|  |
| --- |
| 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](#_Toc140066329)

[Table of Tables iii](#_Toc140066330)

[Acknowledgements iv](#_Toc140066331)

[Abstract v](#_Toc140066332)

[Abbreviations, Symbols and Notation vi](#_Toc140066333)

[Chapter 1 Introduction 1](#_Toc140066334)

[Chapter 2 Literature Review 2](#_Toc140066335)

[Cyber-Scams 2](#_Toc140066336)

[Romance Scams 3](#_Toc140066337)

[Education 4](#_Toc140066338)

[Serious Games 4](#_Toc140066339)

[VR For Education 5](#_Toc140066340)

[Unity and SteamVR 5](#_Toc140066341)

[Chapter 3 Methodology 6](#_Toc140066342)

[Chapter 4 Results 7](#_Toc140066343)

[Chapter 5 Discussion 8](#_Toc140066344)

[Chapter 6 Conclusion and Future Work 9](#_Toc140066345)

[List of References 10](#_Toc140066346)

[Bibliography 11](#_Toc140066347)

[Appendices 12](#_Toc140066348)

# 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.

Anticipated Results

Users will learn that romance scams are not like short term phishing scams, but instead they are a long-term con that leaves its victims suffering from financial and psychological damage. The game can then be used to promote awareness in police campaigns and public events.

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

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.

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.

A graph with a line

Description automatically generated

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

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

What is a cyber scam, popularity of them, 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.

The techniques that scammers use to extract card information have evolved to include real world events. During the COVID-19 pandemic, scammers posed as the World Health Organisation, the UK’s National Health Service, and other companies in phishing attacks. These phishing attacks used email, SMS or Whatsapp to send URLs to fake government websites where victims enter their banking details to receive benefits (Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple, Bellekens, 2021).

Another aspect of life that can be targeted is an individual’s romantic life. Romance scams target individuals looking for love on dating services.

## Romance Scams

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

According to Whitty (2013), romance scams are a multi-staged model. Firstly, the scammer creates a fake profile on a dating website, 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 to avoid detection from the site. 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. Here, 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.

Romance scam victims suffer on two fronts. Firstly, they can lose significant amounts of money but secondly, they suffer emotional distress. Realising that their lover is fictional and created by a scammer felt like the death of someone close to them. For some victims, 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." Serious games are games that aim 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. There have been several serious games designed to raise awareness of cyber-security practices.

One of these is NoPhish, a mobile application designed to educate people in checking URLs (Canova, Volkamer, Bergmann and Borza, 2015). NoPhish uses lives and points to gamify the knowledge of common phishing techniques. These techniques are taught over a series of levels, where the player must reach a certain score to advance to the next level.

After participants played NoPhish, their ability to identify phishing links consistently improved, showing the benefit of serious games. Furthermore, their confidence in identifying phishing links was significantly higher. This shows that serious games are effective in teaching users cyber-security awareness.

This project aims to use virtual reality (VR) as the platform for the game. Checa and Bustillo (2020) performed a review of immersive VR serious games. They found that there is a balance between serious games for education and training. Out of the games for education, 22% are focused on the general public. The games for education are mostly interactive experiences at roughly 50%, whilst passive experiences account for 30%.

Therefore, there is space for a public focused interactive VR serious game.

## VR For Education

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

## Unity and SteamVR

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

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. As discussed, using Unity and SteamVR will allow for the game to be widely available, from home use to exhibition booths at public events.

# 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.

## 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