|  |
| --- |
| Designing a Virtual Reality Game to Educate Users on Romance Scams  Octavia Lea  MSc Ethical Hacking and Cybersecurity |

|  |
| --- |
| School of Design and Informatics  Abertay University |

Table of Contents

[Table of Figures ii](#_Toc140660431)

[Table of Tables iii](#_Toc140660432)

[Acknowledgements iv](#_Toc140660433)

[Abstract v](#_Toc140660434)

[Abbreviations, Symbols and Notation vi](#_Toc140660435)

[Chapter 1 Introduction 1](#_Toc140660436)

[Chapter 2 Literature Review 3](#_Toc140660437)

[Cyber-Scams 3](#_Toc140660438)

[Romance Scams 3](#_Toc140660439)

[Education 5](#_Toc140660440)

[Serious Games 7](#_Toc140660441)

[VR For Education 8](#_Toc140660442)

[Chapter 3 Methodology 10](#_Toc140660443)

[Platform 10](#_Toc140660444)

[Design 10](#_Toc140660445)

[Player and SteamVR 10](#_Toc140660446)

[Mechanics and World 10](#_Toc140660447)

[Plot 10](#_Toc140660448)

[Integrating the Plot 10](#_Toc140660449)

[Chapter 4 Results 11](#_Toc140660450)

[Chapter 5 Discussion 12](#_Toc140660451)

[Chapter 6 Conclusion and Future Work 13](#_Toc140660452)

[List of References 14](#_Toc140660453)

[Bibliography 15](#_Toc140660454)

[Appendices 16](#_Toc140660455)

# Table of Figures

# Table of Tables

# Acknowledgements

# Abstract

Context

With Internet usage rising, cyber fraud is becoming more common and lucrative for scammers. Romance scammers use the Internet to deceive individuals looking for love on dating websites. By forming deep relationships, a scammer can extract substantial amounts of money over many months or years.

Aim

To investigate romance scams and provide a game that will raise awareness and educate the public on romance scams. The game will be played in virtual reality.

Method

The Unity engine will be used to create a PCVR supported game where the player controls a computer program designed to analyse and mark messages as spam. Over the course of several in-game months, the player reads about a character's desire for love result in a romance scam. Surveys performed before and after containing qualitative and quantitative questions will be provided to determine if the game was successful in raising awareness of romance scams.

Results

Keywords

Serious games, Gamification, Romance scams, Cybercrime, Cybersecurity, Virtual reality

# Abbreviations, Symbols and Notation

HMD – Head Mounted Display (VR headset)

VR – Virtual Reality

# Chapter 1 Introduction

What is a scam? Popularity of the Internet, movement to cyber-crime and cyber-scams, romance scams and their effects, interactive education

While advance fee fraud did not start with the Internet, scammers have used the Internet to expand their reach and target victims all over the world.

According to The World Bank (Figure 1, 2022), Internet usage has risen by 133% in the past decade. As people use the Internet more, they move their activities, services, and products onto the Internet. This also includes criminal activities. One of the most common criminal activities on the Internet is fraud.

A graph with a line

Description automatically generated

Figure Change in adoption of communication technologies (World Bank, 2022)

Cyber-fraud has evolved over the years. In 2009, the top 3 scams were advance fee fraud, online auction and shopping, and lottery and sweepstake scams. By 2019, the top 3 scams were phishing scams, threats to life, arrest or other, and identity theft (Australian Competition and Consumer Commission, 2020). The evolution of the internet and improvements in hacking technology has caused this change.

An example of this is the introduction of business email compromise scams. According to Microsoft (no date), there are five types of business email compromise scams that all target different employee roles in the company. These types of scams are only possible with the shift towards using the Internet for most actions and with developments in hacking technology.

However, whilst businesses face anonymous attacks, individuals are still at risk from personalised attacks. Spear-phishing, where scammers use personal information to target specific individuals, is still a threat. Another type of tailored threat is romance fraud.

Romance fraud takes advantage of dating services to target a wide range of individuals, and the anonymity of the Internet allows scammers to impersonate attractive individuals. The scammers then approach victims and groom them emotionally. When the victim’s relationship with the scammer has grown, the scammer then extorts money out of the victim with scenarios such as asking for gifts, helping with travel costs and hospital bills. Once a victim realises that it is a scam or can no longer afford to pay the scammer, the relationship ends. This causes emotional suffering alongside financial suffering and can lead to second waves of scams as the victim believes that the relationship is salvageable.

Romance fraud differs to standard phishing techniques because it is a long-term scam. The long-term nature makes it difficult to inform and warn people, as it can be hard to distinguish from common dating messages at the start. In contrast, people can be made aware of standard phishing scams through training and test cases, where mock scams are sent, and the expected response is to mark as spam.

As a result of this, more bespoke education should be used to inform about romance fraud.

One avenue of education is using serious games. Serious games are a subset of games that have another purpose alongside entertainment. They are used to promote learning, behaviour change, or to present a message. The use of games to educate has several benefits over traditional teaching. Firstly, they are a safe environment for experimentation. This means that players can experiment as mistakes do not pose any physical effect. Secondly, serious games allow for learning at the player’s own pace. Instead of following a teaching plan alongside other individuals with different time commitments, games are a personal experience and can be tackled at the player’s own speed. Thirdly, serious games provide the ability to capture data autonomously. For games that implement choices, data can be captured on the choices selected or the hesitation time before deciding.

Using a serious game to educate people on romance fraud can provide a level of interaction to allow for retention of the signs of romance fraud. Furthermore, the game nature appeals to a wider audience and can be used as a tool by police to educate or set up at events to teach demographics of people that may not be receptive to other methods of teaching.

# Chapter 2 Literature Review

This chapter will review existing literature and provide background knowledge to contextualise the research presented in this report. Cyber-scams in general will first be discussed, leading into a detailed review of romance scam literature. After that, the need for education and VR for education will be discussed. Finally, the problem and solution of this project will be presented.

## Cyber-Scams

Popularity of cyber-scams, advance fee frauds (leads into romance scam)

Scammers across the world are exploiting the growth in Internet usage to great success. The Australian Competition and Consumer Commission (2020) stated that, in Australia, annual fraud losses rose from $69.9 million in 2009 to almost $143 million in 2019. In Spain, fraudulent bank transactions rose 150% from 2012 to 2016, with remote fraud being the main cause (Kemp, Miró-Llinares, and Moneva, 2020). This matches other European countries; the UK saw an increase of 700,000 remote card fraud per year and the European Central Bank also saw increases in remote card fraud.

One of the most well-known types of fraud is advance fee fraud, also known as the “Nigerian Money Scam” or the 419 fraud, from the section of Nigerian penal code it falls under (Rosen, 2004). Advance fee fraud works by tempting victims to part with small amounts of money in the hope of receiving a large payout.

A popular example of this is an email from the relative of a deceased senior government official, who has a large amount of money held in a foreign bank account. In order to retrieve the money, the relative asks the victim for assistance. In return for helping the relative out, the victim will be offered a percentage of the money held in the account. If the victim agrees to help, they will be asked to provide a small advance fee to pay for banking fees and currency exchange. If the victim complies and provides money, they become invested into the scam and it becomes harder to withdraw (Wall, 2007).

Romance scams, like advance fee frauds, are scams that focus on individual communication. Whilst advance fee frauds target individuals looking to get rich with little effort, romance scams instead target lonely individuals looking for love.

## Romance Scams

What is a romance scam, effect on victim, popularity of them, awareness of them (leads into education)

“Romance scams involve people being duped into sending money to criminals who go to great lengths to gain their trust and convince them that they are in a genuine relationship. They use language to manipulate, persuade and exploit so that requests for money do not raise alarm bells. These requests might be highly emotive, such as criminals claiming they need money for emergency medical care, or to pay for transport costs to visit the victim if they are overseas. Scammers will often build a relationship with their victims over time.” (Action Fraud, no date)

Romance scams consist of multiple stages. Firstly, the scammer creates a fake profile on a dating website, often using images of attractive individuals. They then proceed to target individuals who they believe to be vulnerable.

If the individual replies, the scammer grows the relationship with the victim, moving the conversation from the dating site into emails and instant messaging. This prevents the dating site from identifying the scammer and alerting the victim. When the scammer feels that the relationship has progressed far enough, they test the waters by asking the victim to send a small amount of money.

Once the victim is shown to be willing to send money to the scammer, the scammer proceeds to raise the amount asked for. The most common method is through a crisis where the victim is given a time limit in which to comply. These scenarios range from a medical problem to luggage being held up when trying to visit the victim, to helping rebuy items after a robbery as the items are not available in the scammer's country.

If the victim complied with this crisis, new crises would be invented to further scam the victim out of more money. Eventually, the victim either runs out of money or is aware that they have been scammed. (Whitty, 2013)

Victims are typically middle aged (35-54 years), which could be because they have more disposable income to treat their partners or that they frequent dating sites more than younger or older age groups. Common traits that victims shared were impulsivity and lack of self-control. This explains why victims send money for urgent crisis. Other traits include sensation seeking and addiction, which suggests that victims more easily believe the tales of the scammer and carry on trusting the scammer after it's discovered to be a scam. (Whitty, 2018)

Whilst romance scam victims can lose significant amount of money, the financial damage can be less painful than the emotional distress. After realising that their lover is fictional and created by a scammer, some victims felt like the death of someone close. Furthermore, the loss of the relationship was more upsetting than the loss of money. As a result of this, victims would feel unmotivated to report the crime to law enforcement, and in some cases, fall for a second wave of scamming, believing that the scammer did grow feelings for the victim. (Buchanan and Whitty, 2014)

According to Buil-Gil and Zeng (Figure 2, 2021), reports of romance scams in the UK have been consistently rising since 2014. During the COVID-19 lockdown, romance scam reports sharply rose as people stayed at home and used the Internet more.

Despite the rise in reports, the awareness of British people towards romance scams is around 50%. Surveys performed by Whitty and Buchanan (2012) show that while 51.66% of British people had heard about romance scams, most of this knowledge was from the television and a newspaper, and that less than 3% of British people had lost money or knew someone personally who had lost money to an online romance scammer.

Therefore, there is still a need to educate the public on romance scams.

A graph with numbers and lines

Description automatically generated

Figure Romance fraud and 95% prediction intervals

## Education

Examples of how Romance Scams have been talked about to raise awareness. Public campaigns, text in dating apps, interactive awareness (leads into serious games)

Three types of awareness towards romance scams were researched for this project: in-app information, third party information and interactive information.

In 2013, the Online Dating Association (ODA) was formed. The ODA is a trade association formed by many of the largest online dating providers that works to “encourage an online dating sector that is working on behalf of consumers, creating a safe, trustworthy, and positive dating experience, while working on innovative solutions to challenges” (ODA, nd).

In 2017, the ODA created a framework for user safety. Alongside sections pertaining to “User advice & guidance”, and “Addressing user safety”, there is a section for “Managing the risk of fraud”. This section details what dating platforms part of the ODA (services) should do to minimise the impact of fraud on users. This includes providing easy to find and user-friendly advice and guidance on how users can minimise the risk of fraud, alerting other users that have been in close contact with the fraudster and advising the victim to inform law enforcement agencies and other support agents that can help the victim further.

An example of this in action is Tinder’s Safety Center, established in 2020. The Safety Center provides resources and tools for users to be aware of fraudsters and other harmful activity.

The ODA also provides safe dating awareness outside of their services. The Date Safe campaign provides a list of tips to avoid becoming a victim of a romance scam (Figure 3).

A poster of a social media campaign

Description automatically generated

Figure Date Safe Infographic (ODA, nd)

Another form of raising awareness is through public campaigns. Action Fraud carry out several campaigns across social media aiming to inform the public on the dangers of romance scams (Figure 4). The campaigns often contain information on what romance scams are, how to protect yourself or friends and family from romance scams, and who to contact if you suspect you, or someone you know, is a victim of a romance scam. Some also contain case studies of individuals affected by romance scams and statements from the police and dating site operators.

A screenshot of a phone

Description automatically generated

Figure A Romance Scam Campaign poster from Action Fraud

Searching for interactive romance scam awareness returned little results. A prototype platform-based game named “Broken Hearts” was discovered (Bilz, Shepherd, Johnson, 2023), however it is a piece of exploratory work and is not complete. Therefore, the wider scene of serious games will be looked at.

## Serious Games

What is a serious game, examples of serious games, not many for VR (lead into VR)

Serious games are a subsection of games that, according to Chen and Michael (2005), "do not have entertainment, enjoyment, or fun as their primary purpose. That isn’t to say that the games under the serious games umbrella aren’t entertaining, enjoyable, or fun. It’s just that there is another purpose, an ulterior motive in a very real sense." This type of game aims to educate the player through interaction. Serious games are used by the military, educators, non-government organisations and artists to teach, pass on skills or preach messages.

Gamification techniques are often used to make topics interactive as a serious game. Marczewski’s “52 Gamification Mechanics and Elements” (2018) details many of the elements used in making a serious game. These elements are sorted into 8 sections and can be found as Figure 4. The General section includes elements such as adding a narrative, visible progression and consequences. Reward Schedules include elements that provide events and rewards on a schedule or at random. Socialiser consists of elements that allow for multiple users to connect with each other, forming teams or competing. The Free Spirit section describes elements that present free choice through exploration and branching choices. Challenges, quests and boss battles fall under Achiever, while trading, caretaking and purpose are part of the Philanthropist section. Disruptor contains elements such as anarchy, voting and innovation and finally, the Player section has elements like experience points, leaderboards and achievements.

Whilst not all of these elements are relevant to the project, several will be used and discussed when relevant in the Methodology.

A table of gamification elements

Description automatically generated

Figure Periodic Table of Gamification Elements (Marczewski, 2018)

As limited results were found when searching for serious games about romance scams, serious games about cyber-security in general were looked at. One of these is NoPhish, a mobile application designed to educate people in checking URLs (Canova, Volkamer, Bergmann and Borza, 2015a).

NoPhish begins with an interactive demo where the user can send a spam email to themselves. This shows how easy it is to create a fake email with a link that can be redirected to a malicious site. After educating the user on viewing the URL of a website on their phone browser, the game begins.

The game is split into 10 levels, with each level introducing new information about URL spoofing. These range from unrelated domains to brands in the subdomain and typos of the real website. The game is designed with gamification techniques in mind, like introducing a life system and points.

NoPhish reported the results of 19 participants from a lab study (Canova, Volkamer, Bergmann and Borza, 2015b). Before playing NoPhish, most participants correctly identified between 50-64% of the 16 websites provided. After playing NoPhish, 15 out of the 19 participants correctly identified over 90% of the 24 websites. Overall, all participants performed better after playing NoPhish, showing that the game worked in the immediate short term.

A retention study was also conducted five months later to determine if the participants had retained the information from the game. Whilst most participants performed worse than immediately after playing the game, 18 out of the 19 participants performed better than before playing the game, showing that they had retained knowledge about URL spoofing. Furthermore, participant confidence in detecting fake URLs increased both after immediately playing the game and five months later. This shows that serious games can also be used to raise confidence in a topic alongside teaching about a topic.

## VR For Education

VR used in education. Types of VR used (leads into PCVR)

This project aims to use VR as the platform for the game. Checa and Bustillo (2020) performed a review of immersive VR serious games. They found 171 education-based papers and 235 training based papers, which was then filtered down to 68 for each. These findings show that there is space and demand for not just a VR based romance scam serious game, but more VR based cybersecurity serious games.

Checa and Bustillo also categorised the papers into their target audience and typology. They found that out of the games for education, 22% of them are focused on the general public. The typology that most closely correlates to the project is the interactive experience, where the user can interact with the environment, but not freely move through it. Roughly 50% of the education based serious games fell under this typology, the most popular choice.

Finally, the most common conclusion from the papers was that user satisfaction was higher in VR than with other methods. This bodes well for the project, as it aims to be a general public focused interactive experience.

An example of using VR for cybersecurity education is the Cyberinfrastructure Security Education for Professionals and Students (CiSE-ProS) virtual reality environment (Seo, et al., 2019). This research project created an immersive environment where students are taught how to inspect a data center and replace faulty hardware.

After 5 minutes using CiSE-ProS, the experiences of 25 students were very positive. 90% of students retained the knowledge from the exercise immediately afterwards, which then dropped down to 80% after one week. Written responses included praise towards the immersion of the VR environment, and how being able to physically interact made it easier to remember information.

While not fully relevant to this project, CiSE-ProS uses the Unity game engine along with SteamVR for easy VR integration. This combination was praised for it’s ease of use and speed in setting up the VR environment. This bodes well for the project in this report, as Unity with SteamVR will also be used.

Romance scams are a form of cyber scams and can lead to heavy psychological damage alongside the financial impact. While there are awareness campaigns and information shown in dating apps, there is a lack of interactive learning experiences. Therefore, this project aims to create a VR game that will educate users on romance scams.

# Chapter 3 Methodology

Present problem, how will it be tackled and how it was tackled

The aim of this project is to investigate romance scams and provide a game that will raise awareness and educate the public on romance scams. Using the information presented in the previous chapter, the game can be created to accurately depict a romance scam scenario. The game will be created using Unity and SteamVR, as they allow for the game to be widely available, from home use to exhibition booths at public events.

## Platform

Brief explanation of Unity and SteamVR, wide adoption for PC allowing for easy distribution of the game.

Unity is a 3D and 2D game engine that supports a wide variety of platforms including VR. Another game engine that is popular is the Unreal engine. This also supports 3D, 2D and a wide range of platforms including VR. Unity was selected for this project because of its ease of use for quickly creating prototype games.

Whilst Unity has native support for VR, SteamVR will be used as the VR runtime. SteamVR is a tool that allows Unity and other game engines to interface to a connected VR headset. SteamVR supports a plethora of VR headsets, abstracting the controller inputs to the tool layer. This allows for many different types of headsets to play the project, expanding the target audience.

## Design

## Player and SteamVR

## Mechanics and World

## Plot

## Integrating the Plot

# Chapter 4 Results

# Chapter 5 Discussion

Just my work and interpretation and then the work of others

Medium of VR is more restrictive compared to other mediums!!

# Chapter 6 Conclusion and Future Work

# List of References

<https://www.onlinedatingassociation.org.uk/>

<https://www.onlinedatingassociation.org.uk/membership/standards-guidance/putting-safety-first-support-tools/framework-for-user-safety.html>

<https://www.tinderpressroom.com/tinder-introduces-safety-updates>

<https://www.actionfraud.police.uk/a-z-of-fraud/dating-fraud>

<https://www.actionfraud.police.uk/news/swipe-left-to-romance-fraud-family-members-of-online-daters-urged-to-help-protect-their-relatives>

Bilz, A, Shepherd, LA & Johnson, GI, *Broken hearts*, 2023, Software. <https://lynsay.itch.io/broken-hearts>

# Bibliography

If required

# Appendices