The Social Engineer: An Immersive Virtual Reality Educational Game to Raise Social Engineering Awareness

Pascal Jansen
pascal.jansen@uni-ulm.de
Institute of Media Informatics
Ulm University, Germany

Fabian Fischbach
fabian.fischbach@uni-ulm.de
Institute of Media Informatics
Ulm University, Germany

Figure 1: Impressions of the *The Social Engineer*: (a) a player interacting with a USB stick in a company office, (b) welcome scene with introduction in form of a video call, (c) outside view of the virtual company, (d) a player observing employees in the company lobby, (e) a player looking at a social media page of an employee while impersonating a customer.

ABSTRACT

As system infrastructures are becoming more secure against technical attacks, it is more difficult for attackers to overcome them with technical means. Social engineering instead exploits the human factor of information security and can have a significant impact on organizations. The lack of awareness about social engineering favors the successful realization of social engineering attacks, as employees do not recognize them as such early enough, resulting in high costs for the affected company. Current training approaches and awareness courses are limited in their versatility and create little motivation for employees to deal with the topic. The high immersion of virtual reality can improve learning in this context. We created *The Social Engineer*, an immersive educational game in virtual reality, to raise awareness and to sensitize players about social engineering. The player impersonates a penetration tester and conducts security audits in a virtually simulated company. The game consists of a detailed game world containing three distinct missions that require the player to apply different social engineering attack methods. Our concept enables the game to be highly extensible and flexible regarding different playable scenarios and settings. *The Social Engineer* can potentially benefit companies as an immersive self-training tool for their employees, support security experts in teaching social engineering awareness as part of a comprehensive training course, and entertain interested individuals by leveraging fun and innovative gameplay mechanics.

CCS CONCEPTS

• **Applied computing** → **Computer games**; **Interactive learning environments**; • **Security and privacy** → **Human and societal aspects of security and privacy**; **Social engineering attacks**.

KEYWORDS

serious game, educational game, virtual reality, immersive simulation, social engineering, security awareness

ACM Reference Format:
Pascal Jansen and Fabian Fischbach. 2020. The Social Engineer: An Immersive Virtual Reality Educational Game to Raise Social Engineering Awareness. In *Extended Abstracts of the 2020 Annual Symposium on Computer-Human Interaction in Play (CHI PLAY '20 EA), November 2–4, 2020, Virtual Event, Canada.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3383668.3419917

CHI PLAY '20 EA, November 2–4, 2020, Virtual Event, Canada

ACM ISBN 978-1-4503-7587-0/20/11…$15.00
https://doi.org/10.1145/3383668.3419917

1 INTRODUCTION

Social engineering (SE) attacks exploit the human factor of information security to avoid otherwise complex technical means to access well-secured systems [4]. The goal is to obtain confidential information in the course of industrial espionage, information theft, or leaks of upcoming products, which causes enormous costs for the targeted companies if an attack is successful [18, 31]. The number of SE attacks has increased significantly in recent years [12]. According to the 2017 Cost of Cyber Crime Study [24], SE attacks are the second most common type of attacks experienced by companies. Security experts identified the lack of employee awareness as the most dangerous SE threat to organizations [6], as it is essential in detecting and fending off an attack early on. The lack of awareness can be ascribed to the missing of teaching and training options about the threats of SE [28].

Often, SE training is only a small part of traditional security courses taking place over several days and primarily mediated through classroom lectures, e-learning materials, and workshops [23]. The long-term beneficial effects of such courses are unclear [12, 28]. Therefore, interactive teaching opportunities should be considered that may increase the efficiency of such awareness training. One solution with great potential in teaching is the use of educational games [17]. By using the concept of gamification, the effect of learning in education can be enhanced [7]. An immersive experience while playing an educational game further increases the learning effect [5]. Both can be achieved by using virtual reality (VR).

We created *The Social Engineer*, an immersive VR educational game (see Fig. 1). The goal of *The Social Engineer* is to sensitize players to the topic of SE by taking up the role of a SE penetration tester in a virtually simulated company. While exploiting common vulnerabilities to conduct frequently used SE attack methods, players can gain sustainable awareness for SE. The concept of the game has been designed with the help of SE experts from the cybersecurity company SCHUTZWERK [25] to ensure the technical and theoretical accuracy of the SE attack methods and tasks included in the game. In addition to the educational aspect, *The Social Engineer* should attract the interest of the player and the replay value of the game by including entertaining stories and varied tasks.

Our game targets three different user groups. (1) Companies can use the game as an interactive self-training tool to raise awareness about SE among employees and improve the company's information security. (2) Security experts can let participants of SE training sessions play the game supplementary to traditional classroom lectures. (3) Interested individuals can play the game for entertainment purposes at home and get sensitized about SE along the way.

2 RELATED WORK

The Social Engineer is primarily influenced by and based on (1) basic principles of SE in practice, (2) insights of previous works on educational VR games, and (3) previous games about SE.

2.1 Social Engineering

SE can be described as the art of manipulating and deceiving people on a social level to obtain confidential information [16]. The target of a SE attack is a person who has access to desired information, mostly employees of attacked companies [21]. It is usually carried out in direct (e.g. during a personal conversation) or indirect contact (e.g. during a telephone call) with a target person. A social engineer uses insights from the social sciences on human behavior and the principles of persuasion [2]. Often, existing security mechanisms at a technical level cannot prevent such an attack [12, 29]. Our game covers the SE attack methods *impersonation* [14], *voice phishing* [16], *USB baiting* [14], *dumpster diving* [16], *tailgating* [22], and *social networking* [16].

Beyond employee training, security companies can conduct SE penetration tests in companies to detect vulnerabilities inside security mechanisms [3]. Usually, employees are not informed about a penetration test to keep the scenario as realistic as possible. Auditors from the security company who perform a SE penetration test are called penetration testers. Although their goal is to simulate a malicious "attacker", they are subject to strict rules (e.g., prevent real damages, and avoid personal disadvantages of attacked employees) [8]. According to cybersecurity auditors [25], the exposure of a SE penetration test often has a better effect on awareness than SE training lessons because employees can see the impact of an attack themselves. The awareness spreads quickly even among employees who are not directly affected. A serious game that enables a first-hand experience for the player may be beneficial in inducing a lasting change in behavior and general awareness about the risks posed by SE.

2.2 Educational Games in Virtual Reality

Many studies have shown the positive impact of educational games on learning outcomes [5, 7]. Educational games in VR further provide the opportunity for trainees to act out realistic scenarios where safely making the right decisions is pivotal, and training in real life would otherwise be impractical or impossible. Makransky et al. [17] examined the effectiveness of immersive VR as a medium for delivering laboratory safety training. They observed significant differences favoring the immersive VR experience compared to a desktop VR simulation and a conventional safety manual. Virvou and Katsionis [27] found that their educational VR game's likeability and usability increased the students' motivation and engagement during learning. The results of previous works on educational games suggest to use VR for our game as we also aim for an immersive environment to enhance the learning effect and thus the players' awareness of SE.

2.3 Games about Social Engineering

Games in the context of SE are rare. Beckers and Pape [2] implemented an analog card-based board game for eliciting SE security requirements. Further, desktop games to convey the concept of *phishing* [9] and to train defending concepts against *phishing* [30] have been introduced. Zargham et al. [32] presented a mobile game to raise awareness of general privacy and security concerns on mobile devices. However, previous work only covers specific aspects of SE, but the SE domain is much larger. *The Social Engineer* focuses on the combination and staggering of multiple attack methods, which is a common approach in practice and has not been considered in previous games. To the best of our knowledge, we argue that

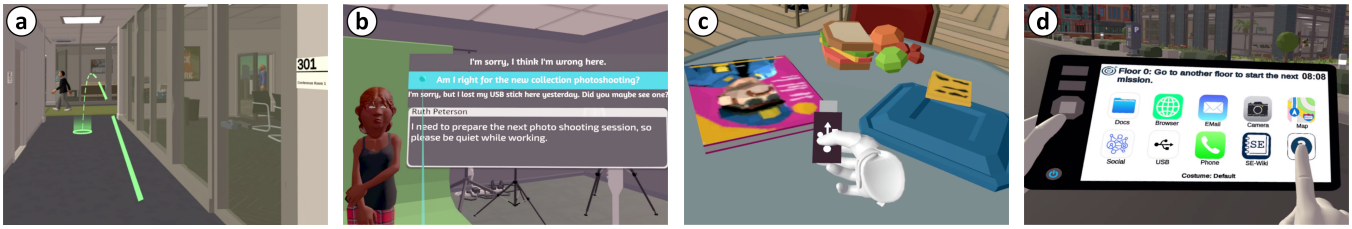

Figure 2: A player performing game interactions of *The Social Engineer*: (a) using the teleportation system to explore the company building, (b) choosing an answer option in a dialogue with an employee, (c) picking up a USB stick, (d) tapping on the virtual tablet to open an app.

our game is the first educational game that enables an immersive sandbox approach in experiencing different SE attack methods.

3 THE SOCIAL ENGINEER

We designed *The Social Engineer*, an immersive VR educational game that can be played in first-person view. The idea is to reveal security vulnerabilities inside an open-world office building that simulates a company with its' employees and security mechanisms.

3.1 Game Concept

The player takes on the role of a penetration tester on behalf of a cybersecurity company. The players' mission is to perform a SE penetration test inside a company by applying conventional SE attack methods without being exposed. Inside the company, the player can walk around and talk with employees or interact with objects. Some of the game mechanics are inspired by well-known sandbox stealth games (e.g., *Hitman* [1], *Thief* [11], or *Invisible, Inc.* [15]) and combined with real SE attack methods to create an unique player experience.

At mission start, the player receives a mission description in form of a video call with the security company (see Fig. 1b). It contains information about the involved company, a list of SE attack methods that are allowed to be applied, and different mission goals. Due to the open-world approach, each mission can be completed in several ways. Mostly, a combination of different SE attack methods in the correct order (see Fig. 1e) is necessary to complete a mission. A mission is fulfilled, when the mission goal is reached by exploiting one or several vulnerabilities without getting exposed. When the player gets exposed, the mission can be restarted at a checkpoint.

We want to use *The Social Engineer* to raise awareness against SE by demonstrating the immediate effect of SE attacks in a company while playing from an attackers' perspective. This concept of subversive design positions the player in a role that is conflicting with the overall goal (building awareness of preventive measures). As shown by previous research [19, 20], this is a legitimate and effective way of raising awareness. After each mission, an overview of revealed vulnerabilities alongside tips to avoid SE attacks in the form of *Do's and Don'ts* is presented to reinforce the learning effect. No specific computer skills or knowledge about SE are required to master the game successfully. A tutorial takes place in several individual rooms where an instructor Non-Player-Character (NPC) explains all game interactions and SE attack methods. During a mission the player can always access information about all applicable SE attack methods in a collection of knowledge that is integrated into the game. Additionally, when being stuck, a player can request help in the form of short instructions that recommend possible approaches to choose or apply the correct SE attack method.

3.2 Game World

We implemented a detailed game world with different missions that cover various aspects of SE. To enable an immersive exploration of the game world, we designed a detailed office building (see Fig. 1c and 1d) that includes rooms equipped with typical office furniture and created NPCs that represent typical employee roles and workflows of an advertising company.

Each NPC has a distinct schedule consisting of multiple schedule goals based on their tasks and role. The NPC reaction to the player is adaptive depending on whether the player is nearby, in sight, in a restricted area, or is interacting with objects. As SE attacks target the human factor of information security, we embedded different vulnerabilities to SE attacks into the NPC behavior. The game time is accelerated by a factor of 6, i.e., one game hour are 10 minutes in the real world. This enables the player to experience a whole office day without spending several hours in the game. The player can jump forward in time or use a fast forward function to wait and observe in-game events (e.g., employees leaving/entering a room, or waiting for meeting start).

The game consists of three missions that are independent of each other but can be played in a single run. The missions take place in different departments of the advertising company and have different goals, namely to (1) take a picture of confidential design drafts inside the creative department, (2) get access to the restricted IT department, (3) and retrieve confidential financial data from a meeting in the management department. In each mission, different SE attack methods lead to success. To complete all missions, players have to perform the SE attack methods *impersonation*, *voice phishing*, *USB baiting*, *dumpster diving*, *tailgating*, and *social networking*.

3.3 Game Interactions

The game in first-person view can be controlled by walking freely inside a predefined VR tracking space and by two VR controllers, represented as virtual hands. The game world interactions needed to carry out SE attacks are divided into four core interactions.

Game World Exploration: The player can explore the virtual company by walking around or using a teleportation system to rotate and navigate the first person character (see Fig. 2a).

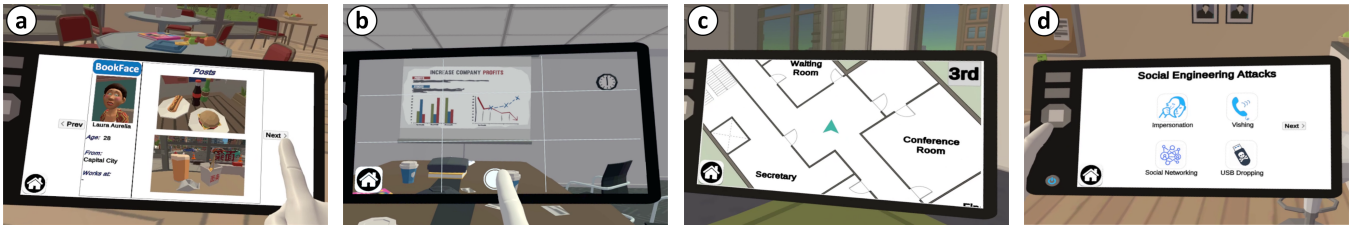

Figure 3: A player using different apps on the virtual tablet: (a) *social media app* with information about employees, (b) *photo app* to take pictures, (c) *map app* showing a floor plan, (d) *wiki app* providing information about SE attack methods.

Dialogue with NPCs: The player can talk with all employees through text-based dialogues that are placed next to the NPCs in the game world (see Fig. 2b).

Object Interaction: Objects like USB sticks and documents can be picked up and grabbed with the hand (see Fig. 2c).

Tablet Interaction: A virtual tablet attached to one hand, is the most important tool of the player (see Fig. 2d). It contains a set of applications that can be used to gather required and additional information as well as to start different SE attacks. Apps included are a *browser app* with information about the company, a *social media app* with profiles from employees (see Fig. 3a), a *phone app* to start phone calls with employees, a *document app* to view found documents, a *photo app* to take pictures of the game world (see Fig. 3b), a *map app* that includes a floor plan (see Fig. 3c), a *wiki app* with information about SE attack methods (see Fig. 3d) and a *help app* that provides hints.

3.4 Design Process and Implementation

After we had come up with the idea of the game, we conducted an informal interview with two SE experts from the cybersecurity company SCHUTZWERK [25]. The main points of the interview were a discussion about the lack of awareness regarding SE in companies, their experiences as a penetration tester, the most important SE attacks, which attacks could easily be implemented into a game, and different gameplay possibilities (e.g., playing the attacker, or being the defender). We had a meaningful discussion that helped to specify further directions of the game. As a result, we created a list of relevant SE attacks, gained insights about how the SE attacks can be conveyed in our game scenario, and identified important aspects for SE awareness.

With this information, we created a paper prototype in form of a board game that consisted of a floor plan as game world, pawn figures as employees, and cards for dialogues and user interfaces. The paper prototype included all game world elements and missions from the final version. We recruited four people to play the paper prototype, while we controlled the game logic in each session. In post-game interviews, we wanted to find out if they understood the concept and evaluated whether the missions' difficulty was appropriate.

Based on the paper prototype, we implemented a desktop-based digital prototype of the game in Unity [26] to determine the technical feasibility of the game concept. The digital prototype contained first implementations of an office building, employees, all missions, and the ability to perform SE attacks. In the form of a think-aloud walkthrough, one SE expert played all three missions of the game and gave feedback about the realism of the missions, game bugs, and visual improvements.

For the final version of *The Social Engineer*, we transformed the desktop game into a VR game and improved the appearance as well as the gameplay. It can be played on a HTC VIVE head-mounted display [13]. We used a previous prototype of the game to develop a concept for progress assessment for adaptive hints in educational VR games [10].

4 FUTURE WORK

In a future user study, we want to evaluate the player experience as well as the effectiveness of our game as a tool to raise awareness about SE. Besides, we plan to extend our game with various levels that represent other workplace environments with different context factors in private and public sectors (e.g., bank, university, or hospital). They enable the integration of other vulnerabilities and SE attack methods. We further plan to integrate a community level editor in our game with tools that are needed to build entirely new environments. Any community created content is primarily intended for private use, but can be part of an awareness training if reviewed in terms of correctness by SE experts.

5 CONCLUSION

In this work, we presented *The Social Engineer*, the first immersive educational game in VR intended to raise awareness about SE by conveying the threats of SE on an organizations' information security. The game enables company employees and interested individuals a first-person open-world sandbox approach in exploring and learning frequently used SE attack methods. It takes place in a detailed simulated company and contains three different missions. The players' goal is to reveal security vulnerabilities by applying various SE attack methods. Thereby, we intend to increase the players' awareness and knowledge about SE and enable them to apply the gained knowledge in their daily work. We argue that *The Social Engineer* is an exciting and fun tool for interactively conveying the threats of SE and promoting player curiosity.

ACKNOWLEDGMENTS

We would like to thank Tobias Drey and Julian Frommel for their support and constructive feedback, and Enrico Rukzio for providing research resources. We want to thank SCHUTZWERK GmbH for providing valuable insights into the work of a penetration tester.

REFERENCES

[1] IO Interactive A/S. 2016. *Hitman.* Game [Microsoft Windows]. (11 March 2016). Square Enix, Tokyo, Japan.

[2] Kristian Beckers and Sebastian Pape. 2016. A serious game for eliciting social engineering security requirements. In *2016 IEEE 24th International Requirements Engineering Conference (RE).* IEEE, 16–25.

[3] John P Ceraolo. 1996. Penetration testing through social engineering. *Information systems security* 4, 4 (1996), 37–48.

[4] Nic Chantler and Roderic Broadhurst. 2008. Social engineering and crime prevention in cyberspace. *Proceedings of the Korean Institute of Criminology* (2008), 65–92.

[5] Meng-Tzu Cheng, Yu-Wen Lin, Hsiao-Ching She, and Po-Chih Kuo. 2017. Is immersion of any value? Whether, and to what extent, game immersion experience during serious gaming affects science learning. *British Journal of Educational Technology* 48, 2 (2017), 246–263.

[6] Marilyn Cohodas. 2014. Poll: Employees Clueless About Social Engineering. https://www.darkreading.com/perimeter/poll-employees-clueless-about-social-engineering-/a/d-id/1316280. (Accessed on 04/05/2020).

[7] Darina Dicheva, Christo Dichev, Gennady Agre, and Galia Angelova. 2015. Gamification in education: A systematic mapping study. *Journal of Educational Technology & Society* 18, 3 (2015).

[8] Trajce Dimkov, André Van Cleeff, Wolter Pieters, and Pieter Hartel. 2010. Two methodologies for physical penetration testing using social engineering. In *Proceedings of the 26th annual computer security applications conference.* 399–408.

[9] Matt Dixon, Nalin Asanka Gamagedara Arachchilage, and James Nicholson. 2019. Engaging Users with Educational Games: The Case of Phishing. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems.* 1–6.

[10] Tobias Drey, Pascal Jansen, Fabian Fischbach, Julian Frommel, and Enrico Rukzio. 2020. Towards Progress Assessment for Adaptive Hints in Educational Virtual Reality Games. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems.* 1–9.

[11] Eidos-Montréal. 2014. *Thief.* Game [Microsoft Windows]. (25 February 2014). Square Enix, Tokyo, Japan.

[12] Enrico Frumento. 2018. Social Engineering: an IT Security problem doomed to get worse. https://medium.com/our-insights/social-engineering-an-it-security-problem-doomed-to-get-worst-c9429ccf3330. (Accessed on 04/02/2020).

[13] HTC Corporation. 2020. *VIVE™ | Discover Virtual Reality Beyond Imagination.* https://www.vive.com (Accessed on 06/01/2020).

[14] Imperva. 2019. *What is Social Engineering | Attack Techniques & Prevention Methods | Incapsula.* https://www.incapsula.com/web-application-security/social-engineering-attack.html (Accessed on 06/01/2020).

[15] Klei Entertainment Inc. 2015. *Invisible, Inc.* Game [Microsoft Windows]. (12 May 2015). Klei Entertainment Inc., Vancouver, Canada.

[16] Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. Advanced social engineering attacks. *Journal of Information Security and Applications* 22 (jun 2015), 113–122. https://doi.org/10.1016/J.JISA.2014.09.005

[17] Guido Makransky, Stefan Borre-Gude, and Richard E Mayer. 2019. Motivational and cognitive benefits of training in immersive virtual reality based on multiple assessments. *Journal of Computer Assisted Learning* 35, 6 (2019), 691–707.

[18] Efthymia Metalidou, Catherine Marinagi, Panagiotis Trivellas, Niclas Eberhagen, Christos Skourlas, and Georgios Giannakopoulos. 2014. The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences* 147 (2014), 424–428.

[19] Martin Mink and Felix C Freiling. 2006. Is attack better than defense? Teaching information security the right way. In *Proceedings of the 3rd annual conference on Information security curriculum development.* 44–48.

[20] Konstantin Mitgutsch and Matthew J Weise. 2011. Subversive game design for recursive learning. (2011).

[21] Francois Mouton, Mercia M Malan, Louise Leenen, and Hein S Venter. 2014. Social engineering attack framework. In *2014 Information Security for South Africa.* IEEE, 1–9.

[22] Pierluigi Paganini. 2018. *The Most Common Social Engineering Attacks.* https://resources.infosecinstitute.com/common-social-engineering-attacks/ (Accessed on 06/01/2020).

[23] Meisam Rezaeian, Nader Sale Gilani, and Hadi Modaghegh. 2015. Information Security Management In Iranian Smart Metering Project. (2015).

[24] Kevin Richards, Ryan LaSalle, M Devost, F van der Dool, and J Kennedy-White. 2017. Cost of cybercrime study, insight on the security investments that make a difference. *Ponemon Institute LLC, MI, USA* (2017).

[25] Schutzwerk GmbH. 2020. *Welcome To Schutzwerk.* https://www.schutzwerk.com (Accessed on 03/01/2020).

[26] Unity Technologies. 2020. *Unity Real-Time Development Platform.* https://unity.com (Accessed on 06/01/2020).

[27] Maria Virvou and George Katsionis. 2008. On the usability and likeability of virtual reality games for education: The case of VR-ENGAGE. *Computers & Education* 50, 1 (2008), 154–178.

[28] Gavin Watson, Andrew Mason, and Richard Ackroyd. 2014. *Social engineering penetration testing: executing social engineering pen tests, assessments and defense.* Syngress.

[29] Alvin M Weinberg. 1966. Can technology replace social engineering? *Bulletin of the Atomic Scientists* 22, 10 (1966), 4–8.

[30] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. 2019. What. hack: engaging anti-phishing training through a role-playing phishing simulation game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems.* 1–12.

[31] Michael Workman. 2007. Gaining access with social engineering: An empirical study of the threat. *Information Systems Security* 16, 6 (2007), 315–331.

[32] Nima Zargham, Mehrdad Bahrini, Georg Volkmar, Dirk Wenig, Karsten Sohr, and Rainer Malaka. 2019. What Could Go Wrong? Raising Mobile Privacy and Security Awareness Through a Decision-Making Game. In *Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts.* 805–812.