**The Innovation Of Cyber Cadets**

Lamar Claiborne

Department of Cybersecurity, Old Dominion University

CYSE 494 Entrepreneurship In Cybersecurity

DR. Brian K. Payne

June 20, 2022

 The leading cause of Cyberattacks in business is due to human error, a company is only as strong as its weakest link. Furthermore, 95% of all security incidents involve human error, because they simply don’t care or are just not informed about the risk at hand. This can stem from using unknown external drives on the company's computers, interacting with adware, or even phishing emails nested with hyperlinks. If either is opened, downloaded, or simply clicked on and can result in your private information being compromised by malicious hackers or even load in malware to decrypt or steal information. The world needs to inform and knowledgeable when it comes to Cybersecurity, and simply protect themselves when it comes to interacting with such websites, applications, and documents on the internet. This is just as important as learning to cross the street these days because one wrong move on the internet could put your life in danger, lead to your identity being stolen, bank accounts being cleaned out, and your private health information can also be compromised. For example, not being knowledgeable enough to know that your home WIFI should be on a private network is a high risk in itself, because if compromised someone could use your IP address and MAC address to find out where you live.

 So, I have created an application called “Cyber Cadets” to help people learn in an entertaining, informing, and innovative way. This application will be used to help people of all ages be able to receive, obtain, and comprehend Cybersecurity information so they’ll be more knowledgeable when it comes to vulnerabilities, attacks, and ways to mitigate being compromised by malicious actors. This application will be accessible on all devices such as cell phones, tablets, desktops, and even laptops. Also, this application will have different forms of difficulty when it comes to learning such as Beginner, Intermediate, Pro, and expert; each level completed will offer a different incentive for the user. Furthermore, within these leveled modules of learning there will be interactive courses, terms and definitions, tutorials, and lastly daily reminders sent to your phone every day to complete your courses, also it will notify you on a certain topic dealing with Cybersecurity every morning. For example, “ Good morning Lamar! Did you know that 95% of humans are the cause of Cyberattacks? Also, don’t forget to finish up your beginner course today for a prize!” Moreover, the mission of this company is to make Cybersecurity an “OUR” problem, it should involve and inform everyone, through engaging activities, and learning how to combat daily online threats. Lastly, our slogan is “ Act now so you don’t have to react later.”

 Social engineering is one of the main attacks used by malicious actors to steal sensitive information, and this can result in a big problem for businesses and just everyday people. Social engineering is a form of psychological manipulation through deception to get users to divulge sensitive information which can be used for fraudulent activities. Social engineering is a problem because it can be exercised by authority where the social engineer is in charge and could be acting like they’re calling from a help desk, the office of a CEO, or even the police. Also, at times Social engineering is exercised by using intimidation by basically threatening the victim that bad things will happen if they don’t compromise. Sometimes a form of consensus or social proof could convince the victim to trust the malicious actor; for example, “ Your co-worker Billy did this for me yesterday, so it shouldn’t be a problem.” One of the biggest problems is that the malicious actor uses scarcity to make the situation seem like it won’t be in the bad state that it’s on for long. Furthermore, the biggest issue is the skill of urgency used by social engineers; which works right alongside scarcity and it makes the victim act quickly without thinking. Moreover, the purpose of the social engineer is to use familiarity, liking, and trust so they can compromise private information that they’re not authorized to have access to.

 However, our application “Cyber Cadets” has a course on social engineering that dives in-depth into the topic of Social engineering, because it’s one of the biggest problems in the cyber world that result in a cyber-crime. We are here to put a stop to malicious actors calling people acting as bill collectors for certain companies to steal money. By utilizing our application users will be informed on what to look for when it comes to social engineering, and simple steps to take to avoid being a victim of it. The application will put the user through real-life scenarios of them interacting with a Social engineer, and their performance determines whether they advance or not. The average organization experiences 700 Social engineering attacks a year, so businesses and society itself must be informed on this matter.

 A Phishing attack is the most used Cyberattack in the cyber-world and has turned out to be very effective at times for malicious actors. Phishing attacks just by themselves are responsible for more than 80% of cyberattacks, and 90% of data breaches are initiated by them also. This problem needs to be addressed the most, because people at home or their job are vulnerable to these attacks every day, and they need to know what to look for so they can protect themselves. Furthermore, a Phishing attack is when someone is sending fraudulent emails or other forms of communication while claiming to be a legitimate company to have a target reveal sensitive information such as credit card numbers or passwords. Moreover, Phishing is the biggest problem because most people fall for this attack, and it can cause a lot of damage.

 Our application has taken the initiative to make sure the biggest course within “Cyber Cadets” is the Phishing course because this is the most common cyberattack. It will inform the user about the many forms of Phishing such as Spear phishing, Vishing, Email phishing, Whaling, and Smishing. The user will understand why these various forms of Phishing are used, and when they're used. Furthermore, also what forms of information can be compromised through each form of interaction, because when you know what you’re up against you don’t panic and you troubleshoot the problem through practiced steps. We hope that our interactive courses, real-life scenarios, terms and definitions, and daily reminders can reduce the success of Phishing attacks as a whole because people are knowledgeable about what these attacks are and how to properly address them.

Furthermore, another common problem and cyberattack that needs to be addressed are Ransomware attacks. A Ransomware attack is a form of malware that holds a victim’s access to a user’s machine hostage until a ransom is paid. For example, you turn on your computer and you receive a fake message saying, “your computer has been locked by the police, if you would like to access your computer again send 25,000 dollars to this bank number.” Ransomware was the third most used cyberattack in 2021, and they’re responsible for 10% of all data breaches throughout the country. Also, on a global spectrum, it was reported that 304.7 million ransomware attacks had occurred in the first part of 2021, and that had increased by 151% since 2020.

To address this problem of Ransomware the Cyber Cadets application will inform the user in-depth on how to protect themselves against Ransomware attacks. For example, elaborating on the importance of always having a backup, an offline backup at that. Also, through the course, we will emphasize the importance of keeping your operating system up to its most recent version, by doing so it will patch certain vulnerabilities. Interactive courses will also be set in place to address the problem of people not knowing how to keep their application up to date, and more importantly inform them on why they do so. Furthermore, we want them to understand that these updates are not just for new features, but are used to put new security patches in place that will keep your information secure. Moreover, we will utilize quiz-based questions, interactive courses, and terms to help the user understand why Ransomware attacks are used and what on your computer could be possibly making you susceptible to them. Also, we will make sure this can be comprehended by all ages because Ransomware attacks have shown that they don’t discriminate nor target certain people in age or organization.

Another common problem that replicates itself consistently, and plays a huge role in the innovation of the Cyber Cadets application are Viruses. Many people on the internet have fell victim to viruses being downloaded on their computer without even knowing, because they simply interacted with fake websites, downloaded malware-infested files, and by opening e-mail attachments that also contain malicious code. A virus is something that infects your computer program that replicates itself when opened, and can modify other computer programs and systems; all viruses are not created equally either. Furthermore, users become compromised by this attack most of the time, because they are simply not aware of what not to avoid and what simply is a red flag. However, in the Cyber Cadets application we will teach our users not to accept anything without reading, open e-mail attachments from random personnel, insert non-specified external media, visit unknown links, and especially not to ignore your computer's updates and security patches. Furthermore, because this is a serious problem that needs to be addressed; there are 6,000 computer viruses released a month and since recorded in 2021 there are 1 billion forms of malware. So, this is a very serious problem that needs to be addressed immediately, and Cyber Cadets will make it mandatory that each user understands this topic in depth.

 Malware has always been a problem that is hard to avoid for anyone on the internet, whether it’s an organization as a whole or a user at home. However, this problem has become more alarming and unrecognizable as of late due to the creation of Trojan malware. The Trojan is a form of malware that masquerades as a legitimate program, but once downloaded it infects the computer/network with disruptive malware; this malware gets its name from the Greek story of the Trojan Horse. Also, Botnets cause a lot of problems for people on the network by infecting the computer with malware that is capable of denying network services to a legitimate host. Each form of malware is hard to detect by a regular person, but there are things you can do in advance to mitigate them from happening. Cyber Cadet's innovation of interactive Cybersecurity courses will address this problem head-on with modules on what are the best practices when it comes to protecting your computer, and if compromised how to handle that situation also.

 The problem that my innovation is addressing is that there are too many people that are not technologically informed, knowledgeable, or literate when it comes to protecting their computer systems. Furthermore, this is a problem because this means they’re not aware that they’re doing a poor job of protecting themselves and their private information. When people are on the internet just interacting with any site, hyperlinks, or attachments they’re essentially putting their lives in danger. However, I have decided to innovate the application “Cyber Cadets” to make learning Cybersecurity practices available to everyone of all ages for free, so we can be better workers and responsible users of the internet. We are targeting users such as businesses who can use it as training, government employees, daily users, and even school systems. This application will offer interactive courses, terms, and tutorials capable for every age group to digest if all courses are completed the user can receive an incentive or reward. Furthermore, each level such as Beginner, Intermediate, Pro, and Expert will offer different rewards; whether it’s store discounts, coupons for grocery stores, gaming cards for kids, and if you pass the expert level you will be rewarded with a “ Cyber Cadet Cybersecurity Expert Certification.” This certification that you can earn from passing the expert level of the course will be able to help job-seeking users have other credentials to include in their resumes when applying for jobs.

 Hopefully, the innovation of this application will help lower the cybercrimes, because users will now be more informed in the field of Cybersecurity, and will know how to protect themselves. Moreover, in 2020 throughout the year over 155.8 million individuals were affected by data exposures, and that is unacceptable because of the simple fact that the majority of them were to human error. So, if our application can keep people engaged in an entertaining but still informative way, and touch every age spectrum this problem could gradually be solved year by year. Furthermore, in terms of reducing the number of cybercrimes and people being technologically informed is the main goal. Also, this app is looking to reduce the problem of monetary loss within organizations, so our economy can continue to grow in the right direction. Since 2015, corporations have lost up to $5 billion a year due to various types of hacks and cyberattacks. Losing money can lead to a lack of trust, and a lack of trust can lead to fewer partnerships, and fewer partnerships can lead to fewer benefits for society, non-profit organizations, and businesses that help keep our country in order. So, this problem of people not being aware of what’s going on around them when it comes to the cyberworld is a big issue, because their ignorance could be a chain reaction of worst to come. Furthermore, so the innovation of this application is not to only affect the creators, but to affect the users in ways that they become more informed and confident when it comes to operating technological systems. We also want the user to understand that their handwork won’t go unnoticed, and that’s why for each level of difficulty that they complete; an incentive will be rewarded them.

 The problem of people not being informed and knowledgeable of Cybersecurity practices, and the innovation of the application “Cyber Cadets” has been put in place to change that narrative in the workplace and at home. However, even those both of these topics are Cybersecurity based, they also relate to Psychology in a sense. Furthermore, I took this Psychology class one semester and it showed me how important the mind was, and how it could also affect your body physically not just mentally. The definition of Psychology is, “the scientific study of the human mind and its functions, especially those affecting behavior in a given context.” Psychology relates to Cybersecurity when it comes to Social engineering because the malicious actor utilizes psychological manipulation to manipulate people into giving up private information they shouldn’t have access to. Also, utilizing Ransomware attacks makes the user act and make decisions they usually wouldn’t make, because the malicious actor would make it urgent and give them a time limit of how long they would have to get them a certain amount of money, and if not they would expose all of their data to the public. Many Cyberattacks take advantage of people not being aware mentally of what’s going on, and they manipulate and scare others to make mistakes that will compromise them.

 However, this problem doesn’t have to affect the mind negatively only; we can utilize the “Cyber Cadets” application to instill confidence and comprehensive skills into users. Interacting and learning from this app every day will instill confidence in the user's minds when it comes to them knowing how to deal with Cyberattacks. Also, their human mind will be more technologically informed and that will lead to them knowing how to mitigate certain Cyberattacks in advance. Furthermore, now that the human mind will be more technologically inclined from the applications courses, the functions of the body will also follow and put this knowledge into action. The human mind will be more motivated to finish these courses because they’ll be notified by doing so they will receive rewards at the end of the modules. Moreover, the “Cyber Cadets” application is tricking the mind to learn responsible Cybersecurity practices in a fun way that doesn’t seem like work, but by doing so the user is also becoming more informed on the topic of Cybersecurity. Mental manipulation can either have a positive or negative effect, it’s up to the person themselves to decide what the outcome will be.

 Information literacy also can relate to the Cybersecurity problem and the application of Cyber Cadets. Information literacy is used to find, evaluate, organize, use, and communicate information in multiple forms. Information literacy also helps aid decision-making, better problem solving, and even the gain of knowledge. Information literacy can relate to Cybersecurity literacy because it depends on individuals being aware of basic skills that they can use to protect themselves, data, and information systems. This form of literacy comes from a basic foundation of developing basic technology and literacy skills. The teachings of information literacy would help users recognize when information is false, and how to do in-depth research to prove it. Furthermore, this relates to our problem because if people possessed these skills they would be able to do research, and realize the difference between Phishing attacks and authentic emails. Information literacy could also help users evaluate information; which could help them better evaluate Cyberattacks and realize what Cybersecurity skills could be put into place to mitigate these attacks because of how they propagate. Furthermore, understanding what initiates an attack could help you understand what actual steps to take to prevent them from happening in the first place. When it comes to information literacy you need to possess the skills of problem-solving and critical thinking; which are very important when it comes to solving Cybersecurity literacy problems and applying “Cyber Cadets” teachings to real-life situations.

 There are so many ways to determine if the innovation is effective or not, forms of success for this innovation can be measured in a multitude of ways. We could determine if the innovation of the “Cyber Cadets” application is effective by welcoming feedback from our customers, on how they feel about the app. Furthermore, we could measure our in-app interactions and metrics to determine whether “Cyber Cadets” is gaining less or more traction than we thought. Also, We will get feedback from everyone and then use that information to enhance our app. We will then test our product in a much larger pool by making the app available for up to 2,000 users and getting feedback from that group. This sample will be random. We will use data analytics to determine how often the app was used and for how long. If by using data analytics we see that more than half of our users are completing modules and that others are utilizing the app to earn certificates; which are helping them get very effective jobs. We are also looking into how many of our users are receiving our “Cyber Cadets” certification, and if that number meets our goals we know our teachings are comprehensible and effective. Even though we want to serve our customers and help them to the best of our ability, the innovation cannot be determined effective if the budget of our business isn’t being met. So, the “Cyber Cadets” innovation will be determined effective, if we’re meeting our target budget and the revenue we’re bringing in is consistent each month and is increasing each year. Moreover, we would like to see that our entertaining and informative forms of education like our tutorials, interactive modules, definitive terms, and “ Cyber Cadets” certification are gaining so much attention from other organizations that they would like to invest in us, and that they truly believe in our mission statement to the point to where they would like to help us spread it further.

 To turn this innovation into a reality we will need many components to set the idea in motion. First, we will focus on the funding of this creation and how we will strategically approach this sector of the business. Initially each executive member of the group that is helping create “Cyber Cadets” will each commit equally to startup cash to get us up and running. Furthermore, we will seek further capital from tech investors who understand the concept. Sponsors can have their ads appear on our app in exchange for financial support. Also, we will seek cash and loans from family and friends if possible. When it comes to building the application we know we’re roughly looking at 150k to 170k, and that’s without factoring in developers. So, the total cost of development for this application will accumulate up to 300k; by the time we hire virtual support consultants also.

 Then, we would have to work on the development side of this innovation; which also has many components that go into it also. The development could be physical, hardware, software, and even cloud-based applications when it comes to making this innovation a reality. First, we would need to focus on the physical; which is where we will formulate a blueprint of how we will like the headquarters of our business to look. Then, hardware is the next stage of development, and this is where we will purchase a ton of servers, switches, CPUs, and network devices to get our servers and domain online. The software will be the last step of the development process, but it will be the most important by far. Furthermore, this is where we will program and develop our application to look and do exactly what we want it to do. Also, this application will require data analysts to analyze the company's data that is going in and out; which will help us continuously grow as a business in the future.

 The hiring process also plays a very big role in making sure that this innovation becomes a reality because we need the right people for our company to push it forward. So, this applies to hiring an app developer or team of App developers to develop the app, because as of right now we do not possess enough coding experience ourselves to successfully make a quality application. Furthermore, so we need to be on the lookout for highly qualified software engineers because we plan for our application to be complex and multi-functional. This process is very vital because we need the developers to use a universal developing language such as JavaScript to make the application shareable across multiple platforms without having to rewrite the app for each platform (Android, Windows, IOS, etc.). So, not only would we have to go through an extensive hiring process when it comes to this, but we will also have to hold various meetings with the app developers, so they can implement our ideas into the app. This must get taken care of because app development can range from 3 months to a year to complete.

 Furthermore, once the innovation of the app is nearing completion it will need to go through a sandbox testing phase. It will be tested in small lab procedures to work out any bugs or computational issues. Once the bugs are fixed within the application they will be ready for user interaction. We will have a rigorous testing process. First, we will ask some friends to try the app out and see how they like it. These friends will consist of those who have technology backgrounds as well as those who do not. We will get feedback from everyone and then use that information to enhance our app. We will then test our product in a much larger pool by making the app available for up to 2,000 users and getting feedback from that group. This sample will be random. We will use data analytics to determine how often the app was used and for how long. Once the testing phase is complete the “Cyber Cadets” application will be published, and available to various app stores such as Amazon, Google Play, Apple App Store, and Windows store.

 Moreover, the next steps when it comes to innovating this application and maintaining it as a whole when it comes to furthering the business will be measuring the highs and lows of the interactions within the application. The data for the “Cyber Cadets” application will be measured through bar graphs, scatter plot graphs, excel spreadsheets, data logs, and simple mathematical percentages to stay up to date on what we need to improve on. Also, when it comes to maintaining the application it’s about making sure our customers are happy, and when in help are fully supported by our tech support team. Furthermore, we will implement components to measure customer satisfaction through simple thumbs or thumbs, also by allowing them to elaborate on their expression through comment boxes. These are the many ways we will go about measuring all of these different forms of data and information : 

 First, I would like to thank the director of the advanced technology center for offering this class and allowing us to express our business ideas that could potentially change the world we live in one day. My classmates and I have innovated an application called “Cyber Cadets” that will be available to users all around the world to help them further their knowledge in Cybersecurity. The “Cyber Cadets” application will include interactive courses, terms and definitions, video tutorials, and certifications. All of these sections and modules will be utilized by the user to gain information in an entertaining and informative way on how to identify and mitigate common Cyberattacks. The purpose of this innovation is to offer our fellow peers free information that they can use to protect themselves from Cybercrime, and hoping that in the future we can play a big part in the decrease in the success of Cybercrimes. Furthermore, I learned so much from this project and it has taught me how to thoroughly plan out a business concept, put words into action, the many components of a business, and budget, and how to put myself inside of the consumer's mind. Moreover, students may find a ton of value within this project, I think it will show them a lot about themselves and will be a valuable learning lesson. The only thing that I would recommend is that the director allows students to have the option to present a presentation about their innovation instead of a paper because some people express themselves better verbally through visual aids.

Sources:

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking Humans? Social Engineering and the Construction of the “Deficient User” in Cybersecurity Discourses. *Science, Technology, & Human Values*, *46*(6), 1316–1339. https://doi.org/[10.1177/0162243921992844](https://doi-org.proxy.lib.odu.edu/10.1177/0162243921992844)

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. <https://doi-org.proxy.lib.odu.edu/10.1080/0144929X.2011.632650>

Silva, S., Silva, R., Pinto, R., & Salles, R. (2013). Botnets: A survey. *Computer Networks (Amsterdam, Netherlands : 1999),* *57*(2), 378-403.

Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for windows based ransomware attacks. *Expert Systems with Applications,* *190*, 116198.

Bergren, M. D. (2004). Spyware. *The Journal of School Nursing*, *20*(5), 293–294. https://doi.org/[10.1177/10598405040200050801](https://doi-org.proxy.lib.odu.edu/10.1177/10598405040200050801)

Szor, P., & Safari Tech Books Online. (2005). *The Art of Computer Virus Research and Defense*.

YANFANG YE, TAO LI, ADJEROH, D., & IYENGAR, S. S. (2017). A Survey on Malware Detection Using Data Mining Techniques. *ACM Computing Surveys*, *50*(3), 1–40. https://doi-org.proxy.lib.odu.edu/10.1145/3073559

Huang, Z., Wang, Q., Chen, Y., & Jiang, X. (2020). A Survey on Machine Learning Against Hardware Trojan Attacks: Recent Advances and Challenges. *IEEE Access,* *8*, 10796-10826.