American Journal of Environmental Science and Engineering
2019; 3(4): 84-87
http://www.sciencepublishinggroup.com/j/ajese
doi: 10.11648/j.ajese.20190304.13
ISSN: 2578-7985 (Print); ISSN: 2578-7993 (Online)

Internet Security and Safety Learning via an Innovative Educational Game

Dora Puselj[1], Marin Vukovic[1], Mia Suhanek[2, *]

[1]Department of Telecommunications, Faculty of Electrical Engineering and Computing, University of Zagreb, Zagreb, Croatia

[2]Department of Electroacoustics, Faculty of Electrical Engineering and Computing, University of Zagreb, Zagreb, Croatia

Email address:

mia.suhanek@fer.hr (M. Suhanek)

[*]Corresponding author

To cite this article:

Dora Puselj, Marin Vukovic, Mia Suhanek. Internet Security and Safety Learning via an Innovative Educational Game. *American Journal of Environmental Science and Engineering*. Special Issue: *Smart Cities – Innovative Approaches*. Vol. 3, No. 4, 2019, pp. 84-87.
doi: 10.11648/j.ajese.20190304.13

Received: November 13, 2019; **Accepted**: November 23, 2019; **Published**: December 4, 2019

Abstract: Nowadays, Internet safety is a very important topic in order to avoid unwanted consequences of various dangers, attacks and frauds. The Internet has over 3.5 billion users today and unfortunately Internet frauds and different types of attack have such a rapid increase that they are currently the most common form of crime. Some of the everyday possible threats to Internet users are frauds with unexpected cash winnings, frauds when buying or selling goods, false personation and personal information theft. Education and knowledge of certain internet safety measures are the first step to achieve at least a basic level of Internet safety. The aim of this paper is to make it easier and more fun to learn about Internet security and ways to protect your data. Thus, we propose an educational game for learning about the fundamentals of Internet safety through interaction with other characters and solving different problems. The proposed game is called *Internet safety* and it is implemented in the Unity game engine. It contains three levels and it is played by controlling the main character who solves problems and tries to find out the way to reach the next level or finish the game. The problems that need to be solved are some of the most common frauds and dangers possible to encounter while using the Internet.

Keywords: Internet Security, Internet Safety, User Data, Educational Game, Unity

1. Introduction

Nowadays, each individual person connected to the Internet is exposed to various attacks and frauds [1-3], shown in Figure 1 [4].

Figure 1. *Internet security [4] .*

In order to avoid the possible consequences of the aforementioned attacks, it is necessary to know in what ways one can be deceived and attacked, and what is the most efficient way to defend or protect personal data. To be precise, the Internet has over 3.5 billion users and in addition to that Internet frauds have such a rapid increase that they are currently the most common form of crime [5]. Unfortunately, in the first half of 2018 more than 25 million user data were compromised or exposed every day. Data from various social networks has been compromised the most, while healthcare data had the most incidents [6, 7]. The most popular target was North America with 72% of published user data and up to 57% of all incidents, while in Europe the number of incidents is decreasing by 38%, however a certain amount of user data (i.e. 28%) is still being revealed [8].

The purpose of this paper is to make it easier and more fun to learn about Internet security and ways to protect your data. In order to achieve that the paper presents a specially

designed game envisaged for learning about the fundamentals of Internet safety through interaction with other characters and solving problems.

2. Possible Threats to Internet Users

Using the Internet can bring many risks that need to be addressed [9, 10]. To be precise, some users want to misuse someone else's data with the goal of material harm to other users. They do this using various methods e.g. malicious electronic messages and other malicious content. According to the ENISA Threat Landscape Report [8] published in 2018, theft, loss or attack of personal information is now the most common form of crime. AV Test statistics [11] show that in 2018, there were 137.5 million new malware copies. In addition, 93% of the malicious software studied have shown that the aforementioned software was polymorphic, meaning it can modify its code to avoid detection (2019 Webroot Threat Report) [11]. The same source states that 50% of the devices that were infected once were affected again in the same year.

A. Frauds with unexpected cash winnings

These are the frauds in which the victim is informed of a large sum of money he or she has just won or inherited. Furthermore, the user is kindly asked for "help" in transferring this money because the attacker for some reason is not able do it alone. Some examples of these types of fraud are false lottery win or false inheritance.

B. Frauds when buying or selling goods

In such frauds, the victim is convinced that he or she is conducting a legal business transaction. In majority of cases, these are fake websites where certain things can be bought, however the goods ordered will never be shipped and therefore will never arrive. In addition, there are also cases where vacation accommodation is offered, however upon arrival it is revealed that this accommodation does not exist at all.

C. False personation

In this scenario, the attacker presents himself or herself as another person, wanting to create a victim's trust and the illusion of an honest and real relationship. One of the most common examples of such fraud is asking for money to buy a plane ticket to meet in person, however the actual meeting never happens. Unfortunately, there is also an extremely dangerous type of fraud within this category, which is pedophilia. In that case the attacker tries to gain the trust of the minor and arranges a meeting while convincing the victim not to tell anyone about the meeting, especially not to the parents [12].

D. Personal information theft

Stealing personal information can be accomplished in many ways. One way is based on the installation of malicious software which can be accomplished by convincing the victim to install a certain useful and interesting application through the website, email or social networks. Technically, when a victim downloads and installs such an application, the attacker can actually access the victim's computer, email box or social profile, and can in addition keep track of all computer activities.

Another method of fraud is the so-called phishing. In that case, the attacker will present himself or herself as a financial institution and you will be contacted via email in order to change your data. The victim is then redirected to a fake website where he or she will fulfil the confidential personal information that the attacker can use in a variety of ways.

Another way to go about this type of frauds are false surveys where the victim is contacted by cell phone, telephone or email addresses and asked to complete the survey. In that way the attacker tries to obtain as many personal information as possible so that they can later use it for malicious purposes.

The greatest concern and the first level of protection against becoming a victim of an attacker over the Internet is the awareness of the user. Knowledge and education about the Internet attacks and frauds can minimize or even eliminate the possibility of becoming a victim and furthermore it can make the Internet a safer place for different users. In order to raise awareness about the importance of Internet security, we propose an innovative game in which a user solves his or hers tasks and problems by educating and introducing themselves to the main concepts of the Internet security. The idea is to learn about all the important facts in this particular field while making it fun, interactive and more efficient.

3. The Game – Internet Safety

Internet safety is an educational game in which the player controls the main character who encounters other characters and solves their problems concerning Internet and Internet safety. The main character can walk in all directions and is surrounded by walls, things and other living beings.

It contains three levels and it is possible to reach the next level by solving all the problems from the previous level. The main character can interact with other characters who present the problems that need to be solved. In addition, sometimes it is necessary to solve the problem on the computer positioned somewhere in the vicinity.

The main interface consists of the menu which leads to the start of the game, game settings and information about the game. The game is made in pixel art style.

A. First level

At the first level, the main character is placed in a space surrounded by walls, shown in Figure 2.

Figure 2. *Internet safety: the first level.*

Furthermore, there is a room and a parrot in it. When the character gets close to the parrot, the dialog with the mission will pop up. The parrot will ask the main character to solve a problem on the computer in the nearby room, which is to check whether the email that the parrot got is safe or not. When the main character goes to the computer, another dialog will pop up, with the question about whether an email from unknown sender and an attachment should be opened. Two options are possible: to open the email and to download the attachment or to delete it. After choosing one of those options, the main character should return to the parrot which will tell whether the choice was correct. Downloading email attachments from unknown senders can be extremely dangerous since it can contain all kinds of malware and the parrot will not approve for sure [13]. If the answer was correct, the parrot will give the main character another mission – which is to check for other unsafe emails on the computer. When going back to the computer in the room, an email content will be shown, which implies the receiver has won the prize of 10 000 dollars. The options possible are to reveal the credit card number via email [13] (which is always a bad idea) or to simply delete such an email. After choosing one of those answers and returning to the parrot, if any of those questions are answered incorrectly, the process will be repeated. It will be necessary to go back to the computer and answer the question correctly. If both of those questions are answered correctly, the main character will receive the key that unlocks the door which leads to the next level.

B. Second level

When starting the second level, the main character is placed in another space which is close to the guard that blocks the pathway to the next level, shown in Figure 2.

Figure 3. *Internet safety: the second level.*

If the main character interacts with the guard, it reveals what is necessary to get to the third level which is three gold coins. Furthermore, other characters appear on this level and those are a young girl, a bearded man and an old man, and each of them will reward the main character with a gold coin if their problems or questions are solved or answered correctly. The young girl asks the main character how to deal with the cyber bully. The main character can either choose to tell her to not let anyone mistreat her and block the bully or refuse to answer. The answer that will lead to a gold coin is obvious and yet might give someone inexperienced an idea how to simply solve a possibly distressing problem that happens very often in the cyber world. The problem presented by the bearded man is from his "personal life", in particular about his perfect girlfriend he met online a week ago. However, she only might look perfect at the first glance, since she asked him to give him money so she can go and meet him because she lives far away. This is quite a typical fraud and the advice that would reward the player with a gold coin if chosen would be to stop contacting the aforementioned girlfriend [13]. Another option is to advise the man to simply give her the money, which is considered the wrong answer in this game. The third character at this level is an old man who, unlike the previous characters, does not ask a question about his immediate personal life problems, but rather about a general fact that should be known to all Internet users. The question is: "How can you delete something forever, once you posted it on the Internet?" While there are many delete buttons, options to hide posts and so on, what is once on the Internet, might be there forever. For example, if one were to post something on the social media and wants to remove it later, anyone could have taken a screenshot and we can never be sure whether it is truly removed or not. When the main character gives the old man the correct answer, a key will be a granted which will unlock the door to another room with the chest. Inside the chest the gold coin can be found and taken. After solving all the three quests, the main character is ready to go to the guard and offer him the gold coins for a way out of this level.

C. Third level

Finally, the third level of this game consists of another space that is filled with mushroom houses, a guard, an elf, a girl with the mantle and a computer, shown in Figure 3.

Figure 4. *Internet safety: the third level.*

The guard informs the main character that what is needed to get to the end of the level is to collect three mushrooms. The girl with the mantle offers to help with the mushroom hunting if a certain task is performed. It is necessary to check one web shop site and determine its safety. The website can be checked on the computer that is located nearby and the password is provided by the girl with the mantle. When the computer is accessed, the dialog pops up with the web shop described as having quite low prizes of products that are much more expensive on other web shops. In addition, the site seems quite unfamiliar. Two options are given: the first is to evaluate the site as completely safe and not in need of

further investigation, and the second is to find out more about this site since it seems suspicious. In this situation it would be necessary to investigate more about the web shop in order to avoid losing money on the products that are fake or will never arrive [13]. By choosing the second and the correct option and returning to the girl with the mantle, the instructions about where to find the mushrooms are given, which is at the yellow mushroom house next to the guard. Two mushrooms are received after finishing this quest. The other quest at this level is given by the elf that stands next to the small green mushroom house. He has a problem and asks for help. He has got a missed call from an unknown number. Moreover, the number looks unusual and the elf is worried about whether he should try to call this number since it might be about something important. This tactic is often used to trick people into returning the missed called and losing a lot of money in the process [13]. The advice considered correct in this game would be not to call back, especially if the number is not previously checked and confirmed as safe. If the advice given to the elf is a good one, he will reward the main character with one mushroom. Another option is to tell the elf that he can call the number for sure, with no worries. Well, that might lead to a big money loss and the elf will not like that! Therefore, there will be no mushroom for that kind of an answer. After completing the two quests described, the main character should have three mushrooms and is ready to pass through the big purple mushroom house. When getting close to it, the main character will basically transport to other side of the mushroom house, which is the end of this level and the end of the game. Thus, the main character helped a lot of people and other beings in this process and hopefully the player learned something too and found out about some of the more common frauds that people "fall for".

4. Conclusion

This paper proposes an educational game with the goal to learn and test users' knowledge about possible dangers on the Internet named respectively *Internet safety*. The game was created in the Unity development environment. It is a game in which the main character aims to find a way out of each room or level. In order to get out of the room, the character has to have certain things, like a key or a coin obtained from the other characters in the game by solving several different tasks. All tasks are related and focused on spreading awareness and knowledge about most common Internet frauds and ways to avoid or resolve them. Educating people about Internet safety is extremely important, especially for young people who have no experience. Nonetheless, anyone can become a victim of an Internet fraud, to be precise that is almost inevitable if one did not take certain protection measures against potential attacks. When creating a game it was very important to develop a fun way to educate the majority of population with respect to the topic discussed in this paper. We have tried to achieve this through interaction with other characters who ask questions and by collecting different items with a purpose of moving to the next level. In future, the game could further be expanded with more levels while solving a certain level could give you certain benefits, such as changing the appearance of the main character.

References

[1] J. Jang-Jaccard and S. Nepal, A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences, Volume 80, Issue 5, 2014, pp. 973–993.

[2] M. Button, C. McNaughton Nicholls, J. Kerr and Rachael Owen, Online frauds: Learning from victims why they fall for these scams, Australian & New Zealand Journal of Criminology, Volume 47, Issue: 3, 2014, pp. 391–408.

[3] G. Norris, A. Brookes and D. Dowell, The Psychology of Internet Fraud Victimization: a Systematic Review, Journal of Police and Criminal Psychology, Volume 34, Issue 3, 2019, pp. 231–245.

[4] https://pixabay.com/

[5] https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

[6] NHCAA (US). A Private-Public Partnership against Health Care Fraud [Internet]. US: National Health Cara Anti-Fraud Association. Consumer Info & Action.

[7] M. K. Sparrow, Health Care Fraud Control Understanding The Challenge, Journal of Insurance Medicine 28, 1996, pp. 86–96.

[8] ENISA Threat Landscape Report 2018. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[9] R. S. Chakraborty, S. Narasimhan and S. Bhunia, Hardware Trojan: Threats and emerging solutions, HLDVT 2009, pp. 166–171.

[10] Cardenas, T. Roosta, G. Taban and S. Sastry, Cyber security basic defenses and attack trends, Fujitsu Lab.

[11] AV-TEST. URL: https://www.av-test.org/en/statistics/malware/. 2019 Webroot Threat Report. URL: https://www.cdn.webroot.com/9315/5113/6179/2019_Webroot_Threat_Report_US_Online.pdf.

[12] J. Strider, A. Third, K. Locke and I. Richardson, Parental Approaches to Enhancing Young People's Online Safety, Melbourne, VIC: Cooperative Research Centre for Young People, Technology and Wellbeing, 2012.

[13] HAKOM - Croatian Regulatory Authority for Network Industries URL: http://privatnost.hakom.hr/.