

**STRANGER DANGER: EDUCATIONAL GAME FOR  
CYBERSECURITY AWARENESS**

A Thesis  
Presented to  
The Academic Faculty

By

Ziang Ren

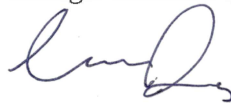
In Partial Fulfillment  
of the Requirements for the Degree  
Bachelor of Science in the  
College of Computing

Georgia Institute of Technology  
December 2019

**STRANGER DANGER: EDUCATIONAL GAME FOR  
CYBERSECURITY AWARENESS**

Approved by:

Dr. Sauvik Das, Advisor  
College of Computing  
*Georgia Institute of Technology*



Date Approved: 12/11/2019

Dr. Mark Moss, 2<sup>nd</sup> Thesis Reader  
College of Computing  
*Georgia Institute of Technology*



Date Approved: December 10, 2019

# TABLE OF CONTENTS

	Page
ABSTRACT	iii
<u>CHAPTER</u>	
1 INTRODUCTION	1
2 LITERATURE REVIEW	5
3 METHODOLOGY	10
4 PRELIMINARY RESULTS AND DISCUSSIONS	15
REFERENCES	17

## **ABSTRACT**

Cybersecurity is a concern for both organizations and individual users. Although there are a variety of security tools available, the number of cybersecurity incidents is still high. One cause of this phenomenon is that users are typically unaware or underestimating the potential negative consequences of their insecure behaviors on the internet. This leads to a lack of motivation among users for adopting security tools that require additional efforts in order to access a desired service. Conventional methods in promoting people's awareness of cybersecurity such as information sessions hosted by cybersecurity professionals have been shown to be ineffective. Video games is a novel approach in cybersecurity education has achieved some success in training cybersecurity professionals. However, whether video games are an effective method for educating the general public about the basic concepts of cybersecurity remains untested. This study presents Stranger Danger, a video game that simulates real-world exploits and teaches its users via negative reinforcements. The purpose of the study is to examine whether video games are effective in teaching the general public about basic cybersecurity concepts.

# CHAPTER 1

## INTRODUCTION

The term “Stranger Danger” describes a notion that all strangers can potentially be dangerous. While this term describes more of a moral panic than people’s daily behavior, most people do take some caution while interacting with people that they do not know in real life. However, they fail to maintain an adequate level of caution when they interact with people on the Internet. This can be potentially harmful: it is just as dangerous to fill in your bank credentials on an unsecured webpage as to trust a complete stranger with them in real life.

Such a difference in the level of caution has been identified by security professionals to lead to loss of personal property. This suggests that improving people’s awareness of security when they are using the internet can potentially reduce incidents that causes property loss. Researchers have been investigating the root cause of why people are less careful when they are interacting with the Internet to formulate ways to promote their awareness of security. Huang et al. concluded that people underestimate the risks of cybersecurity threats and therefore engage in insecure practices (Huang, Rau, & Salvendy, 2010). As a countermeasure, many companies host information sessions where security professionals are invited to talk about secure practices on the internet. Other measures include mandatory online training and posters on internet safety. These methods have been found ineffective because they fail to effectively convey the concepts of cybersecurity. In addition, they also do not retain the audiences’ attention well (Nagarajan, Allbeck, Sood, & Janssen, 2012). Even more unfortunate is that fact that

individual users who are unemployed or not enrolled in their company's internet safety programs are completely left out of any training (Sasse, 2003).

Another factor, suggested by Das et al., is that people are significantly affected by how their friends and family react to security practices. A person is discouraged from adopting secure online behaviors if the people around them also frequently engages in insecure behaviors (Das, Kim, Dabbish, & Hong, 2014). Additionally, the usability of existing security tools is also a factor. Some security tools require deliberate effort from the user while the benefit of using them is not immediately obvious. Users may be unwilling to apply these security tools. Such a security tool that is commonly used today is the 2-Factor Authentication (2FA). In 2FA, the user is usually required to submit their password and receive a confirmation code on another device, typically their smartphones. 2FA is more secure than the password-only approach because it uses "what the user knows" (the password) and "what the user has" (the other device, typically a smartphone). An attacker needs to break both factors in order to gain access to the user's account, which is significantly more difficult than if the user had only their password for authentication. However, because 2FA requires the user to take an additional step to authenticate and the immediate benefit from the additional protection is not apparent, many users are unwilling to use 2FA.(Das, Kim, Dabbish, & Hong, 2014) (Sasse, 2003).

One approach to solve the existing problems with the currently training methods and security tools is to formulate a more effective training method that can capture people's attention and convey the cybersecurity concepts. Nagarajan et al. suggest that the above shortcomings of conventional training methods can be overcome by using video games for training. With an appropriate choice of genre and mechanics, video

games can effectively engage their audiences and convey the concepts of cybersecurity (Nagarajan, Allbeck, Sood, & Janssen, 2012). Currently, there are relatively few attempts at creating such a “training video game” and whether video games can be a viable method for cybersecurity training needs to be further tested. One of the few attempts at using video games as a means of training is the CyberNEXS platform. The CyberNEXS platform is an emulation game that provides training in offensive, defensive and forensics skills in cybersecurity by placing users in a simulated environment to either exploit or defend a vulnerable system. CyberNEXS is widely accepted as a platform for training cybersecurity professionals (Nagarajan, Allbeck, Sood, & Janssen, 2012).

However, there is no tested evidence to suggest that a simulation video game such as CyberNEXS can be applied to educate the general public on the concepts of cybersecurity. CyberNEXS is designed to train security professionals with rigorous and competitive procedures. An ordinary user of the Internet may not have the motivation to dedicate a significant portion of their time to understanding cybersecurity at a professional level. Therefore, a professional training video game may not achieve the desired results on the general public (Huang, Rau, & Salvendy, 2010) (Nagarajan, Allbeck, Sood, & Janssen, 2012). Our research intends to explore this missing step in applying video games to teach the general public by developing a video game that specifically targets the general public. The video game is developed under the design suggestions provided by Nagarajan et al. and based on the findings of social influences on people’s security behaviors by Das et al. and the usability studies by Sasse and Davis. We expect that by building such a training video game that specifically targets the general public, we can test the hypothesis that video games can be an effective way of

educating people's awareness on cybersecurity. We expect that our research can contribute to the field of cybersecurity as a precedent for applying video game as a formal means of training to inspire further researches in the field and provide industries and the society with a more effective means to promote cybersecurity awareness and reduce property losses caused by insecure cybersecurity behaviors.

## CHAPTER 2

### LITERATURE REVIEW

Cybersecurity has been an issue with computer networks since 1971, when Bob Thomas created what was later considered the first computer “worm” that can infect computers, duplicate itself and spread through the ARPAnet (predecessor of the Internet). By this time, cybersecurity was more concerned with organizations rather than individual users (Collins, 2012). With the introduction of the Internet to civilian use, cybersecurity has become an important concern for individual users. Compared to organizations, individual users are more susceptible to cybersecurity exploits because they are less aware and prepared and generally do not have plans to minimize losses (Sasse, 2003).

To protect users from cybersecurity exploits, a variety of security tools are introduced that can be adopted by either organizations to protect their users or by individual users to enhance their security on the Internet. A widely adopted example is password authentication. In password authentication, users are required to submit their account (typically a username or email address) and a password in order to access a service. Access is granted only when the user submits a correct combination of account and password. However, it is possible for a malicious attacker to obtain this combination and pose as an authenticated user. Two-factor authentication (2FA) is an enhancement of password authentication. 2FA adds another security layer on top of the account-password combination by requiring the user to authenticate on “what they have”. This is typically a device other than what they are using to access a service (such as a smartphone), or another service that they have access to (such as email or text messages).

However, even with this sophisticated and secure authentication methods, reports of account breaches from end users are still prevalent (Sasse, 2003). It seems that as much as users want to protect their information against malicious attackers, they fail miserably in doing so. Studies have proposed several possible causes for this alarming difference between the abundance of cybersecurity tools that are available and the prevalence of cybersecurity breaches. Sasse suggests that a potential cause for this is that the current cybersecurity tools are simply not usable enough for the general populace (Sasse, 2003). In particular, Sasse argued against the 2FA system as it adds to the burden of users by requiring them to perform an additional step to access a service (Sasse, 2003). This additional step usually involves authenticating into another service. For example, a user is required to log into their email account to receive a 2FA email in order to access their social media account.

Moreover, the benefit of adding an extra layer of security such as 2FA is not immediately clear to the user. This is a general problem with security tools. A user may not realize the benefits of a security tool until they are exposed to malicious exploits and sustained financial losses (Das, Kim, Dabbish, & Hong, 2014). Additionally, users are generally inclined to underestimate the cybersecurity threats that they are exposed to (Huang, Rau, & Salvendy, 2010). These factors, combined with the difficulty of use, causes the users to have little motivation in adopting security tools to enhance their safety on the internet (Das, Kim, Dabbish, & Hong, 2014).

The lack of individual awareness of cybersecurity is also affecting companies and organizations. Researchers suggest that human factor is a major cause of cybersecurity breaches in companies and organizations(Sasse, 2003). To reduce the risk of

cybersecurity breaches caused by the human factor, companies and organizations usually train their employees on certain aspects of cybersecurity. These training are conducted in various forms including the use of infographics, posters, educational broadcasts, lectures and community talks (Nagarajan, Allbeck, Sood, & Janssen, 2012). However, their effects were unsatisfactory. Some identifiable shortcomings of these methods include: “...the existing training is conducted in very low frequencies; too much information is given at one time; training environments are usually not realistic; trainers are not efficient communicators; no reinforcement is imposed on the users’ behavior; no measurements on the users’ behavior are conducted; fail to retain users’ action (Nagarajan, Allbeck, Sood, & Janssen, 2012)...”

The above researches suggest that one way to reduce security breaches, particularly when we are targeting individual users, is to provide them with a motivation to use the available security tools such as 2FA. This motivation can be in the form of negative reinforcements where users are directly exposed to the consequences of cybersecurity breaches. In this case, video games would be an ideal environment to apply this negative reinforcement as they can simulate the exploits and consequences without harming the users in the real world. For example, a user can receive a penalty on in-game currency if they perform certain insecure behaviors. We hypothesize that by exposing users to these simulated harms, they would become more aware of the consequences of insecure behaviors on the internet and adopt more secure behaviors to prevent losses in the real world.

Video games are an alternative and relatively novel approach to cybersecurity training. Nagarajan et al. examines the platform, CyberNEXS (Network Exercise System)

that is widely adopted in professional cybersecurity training (Nagarajan, Allbeck, Sood, & Janssen, 2012). The CyberNEXS platform features a variety of video game modes that closely simulates the real-world internet environment. Within this simulated environment, players can either form red and blue teams to practice attack and defense skills or maintain critical services within a system, detect and report evidence of intrusion and malware and track networking activities. The platform is designed to provide comprehensive training on offensive, defensive and forensics cybersecurity skills, and is the de facto standard platform for training and certifying cybersecurity personnel (Nagarajan, Allbeck, Sood, & Janssen, 2012). Nagarajan, Ajay, et al. examined the reasons that make this platform an efficient tool to educate candidates on cybersecurity and points out that the platform covers most crucial aspects of cybersecurity. These aspects include “...methods to monitor and measure compliance and developing specifications to ensure compliance with security requirements; handling e-mails and attachments from unknown senders and spams; implementation of new technology; monitoring allowed and prohibited web usage; data backup and storage procedures; incident response procedures and trigger points; implications of shoulder surfing; use of personal system and software in work environment; creating, editing and managing changes to host or network access control lists; individual responsibility and accountability; physical access to spaces and incentive schemes (Nagarajan et al. 258).”

The success of CyberNEXS as a tool for training cybersecurity professionals suggested that similar software can be used to teach the general public about some basic concepts of cybersecurity in a non-professional context. An appropriate implementation can potentially be used as a novel method by companies to train their employees on

cybersecurity to reduce the risk of human factors in causing a security breach. With careful design, a training video game may serve this purpose. In the void of previous researches, we intend to test if video games can be used to reduce the risk of human factors in causing a security breach and formulate the appropriate design for this purpose.

## CHAPTER 3

### METHODOLOGY

The degree of engagement and similarity to real life are the primary reasons we identified video games as the proposed new method of cybersecurity awareness training. Generally, a video game of the simulation genre represents events in the real world realistically or with some artistic adaptations. The user's actions and decisions affect how the game responds to the user. The responses from the game to the user is also either a realistic representation or an artistic adaptation of real-world events. The user-behavior to in-game response cycle is an important factor in educating users on basic cybersecurity concepts. By responding positively to secure user behaviors (frequently changing passwords, strict privacy settings, avoiding unsecured networks) and negatively to insecure ones, the game makes use of the feedback cycle to engage its users and educate them effectively on cybersecurity concepts.

#### **Implementation of the Game**

##### **Game Mechanics**

Here we first give an overview of how the game interacts with the user.

Within the game, the user's level of security is represented by the "security index" (index). The user's activities within and outside of the game affects their index. An insecure behavior decreases the index, and a secure behavior increases the index. The game uses the index to decide whether to drop a "security breach" (security breach) for the user. The security breach is spawned for the user without their knowledge. The security breach is visible to and can be "exploited" (interacted) by all other players. When a security breach is interacted by another user, the user who spawned the security

breach will receive an in-game penalty and their security indices is decreased, making them more likely to spawn the security breaches and thus susceptible to further exploits. The user will also receive a set of tips on secure behaviors on the Internet. If the user can follow these tips, they will receive in-game rewards and their security index will be increased.

To calculate the security index for each user, we plan to track some of the most common user behaviors that introduces vulnerabilities to their presence on the Internet. Typical examples of these insecure behaviors include: using password that are too short (a 16-digit password is more difficult to crack compared with an 8-digit password), too common (a typical example is simply “password”), or can be derived from insecure sources (a typical example is a person’s birthday); not updating their password for an extended period of time; transmitting personal or financial information on an unsecured network. These behaviors are used to calculate the “security index” of the user. The “security index” serves as a random variable in a probabilistic function used to spawn “security breaches” for the user.

The “security breaches” are in-game representations of the user’s insecure behavior. The “security breaches” are spawned without the user’s knowledge. This is intended to simulate real-world security breaches where victims are unaware of the exploits until they are exposed to the negative consequences. The “security breaches” are then uploaded to the database so that other instances of the game can retrieve display them for other users. While not visible to the user who spawned them, the “security breaches” can be interacted by any other user. When the “security breaches” are interacted, notifications will be sent to the user who spawned the “security breaches”.

The notifications contain a brief description of the security breach, why it occurred, and how to prevent them from occurring in the future. A set of optional details describing the breach and appropriate countermeasures is also provided when the user reviews the “security breaches” in game. The user who spawned the security breaches will also be deducted “security points”, an in-game indicator of how secure a user is and can be used as the in-game currency. If the user is able to follow the recommendations provided by the game, they will receive in-game rewards and an increase in their security index.

The overall goal of design is to provide users with a competitive environment where they must constantly be aware of the safe and unsafe behaviors and unsafe behaviors are penalized. We expect that through this negative reinforcement, users can learn what behaviors are insecure and cause undesirable consequences. We are also dedicated to creating a simulation environment in the game that is comparable to the real-world so that the users can easily associate their in-game experiences to real-world situations where they are vulnerable to exploits. We hope that creating such an association can help the users apply what they have learned from the game to the real-world situations to prevent or reduce losses from a cybersecurity breach.

### **Game Infrastructure**

It is common in the video game industry to use a game engine to rapidly develop feature-rich games across platforms. The game, temporarily named “Stranger Danger”, is being implemented with Unity Engine. The scripts are written in C#, the official scripting language supported by Unity.

The Unity Engine has good rapid and cross-platform development capabilities. Existing scripts, except for platform-specific functionality that requires explicit scripting,

can be used across platform without any changes. The Unity Market Place, an online store for scripting, editing and visual assets, provide abundant material to extend new functionality from.

User authentication and database services are implemented with Firebase SDK for Unity. Firebase is an application development platform that provides industry-standard web and mobile application services. Compared self-implemented authentication and database services, the functionality provided by Firebase is more secure, stable and scalable. The most commonly used Firebase services, including authentication and database, also have cross platform support. Notably, Firebase services are optimized for the two major mobile platforms: iOS and Android, which are the target platforms of the video game.

The real-time geo-location functionality is implemented with Mapbox SDK for unity. Mapbox is an established provider of online maps. Their map sources are highly customizable and optimized for mobile platforms. There have been video games on mobile platforms with real-time geo-location features implemented with Mapbox SDK and Unity. A famous example is the Pokémon GO, a mobile game that allows player to collect virtual pets based on their real-time location. This suggests that the Mapbox SDK has reasonably well support for video games on mobile platforms. In our developmental build, we use the *C#* interface provided by the Mapbox SDK to access their functionality in Unity. This is implemented in the standard method of attaching behavior scripts to Unity in-game objects. The scripts contain references to the Mapbox geo-location services that are injected at run-time.

## **Deployment**

The game is planned to be deployed on Google Play Store for Android platforms, the App Store for iOS platforms, and itch.io for the Web + HTML5 platform.

### **Collecting User Response**

We rely on self-reports from users to examine if and to what extent playing this video game helps them become more aware of cybersecurity and adopt safer behaviors. We plan to collect the self-reports by having our users answer an online questionnaire that is designed to check their cybersecurity behaviors (for example, if they are using strong enough passwords and changing passwords frequently). The users' answers will be quantized into a score that indicates how secure their behaviors are. The users will be required to answer the questionnaire at variable intervals several times during the study. We group the scores by user to see if there is a statistically significant increase in this score over the course of the study. We will also examine the proportion of the users who exhibited this increase in their scores. Such an increase would suggest that playing this video game helps our users to adopt more secure behaviors on the internet.

The exact format and questions of the questionnaire have not been designed at this point because they are dependent on the content of the game. The questionnaire will be finalized after we have finished implementing the game.

## **CHAPTER 4**

### **PRELIMINARY RESULTS**

We are currently implementing the video game. We expect to deploy a functional complete working prototype by the end of December 2019. We expect that we will spend six months to finalize the in-game content and the self-report questionnaire. As of right now, no statistics is collected as they are dependent on the video game.

### **DISCUSSION**

Using video games to educate the general public about the basic concepts of cybersecurity is a novel approach. There is no tested precedent for us to refer to when developing such a video game. Furthermore, our research is in the early stages. We have still yet to complete a working prototype of the video game. Without precedents and test data, we do not know if our implementation can reach the goal of effective teaching the general public about the basic concepts of cybersecurity. However, based on the theoretical researches and comparable examples such as the CyberNEXS, we are confident that using video games a means of training is a correct direction. We can imagine that a successful implementation of the game that completes our proposed goal can be used to replace the existing training methods adopted by companies. This might help not only in reducing the costs that the companies spend on hosting information sessions but also in reducing the number of security incidents and losses sustained by the companies as a result of this more effective training method. Such a video game would also benefit individual users as it provides them with cybersecurity knowledges that they otherwise would not actively seek from less engaging sources such as information sessions.

However, we are aware that video game development generally takes many iterations. The final implementation may be well different from what we proposed in this thesis as we adapt each implementation to the self-reports by our users. We expect each iteration to provide us with knowledge of what is a good combination of genre, mechanics and other elements of the game. We expect include an analysis of each iteration in our result. We would examine how different elements, such as the choice of genre, affect the users' perceptions of cybersecurity concepts. In other words, we want to provide not only evidences that supports video games as an effective training method, but also why they are effective. We hope that such a comprehensive analysis would inspire future researches in applying video games as a means of cybersecurity training.

Again, we would like to reiterate that we are still in the early stages of our research. We would require concrete results before making any claims. Our current goal is to deliver a working prototype of the video game and deploy it to pioneering tests. The future direction of the research is dependent on the feedback we receive from these tests.

## REFERENCES

- [1] A. Collins, *Contemporary Security Studies*, Oxford University Press, 2012.
- [2] S. Das, *Computer scientists in action: Sauvik Das, usable security & privacy.*, vol. 25, 2018, pp. 61-62.
- [3] S. Das, T. H.-J. Kim, L. A. Dabbish and J. I. Hong, "The Effect of Social Influence on Security Sensitivity," in *10th Symposium On Usable Privacy and Security*, Menlo Park, 2014.
- [4] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology.," *MIS Quarterly*, vol. 13, no. 3, pp. 319-340, September 1989.
- [5] A. Nagarajan, J. M. Allbeck, A. Sood and T. L. Janssen, "Exploring game design for cybersecurity training," in *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems*, 2012.
- [6] A. M. Sasse, *Computer security: Anatomy of a usability disaster, and a plan for recovery.*, 2003.
- [7] D.-L. Huang, P.-L. P. Rau and G. Salvendy, "Perception of information security," *Behavior and Information Security*, vol. 29, no. 3, pp. 221-232, 2010.