An Analysis of the Level of Concern Displayed Among the Malone University Undergraduate Student Body in Regards to their Online Personal Information Security

Scott Markle
Malone University; HON 496
December 1st, 2020
Advisor: Dr. Kyle Calderhead, Ph.D

Submitted in Partial Fulfillment of the Requirements for Graduation from the Malone University Honors Program

Abstract

The 21st century is one that is dominated by rapid technological advancements. Increased utilization of these technological betterments have created a multitude of security vulnerabilities. In this thesis, I assess the level of concern displayed among the undergraduate student population of Malone University, located in Canton, Ohio, in regards to the vulnerability of their personal online information. Nine questions, with focuses in cybersecurity scenarios, defense strategies, and threat response, were asked of participants in an online survey. From the quantitative results of these questions, trends were interpreted and conclusions drawn.

Keywords: cybersecurity, Malone University, technology, vulnerabilities, cyberpsychology, information, students, college, concern, Likert scale

Acknowledgements

My dearest thanks to my thesis advisor, Dr. Kyle Calderhead, Ph.D., for all of the insight, advice, and knowledge he provided me with over the course of this long endeavor, as well as during my time at Malone University as a whole. My additional thanks to Prof. Ann Lawson, M.B.A., and Dr. Jim Glasgow, Ph.D., for being wonderful members of my thesis committee. Your wisdom and expertise in your respective fields helped add so much depth to this research.

My additional thanks to Julia Karmie and James Kontur, two of my dear friends from high school, who began their thesis experiences with me at Malone at the same time. We all went through the same struggles with our respective projects during a time when the world flipped on its head. All of the suggestions and advice you two gave me during the final months of this research will forever be appreciated.

I would also like to extend my gratitude to all of my brothers in Christ here at Malone University who supported me through every step of this process. Kyle, Lane, Christian, Ben, Max, Evan, Mitch, Daelen, Dan, Trent, and everyone else whom I can't fit into this page, your kindness and brotherhood will be with me forever.

To you, the reader of this research paper, I thank you for taking an interest in this work. I hope you find it as enlightening and informative as I did.

Finally, I would be remiss if I did not thank my parents, Jon and Cheryl, as well as my older brother, Jonathan. For all the years that you pushed me to never be satisfied with where I was, whether it be academically or spiritually, words can never truly express how much I love you.

Table of Contents

1. **Abstract** ……[Page 1]
2. **Acknowledgements** ……[Page 2]
3. **Introduction** ……[Page 4]
4. **Literature Review** ……[Page 6]
5. **Methodology** ……[Page 11]
6. **Analysis and Data Graphics** ……[Page 14]
7. **Discussion** ……[Page 20]
8. **Conclusion** ……[Page 26]
9. **Works Cited** ……[Page 29]

Introduction

In a world dominated by daily technological advancements and an increasing reliance upon these new technologies, there are a seemingly unlimited number of vulnerabilities within those technologies just waiting to be exploited. According to PurpleSec, a cybersecurity services company based in Washington, D.C., over the course of a ten-year period (2009-2019), the annual number of malware infections in the United States of America increased from an estimated 12.4 million in 2009 to an estimated 812.67 million in 2019, an increase of approximately 655.38%. In addition, in the year of 2020, with the COVID-19 outbreak uprooting nearly every corner of everyday life, PurpleSec reported an uptick of highly sophisticated phishing email campaigns run by hackers. These individuals would pose as representatives of the Center for Disease Prevention and Control (CDC) or of the World Health Organization (WHO) and began plaguing individuals across the United States. These hackers were able to take advantage of the weary state that the COVID-19 pandemic had left the citizens of the United States of America in order to steal vital personal information. This example is but one of many cybersecurity threats that continue to plague the world every day.

For college students, especially in the current state of the world, having a positive personal wellbeing is certainly at the forefront of concern, whether that concern be primarily focused on physical, mental, financial, or spiritual wellness. However the World Wide Web, which is almost a necessity for modern college

students, is not always included in those concerns. Though parents will often tell students who are leaving to go to college, “Don’t go off campus alone,” or “Be careful if you go to a campus party,” the generational gap in regards to technology often leaves students without a reminder to be mindful of their online activities. Outside of the warning, “Be careful when using your credit card for online purchases,” college students outside the fields of Computer Science and Cybersecurity display less proficiency in managing their online information security. In fact, a study performed by a student at Central Washington State University found that students at institutions of higher education are the fastest growing target of cyber-attacks in the world. This is in large part due to this surprising lack of knowledge and education regarding cybersecurity, “despite the immense availability of information and practices” that could curtail the deficit (Hunt, 2016). Furthermore, Toptal, a renowned company composed of software engineers, noted that the education industry in general “ranks last in cybersecurity preparedness out of all industries surveyed” in each of the past 5 years. This translates to a severe fundamental deficiency of cybersecurity preparedness in the student populations of those educational institutions (*2019 Cyber Security Statistics Trends & Data*).

The purpose of this research is to analyze the level of concern among the undergraduate student body of Malone University, with the knowledge of the general deficit of comprehension of cybersecurity in the education industry, in regards to their personal online information security.

Literature Review

As stated by clinical psychologist Michael Seto in the journal *Pediatrics* on the impact of technology on the development of youths,

> "We are living in the most unregulated social experiment of all time - a generation of youth who have been exposed to extreme content online (Aiken, p.16)."

The world we live in today is one dominated by technology, with the World Wide Web and other technologies acting as omnipresent factors in almost every facet of the world and in life. In the year 2020, we have phones incorporated into wristwatches, surgical implants that allow for real-time monitoring of health data in patients with heart conditions, drones discharged for delivery of small quantities of groceries, and even 3D printers with the capability to print an edible pizza. Experts estimate that approximately 4.57 billion people (Clement, *Digital Users Worldwide - 2020*), which is nearly 60% of the world's population, are now active on the Internet, connected to each other in ways that were not possible less than fifty years ago. What was done in the 20th century via telephone and one-to-one-interaction can now be done much more conveniently and rapidly in the 21st century via computers, smart devices, and more. Furthermore, these advancements in the various fields of technology have drastically reduced the need for human involvement in the modern workforce. After all, machines are able to perform

thousands of calculations in short amounts of time, they do not fall ill like humans do, and most of all, they do not need to be paid.

With every new technological advancement, however, comes dozens of new technological vulnerabilities, silently waiting to be exploited. Security has often, and unfortunately, been subjected to the role of afterthought since the release of the World Wide Web to the public in April of 1993. Furthermore, despite the countless advancements made in security in the past 27 years since that public release, no amount of defense can ever properly and truly account for the numerous variables that make up human nature. The negative traits of individuals across the world, such as greed, lust, and sadism, combined with the anonymity provided by the Internet, have the potential to cause unparalleled damage to innocent users of our technological world. As stated by Mary Aiken, one of the world's most foremost experts in the field of forensic cyberpsychology,

> "Cyber space is a breeding ground for mutations. Real-world behavior migrates there and escalates or accelerates (Aiken, 2017)."

This mirroring of real-world behavior on the World Wide Web can also cause emulation of ignorance, wanton or not, of the dangers lurking in the dark corners of the Internet.

Generation Z is the first generation of individuals to grow up with the technology commonly seen today: smartphones, streaming services, Amazon, etc. As reported by Turn-Key Technologies, approximately 54% of college students

> "bring at least two internet-connected devices to campus, and another 22% of students bring three or four internet-connected devices to campus (Badrick, *College Campuses Continue to Struggle with Cybersecurity,* 2018)."

These types of technologies, now normalized by today's society, have revolutionized the educational experience. Professors are now able to circumvent the risks of mass in-person learning caused by the COVID-19 pandemic through the use of live streaming services such as Google Meet and Zoom to provide a functional learning environment for students unable to attend class physically. Online search engines, such as Google and Bing, have turned what used to be hours spent combing through textbooks in libraries into a simple expeditious matter. As reported by the website Campus Technology, a SurveyMonkey study from 2017 reported that

> "the majority of students (66 percent) said their overall technology experience at school has been excellent or good. What's more, most students (75 percent) said technology has had a significantly positive or positive impact on their academic success. Just 3 percent said the opposite (Kelly, *Survey: Most Students Say Technology Boosts Academic Success*)."

So as can be plainly seen, college students and technology are now a nearly inseparable combination. However this union has opened the gateway to a seemingly immeasurable amount of digital dangers. But why do students continue to willingly expose themselves to the dangers hidden in the recesses of the network? Mary Aiken states that it is "a combination of adolescent risk-taking and curiosity (Aiken, 2017)." That being said, it is not as if every college student is actively attempting to invite these hidden threats into their personal devices. It is simply the

fact that most students do not seem to be aware of the dangers they are exposing themselves to.

Individual tendencies and actions of college students aside, why exactly are institutions of higher education so vulnerable to attacks, and thereby increasing the risk of students being attacked as well? One reason, according to Toptal,

> "has to do with academia's unique culture, which prides itself on a degree of openness and transparency that most industries lack (*2019 Cyber Security Statistics Trends & Data*)."

A study conducted by the Indiana University Center for Applied Cybersecurity Research found that

> "colleges and universities have historically focused efforts on making sure that "[their] faculty and [their] students and [their] public and [their] donors [can] connect pretty easily to them." This has made college and university computer networks, the article says, "as open and inviting as their campuses (*2019 Cyber Security Statistics Trends & Data*).""

One other reason, as Toptal notes in their article, is simply for the fact that colleges, universities, and other institutions of higher education were of the first places that had Internet accessibility. As these places were some of the earliest adopters of the digital resources that have been refined into the tools we have today, many of them still utilize older systems and practices that by today's defense standards are incredibly insecure.

The duration of this accessibility, combined with the visibility of these educational institutions, means that cyberattackers have long had the time and

capacity to analyze these establishments for vulnerabilities to exploit. What's more, the Internet, and the World Wide Web as a whole, is an open environment that continues to grow with each passing second. Keith K. Hartranft, chief information security officer at Lehigh University, personally believes this to be the biggest challenge facing educational institutions in this area. Because of the "flat" nature, as Hartranft describes, of the higher education cyber environment, the decreasing separation and/or segmentation of personal data in the greater network only leads to more and more vulnerabilities opening up with each passing day (Davis, *Managing Cybersecurity in Higher Education*). All of these factors, when observed in conjunction with the general recklessness of students online, leaves the students much more vulnerable to become victims of these potential attacks and exploits.

Methodology

For my survey data collection, I chose to utilize the Likert scale, also known as the "rating scale." The primary principle of this form of data collection, according to *Basic Marketing Research,* is that when participants respond to questions that utilize this scale,

> "respondents specify their level of agreement or disagreement on a symmetric agree-disagree scale for a series of statements. Thus, the range captures the intensity of their feelings for a given item (Burns, *Basic marketing research: Using Microsoft Excel Data Analysis,* 2008)."

A commonly employed 5 point Likert scale example to measure satisfaction in survey format is: "Very satisfied," "Satisfied," "Neither satisfied nor dissatisfied," "Dissatisfied," and "Very dissatisfied."

This methodology was utilized in part due to a cybersecurity judgment questionnaire that I discovered during my initial research period. This example, which was performed at a northeastern United States university, consisted of 16 practical scenarios about cybersecurity in which respondents had to judge their level of presumed risk upon on a Likert scale of 1-6 (lowest risk = 1, highest risk = 6) (Yan et al., *Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?*). The participants' responses to the questionnaire identified the weakest links in their cybersecurity judgment, the study specifically highlighting the areas of least proficiency as areas involving the

identification of indicators of certain potential cybersecurity intrusions, as well as areas involving their understanding of protecting cybersecurity in their devices in daily life.

After reviewing the survey and its methodology, I also chose to mirror the style of questions that were taken advantage of by this study. One question states,

> "Peyton is on his computer at work surfing the internet when a popup appears informing him that his computer has a Trojan horse virus. He clicks the link and is informed to purchase another virus scanner that will clean the virus (Yan et al., *Science Direct,* 2018)."

Furthermore, the scenario presented in the question was based on a real-life case that is often highlighted in modern media, all while being condensed into around 50 words in length.

Immediately after reading the various scenarios, I came to the conclusion that mirroring the style, wording, and length of questions found in this questionnaire for my own survey would allow for an effective application of the Likert scale, as well as provide a clear indication of the trends of the data I wished to acquire and review. In addition, per the suggestion of the employees of the Malone University I.T. Department upon my consultation of their expertise, I created two questions that asked respondents to provide their opinion, once again utilizing the Likert scale, of effective security measures employed by various companies across the world that are not currently provided by some of the services that Malone University is partnered with. After numerous drafts, with the aid of my thesis committee so as to ensure that my questions would be as unbiased, realistic, and

concise as possible, 9 questions were ready to be asked to the Malone University student body for my survey. For my usage of the Likert scale, I chose a range of 1, which represented a participant displaying the least amount of agreement or concern to the scenario or suggestion posed by an individual question, to 10, which represented a participant displaying the highest amount of agreement or concern to the scenario or suggestion posed by an individual question.

The topic of research, the nine questions, and the use of the Likert scale as selection of methodology, were all approved by the Malone University Institutional Review Board. The survey would take approximately 5 minutes to complete, with no known benefits to participants other than entry into a random drawing for 5 gift cards upon the conclusion of all data collection. The Institutional Review Board also required provisions to ensure the privacy of respondents, both from each other, as well as from myself and my thesis advisor, Dr. Kyle Calderhead, Ph.D., which were successfully implemented, while simultaneously allowing for data collection to go about without obstruction.

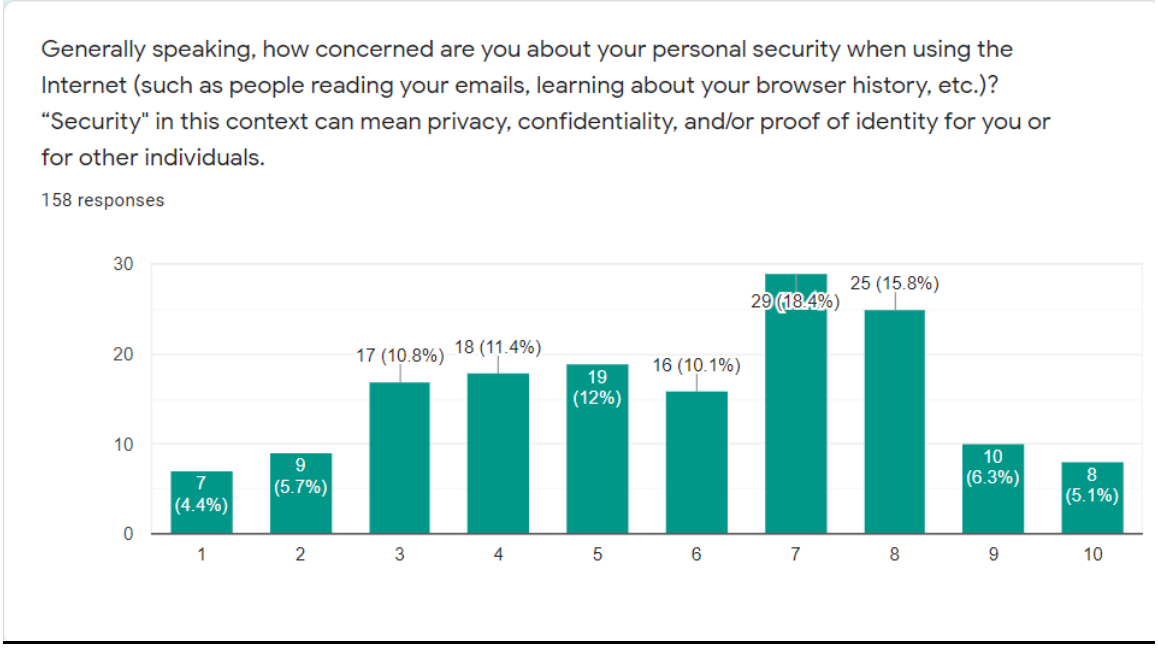
Analysis and Data Graphics

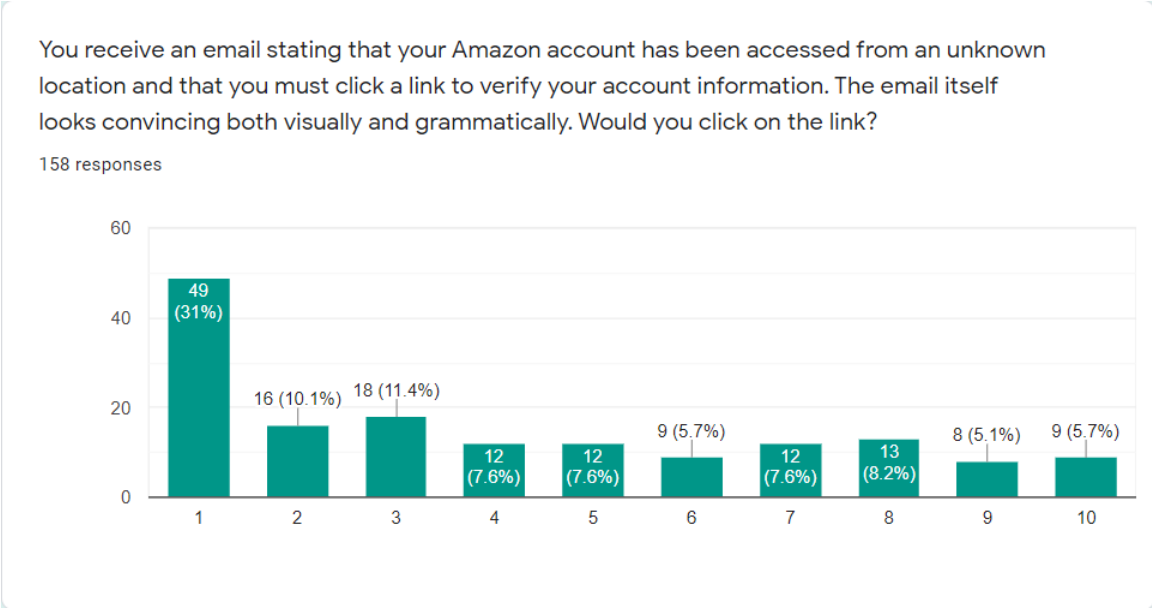
Shown below are graphics displaying each question, the number of responses, and the distribution of responses on a Likert scale of 1 (which represents having a very low level of concern/agreement to the question posed to the respondent) to 10 (which represents a high level of concern/agreement to the question posed to the respondent). Per the previously mentioned provisions provided by the Institutional Review Board to protect respondent privacy, there are no distributions by gender, academic status, or major(s). Despite the nature of these caveats, a clear indication of data trends was still possible to discern.

The survey was distributed via email to the undergraduate student body in the form of a Google Forms document. As previously stated all respondents were assured that the privacy of their personal information would be kept confidential from other respondents as well as from myself and my thesis advisor. This was done so as to reflect not only the provisions set in place by the Institutional Review Board, but also to reflect the principles of privacy being researched by this study.

Between the nine questions and 1418 total responses between those questions, 852 of the responses provided a response of at least “6” on the Likert scale of 1 to 10, depending on the question, which equates to approximately 60.1% of the responses. The remaining 566 responses, equating to approximately 39.9% of the total number of responses, represent answers between “1” and “5” on the Likert scale, likewise depending on the question. Of the total number of responses, 198 of them (approximately 14.0% of all responses), reported a “10” on the Likert scale.

147 of the total responses (approximately 10.4% of all responses) reported a “1” on the Likert scale.



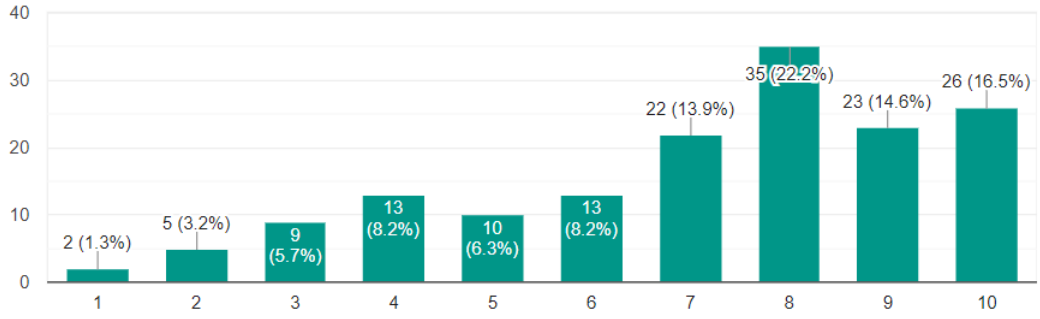


1

[1] Questions 1 and 2

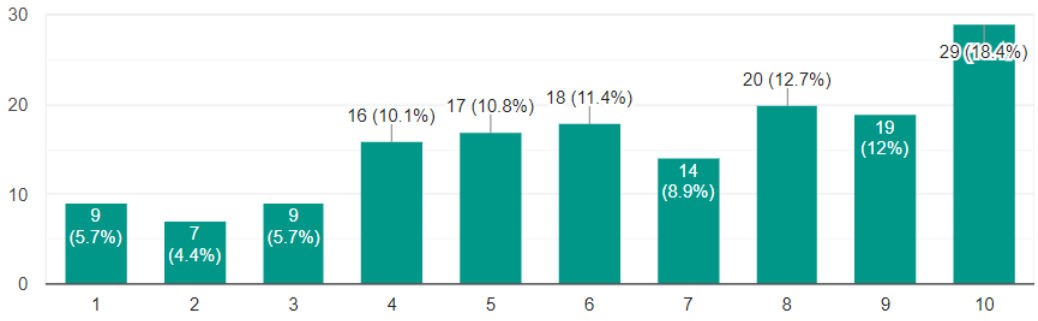
Your favorite fast food restaurant made national news for having a credit card number reader unknowingly placed inside one of their card swipe machines. You purchased food with your credit card from them during the time period and you do not know if your card number has been stolen or not. How do you feel? Do you feel any sense of concern or panic?

158 responses



A social media app reports that the location data for over 14 million users, including yours, has been sold to numerous companies and corporations with the purpose of sending messages to mobile devices whenever it enters or exits certain geographical areas. How does that make you feel?

158 responses

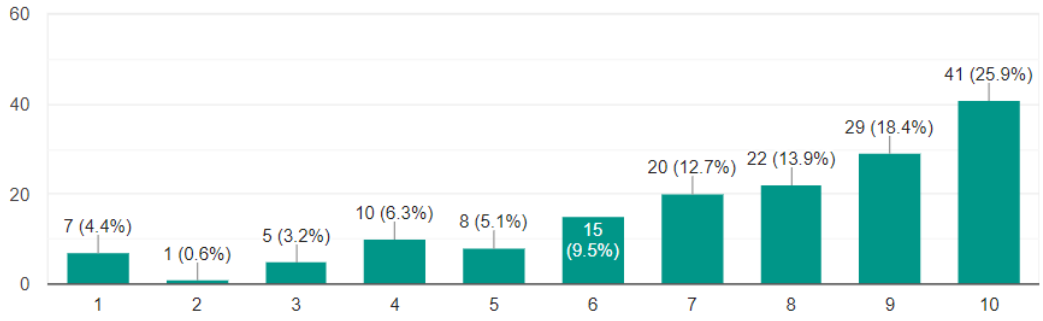


2

[2] Questions 3 and 4

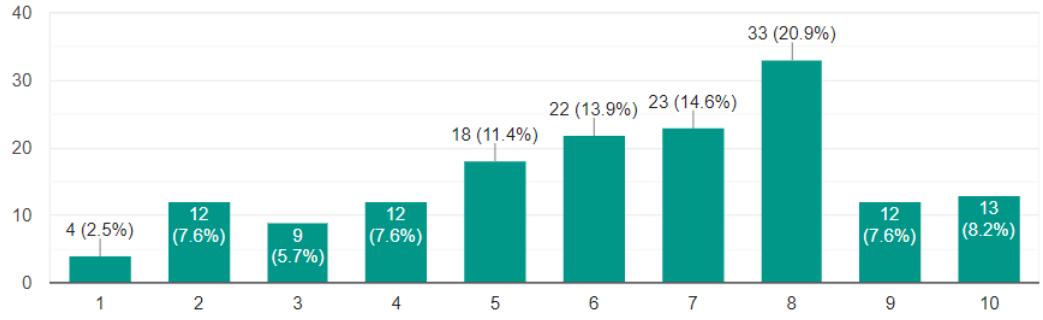
Amazon's servers are hacked and the names and email addresses of millions of customers, including yours, are put up for display on a popular information-sharing website. Do you feel the need to perform certain tasks to protect your information (i.e. changing passwords, deleting email addresses, etc.)?

158 responses



When working in a group for a company or some other form of organization, it is important for shared information to be kept secure through the use of a variety of protective cyber-measures. Though the risk for an elicit breach is low, how concerned would you be in establishing strong cybersecurity protocols, such as long and complex passwords, dealing with the potential for disgruntled employees, etc.?

158 responses

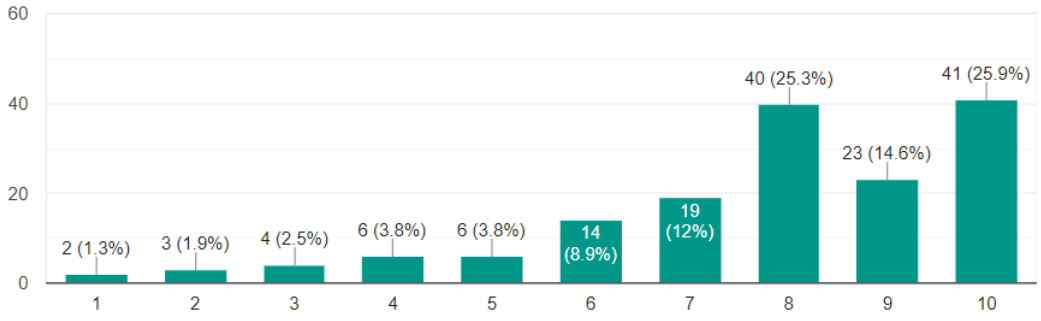


3

[3] Questions 5 and 6

Many websites use two-factor authentication to provide an extra layer of security for sensitive information. Examples of two-factor authentication include security questions and sending codes via SMS message. Do you feel that the addition of a two-factor authentication system would be beneficial in protecting your personal information?

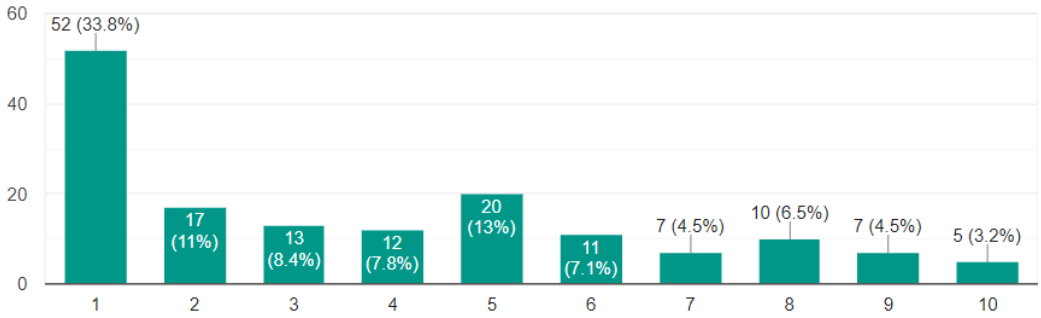
158 responses



4

Malone students will at times disconnect from the university's Wi-Fi in order to access certain webpages or download various things from the Internet. When this is done, the safeguards of Malone's cyber infrastructure are bypassed, enabling data to be funneled into the device without the safeguards being triggered. Do you do this? If you do, are you or are you not concerned when doing it?

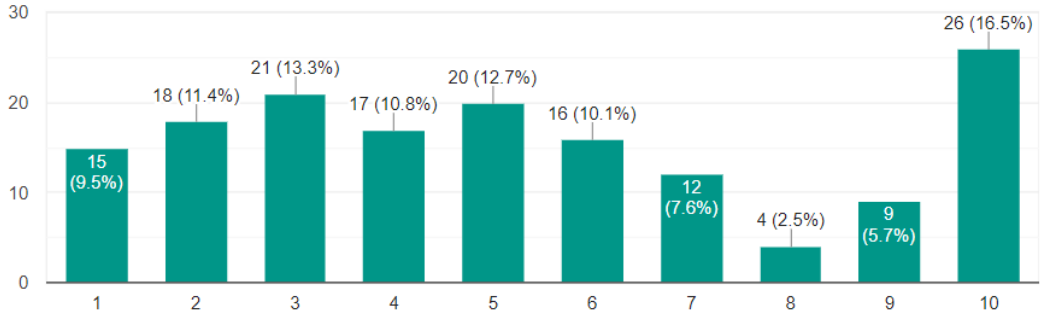
154 responses



[4] Questions 7 and 8

It is common for people to reuse passwords for multiple web services, such as Facebook, Google, and Amazon. Malone's web services, such as Google Drive, Moodle, and MaloneXpress, all use self-created, common passwords as well. What number of webpages do you feel it is safe to use the same password for?

158 responses



5

[5] Question 9

Discussion

Analysis of the data that my research revealed showed that the undergraduate student body of Malone has a fair level of cybersecurity competency. To put a number to this summation, the cumulative average of all responses was approximately 6.01 out 10, which demonstrates decent proficiency in regards to the general knowledge of basic cyber security guidelines and recommendations, as well as an adequately reasonable competency level of threat response, both theoretically and practically. Of the nine questions, there were three that were personally designed to be considered "more concerning" than others (for reference, questions 1, 2, and 3). The cumulative average between those three questions was approximately 5.65 out of 10, further highlighting my assumption that the student body of Malone only has a fair grasp of general cybersecurity knowledge.

The first question of the survey, "Generally speaking, how concerned are you about your personal security when using the Internet (such as people reading your emails, learning about your browser history, etc.)? "Security" in this context can mean privacy, confidentiality, and/or proof of identity for you or for other individuals," garnered an approximate average response of 5.77 out of 10, demonstrating moderately satisfactory awareness of the potential dangers to an individual's online information security. However despite this assessment, the average response number was personally quite a bit lower than I had hoped it would be. It was my personal hope that the average response for the first question in particular would be approximately "7" or higher, so it was incredibly surprising to

see that the number was nearly a point and a half from what I had anticipated it would be. This "personal hope" number was formulated in large part to personal observations of college student behavior garnered over seven semesters of study, compounded with general knowledge of the idiosyncrasies of human-technology interaction in today's society. Based on the results of this first question, I went looking through the other questions to find areas that the students in the sample seemed to struggle with. I went through with the hope that the numerical responses to those questions could help understand why my assumption about the average response number for the first question was incorrect.

The first area of notice that students in the sample seemed to struggle with are identification of cyber threats disguised or hidden in emails, such as the prompt of the email, a suspicious link, or poor grammar. The second question, "You receive an email stating that your Amazon account has been accessed from an unknown location and that you must click a link to verify your account information. The email itself looks convincing both visually and grammatically. Would you click on the link?" highlights this struggle. The question only garnered 51 answers of "6" or higher, or approximately 32.27% of the 158 responses for that question. Conversely, 49 respondents, approximately 31.01%, answered the question with a "1."

One of the most common methods of cyber hackers is to send emails out to individuals, for example, with a PayPal account. The email will typically ask the individual a question along the lines of the following statement: "Please follow the link below and login to your account and renew your account information," with a link seemingly directing the individual to the PayPal website. The link, however,

may take you to a website that infects your computer with malware, such as ransomware (a computer virus that completely locks you out of your computer until you pay the ransomer) or a keystroke logger (a computer virus that captures everything you type into your computer, such as your passwords and credit card information). Or it might even download the virus directly without going to a web page. As stated by an employee of Tip Top Security, a company which creates online safety guides for regular Internet users, "Malicious web pages are the most common way that computers get infected (Bobby, *The Truth About Clicking Links in Email and What To Do Instead*)."

Given this information, it is not difficult to understand why Malone students would have a difficult time recognizing suspicious emails. Tip Top Security's website provides guidelines on what email links that an individual *should* click on, stating:

> "Some examples of when to click [on links] include: You just ordered something from Amazon. Feel free to click the shipment tracking link in the email they send you, just make sure it's exactly what you're expecting. If you get a tracking link that you weren't expecting, or for a product you don't recognize, delete the email right away. Another example could be when immediately after you sign up for an account on a website. If they send you a link to confirm your email address, it's okay to click it, but again, make sure it's exactly what you're expecting and you specifically remember requesting it. (Bobby, *The Truth About Clicking Links in Email and What To Do Instead*)."

It would have been better for Malone students who responded with a "1" to have considered going directly to Amazon's website through an Internet search provider,

and confirming at the website itself whether or not the contents of the email received are true. A personal friend of mine, cyber security expert Tyler Hudak of TrustedSec's Incident Response and Practical Lead Team, who has had over 20 years of practical experience in malware incident response and information security, gave me this advice on this specific topic when I shadowed him for a day in the summer of 2019:

> "The bottom line is that unless you explicitly know and trust it, avoid it. That's all there is to it. Make this a habit and you can avoid one of the biggest mistakes in internet safety (Markle and Hudak Interview, 2019)."

Question 9 of the survey was also quite revealing about Malone University students and information security. The question stated, "It is common for people to reuse passwords for multiple web services, such as Facebook, Google, and Amazon. Malone's web services, such as Google Drive, Moodle, and MaloneXpress, all use self-created, common passwords as well. What number of webpages do you feel it is safe to use the same password for?" Of the 158 responses to the question, 104 responded with a "4" or higher, which is approximately 65.82%. Reusing a password is very risky, as my cybersecurity experts would say. A poll done by the webpage Security Boulevard revealed that "59% of people use the same password everywhere (Truta, *59% of people use the same password everywhere, poll finds,* 2018)." My shadowing experience with Tyler Hudak in the summer of 2019 also revealed his opinions on this matter:

> "One of the worst things that any user of the Internet can do is keep reusing the same password. If someone gets their hands on your password, and that

> password is used for multiple websites, or even your banking information, that person can access all of that information without any issue. The best thing that I can suggest is to keep using different passwords for different websites. The most common excuse I hear from people who use the same two or three passwords for multiple web pages is that they would easily forget all of their passwords, and that having only a few eliminates that risk. While that is a valid point, that argument loses its support once you learn that there are dozens of highly sophisticated and secure password managers that can help create and store thousands of different passwords and help a user not need to remember them all (Markle and Hudak Interview, 2019)."

A 2014 study done by one such password manager, LastPass, shows that by the age of 18, one-third of all United States of America citizens will have their information stolen, many of them without even knowing it. The primary causality for this statistic, the study argues, is human nature.

> "It's only human that, when confronted with an overwhelming number of websites, devices, apps and networks that require login credentials, we're hit by "Security Fatigue." This can result in a "don't give a damn" attitude about password reuse. Reusing a password is simply the path of least resistance (Pixel Privacy, *The Real Life Risks of Re Using The Same Passwords*)."

It can be reasonably inferred that this argument applies to the mentality of the Malone University undergraduate student body as well, given the statistical results of the question.

Going forward, given the sample size in relation to the overall undergraduate population of Malone University, I can say with 95% confidence, after calculations, that the approximated averages for each individual question have a margin of error of approximately 5.41%. This means, in short, that there is a 95% likelihood that the true values for each of the nine questions is within ±5.41% of the measured/surveyed values, thereby supporting the legitimacy of the findings of this research.

Conclusion

In conclusion, though the undergraduate student body of Malone University has a reasonable understanding of the dangers facing the security of their personal information online, there is still much room for improvement. With the world constantly evolving and digital advancements continuing to dominate the 21st Century, there will be no shortage of potential dangers hidden within the World Wide Web. With cybercriminal activity continuing to become the greatest threat to every company worldwide, the damage these activities will enact on the world will be nothing short of disastrous. In the year of 2015, cybercriminal activity cost the world an estimated $3 trillion dollars annually. The Herjavec Group, a leading global information security advisory firm and a co-author of the Official Annual Cybercrime Report, estimate that starting next year, 2021,

> "cybercrime will cost the world $6 trillion annually…[this] represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined (Morgan, *Cybercrime Damages $6 Trillion by 2021,* 2018)."

Allow me to put this number into perspective: an individual is given $6 trillion. If they spend $1 million dollars per day, they would only have spent their first $1 trillion after approximately 2,800 years (Treadwell, 2020).

While there will most likely never be an end-all, be-all solution to the growing number of threats facing the digital world, there are plenty of measures that all people, no matter if they are a current, former, or future college student, or even someone who never went to college at all, can enact to help protect themselves and their information online. First, make more than one copy of your information: one of the most crucial elements of data security involves the utilization of data backups, for even if a cyber attacker is successful in retrieving data, data backups can help individuals confirm which systems, applications, etc. were breached, while simultaneously ensuring that any information potentially stolen is not lost forever to them.

Second, taking one or two cybersecurity electives to help solidify basic knowledge is an easy option for future or current college students. These classes aid in basic threat identification and assessment, and many even offer methodology on how to formulate a personal checklist to ensure that an individual is taking as many precautions with their passwords, banking information, etc., as they feel are necessary. Even though the digital threats faced today will undoubtedly not resemble the threats faced 15+ years from the present, understanding the various potential situations one can face when traversing the digital highway is beneficial to anyone as the world continues to advance technologically and digitally. As supported by Toptal,

> "Understanding vulnerabilities, how common cyberattacks work, and how to prevent such attacks is fundamental to creating a more secure – and

financially stable – future for higher education (*2019 Cyber Security Statistics Trends & Data*)."

A cybersecurity major was recently started at Malone University, and it is my personal recommendation, not due to being a student of Computer Science but rather given the results of my study, that the university consider altering the General Education requirements to include, at the bare minimum, an introduction to cybersecurity course.

Finally, as stressed numerous times over the course of this paper, take the time to think things over. If a situation arises that brings about thoughts such as, for example, "Is this a safe thing to be doing?", or, "What are the potential consequences for this particular action online?" As previously stated, do not open attachments or click on links in emails that you were not expecting to receive, and if there even a hint of suspicion in your mind, whether it be from the grammar of the email, for example, exercise caution.

Malone University's undergraduate student population, like the students of institutions all over the world, is one where technology has been interwoven into every aspect of daily life. This study has shown that even if there does appear to be a decent general knowledge of the threats and recommendations that lurk in the recesses of the World Wide Web and Internet of Things, human nature is a variable that needs to be more thoroughly addressed in the decision making process that is associated with the traversal of the current age of technology.

Works Cited

Alvin C. Burns. 2008. Basic Marketing Research : Using Microsoft Excel Data Analysis. (2008). Retrieved November 9, 2020 from archive.org/details/basicmarketingre0000burn/page/245

Anon. 2020. 2019 Cyber Security Statistics Trends & Data. (October 2020). Retrieved November 9, 2020 from purplesec.us/resources/cyber-security-statistics/

Anon. 2020. The Real Life Risks of Re Using The Same Passwords (And How to Establish a Safe Password Policy). (January 2020). Retrieved November 9, 2020 from https://pixelprivacy.com/resources/reusing-passwords/

Bobby. 2015. The Truth About Clicking Links in Email and What To Do Instead. (May 2015). Retrieved November 9, 2020 from https://tiptopsecurity.com/the-truth-about-clicking-links-in-email-and-what-to-do-instead/

Craig Badrick. 2018. College Campuses Continue to Struggle with Cybersecurity. (January 2018). Retrieved November 9, 2020 from http://www.turn-keytechnologies.com/blog/article/college-campuses-continue-to-struggle-with-cybersecurity/

Donna Davis. 2017. Managing Cybersecurity in Higher Education. (2017). Retrieved November 16, 2020 from https://www.ue.org/education-matters/profiles-in-managing-risk/managing-cybersecurity-in-higher-education/

Filip Truta. 2018. 59% of people use the same password everywhere, poll finds. (May 2018). Retrieved November 9, 2020 from https://securityboulevard.com/2018/05/59-of-people-use-the-same-password-everywhere-poll-finds/

J. Clement. 2020. Internet users in the world 2020. (October 2020). Retrieved November 9, 2020 from http://www.statista.com/statistics/617136/digital-population-worldwide/

Jaine Treadwell . Just how much is $1 trillion? (May 2020). Retrieved November 15, 2020 from https://www.troymessenger.com/2020/05/30/just-how-much-is-1-trillion

Mary Aiken. 2017. *The cyber effect: one of the world's experts in cyberpsychology explains how technology is shaping the development of our children, our behavior, our values and our perception of the world--and what we can do about it*, New York, NY: Spiegel & Grau.

Rhea Kelly. 2017. Survey: Most Students Say Technology Boosts Academic Success. (September 2017). Retrieved November 9, 2020 from campustechnology.com/articles/2017/09/28/survey-most-students-say-technology-boosts-academic-success.aspx.

Scott T. Markle and Tyler Hudak. 2019. Shadowing TrustedSec's Tyler Hudak, an Expert in Information Security and Practical Cyber Defense. (June 2019).

Steve Morgan. 2018. Cybercrime Damages $6 Trillion by 2021. (December 2018).

Toni Hunt. 2016. *Cyber Security Awareness in Higher Education.* dissertation. Digital Commons - Central Washington State University.

Zheng Yan et al. 2018. *Computers in Human Behavior* 84 (July 2018), 375–382. DOI:http://dx.doi.org/https://doi.org/10.1016/j.chb.2018.02.019