial", data = test_frame)
##
## Deviance Residuals:
##     Min       1Q   Median       3Q      Max
## -2.1350   0.4698   0.5355   0.8219   0.9432
##
## Coefficients:
##              Estimate Std. Error z value Pr(>|z|)
## (Intercept)  0.64864    0.18039   3.596 0.000324 ***
## AGeGRoupC    0.23219    0.33432   0.695 0.487366
## creditb      0.26312    0.29152   0.903 0.366742
## Stem         1.05032    0.37468   2.803 0.005059 **
## SecCourses  -0.02308    0.12969  -0.178 0.858784
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
```

```
##
## (Dispersion parameter for binomial family taken to be 1)
##
##     Null deviance: 408.88  on 379  degrees of freedom
## Residual deviance: 388.52  on 375  degrees of freedom
## AIC: 398.52
##
## Number of Fisher Scoring iterations: 4
exp(cbind(Odds_Ratio = coef(model8), confint(model8)))
## Waiting for profiling to be done...
##             Odds_Ratio     2.5 %   97.5 %
## (Intercept)  1.9129315 1.3497971 2.741992
## AGeGRoupC    1.2613539 0.6628815 2.475013
## creditb      1.3009885 0.7368317 2.317397
## Stem         2.8585766 1.3872002 6.057280
## SecCourses   0.9771889 0.7589115 1.265109
# Create Profile
model9 = glm(creatpc~AGeGRoupC+AGeGRoupC+creditb+Stem+SecCourses,
family="binomial", data=test_frame )


summary(model9)
##
## Call:
## glm(formula = creatpc ~ AGeGRoupC + AGeGRoupC + creditb + Stem +
##     SecCourses, family = "binomial", data = test_frame)
##
## Deviance Residuals:
##      Min        1Q    Median        3Q       Max
## -2.30448  -0.05244   0.58659   0.81794   1.00960
##
## Coefficients:
##             Estimate Std. Error z value Pr(>|z|)
## (Intercept)  0.40843    0.17577   2.324   0.0201 *
## AGeGRoupC    0.90968    0.36931   2.463   0.0138 *
## creditb      0.48180    0.28381   1.698   0.0896 .
## Stem         0.42548    0.35725   1.191   0.2337
## SecCourses   0.08927    0.13026   0.685   0.4931
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
##
## (Dispersion parameter for binomial family taken to be 1)
##
##     Null deviance: 427.37  on 379  degrees of freedom
## Residual deviance: 398.52  on 375  degrees of freedom
## AIC: 408.52
##
## Number of Fisher Scoring iterations: 4
```

```
exp(cbind(Odds_Ratio = coef(model9), confint(model9)))
```

```
## Waiting for profiling to be done...
##             Odds_Ratio     2.5 %   97.5 %
## (Intercept)   1.504449 1.0690115 2.132362
## AGeGRoupC     2.483528 1.2409596 5.344576
## creditb       1.618980 0.9321119 2.843890
## Stem          1.530320 0.7619597 3.104365
## SecCourses    1.093371 0.8497194 1.419364
```

```
# Create Profile Accetable
model10 = glm(profc~AGeGRoupC+creditb+Stem+SecCourses, family="binomial",
data=test_frame )


summary(model10)
```

```
##
## Call:
## glm(formula = profc ~ AGeGRoupC + creditb + Stem + SecCourses,
##     family = "binomial", data = test_frame)
##
## Deviance Residuals:
##     Min       1Q   Median       3Q      Max
## -1.4846  -1.2008   0.8986   1.1080   1.2293
```

```
##
## Coefficients:
##              Estimate Std. Error z value Pr(>|z|)
## (Intercept) -0.121169   0.165144  -0.734   0.4631
## AGeGRoupC    0.002897   0.259501   0.011   0.9911
## creditb      0.110488   0.239669   0.461   0.6448
## Stem         0.001731   0.294196   0.006   0.9953
## SecCourses   0.176065   0.103447   1.702   0.0888 .
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
##
## (Dispersion parameter for binomial family taken to be 1)
##
##     Null deviance: 523.38  on 379  degrees of freedom
## Residual deviance: 515.39  on 375  degrees of freedom
## AIC: 525.39
##
## Number of Fisher Scoring iterations: 4
```

```
exp(cbind(Odds_Ratio = coef(model10), confint(model10)))
```

```
## Waiting for profiling to be done...
##             Odds_Ratio     2.5 %   97.5 %
## (Intercept)  0.8858846 0.6401256 1.224347
## AGeGRoupC    1.0029009 0.6028285 1.670851
## creditb      1.1168231 0.6972878 1.787060
## Stem         1.0017320 0.5607702 1.782207
## SecCourses   1.1925151 0.9748977 1.464035
```

```
# Courses influence Behavior
model11 = glm(inflc~AGeGRoupC+creditb+Stem+SecCourses, family="binomial",
data=test_frame )


summary(model11)
```

```
##
## Call:
## glm(formula = inflc ~ AGeGRoupC + creditb + Stem + SecCourses,
##     family = "binomial", data = test_frame)
##
## Deviance Residuals:
##     Min       1Q   Median       3Q      Max
## -2.2182  -0.4148  -0.3633   0.4757   1.9936
##
## Coefficients:
##             Estimate Std. Error z value Pr(>|z|)
## (Intercept)  -2.6852     0.2866  -9.370  < 2e-16 ***
## AGeGRoupC    -0.0269     0.3425  -0.079    0.937
## creditb       0.2755     0.3157   0.873    0.383
## Stem          1.4259     0.3281   4.346 1.39e-05 ***
## SecCourses    0.8454     0.1311   6.447 1.14e-10 ***
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
##
## (Dispersion parameter for binomial family taken to be 1)
##
##     Null deviance: 511.49  on 379  degrees of freedom
## Residual deviance: 310.77  on 375  degrees of freedom
## AIC: 320.77
##
## Number of Fisher Scoring iterations: 5
exp(cbind(Odds_Ratio = coef(model11), confint(model11)))
## Waiting for profiling to be done...
##             Odds_Ratio      2.5 %    97.5 %
## (Intercept) 0.06821002 0.03760289 0.1160972
## AGeGRoupC   0.97346007 0.49460943 1.9026241
## creditb     1.31722398 0.70518767 2.4401379
## Stem        4.16169946 2.19250971 7.9663331
## SecCourses  2.32880528 1.81357149 3.0383864
```

APPENDIX F.

RESEARCH QUESTION 1 RESULTS AND DISCUSSION

In this section, the results of the search question 1 are presented. The Chi-square test in R-Studio was used to test for the independence between the main outcomes of interest (knowledge, attitude, and awareness) and STEM student status (yes or no). Several of the outcomes had warnings for the chi-square tests because the expected frequencies in the cells were less than five and thus the Chi-square tests were not valid. Therefore, these variables were collapsed for the Chi-square test to become valid. Answers to questions in the “Extremely Likely” (or Extremely Agree) or “Likely” (or Agree) were combined into one category (Extremely Likely/likely or Extremely Agree/Agree). On the other hand, Extremely Unlikely and Unlikely or Extremely Disagree and Disagree values were combined into another category (Extremely unlikely/unlikely). The Unsure or do not care answers were combined into a new category Maybe.

The analysis is based on 380 participants of which 122 were non-STEM (32%) and 258 were STEM students (68%).

Research Question 1:

Does security awareness (STEM programs) positively influence students’ likelihood of adopting security best practices (knowledge, attitude, awareness) while using smart TVs?

<u>Results from Attitude Towards SMART TV</u>

1-Survey question (RQ1): Does Smart TV interaction require mental effort?

Overall, 40% of all participating students said yes Smart TV requires mental effort, 51% indicated as somehow and 9% stated no.

There was no association between mental effort while using smart TV and STEM student status. More non-STEM students (43%) indicated that requires mental effort to deal with Smart TV than STEM students (38%). On the other hand, there was a slight difference for the -STEM students who indicated that it does require some effort (Table 1). This difference was not statistically significant (the p-value for the Chi-square test is 0.537).

	Yes	**Somewhat**	**No**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	98(38%)	132(51%)	28(11%)	258(100%)
Non-STEM	52 (43%)	60 (49%)	10(8%)	122(100%)
Total	150(40%)	192(51%)	38(9%)	380(100%)

Table 1. Smart TV Interaction Effort by STEM/non-STEM Status

2- Survey question (RQ2): Do you feel confident about checking and using the Smart TV settings?

	Yes	**No**	**Total**
	N (%)	**N (%)**	**N (%)**
STEM	229**(**89%)	29 (11%)	258(100%)
Non-STEM	116(95%)	6 (5%)	122(100%)
Total	345(91%)	35(9%)	380(100%)

Table 2 Smart TV Settings Confidence by STEM/non-STEM status

Ninety-one percent of students had confidence in checking and using Smart TV in total, (Table 2). There was no association between feeling confident about checking and using the Smart TV settings and STEM/non-STEM student status (Table 2). Ninety five percent of non-STEM students started that they are confident about checking Smart TV settings, versus 89% STEM students (The p-value for the Chi-square test is 0.11, Table 2).

3- Survey question (RQ3): Do you feel confident about disabling some features that are not needed on the Smart TV?

There was no association between feeling confident about disabling some smart TV features and STEM/non-STEM student status. Seventy-seven percent of STEM students stated that they feel confident about disabling some smart TV features versus 74% of non-STEM students (Table 3). The p-value for the Chi-square test is 0.61.

	Yes	**No**	**Total**
	N (%)	**N (%)**	**N (%)**
STEM	198(77%)	60 (23%)	258(100%)
Non-STEM	90(74%)	32 (26%)	122(100%)
Total	288(91%)	92(9%)	380(100%)

Table 3. Smart TV Disabling Features by STEM/non-STEM Status

Results from Knowledge Towards SMART TV

4- Survey question (RQ4): What are the chances of your privacy being invaded?

Overall, 44%, 30% and 26% of students had indicated that they agreed, maybe or disagreed with question four**,** Table 4. There was an association between the chances of privacy being invaded and STEM/non-STEM student status (Table 4). Forty seven percent of STEM students stated that they agreed with the chances of their privacy being invaded versus 38 % of non-STEM students. Moreover 45% of non-STEM students thought it might happen versus 23% STEM. This association was statistically significant (the p-value for the Chi-square test is 0.000054).

	Agree	**Maybe**	**Disagree**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	122(47%)	59(23%)	77(29%)	258(100%)
Non-STEM	46 (38%)	55(45%)	21(17%)	122(100%)
Total	168(44%)	114(30%)	98(26%)	380(100%)

Table 4. Likelihood of Privacy Invasion by STEM/non-STEM Status

5- Survey question (RQ5): What are the chances of your smart TV being hacked?

Overall, 23% of students agreed with the questions on what the chances of your smart TV being hacked (Table 5). There was an association between the chances of smart TV being hacked and STEM/non-STEM student status. A slightly higher percent of STEM (25%) thought their smart TV will be hacked versus 20 % of non-STEM. More importantly, 43% of STEM disagree their smart TV will be hacked versus 26%, this may be because STEM students will take precautions at not to be hacked. Moreover, 53% of Non-STEM thought it might happen versus 32% STEM (the p-value for the Chi-square test is 0.0002827).

	Agree	**Maybe**	**Disagree**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	64(25%)	83(32%)	111(43%)	258(100%)
Non-STEM	25 (20%)	65 (53%)	32(26%)	122(100%)
Total	89(23%)	148(39%)	143(38%)	380(100%)

Table 5. Chances of smart TV being hacked by STEM/non-STEM Status

Results from Attitude Towards SMART TV

6- Survey question (RQ6): It would be a severe problem if my privacy was invaded while using my smart TV

There was no association between being a severe problem if privacy was invaded while using smart TV and STEM/non-STEM student status (Table 6). There is no difference between STEM and non-STEM agree, and they agree that it will be a severe problem if privacy was invaded (the p-value for the Chi-square test is 0.11)

	Agree	**Maybe**	**Disagree**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	206(80%)	21(7%)	31(12%)	258(100%)
Non-STEM	100 (82%)	13(11%)	9(7%)	122(100%)
Total	306(81%)	34(9%)	40(10%)	380(100%)

Table 6. Privacy B**eing Invaded is Severe by STEM/non-STEM Status**

7- Survey question (RQ7): It would be problematic if my smart TV was hacked

There was no association between it being problematic if smart TV was hacked and STEM/non-STEM student status. One percent more STEM students than non-STEM agreed that it would be problematic if smart TV were hacked, which is not of statistical difference. On the other hand, STEM students disagreed: 4%. while 5% more non-STEM thought that it may take place. (Table 7). The p-value for the Chi-square test is 0.3929.

	Agree	**Maybe**	**Disagree**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	188(73%)	34(13%)	36(14%)	258(100%)
Non-STEM	88 (72%)	22(18%)	12(10%)	122(100%)
Total	276(73%)	56(15%)	48(12%)	380(100%)

Table 7. TV Being Hacked is Problematic by STEM/non-STEM Status

8- Survey question (RQ8): How likely is it that in-home audio, recorded for voice recognition purposes, or your smart TV camera and microphone will be accessed by third parties such as: TV/Streaming Providers?

There was no association between the likelihood of home features being accessed by third parties and STEM/non-STEM student status. Seven percent more STEM students than non-STEM thought TV camera and microphone will be accessed by third parties (Extremely Likely and Likely)

While an equal number of STEM students than non-STEM thought TV camera and microphone will not be accessed by third parties (Extremely unlikely and Unlikely. On the other hand, 7% more non-STEM students than STEM were not sure Table 8. The p-value for the Chi-square test is 0.24.

	Extremely Likely/ Likely	**Unsure**	**Extremely unlikely/Unlikely**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	139(54%)	62(24%)	57(22%)	258(100%)
Non-STEM	57 (47%)	38(31%)	27(22%)	122(100%)
Total	196(52%)	100(26%)	84(22%)	380(100%)

Table 8. Third parties Accessing TV Features by STEM/non-STEM Status

9- Survey question (RQ9): How acceptable would it be if your in-home audio, recorded for voice recognition purposes was accessed by third parties or your smart TV camera and microphone were used to watch and listen to you?

There was a statistically significant association between it not being acceptable for smart TV features accessed by third parties and STEM/non-STEM student status. Fifteen percent more STEM students than non-STEM said it would not be acceptable if smart TV features were used to watch and listen to them. Some statistical differences, Table 9. Thirteen percent more non-STEM than STEM students thought it may take place. The p-value for the Chi-square test is 0.00037.

	Agree	**Maybe**	**Disagree**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	21(8%)	18(7%	219(85%)	258(100%)
Non-STEM	10 (9%)	27(20%)	85(70%)	122(100%)
Total	31(8%)	45(12%)	304(80%)	380(100%)

Table 9. Third parties Accessing TV Features Acceptance by STEM/non-STEM Status

10- Survey question (RQ10): In order to have a more secure home environment and prevent other parties to misuse voice recognition features, or use a smart TV camera and microphone to watch and listen to you, will you consider disabling those features?

There was an association between disabling smart TV features to protect privacy and STEM/non-STEM student status. Eleven percent more STEM students than non-STEM said they will consider disabling smart TV features which can be used for spying on them. Statistical difference. However, 6% more STEM students than non-STEM said they will not consider disabling those features. While 16% more non-STEM than STEM students said they may disable the features, Table 10. The p-value for the Chi-square test is 0.0004,

	Agree	Maybe	Disagree	Total
	N (%)	N (%)	N (%)	N (%)
STEM	209(81%)	23(9%)	26(10%)	258(100%)
Non-STEM	85 (70%)	31(25%)	6(4%)	122(100%)
Total	294(77%)	54(14%)	32(9%)	380(100%)

Table 10. Disabling Smart TV Features by STEM/non-STEM Status

11- Survey question (RQ11): If you want to install third-party apps, would you research the app to see how safe it is before you install it on your smart TV?

There was an association between researching smart TV apps before installing it on smart TV to protect privacy and STEM/non-STEM student status. 8 % more STEM students than non-STEM said they will research TV apps to see how safe it is before they install it on smart TVs. Some statistical differences. However, 1% more STEM students than non-STEM said they will not research TV apps. Ten percent more non-STEM than STEM said they may, Table 11. The p-value for the Chi-square test is 0.05.

	Agree	Maybe	Disagree	Total
	N (%)	N (%)	N (%)	N (%)
STEM	155(60%)	36(14%)	67(26%)	258(100%)
Non-STEM	63 (52%	29(24%)	30(25%)	122(100%)
Total	218(57%)	65(17%)	97(26%)	380(100%)

Table 11. Research Smart TV Apps by STEM/non-STEM Status

12- Survey question (RQ12): By allowing new software to be installed on your Smart TV to enable third-party apps, your TV may become vulnerable to malicious software being installed. Would you consider refraining from installing third-party apps on your smart TV?

There was no association between refraining from installing TV apps and STEM/non-STEM student status. An equal number of percent in non-STEM students and STEM said they will refrain from installing TV apps (Table 12). Moreover, 19% of STEM students vs 11% on non- STEM students said they may refrain from installing TV apps, Table 11. The p-value for the Chi-square test is 0.07)

	Agree	**Maybe**	**Disagree**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	155(60%)	54(21%)	49(19%)	258(100%)
Non-STEM	73 (60%)	35(29%)	13(11%)	122(100%)
Total	228(60%)	89(23%)	62(17%)	380(100%)

Table 12. Refrain from Installing TV Apps by STEM/non-STEM Status

<u>Results from Awareness Towards SMART TV</u>

13- Survey question (RQ13): What is the likelihood of your smart TV manufacturer collecting data including your viewing history and search patterns from your home environment?

There was an association between thinking **s**mart TV manufacturers will collect data from home environments and STEM/non-STEM student status. Twenty-one percent more STEM students than non-STEM said they **s**mart TV manufacturer will collect their data including viewing history and search patterns from home environments. This is a significant statistical difference. Twenty-one percent more non-STEM students than STEM said this may take place. The p-value for the Chi-square test is 7.904e-06

	Agree	**Maybe**	**Disagree**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	214(83%)	34(13%)	8(3%)	258(100%)
Non-STEM	76 (62%)	42(34%)	4(3%)	122(100%)
Total	290(76%)	76(20%)	12(4%)	380(100%)

Table 13. Likelihood of Data Collected from Smart TV by STEM/non-STEM Status

14- Survey question (RQ14): How likely will data collected from your Smart TV be combined with data collected from your other IoT devices (smartphone, tablet, laptop) to create a detailed profile of your habits and interests?

There was an association between the likelihood of **s**mart TV manufacturers collecting data from home environments and creating detailed profiles of users and STEM/non-STEM student status.

Twelve percent more STEM students than non-STEM said they **s**mart TV manufacturer will create detailed profiles of their habits and interests. Thirteen percent more non-STEM than STEM students said **s**mart TV manufacturers may create detailed profiles of their habits and interests. Table 14. The p-value for the Chi-square test is 0.015.

	Agree	**Maybe**	**Disagree**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	204 (79%)	44 (17%)	10 (4%)	258(100%)
Non-STEM	82 (67%)	37(30%)	3 (3%)	122(100%)
Total	286 (75%)	81(21%)	13(4%)	380(100%)

Table 14. Likelihood of Creating Profile from Collected Data by STEM/non-STEM Status

15- Survey question (RQ15): Is collecting data from several sources to create a detailed profile of you acceptable?

There was an association between it being unacceptable to create profiles of users from smart home environments and STEM/non-STEM student status. Thirteen percent more STEM students than non-STEM said creating a detailed profile of them is not acceptable, Table 15.1% more STEM students than non-STEM said creating a detailed profile of them is acceptable. On the other hand, 25% more non-STEM than STEM was unsure. The p-value for the Chi-square test is 9.089e-07.

	Agree	**Maybe**	**Disagree**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	57(22%)	49 (19%)	152(59%)	258(100%)
Non-STEM	12 (10%)	54(44%)	56(46%)	122(100%)
Total	69(18%)	103(27%)	208(55%)	380(100%)

Table 15. Creating Profile from Collected Data Unacceptable by STEM/non-STEM Status

16- Survey question (RQ16): Is protecting your privacy more important than using smart TV features

There was no association between protecting privacy being more important and STEM/non-STEM student status. Four percent more STEM students than non-STEM said protecting privacy is more important than using smart TV features, Table 16. Three percent more STEM students than non-STEM said it is not. Eight percent more non-STEM were unsure than STEM students. The p-value for the Chi-square test is 0.2.

	Agree	**Maybe**	**Disagree**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	144(56%)	41 (16%)	73(28%)	258(100%)
Non-STEM	63(52%)	29 (24%)	30 (25%)	122(100%)
Total	207(55%)	70(18%)	103(27%)	380(100%)

Table 16. Protecting Privacy is More Important by STEM/non-STEM Status

17- Survey question (RQ17): Did the security/privacy course(s) that you took influence you to have a more proactive security behavior to protect your privacy?

There was an association about protecting privacy being more important and STEM/non-STEM student status. Twenty-six percent more STEM students than non-STEM said taking security/privacy course(s) influenced their security behavior to protect their privacy (Options: Definitely Yes, Yes), which was statistically significant. One percent more non-STEM than STEM students said they were unsure.

Twenty-six percent more non-STEM than STEM students said it is not applicable which is expected since non-STEM students are not required to take security or privacy courses. The p-value for the Chi-square test is 0.213.

	Agree	**Maybe**	**Disagree**	**Total**
	N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	126(49%)	28(11%)	104 (40%)	258(100%)
Non-STEM	27(22%)	15 (12%)	80 (66%)	122(100%)
Total	153(40%)	43(11%)	184(49%)	380(100%)

Table 17. Protecting Privacy is More Important by STEM/non-STEM Status

18- Survey question (RQ18): How many security/privacy courses did you take in the past?

Out of a total of 380 students: 39%, 148 Students did not take any security courses: 80 STEM (31%) and seventy non-STEM (57%). Some non-STEM students did take security classes, a total of fifty-two, while 180 STEM students took one or more security classes. The analysis is based on 380 participants of which 122 were non-STEM (32%) and 258 were STEM students (68%).

	0 course	**1 course**	**2 courses**	**3 courses**	**4 courses**
		N (%)	**N (%)**	**N (%)**	**N (%)**
STEM	78 (30%)	49(19%)	41(16%)	23 (9%)	67(26%)
Non-STEM	70 (57%)	26(21%)	13 (11%)	7 (6%)	6(5%)
Total	148 (39%)	75(20%)	54(14%)	30(8%)	73(19%)

Table 18. Security/Privacy Courses

Results Discussion Summary

The collected data from the Survey Monkey survey was analyzed in R-Studio to answer the research questions. There were eighteen variables of interest (outcomes), which are the eighteen survey questions. These were tested against both STEM and non-STEM students and were compared to the three predictors: knowledge, awareness, and attitude which is the expected outcome of being in STEM programs (Hypothesis).

RESEARCH QUESTION 2 RESULTS AND DISCUSSION

There were 190 junior/senior participants and 190 freshmen/sophomores. The breakdown was as follows:

- Category value 1: 83 (22%) were juniors and 107 (28%) were seniors.
- Category value 0: 145 (38%) were Freshmen and 45(12%) were sophomores.

Research Question 2: **Do junior/senior and freshmen/sophomore students differ significantly in the two categories?**

Results from Attitude Towards SMART TV

1-Survey question (RQ1): does Smart TV interaction require mental effort

There was no association between Smart TV interaction effort and student credit status, for both categories: Freshmen/Sophomore and Junior/Senior Students a total of 150 students said it requires no effort in dealing with smart TV versus 190 who mentioned it somewhat requires effort. Some slight differences between the two categories.

	Yes	**No**	**Somewhat**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	23(12%)	78(41%)	89(47%)	190 (100%)
Freshmen – Sophomore	17 (9%)	72(38%)	101(53%)	190 (100%)
Total:	40 (11%)	150(39%)	190 (50%)	380 (100%)

Table 1. Smart TV Interaction Effort by Credits/Status

FS= Freshmen – Sophomore value 0

JS = Junior – Senior value 1

2- Survey question (RQ2): Do you feel confident about checking and using the Smart TV settings?

	Yes	**No**	**Total**
	N(%)	**N(%)**	**N (%)**
Junior – Senior	177(93%)	13(7%)	190 (100%)
Freshmen – Sophomore	169 (89%)	21(11%)	190 (100%)
Total:	346 (91%)	34(9%)	380 (100%)

Table 2. Smart TV Settings Confidence by Credits Status

There was no association between feeling confident about checking and using the Smart TV settings and student credit status, for both categories: Freshmen/Sophomore and Junior/Senior Students a total of 347 (91%) students are confident about checking and using the Smart TV settings. Some slight differences between the two categories

3- Survey question (RQ3): Do you feel confident about disabling some features that are not needed on the Smart TV

There was no association between feeling confident about disabling some smart TV features and student credit status, for both categories. A total of 150 students are confident about disabling features versus 190 that are not so sure. Slight differences between the two categories.

	Yes	**No**	**Total**
	N(%)	**N(%)**	**N(%)**
Junior – Senior	144(76%)	46(24%)	190 (100%)
Freshmen – Sophomore	142(75%)	48(25%)	190 (100%)
Total:	286 (75%)	94(25%)	380 (100%)

Table 3 Smart TV Disabling Features by Credits Status

Results from Knowledge Towards SMART TV

4- Survey question (RQ4): What are the chances of your privacy being invaded?

There was an association between the chances of privacy being invaded and the credit status of students, for both categories: Freshmen/Sophomore and Junior/Senior Students. 19

more Junior/Senior Students agreed with the question versus freshman – Sophomore. On the other hand, 19% more thought it may take place. Freshman – Sophomore, a significant difference (p-value = 0.000593).

	Agree	**Disagree**	**Maybe**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	103(54%)	49(26%)	40(20%)	190 (100%)
Freshmen – Sophomore	67 (35%)	48(25%)	76(40%)	190 (100%)
Total:	170 (43%)	97(26%)	116 (31%)	380 (100%)

Table 4. Likelihood of Privacy Invasion by Credits Status

5- Survey question (RQ5): What are the chances of your smart TV being hacked?

There was an association between thinking that chances of smart TV being hacked and students' credit status. The values for agree, maybe and disagree were 23%, 39%, 38% respectively with some differences between the two categories (p-value = 0.009138).

.	**Agree**	**Maybe**	**Disagree**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	52(27%)	61(32%)	77(41%)	190 (100%)
Freshmen – Sophomore	36(19%)	87(46%)	67(35%)	190 (100%)
Total:	88 (23%)	148(39%)	144 (38%)	380 (100%)

Table 5. Chances of smart TV being Hacked by Credits Status

<u>Results from Attitude Towards SMART TV</u>

6- Survey question (RQ6): It would be a severe problem if my privacy was invaded while using my smart TV?

There was no association between being a severe problem if privacy was invaded while using smart TV and students' Credits Status, for both categories. An equal number of both agreed that it would be a severe problem for privacy to be invaded for a total of 81%.

	Agree	**Disagree**	**Maybe**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	154(81%)	25 (13%)	11(6%)	190 (100%)
Freshmen – Sophomore	154(81%)	15 (8%)	21(11%)	190 (100%)
Total:	308 (81%)	40(11%)	32(8%)	380 (100%)

Table 6. Privacy Being Invaded is Severe by Credits Status

7- Survey question (RQ7): It would be problematic if my smart TV was hacked

There was no association between being a severe problem if privacy was invaded while using smart TV and students' Credits Status, for both categories. An equal number of both agreed that it would be a severe problem for privacy to be invaded for a total of 73%.

	Agree	**Disagree**	**Maybe**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	139 (73%)	26(14%)	25(13%)	190 (100%)
Freshmen – Sophomore	139 (73%)	21(11%	30(16%)	190 (100%)
Total:	278 (73%)	47(12%)	55(15%)	380 (100%)

Table 7. Problematic for TV Being Hacked by Credits Status

8- Survey question (RQ8): How likely is it that in-home audio, recorded for voice recognition purposes, or your smart TV camera and microphone will be accessed by third parties such as: TV/Streaming Providers?

There was an association between the likelihood of home features being accessed by third parties and students" Credits Status. The values for agree, maybe, and disagree were

52%, 26%, 22% respectively with some differences between the two categories: 7%, 15%, 15% statistical significance (p-value = 0.003331).

	Agree	**Disagree**	**Unsure**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	105(55%)	49(26%)	36(19%)	190 (100%)
Freshmen – Sophomore	91 (48%)	34(18%)	65(34%)	190 (100%)
Total:	196 (52%)	83(22%)	101 (26%)	380 (100%)

Table 8. Likelihood of Features Accessed by Credits Status

9- Survey question (RQ9): How acceptable would it be if your in-home audio, recorded for voice recognition purposes was accessed by third parties or your smart TV camera and microphone were used to watch and listen to you?

There was no association between not being acceptable for smart TV features being misused and students' Credits Status, for both categories. An equal number of both agreed that it would not be acceptable.

	Agree	**Disagree**	**Maybe**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	17 (9%)	163(86%)	10(5%)	190 (100%)
Freshmen – Sophomore	15 (8%)	143(75%)	32(17%)	190 (100%)
Total:	32 (8%)	306(80%)	42(12%)	380 (100%)

Table 9. TV Features Access Acceptable by Credits Status

10- Survey question (RQ10): In order to have a more secure home environment and prevent other parties from misusing voice recognition feature, or use smart TV camera and microphone to watch and listen to you, will you consider disabling those features?

	Agree	**Disagree**	**Maybe**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	162 (85%)	15(8%)	13(7%)	190 (100%)
Freshmen – Sophomore	135(71%)	13(7%)	42(22%)	190 (100%)
Total:	297(78%)	28(7%)	55(15%)	380 (100%)

Table 10. Disabling Smart TV Features by Credits Status

There was an association between disabling smart TV Features and students' credits status (p-value = 5.981e-05). 14% more Junior – Senior agreed to disable the features which may be used. On the other hand, 14% less Junior – Senior disagreed. Significant difference.

11- Survey question (RQ11): If you want to install third-party apps, would you research the app to see how safe it is before you install it on your smart TV?

There was an association between researching smart TV apps to see if they are safe and students' Credits Status for both categories. 9% more Junior – Senior students agree that they will research the app while 12% more Freshmen – Sophomore said they might. Significant difference (p-value = 0.00738).

	Agree	**Maybe**	**Disagree**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	118(62%)	21(11%)	51(27%)	190 (100%)
Freshmen – Sophomore	100 (53%)	44(23%)	46(24%)	190 (100%)
Total:	218 (57%)	65(17%)	97 (26%)	380 (100%)

Table 11. Research Smart TV Apps by Credits Status

12- Survey question (RQ12): By allowing new software to be installed on your Smart TV to enable third-party apps, your TV may become vulnerable to malicious software being installed. Would you consider refraining from installing third-party apps on your smart TV?

There was an association between refraining from installing TV apps and STEM/non-STEM student status for both categories: Freshmen/Sophomore and Junior/Senior Students, Table 12. 8% more Junior – Senior students agree that they will refrain from installing third-party apps while 11% more Freshmen – Sophomore said they might (p-value = 0.0386).

	Agree	**Maybe**	**Disagree**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	122(64%)	34(18%)	34(18%)	190 (100%)
Freshmen – Sophomore	106(56%)	55(29%)	29(15%)	190 (100%)
Total:	228 (60%)	89(23%)	63(17%)	380 (100%)

Table 12. Refrain from Installing TV Apps by Credits Status

Results from Awareness Towards SMART TV

13- Survey question (RQ13): What is the likelihood of your smart TV manufacturer collecting data including your viewing history and search patterns from your home environment?

There was an association between thinking **s**mart TV manufacturers will collect data from home environments and students by Credits Status 10% more Junior – Senior students agree that smart TV manufacturers collect data from home environments while 10% more Freshmen – Sophomore disagree Significant difference. p-value = 0.004648

	Agree	**Disagree**	**Maybe**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	158(82%)	9(5%)	25(13%)	190 (100%)
Freshmen – Sophomore	118 (72%)	4(2%)	65(26%)	190 (100%)
Total:	276 (73%)	13(3%)	90(24%)	380 (100%)

Table 13. Likelihood of Data Collected from Smart TV by Credits Status

14- Survey question (RQ14): How likely will data collected from your Smart TV be combined with data collected from your other IoT devices (smartphone, tablet, laptop) to create a detailed profile of your habits and interests?

There was an association between the likelihood of **s**mart TV manufacturers will collect data from IoT devices and create detailed profiles of users and by Credits Status. 16% more Junior – Senior students agreed while 16% more Freshmen – Sophomore disagreed. Significant difference. p-value = 0.0005617.

	Agree	**Maybe**	**Disagree**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	158(83%)	25(13%)	7 (4%)	190 (100%)
Freshmen – Sophomore	127 (67%)	53(28%)	10 (5%)	190 (100%)
Total	285 (75%)	78(21%)	17(4%)	380 (100%)

Table 14. Likelihood of Creating Profile from Collected Data by Credits Status

15- Survey question (RQ15): Is collecting data from several sources to create a detailed profile of you acceptable?

There was no association between being unacceptable to create profiles of users from smart home and student credit status, for both categories: Freshmen/Sophomore and Junior/Senior Students. Some slight differences between the two categories.

	Agree	**Maybe**	**Disagree**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	29 (15%)	49 (26%)	112 (59%)	190 (100%)
Freshmen – Sophomore	38 (21%)	55(29%)	97 (51%)	190 (100%)
Total:	67 (18%)	104(27%)	209 (55%)	380 (100%)

Table 15. Likelihood of Creating Profile from Collected Data by Credits Status

16- Survey question (RQ16): Is protecting your privacy more important than using smart TV features?

There was no association between protecting privacy being more important and students' credit status for both categories (p-value = 0.04439).

	Agree	**Maybe**	**Disagree**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	99 (52%)	32(17%)	59(31%)	190 (100%)
Freshmen – Sophomore	108 (57%)	38(20%)	44(23%)	190 (100%)
Total:	207 (55%)	70(18%)	103 (27%)	380 (100%)

Table 16. Protecting Privacy is More Important by Credits Status

17- Survey question (RQ17): Did the security/privacy course(s) that you took influence you to have a more proactive security behavior to protect your privacy?

There was an association about security/privacy course(s) that influenced to have a more proactive security behavior and students' Credits Status for both categories: Freshmen/Sophomore and Junior/Senior Students. 207 students in total (55%) agree that protecting privacy comes first, with a close percentage between the two categories, 52% versus 57% (p-value = 1.489e-07).

	Agree	**Maybe**	**Disagree**	**Total**
	N(%)	**N(%)**	**N(%)**	**N (%)**
Junior – Senior	103(54%)	15(8%)	72(38%)	190 (100%)
Freshmen – Sophomore	49 (26%)	30(16%)	110(58%)	190 (100%)
Total:	152 (40%)	46(12%)	182 (48%)	380 (100%)

Table 17. Influence Behavior Important by Credits/Class Status

18- Survey question (RQ18): How many security/privacy courses did you take in the past?

Out of a total of 380 a total of 149 Students did not take any security courses: 46 Junior – Senior (24%) and 103 Freshmen – Sophomore (54%). The values for both categories were close for 1-3 courses except for 4 courses, it is 32% for Junior – Senior while 6% for Freshmen – Sophomore.

	0 course	**1 course**	**2 courses**	**3 courses**	**4 courses**
	N (%)	**N (%)**	**N (%)**	**N (%)**	**N (%)**
Junior – Senior	46(24%)	32(17%)	32(17%)	19(10%)	61(32%)
Freshmen – Sophomore	103(54%)	42(22%)	25 (13%)	11 (6%)	11(6%)
Total	149(39%)	74(19%)	57(15%)	30(8%)	72(19%)

Table 18. Security/Privacy Courses

	STEM			CREDITS			P-value
	Agree	Disagree	Maybe	Agree	Disagree	Maybe	
	N(%)	N(%)	N(%)	N(%)	N(%)	N(%)	
R1Q**4**	122(47%)	59(23%)	59(23%)	46 (38%)	21(17%)	21(17%)	**5.48 e -5**
R2Q**4**	103(54%)	49(26%)	40(21%)	67 (35)	48(25%)	76(40%)	**6.791 e -5**
R1Q**5**	64(25%)	111(43%)	83(32%)	25 (20%)	32(26%)	32(26%)	**0.0002**
R2Q**5**	52(28%)	61(32%)	77(41%)	36(19)	87(46%)	67(35%)	**0.0009**
R2Q8	105(55%)	49(26%)	36(19%)	91 (48%)	34(18%)	65(34%)	**0.0003**
R1Q9	21(8%)	219(85%)	18(7%)	10 (9%)	85(70%)	27(20%)	**0.00037**
R1Q10	209(81%)	26(10%)	23(9%)	85 (70%)	6(4%)	31(25%)	**0.00042**
R2Q10	162 (85%)	28(15%)		135(71%)	55(29%)		**0.001**
R2Q11	118(62%)	21(11%)	51(27%)	100 (53%)	44(23%)	46(24%)	**0.007**
R2Q12	122(64%)	34(18%)	34(18%)	106(56%)	55(29%)	29(15%)	**0.03**
R1Q13	214(83%)	44(17%)		76 (62%)	46(38%)		**7.9e-06**
R2Q13	156(82%)	34(18%)		137 (72%)	53(28%)		**0.02**
R1Q14	204 (79%)	10 (4%)	44 (17%)	82 (67%)	3 (3%)	37(30%)	**1.126e-05**
R2Q14	158(83%)	(0%)	32 (17%)	127 (67%)	1(1%)	62 (33%)	**0.0009**
R1Q15	57(22%)	152(59%)	49(19%)	12 (10%)	56(46%)	54(44%)	**0.01504**
R1Q16	144(56%)	73(28%)	41(16%)	63(52%)	30 (25%)	29 (24%)	**9.089e-07**
R1Q17	126(49%)	104(40%)	28(11%)	27(22%)	80 (66%)	15 (12%)	**2.57e-06**
R2Q17	99(52%)	32(17%)	59(31%)	108 (57%)	38(20%)	44(23%)	**0.04**

Table 19. Comparison between Research Questions 1 & 2 Results that are Statistically Significant

APPENDIX G.

LOGISTIC REGRESSION MODELS

Per the internet, “ the logistic regression is a statistical approach that is used to analyze the relationship between a dependent variable and one or more predictors. It is a regression model that is used when the outcome (dependent variable) is binary. In other words, logistic regression is used when we want to predict the probability of an event occurring based on some predictor variables.”

Logistic regression was utilized to identify predictors that played important roles in affecting students' attitudes, awareness, and knowledge. The different 11 survey questions’ values were changed to binary (0 or 1) to perform logistic regression. Models were created for the 11 different survey questions in R using the glm function. The threshold for statistical significance was considered as 0.05. The list of all the models and the output from R are presented in the Appendix. The predictors were age group (AGeGRoup), creditlb, STEM status and security courses (SecCourses).

AgeGRoup is the age range of the participating students. This was collected as a categorical variable in the survey.

AGeGRoupC 1: were students in the 18-21 age group and were assigned a value 1. Seventy-three percent of the participants were in this age group.

AGeGRoupC 2: were students in the 22-25 age group and were assigned a value of 2. Thirteen percent of the participant were in this age group

AGeGRoupC 3: were students in the 26-30 age group has value of 3, 4.8% of the participants, were in this age group

AGeGRoupC 4: were students in the 31-34 age group and were assigned a value of 4. Three and half percent of the participants, were in this age group

AGeGRoupC 5: were students in 35+ age group and were assigned a value 5. More than five percent of the participants were in this age group.

Agergroups 2-5 were combined later for better results as the glm model was not converging.

Creditlb is the number of credits students have taken at the time of the survey. Freshman and sophomore categories were combined into one group and were assigned the value of zero (referent) whereas junior and senior students were combined into another category and were assigned the value of one. The number of participants in each category was 190 students.

STEM is the STEM status, where STEM students in any of the various majors in Beacom College, Mathematics or Science. Non-STEM students are all the students who are in the other majors and their binary value is 0 (referent). STEM students were almost two-thirds of Non-STEM. 258 students were STEM students (68%) and 122 were non-STEM students (32%). The binary value for STEM Students is one in the model.

SecCourses: is the number of security courses that the participating students took:

SecCourses 0: a total of 149, 39% of participating students took zero security courses,

SecCourses 1: a total of 74, 19% of the participants, took one security course,

SecCourses 2: a total of 56, 15%, of the participants, took two security courses,

SecCourses 3: a total of 29, 8% of the participants took three security courses.

SecCourses 4: a total of 72, 19% of the participants, took four or more security courses.

The number of courses was categorized as a binary predictor due to converging issues in the glm.

1-Survey question: What are the chances of your privacy being invaded?

For this question, the potential answers were: it is definite, it is likely, unsure, it is not likely, and it is not possible. To use the logistic regression model, the answers were made into binary values. The categories were it is definite, and it is likely were combined into one category as the event of interest (coded a value=1), and the rest of the choices were combined into another category (coded a value=0). A logistic regression model was fitted in R with privqc as the outcome using the glm function. The results of the model are listed in Table 1.

Predictors	**Odds Ratio (95% CI)**	**P-value**
Age Groups		
22-25, 26-30, 31-34, 35+ vs 18-21	1.42(0.86- 2.37)	0.1697
Class /Credits		
Juniors/Seniors vs. Freshman/Sophomore	1.56 (0.97- 2.51)	0.0656
Major		
STEM vs. Non-STEM	1.15 (0.64 - 2.06)	0.6285
Security Courses		
1 -4 courses vs. 0 course	1.14 (0.93- 1.39)	0.1970

Table 1. Odds Ratios and 95% CI from the Logistic Regression Results Modelling Definitely/Likely on Privacy Invasion (privqc)

None of the predictors were statistically significant of the outcome (Table 1). Students who were in these age groups: 22-25, 26-30, 31-34, 35+ were 1.42 more likely to respond agree or definitely agree on privacy invasion compared to students who were 18-21 years (Table 1). Senior and junior students were 1.56 times more likely to agree on privacy invasion than freshmen and sophomores. Moreover, students who took 1-4 security courses were 1.14, more likely to definitely agree/agree on privacy invasion than students who did not take any security courses. Lastly, STEM students were 1.15, more likely to definitely agree/agree on privacy invasion than non-STEM students.

2- Survey question: What are the chances of your smart TV being hacked?

For this question, the potential answers were it is definite, it is likely, unsure, it is not likely, and it is not possible. The categories it is definite, and it is likely were combined into one category (coded as 1) and the rest of the choices were combined into another category (coded as 0).

Predictors	**Odds Ratio (95% CI)**	**P-value**
Age Groups		
22-25, 26-30, 31-34, 35+ vs. 18-21	0.90 (0.50- 1.59)	0.723
Class /Credits		
Juniors/Seniors vs. Freshman/Sophomore	1.49 (0.86- 2.59)	0.160
Major		
STEM vs. Non-STEM	0.97 (0.49- 1.89)	0.919
Security Courses		
1 -4 courses vs. 0 course	1.14 (0.90 -1.43)	0.245

Table 2. Odds Ratios and 95% CI from the Logistic Regression Results Modelling Definitely/Likely on Hacking Issues (Hackqc)

None of the predictors were statistically significant of the outcome (Table 2). Seniors and junior students were 1.49 times more likely to agree on being hacked than freshmen and sophomores. Furthermore, students who took 1-4 security courses were 1.14 more likely than students who did not take security courses to indicate that being hacked was definitely likely and likely.

3- Survey question: How likely is it that in-home audio, recorded for voice recognition purposes, or your smart TV camera and microphone will be accessed by third parties such as TV/Streaming Providers?

The potential answers were extremely likely, likely, not sure, unlikely and extremely unlikely. Answers from extremely likely and likely were combined into one category (coded as 1) and the rest of the answers were combined into another category (coded as 0).

Predictors	**Odds Ratio (95% CI)**	**P-value**
Age Groups		
22-25, 26-30, 31-34, 35+ vs 18-21	1.28 (0.77- 2.14)	0.34077
Class /Credits		
Juniors/Seniors vs. Freshman /Sophomore	0.93 (0.58-1.48)	0.75316
Major		
STEM vs. Non-STEM	0.76 (0.41- 1.33)	0.32440
Security Courses		
1 -4 courses vs. 0 course	***1.35 (1.11-1.67)***	***0.00374****

Table 3. Odds Ratios and 95% CI from the Logistic Regression Results Modelling Extremely Likely/Likely Mic/Camera Access (camerac)

In multivariable logistic regression where the event of interest was extremely likely or likely, students who took 1-4 security courses were 1.35 more likely than students who took no security courses to agree that their smart TV features such as Microphone, Audio and Camera would be accessed (p-value 0.00374, Table 3).   This variable was a statistically significant predictor of the outcome. In addition, students who took 1-2 courses were 1.57 more likely to indicate that it is extremely likely/likely that their smart TV features would be accessed than students who took zero security courses. Furthermore, students who were in 22-25, 26-30, 31-34, 35+ age groups were 1.32 more likely to agree that their smart TV features would be accessed than students in the 18-21 age group. However, age was not a statistically important variable in predicting the outcome.

4- Survey question: How acceptable would it be if your in-home audio, recorded for voice recognition purposes was accessed by third parties or your smart TV camera and microphone were used to watch and listen to you?

For this question, the potential answers were completely acceptable, somewhat acceptable, not sure, unacceptable and completely unacceptable. Answers from completely acceptable and somewhat acceptable were combined into one category (coded as 1) and the rest of the choices were combined into another category (coded as 0).

Predictors	**Odds Ratio (95% CI)**	**P-value**
Age Groups		
22-25, 26-30, 31-34, 35+ vs 18-21	0.64 (0.33 1.27)	0.1957
Class /Credits		
Juniors/Seniors vs. Freshman/Sophomore	1.69 (0.92- 3.17)	0.0966
Major		
STEM vs. Non-STEM	1.60 (0.74- 3.49)	0.2341
Security Courses		
1 -4 courses vs. 0 course	1.21 (0.92- 1.63)	0.1829

Table 4. Odds Ratios and 95% CI from the Logistic Regression Results Modelling Completely Agree/ Somewhat Agree Access Acceptable (accessc)

None of the predictors were statistically significant. STEM students are 1.6 more likely to respond that it was not acceptable for their smart TV features to be accessed by third parties to spy on them (Table 4). Likewise, senior, and junior students were 1.69 times more likely to agree on that as well. Moreover, students who took 1-4 security courses were 1.21

more likely than students who took no security courses to indicate that they will not accept that their smart TV features be accessed by their parties.

5- Survey question: In order to have a more secure home environment and prevent other parties from misusing voice recognition features, or using a smart TV camera and microphone to watch and listen to you, will you consider disabling those features *disablec*?

For this question, the potential answers were: definitely would not, might not disable., unsure, and might disable. Answers from definitely will disable and "might disable categories were combined into one category and coded a value of 1 and the rest of the choices were combined into another category coded a value is zero.

Predictors	**Odds Ratio (95% CI)**	**P-value**
Age Groups		
22-25, 26-30, 31-34, 35+ vs 18-21	0.97 (0.51- 1.91)	0.933232
Class /Credits		
Juniors/Seniors vs. Freshman/Sophomore	***1.92 (1.08- 3.49)***	***0.028531*****
Major		
STEM vs. Non-STEM	1.21(0.59- 2.50)	0.601506
Security Courses		
1 -4 courses vs. 0 course	1.18 (0.91- 1.55)	0.230387

Table 5. Odds Ratios and 95% CI from the Logistic Regression Results Modelling Definitely Will Disable/ Might Disable Features (disablec)

In multivariable analysis where the outcome is disablec class/credit was a statistically significant predictor of the outcome (Table 5). Seniors and junior students were 1.92 times more likely than freshmen and sophomores to agree/definitely agree that they will disable the smart TV feature **(**p-value =0.028531). Moreover, STEM students were 1.21 more likely to agree to disable the features than non-STEM students.

6- Survey question: If you want to install third-party apps, would you research the app to see how safe it is before you install it on your smart TV?

For this question, the choices were: definitely yes, yes, unsure, no and definitely not. Answers from definitely yes and yes were combined into one category and were coded as 1 and the rest of the choices were combined into another category and coded as zero.

Predictors	**Odds Ratio (95% CI)**	**P-value**
Age Groups		
22-25, 26-30, 31-34, 35+ vs 18-21	0.97 (0.62- 1.74)	0.889
Class /Credits		
Juniors/Seniors vs. Freshman/Sophomore	1.92 (0.70- 1.82)	0.611
Major		
STEM vs. Non-STEM	1.21 (0.90- 2.91)	0.107
Security Courses		
1 -4 courses vs. 0 course	1.18 (0.87- 1.30)	0.564

Table 6. Odds Ratios and 95% CI from the Logistic Regression Results Modelling Definitely Yes/Yes on Research Apps (rappsc)

In multivariable logistic regression analysis, none of the variables predicted the outcome rappsc (Table 6). Seniors and junior students were 1.92 times more likely to agree that they will research smart TV apps before installing them than freshmen and sophomores. STEMS Students are also 1.21 more likely well than those non-STEM students.

7- Survey question. By allowing new software to be installed on your Smart TV to enable third-party apps, your TV may become vulnerable to malicious software being installed. Would you consider refraining from installing third-party apps on your smart TV?

For this question, the potential answers were definitely yes, yes, unsure, no and definitely not. Answers from definitely yes and yes were combined into one category (coded as 1) and the rest of the answers were combined into another category (coded as zero).

Predictors	**Odds Ratio (95% CI)**	**P-value**
Age Groups		
22-25, 26-30, 31-34, 35+ vs 18-21	1.07 (0.64- 1.80)	0.798
Class /Credits		
Juniors/Seniors vs. Freshman/Sophomore	1.28 (0.80 - 2.06)	0.308
Major		
STEM vs. Non-STEM	0.90 (0.50 - 1.62)	0.734
Security Courses		
1 -4 courses vs. 0 course	1.08 (0.88- 1.32)	0.480

Table 7. Odds Ratios and 95% CI from the Logistic Regression Results Modelling Definitely Yes/Yes Refraining Installing Apps (NoAppsc)

In multivariable analysis where the outcome is NoAppsc none of the variables predicted the outcome (Table 7). Seniors and junior students were 1.28 times more likely to agree that they will refrain from installing TV apps than freshmen and sophomores.

8- Survey question: What is the likelihood of your smart TV manufacturer collecting data including your viewing history and search patterns from your home environment?

For this question, the potential answers were: extremely likely, likely, unsure, unlikely, and extremely unlikely. Answers of extremely likely and likely were combined into one category (coded as 1) and the remaining answers were combined into another category (coded as 0).

Predictors	**Odds Ratio (95% CI)**	**P-value**
Age Groups		
22-25, 26-30, 31-34, 35+ vs 18-21	1.26 (0.66 -2.48)	0.487366
Class /Credits		
Juniors/Seniors vs. Freshman /Sophomore	1.30 (0.74 - 2.32)	0.366742
Major		
STEM vs. Non-STEM	***2.86 (1.39- 6.06)***	***0.005059*****
Security Courses		
1 -4 courses vs. 0 course	0.98 (0.76- 1.27)	0.858784

Table 8. Odds Ratios and 95% CI from the Logistic Regression Results Modelling Extremely Likely/Likely on Data Collection (DataCollb)

In multivariable logistic regression, STEM status predicted the outcome (Table 8). STEM students were 2.86 more likely to respond extremely likely/likely than non-STEM students that TV manufacturers will be collecting data from their home environment. Moreover, seniors and junior students were 1.30 times more likely to agree that their data will be collected than freshmen and sophomores. Moreover, students in the 22-25, 26-30, and 35 + age groups were 1.26 more likely to agree that TV manufacturers will be collecting data from their home environment than students in the 18-21 age group.

9- Survey question**.** How likely will data collected from your Smart be combined with data collected from your other IoT devices to create a detailed profile of your habits and interests?

For this question, the potential answers were extremely likely, likely, unsure, unlikely, and extremely unlikely. Answers of extremely likely and likely were combined into one category and coded as 1 and the rest of the answers were combined into another category and coded as zero.

Predictors	**Odds Ratio (95% CI)**	**P-value**
Age Groups		
22-25, 26-30, 31-34, 35+ vs 18-21	***2.48 (1.24- 5.34)***	***0.0138*****
Class /Credits		
Juniors/Seniors vs. Freshman / ophomore	1.62 (0.93- 2.84)	0.0896
Major		
STEM vs. Non-STEM	1.53 (0.77- 3.10)	0.2337
Security Courses		
1 -4 courses vs. 0 course	1.09 (0.85 - 1.42)	0.4931

Table 9. Odds Ratios and 95% CI from the Logistic Regression Results Modelling Creating Profiles Results (creatpc)

In a multivariable analysis where the outcome was creatpc, age group predicted the outcome (Table 9). Students who were in the 22-25, 26-30, 31-34, 35+ age groups were 2.48 more likely to agree that their profiles will be created from the different smart TV devices than students in the 18-21 age group (p-value =0.0138, Table 9). Seniors and junior students were 1.62 times more likely to agree that their profiles will be created than freshmen and sophomores. STEM students were 1.53 more likely to agree that their profiles will be created than non-STEM students. However, major and credits were not statistically important variables in predicting the outcome.

10- Survey question: Is collecting data from several sources to create a detailed profile of you acceptable?

The potential answers to this question were: extremely acceptable, acceptable, not sure unacceptable and extremely unacceptable. Unacceptable and extremely unacceptable were combined into one category and were assigned a value of 1 and the rest of the choices were combined into another category and were assigned a value of zero.

Predictors	**Odds Ratio (95% CI)**	**P-value**
Age Groups		
22-25, 26-30, 31-34, 35+ vs 18-21	1.00 (0.60- 1.67)	0.9911
Class /Credits		
Juniors/Seniors vs. Freshman/Sophomore	1.12 (0.70- 1.79)	0.6448
Major		
STEM vs. Non-STEM	1.00 (0.56 - 1.78)	0.9953
Security Courses		
1 -4 courses vs. 0 course	1.19 (0.97- 1.46)	0.0888

Table 10. Odds Ratios and 95% CI from the Logistic Regression Results Modelling Extremely Acceptable /Acceptable Create Profile Acceptable (profc)

In multivariable analysis where the outcome was profc, none of the variables predicted the outcome (Table 10). Students who took security classes were 1.19 more likely to agree that creating their profiles from collected data was not acceptable than those students who took no security classes. Seniors and junior students were 1.12 times more likely to agree than freshmen and sophomores that creating their profiles from collected data is not acceptable than students who took no security classes.

11- Survey question**:** Did the security/privacy course(s) that you took influence you to have a more proactive security behavior to protect your privacy?

Predictors	**Odds Ratio (95% CI)**	**P-value**
Age Groups		
22-25, 26-30, 31-34, 35+ vs 18-21	0.97.(049- 1.90)	0.937
Class /Credits		
Juniors/Seniors vs. Freshman/Sophomore	1.32 (0.71- 2.44)	0.383
Major		
STEM vs. Non-STEM	***4.16 (2.19- 7.97)***	***1.39e-05 *****
Security Courses		
1 -4 courses vs. 0 course	***2.33 (1.81- 3.04)***	***1.14e-10 *****

Table 11. Odds Ratios and 95% CI from the Logistic Regression Results Modelling Courses Influence Behavior (inflc)

In multivariable analysis where the outcome is *inflc* both STEM status students and security course were predictors of the outcome (Table 11). STEM students were 4.16 times more likely to agree that the courses they took influenced their behavior proactively to protect their privacy. Students who took 1-4 security classes were 2.33 more likely to agree on those as well than students who did not take any security classes. Seniors and junior students were 1.32 times more likely to agree than freshmen and sophomores that the courses they took influence their behavior to protect their privacy.

Question	STEM Status Vs Non-STEM)	Security Courses (1-4 vs. 0 course)	Class (Juniors/Seniors vs. Freshman/Sophomore)***	Age Groups 22-25, 26-30, 31-34, 35+ vs. 18-21
Mic/Camera Access (camerac)		1.35 (0.00374)		
Disable Features (disablec)			1.92 (0.0285)	
Data Collection (DataCollb)	2.86 (0.0050)			
Creating Profiles (creatpc)				2.48 (0.0138)
Influence Behavior (inflc)	4.16 (1.39e-05)	2.33 (1.14e-10)		

Table 12. Summary of Statistically Significant Predictors Affecting the Outcomes Concerning students' attitudes, awareness, and knowledge.

Table 12 presents the odds ratio and the p-value of the statistically significant factors from all the logistic regression analyses. STEM status and security courses were important factors in two of the logistic regression models. And both predictors appear to affect students' behavior. On the other hand, class and age did not play as much as a role. This could be due to the fact that the majority of the students were in the 18-21 age group. It is recommended that all students take security courses regardless of their major.