

A dissertation submitted to the **University of Greenwich**
in partial fulfilment of the requirements for the Degree of

Master of Science

in

Computer Forensics and Cyber Security

Assessing User's Susceptibility and Awareness of Cybersecurity Threats

Name: Selvaguru Sethuraman

Student ID: 001201478

Supervisor: prof. Naghmeh Moradpoor

Submission Date: 17 January 2023

Word count: 11,529

Assessing User's Susceptibility and Awareness of Cybersecurity Threats

Selvaguru Sethuraman

Computing & Mathematical Sciences, University of Greenwich, 30 Park Row, Greenwich,
UK.

(Submitted 17 January 2023)

ABSTRACT:

In today's digital age, cybersecurity threats are a major concern for individuals and organizations alike. Understanding user susceptibility to these threats and their awareness of how to protect themselves is crucial for mitigating risk. This project aims to assess user susceptibility and awareness of cybersecurity threats through a combination of real time surveys and experiments. By analysing the results, we hope to identify areas where users are most at risk and develop strategies for increasing awareness and improving cybersecurity practices. The findings from this project will be useful for individuals and organizations looking to safeguard against cybersecurity threats and protect sensitive data. By understanding user susceptibility and awareness of cybersecurity threats, we can work towards protecting sensitive data and safeguarding against potential attacks. And also investigate the user's understanding of security measures and their willingness to take preventive action. The results of this study will provide insight into the users' attitudes towards cybersecurity and will be useful for developing effective security education and awareness programs. This project is going to test users with real time cyber awareness model which is configured with google analytics to track every individual user activity and to give cyber awareness training based on their levels.

Keywords: cyber awareness, awareness training, Google Analytics, user tracking, user cyber analysis.

PREFACE

The increasing reliance on technology in our daily lives has led to a growing concern about the security of personal and sensitive information. Cybersecurity threats, such as hacking, phishing, and malware, have become more prevalent and sophisticated, putting individuals and organizations at risk of data breaches and financial loss. It is essential to understand the susceptibility and awareness of users towards these threats to develop effective strategies for protecting against them.

This project aims to assess the susceptibility and awareness of users towards cybersecurity threats. The Project will include a comprehensive analysis of the current state of cybersecurity awareness and susceptibility among a various group of individuals. Additionally, the project will investigate the effectiveness of different strategies for raising awareness and reducing susceptibility to cybersecurity threats. The findings of this research will be valuable for individuals, organizations, and policymakers in developing effective strategies for protecting against cybersecurity threats.

ACKNOWLEDGEMENTS:

I would especially like to thank prof. Naghmeh Moradpoor for agreeing to be my supervisor and for his consistent advice, feedback, guidance, and support throughout the lifecycle of this MSc Assessing User's Susceptibility and Awareness of Cybersecurity Threats project.

I want to thank both prof. Naghmeh Moradpoor and prof. Dwijen Shilu for agreeing to have the project demonstration on the schedule day.

List of Contents

ABSTRACT:.....	i
PREFACE	ii
ACKNOWLEDGEMENTS:.....	ii
List of Figures:	v
List of Table:	vi
List of Acronyms:.....	vi
1.Introduction:	1
Overview:	1
Road Map of report:	2
2.Literature Review:.....	3
Overview	3
Summary	7
3.Analysis of the system:	8
Legal, Social, Ethical and Professional issues:.....	8
4.Planning to design the cyber awareness model:	10
5.Implementing the design and idea of cyber awareness model:.....	11
Unsafe browser extension install:.....	12
Phishing page asking for Gmail username and password:	13
Accessing Camera and Mic without user knowledge:	14
Sensitive Information asked by chatbot:	15
Malicious link clicks:.....	16
Reverse shell install:.....	17
User intension to pay to untrusted source:	18
Uploading personal profiles to untrusted source:.....	19
6.Cyber awareness model Working:	20
Data Layer:	20
Google Tag Manager:.....	20
Google Analytics:	21
Data Transfer form website to Google Tag manger:	22
Data Layer Push JavaScript Sample Code:	22
How Data Received by Google tag manager:	23
Data Transfer form Google Tag manger to Google Analytic:.....	24
Google Tag Manager Variable:.....	24
Google Tag manager Tags:.....	24
Google tag manager Trigger.	24

How data send to Google analytics:	25
7.Realtime Deploy for user evaluation:	28
System Configuration:.....	28
8.Steps to Third Person Redeploy this cyber awareness Model:.....	33
Steps to get measurement ID in google analytics:	34
9.Why Google Analytics is used over dedicated cyber threats protection software:	36
10.Product Testing before deploying:	36
web unit testing:	37
Web integration testing:.....	37
web End-to-end tests:.....	38
11.Perform Result Analysis:	40
Realtime Report:	41
Google analytics Acquisition:	42
Google analytics engagement:.....	43
Google analytics Demographic details: Country:.....	44
Google analytics-Tech:	45
Google analytics user exploration:	46
12.User Evaluation:	47
Analysing some user's evaluation report:.....	48
13.conclusion.	51
References:	52
Appendix:	54

List of Figures:

Figure 1: Index Page	11
Figure 2: Browser extension	12
Figure 3: Gmail Login	13
Figure 4: Gmail password field.....	13
Figure 5: mic and camera permission	14
Figure 6: chatbot	15
Figure 7: Offers.....	16
Figure 8: Auto download	17
Figure 9: Deals.....	18
Figure 10: Photo upload.....	19
Figure 11: Working Flow.....	20
Figure 12: DataPush code	22
Figure 13: GTM Variable	23
Figure 14: GTM Variable	23
Figure 15: ID refer	25
Figure 16: config Trigger.....	26
Figure 17: config Tag.....	27
Figure 18: GTM setup.....	28
Figure 19 : GTM script to code.....	29
Figure 20: GTM preview	29
Figure 21: Tag firing	30
Figure 22: GTM configuration.....	31
Figure 23 : GA Realtime.....	31
Figure 24: GTM setup.....	33
Figure 25: GTM admin view	33
Figure 26: GA Measurement ID	34
Figure 27: GA Measurement ID	35
Figure 28: GA Realtime Report.....	41
Figure 29 : GA acquisition.....	42
Figure 30: GA events	43
Figure 31: GA events	44
Figure 32: Country view	44
Figure 33: country View	45
Figure 34: Tech details.....	45
Figure 35: user explorer	46
Figure 36: All user details.....	46
Figure 37: All users Details	47
Figure 38: user activity	48
Figure 39: 2nd user Activity	49

List of Table:

Table 1: Trigger vs Tag.....	25
Table 2: GTM vs GA	32

List of Acronyms:

GTM – Google Tag Manager,

GA – Google Analytics .

1.Introduction:

Overview:

In today's digital age, cybersecurity threats have become a major concern for organizations of all sizes. With the increasing use of technology in business operations, the risk of data breaches, cyber-attacks, and other cybercrime activities has risen exponentially. As a result, assessing the susceptibility and awareness of users to cybersecurity threats has become a critical task for organizations.

When assessing a user's susceptibility and awareness of cybersecurity threats, it is important to consider a variety of factors. These factors include the user's understanding of the importance of cybersecurity, the extent to which the user is taking steps to protect their devices, and their ability to recognize potential threats. A major step in assessing a user's susceptibility to cybersecurity threats is to understand their knowledge of basic security principles. This includes understanding the importance of strong passwords, two-factor authentication, and other measures such as using up-to-date antivirus software. It is also important to understand if the user knows how to recognize phishing scams, malicious downloads, and other potential threats. In addition to understanding their knowledge of security principles, it is also important to assess the user's behaviour. Are they taking proactive steps to protect their devices, such as keeping their software up-to-date and avoiding suspicious websites and downloads? It is also important to understand if the user is familiar with the security settings of their devices and if they are taking advantage of them. By assessing the susceptibility and awareness of users, organizations can improve their cybersecurity posture and protect their assets and sensitive information from cybercriminals.

The main goal of this project is to assess the user's cyber awareness about real world cyber threats and based on the evaluation result of individual user, cyber awareness training is given to them. Let's how it is achieved.

Road Map of report:

- Planning to design the cyber awareness model.

In this phase planning is made to design cyber awareness model.

- Implementing the design and idea of cyber awareness model.

Cyber Threats modules that are implemented in this project are explained.

- Unsafe browser extension installs,
- Phishing page asking for Gmail username and password,
- Accessing Camera and Mic without user knowledge,
- Sensitive Information asked by chatbot by user manipulation questions,
- Malicious link clicks,
- Reverse shell install, user intension to pay to untrusted source,
- Uploading personal profiles to untrusted source.

- Cyber awareness model Working.

Core working of this project is explained here.

- Realtime Deploy for user evaluation.

Cyber awareness model is deployed for user evaluation and step of deployment.

- Steps to Third Person Redeploy this cyber awareness Model.
- Product Testing before deploying.

In this phase this cyber awareness model is tested.

- Perform Result Analysis.

Will see how to analysis the Google Analytics Reports.

- User Evaluation

In this phase evaluating some user with their results gets for Analytics.

2.Literature Review:

Overview

Cybersecurity threats are an ever-growing concern for individuals and organizations. With the growth of digital connected devices, the potential for malicious actors to exploit these devices and their user's data has become a major concern. As such, it is important to assess the susceptibility and awareness of users to cybersecurity threats. This literature review will focus on research that has been conducted in order to assess the susceptibility and awareness of users to cybersecurity threats.

One study conducted by Kankanhalli, and Tan (2018) examined the susceptibility of users to phishing threats. The study utilized a survey to assess the risk perception and behaviour of users when it comes to phishing attacks. The results of the study indicated that the majority of users were not aware of the risks posed by phishing attacks and had not taken any steps to protect themselves from this type of threat. The results also showed that users were more likely to respond to phishing emails if they were perceived as being from a trusted source.

A study by Arachchilage. (2014) examined users' susceptibility and awareness of cyber threats. The study surveyed 632 participants to assess their attitudes and behaviours related to various online activities such as, online banking, online shopping, and social networking. The survey results indicated that the majority of users were aware of the risks associated with online activities, but they were not necessarily taking steps to protect themselves. Additionally, the survey showed that users were more likely to engage in risky behaviour when they had less knowledge about the associated risks.

A different study by Ikhaila. (2017) utilized a survey and experiment to evaluate users' susceptibility and awareness of phishing threats. The survey results showed that users who had higher levels of technical knowledge about phishing were more likely to have a better understanding of the risk associated with phishing emails. The experiment also showed that users who had higher levels of technical knowledge about phishing were less likely to click on a malicious links. A study by Tewari, A, (2016) investigated the effect of user characteristics on the risk of being exposed to cyber threats. They found that younger users were more likely to be exposed to threats due to their lack of experience and knowledge. In addition, they found that users who had a higher level of technical knowledge and experience were more likely to be aware of potential threats and take steps to protect themselves. A study by Dhamija. (2006) examined users' awareness of cybersecurity threats and the strategies they employed to protect themselves. The study found that users had a limited understanding of cybersecurity threats

and the measures they could take to protect themselves. Specifically, users primarily relied on antivirus software and password protection for security. Furthermore, the study found that users were more likely to be aware of threats when they had experienced a security breach or had received security training.

The research in this area has focused on user susceptibility to cyber threats. Studies have shown that users are often unaware of the risks they face when they engage in online activities. For example, a study by Banday. (2007) found that users were more likely to click on malicious links if they were presented with a familiar website that contained the malicious content. This suggests that users may be unaware of the risks associated with certain online activities and may be more likely to take risks if they are presented with a familiar environment.

This study is by Kirda. (2005) examined the susceptibility of users to phishing attacks and their ability to distinguish between legitimate and malicious websites. The results showed that users were more likely to click on malicious links when presented with a range of different stimuli. The study also found that users were more likely to click on a malicious link when they were presented with a reward associated with the link, such as a free download. A study by Marriott, C. (2018) looked at how user characteristics can affect their susceptibility to phishing scams. The study found that users with lower levels of education, those who had previously experienced a cyberattack, and those who had previously received phishing emails were more likely to click on malicious links. The authors also found that users who had experienced cyberattacks in the past were more likely to recognize phishing emails. In a study by Athulya. (2020), the authors investigated the effectiveness of cybersecurity awareness campaigns in reducing user susceptibility to phishing attacks. The study found that users who received awareness training were significantly less likely to click on malicious links and were more likely to recognize phishing emails. The authors suggest that these findings demonstrate the importance of providing users with regular cybersecurity training and awareness campaigns.

One approach to assessing user susceptibility and awareness is through surveys. Several studies have used surveys to measure user's knowledge and understanding of cybersecurity threats, their attitudes towards security, and their self-reported security practices. For example, a survey conducted by Aleroud. (2017) found that users had a low level of awareness of the security threats posed by malware, phishing, and social engineering. Similarly, a survey conducted by Jun et al. (2016) revealed that users had a limited understanding of the security risks associated with online activities such as email, file sharing, and social media.

One of the first studies to examine user awareness of cybersecurity threats was conducted by Alsufyani. (2018). The authors surveyed staff members of an organization in Saudi Arabia and found that, despite the high use of technology, the majority of participants had inadequate cybersecurity awareness. The study suggested that the organization should develop strategies to increase the security awareness of its users.

One way to assess user susceptibility is using phishing simulations (Wang et al., 2018). These simulations provide a realistic scenario for users to identify and respond to potential phishing attempts, allowing organizations to evaluate their susceptibility to these types of attacks (Wang et al., 2018). Another approach is to assess user susceptibility through their browsing behavior, as certain patterns of behaviour may indicate a higher risk of falling victim to a cyberattack (Kshetri, 2018).

Assessing user awareness of cybersecurity threats can also be done through the use of surveys and questionnaires (Kshetri, 2018). These methods allow organizations to evaluate the level of knowledge and understanding of users regarding potential threats and identify areas where additional education and training is needed (Kshetri, 2018). Additionally, conducting regular security awareness training and drills can help increase user awareness and improve their ability to identify and respond to potential threats (Wang et al., 2018).

While assessing user susceptibility and awareness of cybersecurity threats is important, it is not the only step organizations should take to protect against potential attacks (Kshetri, 2018). Implementing security measures such as firewalls, antivirus software, and intrusion detection systems can also provide an added layer of protection (Kshetri, 2018). Additionally, organizations should have incident response plans in place to quickly respond to potential threats and minimize the impact of an attack (Wang et al., 2018).

One of the key factors that has been found to influence user susceptibility to cybersecurity threats is their level of awareness. Studies have shown that users who are more aware of the potential risks and threats associated with cybersecurity are less likely to fall victim to cyber attacks (Alhabash et al., 2018; Wang et al., 2018). This is likely due to the fact that users who are more aware of the risks are more likely to take precautions, such as using strong passwords and avoiding suspicious links or emails.

Another key factor that has been found to influence user susceptibility to cybersecurity threats is their level of technical expertise. Studies have shown that users who are more technically proficient are less likely to fall victim to cyber-attacks (Kotzé & Zinn, 2016; Wang et al., 2018). This is likely due to the fact that users who are more technically proficient are better able to understand and navigate the technical aspects of cybersecurity, such as software updates and security settings.

In addition to these factors, research has also shown that users' susceptibility to cybersecurity threats can be influenced by several other factors, such as their gender, age, and socio-economic status (Alhabash et al., 2018; Kotzé & Zinn, 2016). For example, studies have found that women tend to be more susceptible to cyber-attacks than men (Alhabash et al., 2018; Kotzé & Zinn, 2016), and that older adults tend to be more susceptible than younger adults (Kotzé & Zinn, 2016).

Study conducted by Kotzé (2016) examined the level of cybersecurity awareness among university students in South Korea. The study found that the students had a relatively low level of knowledge of cyber threats, as well as a low perceived risk of being affected by a cyber attack. The study also noted that students had limited understanding of the appropriate cybersecurity measures that should be taken to protect their data and systems.

Assessing user susceptibility and awareness of cybersecurity threats is crucial for organizations to understand the risks they face and develop strategies to mitigate them. While there are various methods for assessing these factors, the use of phishing simulations, browsing behaviour analysis, surveys and questionnaires, regular security awareness training and drills, and incident response plans are some of the most effective.

More recent research has begun to focus on the use of more sophisticated methods to assess user's susceptibility and awareness of cybersecurity threats. This includes the use of game-based approaches, such as the use of computer simulations, as well as the use of more advanced data analytics to analyse user behaviour. These methods have been shown to be more effective than traditional assessment methods in providing a more accurate assessment of user. Some studies suggest that certain demographic groups may be more aware of cyber threats, such as older individuals, more educated individuals, and those with a higher level of technical skill.

Users may have a low level of awareness about cybersecurity threats and may not fully understand the risks associated with their online behaviour. This can make them more susceptible to attacks. There is a need for more education and training to help users become more aware of cybersecurity threats and how to protect themselves. Factors such as age, gender, technical expertise, and attitudes towards security can influence users' susceptibility to cybersecurity threats. Research has identified a number of approaches that can be effective in increasing users' awareness and knowledge about cybersecurity threats, including the use of gamification and other interactive methods. There is a need for more research to understand how to effectively assess and measure users' susceptibility and awareness of cybersecurity threats.

Summary

Overall, the literature suggests that users may not have a sufficient level of awareness about cybersecurity threats and may not take the necessary precautions to protect themselves online. To address this issue, there is a need for more education and training, as well as research to understand how to effectively assess and measure users' susceptibility and awareness.

3. Analysis of the system:

Legal, Social, Ethical and Professional issues:

This project model Assessing user's susceptibility and awareness of cybersecurity threats can raise several legal and social issues

Privacy concerns: One of the primary legal and social issues raised by assessing user's susceptibility and awareness of cybersecurity threats is privacy. Many users may be unsure to share personal information or allow others to access their devices or networks because of concerns about privacy.

Discrimination: Assessing users' susceptibility and awareness of cybersecurity threats may also raise concerns about discrimination. For example, if certain groups of users are found to be more susceptible to cyber threats, they may be unfairly targeted for additional security measures or be denied certain services.

Bias: The methods used to assess users' susceptibility and awareness of cybersecurity threats may be biased. For example, if an assessment is based on the type of device or software a user has, users with older or less expensive devices may be disproportionately identified as more susceptible to cyber threats.

Inconvenience: Assessing users' susceptibility and awareness of cybersecurity threats may also create inconvenience for users, especially if it involves lengthy questionnaires or other time-consuming activities. This could lead to low participation rate and negatively impact the effectiveness of the assessment.

False-positive: Another social and legal issue with assessment methodologies is, the possibility of getting false-positive results, this may lead to wrong classification of users and can have legal implications.

Legal compliance: Organizations/individual who going to use this model may need to ensure compliance with data protection laws and regulations when assessing users' susceptibility and awareness of cybersecurity threats.

User trust - Organizations/individual who going to use this model must ensure that users trust the assessment process and that the data collected is used responsibly and securely.

Accessibility of resources - Organizations/individual who going to use this model must ensure that the resources used to assess user susceptibility and awareness of cybersecurity threats are accessible and understandable to all users.

The potential for increased surveillance of users' activities by Organizations/individual conducting cybersecurity assessments with this model.

Ethical concerns around assessing the susceptibility and awareness of cybersecurity threats. Since this process may be done for the purpose of identifying and mitigating security vulnerabilities, it can potentially lead to profiling or discrimination of certain individuals or groups if not done in an unbiased and fair manner.

4.Planning to design the cyber awareness model:

List of requirements is needed to achieve this project.

- Most common cyber threats must identify based on research.
- Find perfect way to integrate those cyber threats with Realtime scenario.
- Find platform to Tracking each and every individual user's activity, their behaviour, and how they react to cyber threats.

For achieving first point in the requirement - Identifying the common cyber threats: This step would involve researching and identifying the most common types of cyber threats, such as phishing, malware, and social engineering attacks and noted to integrate in model.

For achieving second point in the requirement - Website Simulation: One of the ways to integrate cybersecurity threats into a website is to create a website simulation that imitate a real-life cyber threat. Users can be directed to a simulated website that looks similar to the real website. The simulation can test users' ability to identify and avoid cyber threat attempts.

In this project Realtime user evaluation is achieved with website simulation for that google analytic is suggested for tracking user activity. Basically, Google analytics is used for SEO's and digital marketing but here in this project with different way of creativity google analytic is used to achieve this project goal. Let's see about in detail below.

5.Implementing the design and idea of cyber awareness model:

Gathered cyber threats, some common and some uncommon but still in Real-world cyber threats like unsafe browser extension install, phishing page asking for Gmail username and password, Accessing Camera and Mic without user knowledge, Sensitive Information asked by chatbot by user manipulation questions, malicious link clicks, reverse shell install, user intension to pay to untrusted source, uploading personal profiles to untrusted source. This are cyber threats going to deploy in website simulations.

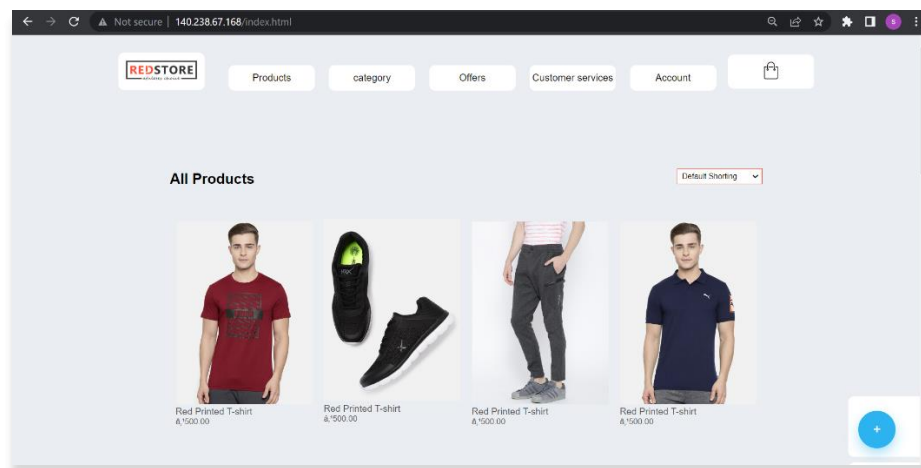


Figure 1: Index Page

The Fig 1 is the index page of the simulated website with the theme of online shopping which makes look real to user. This website is developed with HTML, CSS, and JavaScript.

Cyber Threats modules:

- Unsafe browser extension install,
- Phishing page asking for Gmail username and password,
- Accessing Camera and Mic without user knowledge,
- Sensitive Information asked by chatbot by user manipulation questions,
- Malicious link clicks,
- Reverse shell install, user intension to pay to untrusted source,
- Uploading personal profiles to untrusted source.

Unsafe browser extension install:

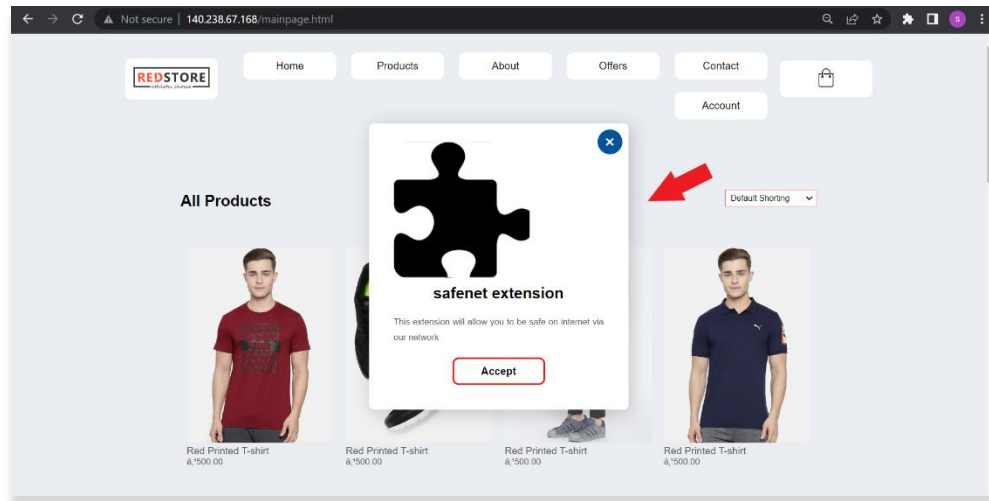


Figure 2: Browser extension

The Fig 2 show that this simulated website makes Popup window asking for extension to install with a description “This extension will allow you to be safe on internet via our network”. This case makes user to either accept or reject the installation of browser extension.

Code used: HTML, CSS, and JavaScript.

Impact of accepting Unsafe browser extensions:

Unsafe browser extensions can have a variety of negative impacts. They can allow malicious actors to gain access to a user's personal information, such as passwords and banking information, as well as inject malicious code or tracking scripts into webpages. They can also be used to hijack a user's browsing session or redirect them to malicious websites. Unsafe browser extensions can also be used to deliver malware, monitor a user's activity, or even steal their credentials. It is important to only install trusted browser extensions to ensure the safety of your personal information and browsing experience.

Phishing page asking for Gmail username and password:

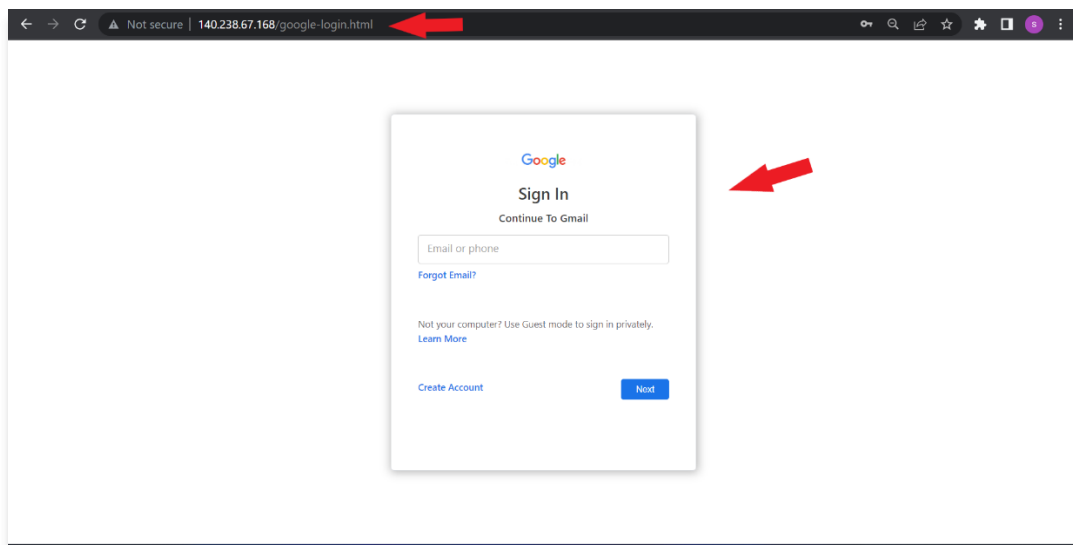


Figure 3: Gmail Login

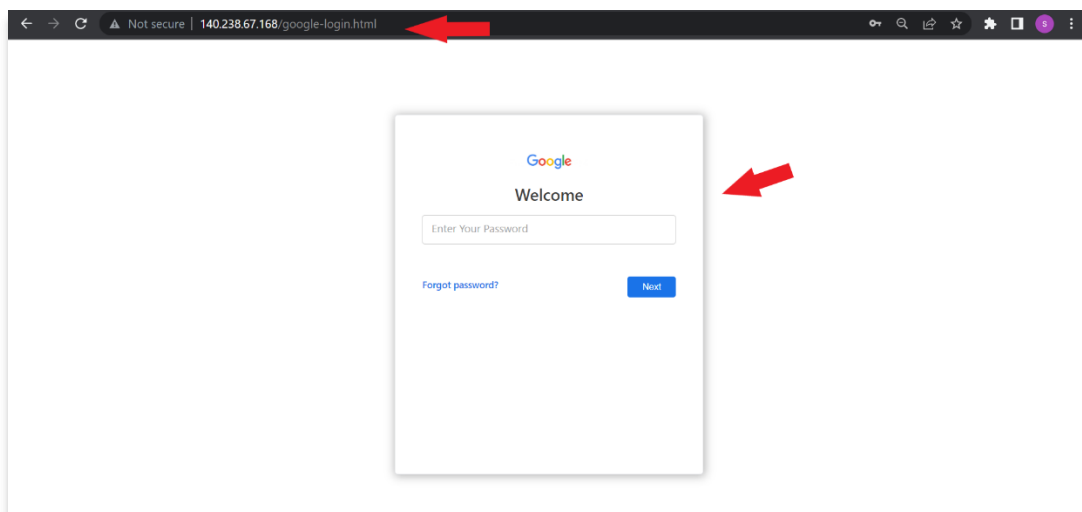


Figure 4: Gmail password field

The Fig 3 asks for Gmail username and Fig 4 asks for Gmail password. Both the page looks like exact Google's login page which make user to feel genuine Google login page but it's not by seeing URL.

Impact of fake Google login phishing page:

The impact of a fake Google login phishing page can be severe. It can lead to the theft of sensitive information, such as passwords, and other personal data. If the user visits the fake Google login page, their credentials could be stolen, leaving them vulnerable to identity theft and other fraud. This can lead to financial loss, identity theft, and even a loss of reputation. If the phishing page is successful, it may be used to allowing for further exploitation of the system. After a Google account takeover, an attacker may have access to the account holder's personal information, emails, contacts, and any other data stored in the account. They may use this information for fraudulent activities such as identity theft or phishing attacks, or to spread malware or spam. They could also use the account to gain access to other online accounts connected to the Google account, such as social media or financial accounts. Additionally, they could also use the account to impersonate the account holder and send emails or messages to their contacts. Overall, a Google account takeover can have serious consequences for the privacy and security of the account holder and their contacts

Code used: HTML, CSS, and JavaScript.

Accessing Camera and Mic without user knowledge:

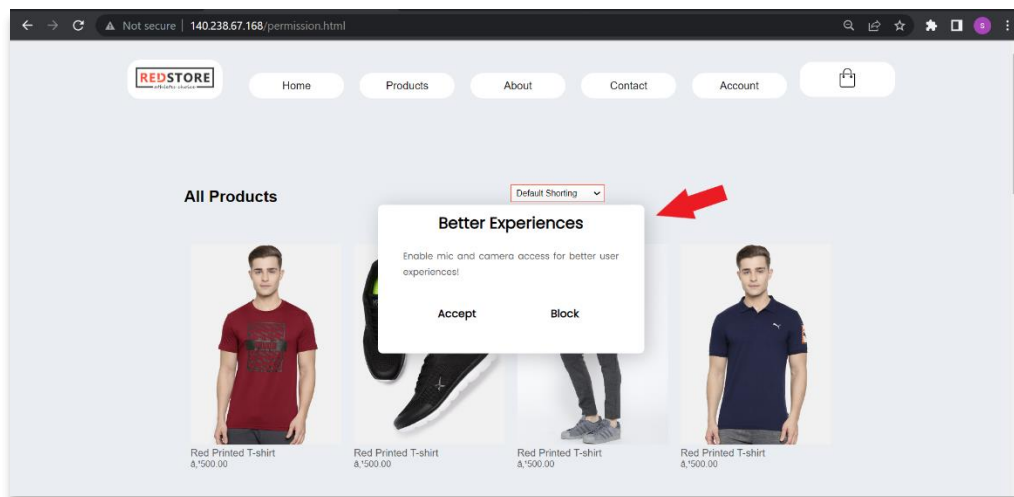


Figure 5: mic and camera permission

The Fig 5 show that this simulated website makes Popup window asking to accept or block mic and camera access with a description “Enable mic and camera access for better user experiences!”. This case makes user to either accept or reject access.

Impact of accepting mic and camera access in browser in untrusted website:

The impact of accepting microphone and camera access in an untrusted website can be significant. If the website is malicious, it could use the microphone and camera access to record audio and video without your knowledge. The website could use the recordings to spy on you, collect personal information, or use the recordings for malicious purposes. Furthermore, the website could use the recordings to create a profile of the user, which could be used for malicious purposes. Finally, if the website is malicious, it could use the recordings to blackmail the user. In short, if you do not trust the website, it is best to not grant microphone and camera access.

Code used: HTML, CSS, and JavaScript.

Sensitive Information asked by chatbot:

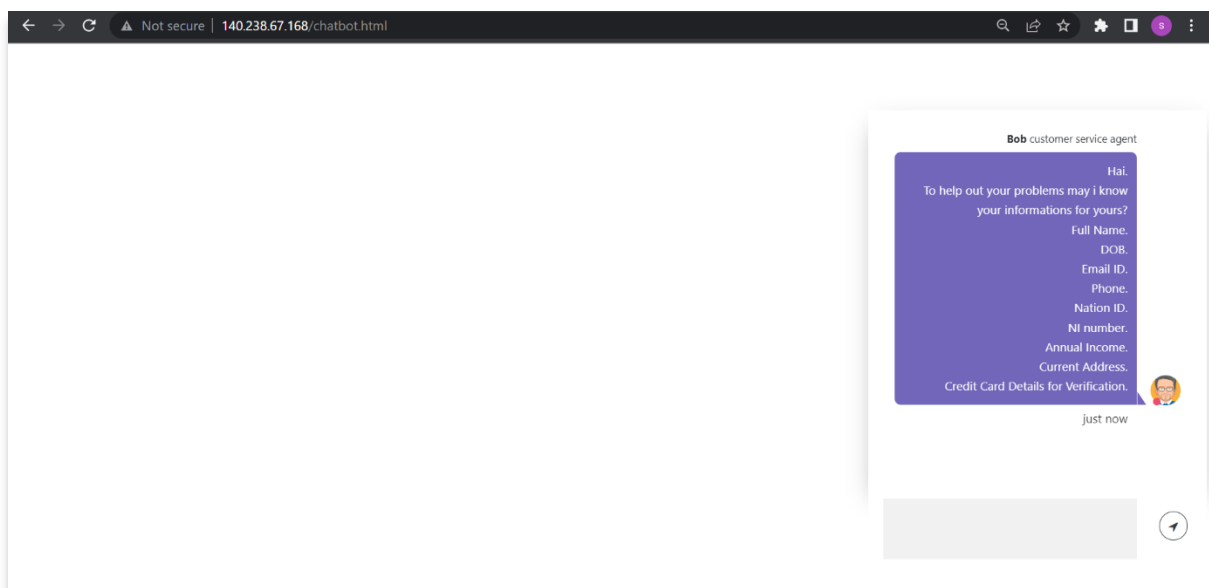


Figure 6: chatbot

The Fig 6 show that Chatbot asks for user's details, in this way user got tricked to enter their details.

Impact of Sensitive Information asked by chatbot:

Asking for sensitive information such as personal identification numbers, financial information, or login credentials by a chatbot can pose a significant security risk. This

information can be used for fraud or identity theft if it falls into the wrong hands. The impact of disclosing sensitive information to a chatbot is significant. It can lead to identity theft and other forms of fraud. It can also lead to the release of confidential information, which can cause a variety of problems, including financial loss, reputational damage, and legal responsibility. For example, if a person's records are leaked, it could have a major impact on their personal and professional life and could even result in legal consequence.

Code used: HTML, CSS, and JavaScript.

Malicious link clicks:

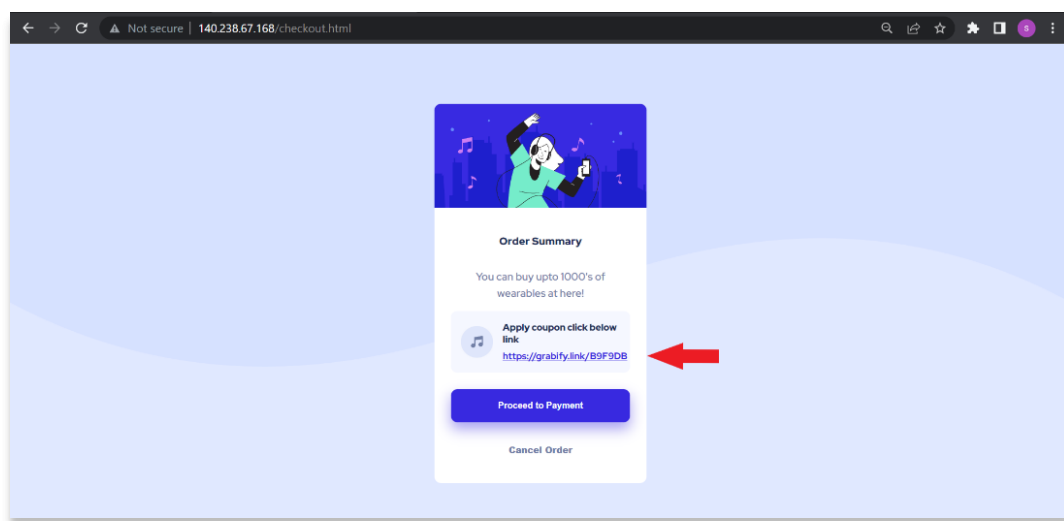


Figure 7: Offers

The above Fig 7 show how user might tricked to click the malicious link.

Impact of clicking the malicious link:

Clicking a malicious link can result in a variety of negative outcomes. Your device may become infected with malware, which can steal sensitive information, delete important files, or even gain control of your device. You may also be exposed to phishing scams that attempt to collect sensitive information, such as passwords and financial details. In some cases, clicking a malicious link can result in your device becoming part of a botnet, which is a group of connected computers used to launch attacks on other networks. Additionally, clicking a

malicious link can lead to malicious websites that can infect your computer with malicious software. The link may lead to a website that is designed to download malware or viruses onto the user's device. The malware or virus can then be used to gain access to the user's personal information, steal their identity, or hold their files for ransom. The link may also lead to a phishing site that is designed to trick the user into providing sensitive information, such as login credentials or financial information. Additionally, the link may also lead to a website that is designed to exploit vulnerabilities in the user's browser or operating system.

Code used: HTML, CSS, and JavaScript.

Reverse shell install:

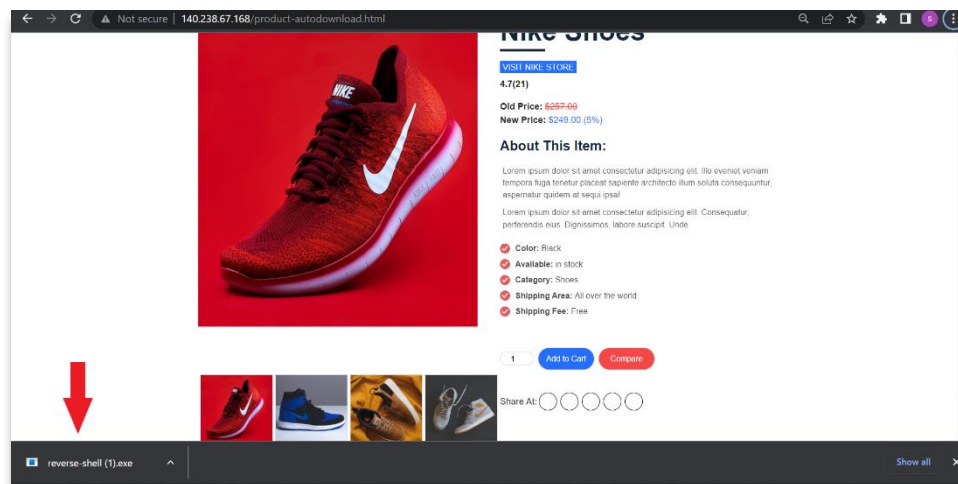


Figure 8: Auto download

The above Fig 8 show that Reverse shell auto downloaded. This makes user to execute any kind virus/malware to their system gain access of their system.

Impact of Reverse shell install:

A reverse shell is a type of malicious software that allows an attacker to gain control of a remote machine and establish a command shell session with it. This type of attack can be used to gain access to sensitive information, execute malicious code, or to launch further attacks on the

target system. The impact of a reverse shell can be significant, as an attacker can use the session to gain access to data and confidential information, or to launch further attacks on the target system. Additionally, the attacker can use the session to modify system configurations, install additional malicious software, or even gain access to other systems on the same network.

Code used: HTML, CSS, and JavaScript.

User intension to pay to untrusted source:

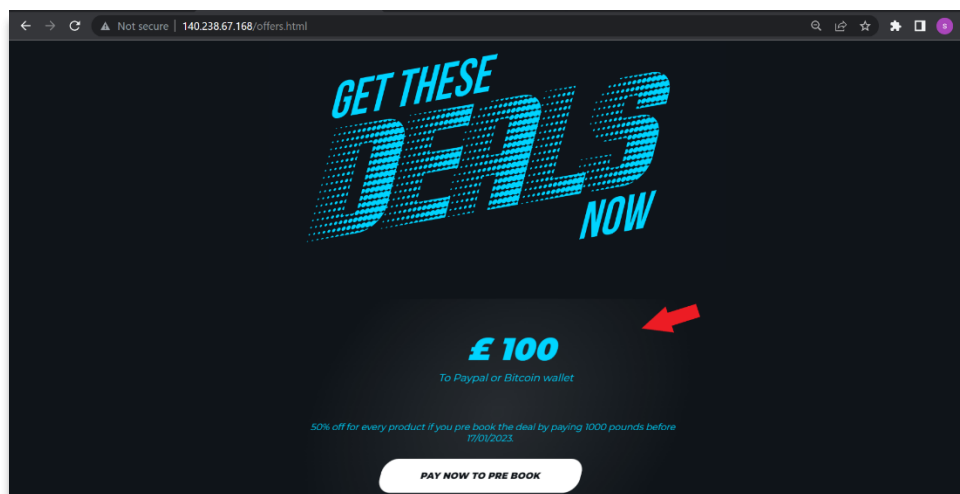


Figure 9: Deals

The above Fig 9 show how to manipulate the user to get paid. Most of the trusted source would make their payment via direct card and bank methods. But here it is made via PayPal or bitcoin which make feel doubt who have cyber awareness but for one who without cyber awareness?

Impact of User intension to pay to untrusted source:

The impact of a user's intention to pay to an untrusted source can be significant and long-lasting. If a user makes a payment to an untrusted source, he or she runs the risk of being scammed, of losing money, or of having his or her personal information stolen. Furthermore, if a user makes a payment to an untrusted source, the user may be subject to fraud and identity theft, as well as the potential for legal action from the untrusted source. Additionally,

if a user makes a payment to an untrusted source, the user's reputation may be damaged, as other potential customers may be less likely to trust the user in the future.

Code used: HTML, CSS, and JavaScript.

Uploading personal profiles to untrusted source:

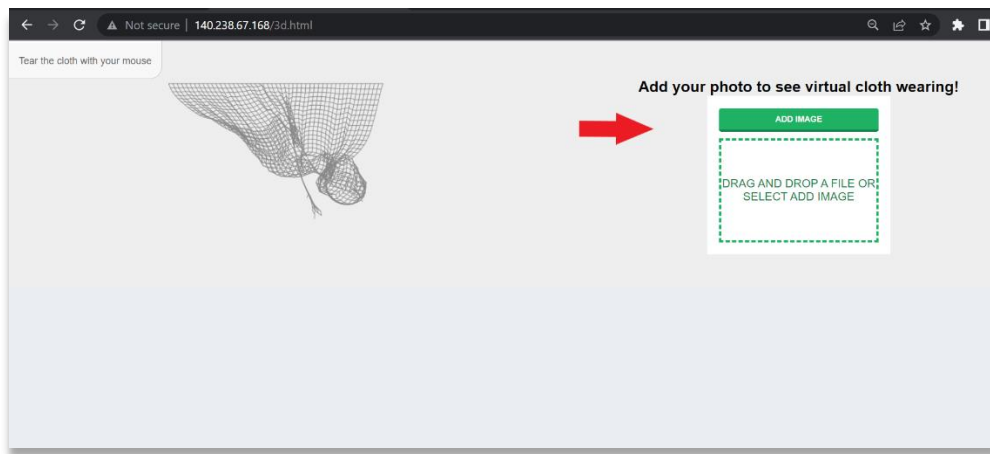


Figure 10: Photo upload

The above Fig show how user might get tricked to upload their photos.

Impact of Uploading profile photo to untrusted source:

The impact of uploading a profile photo to an untrusted source can be significant. It is possible that the photo could be used for malicious purposes, such as identity theft or other scams. Additionally, the photo could be used to target the person in question with targeted advertising or other forms of profiling. Furthermore, the photo could be altered in order to misrepresent the person or to cause embarrassment. Finally, there is always the possibility that the photo could be distributed to other sites without the person's permission or knowledge.

Code used: HTML, CSS, and JavaScript.

6.Cyber awareness model Working:

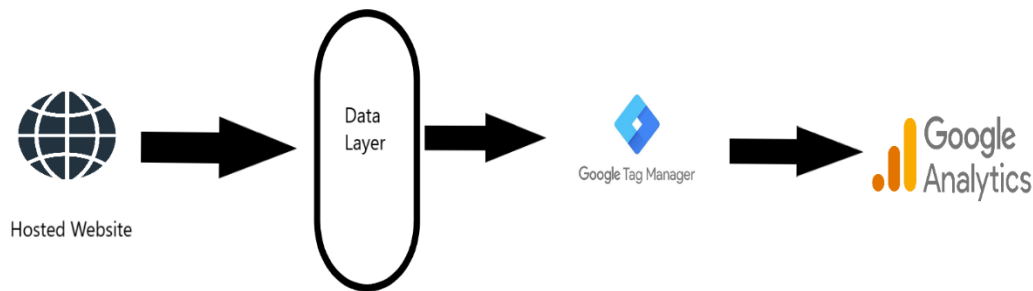


Figure 11: Working Flow

Website deployed with Cyber awareness modules which is mentioned above -

<http://140.238.67.168/>

Data Layer:

The Data Layer is a powerful tool that allows you to pass information from your website to Google Tag Manager (GTM). It is a JavaScript object that can be used to store data that can then be used to populate variables in your tags, trigger events, and track user behaviour on your website. The Data Layer makes it easy to add and manage marketing and analytics tags without the need for code changes.

When the Data Layer is working correctly, it means that the JavaScript object is correctly storing and passing information to GTM. This information can then be used to trigger events and track user behaviour, allowing you to gather valuable insights about your website visitors. Additionally, the Data Layer can also be used to pass information to other tools and platforms, such as Google Analytics and Google Ads, providing an even more comprehensive view of your website's performance.

Google Tag Manager:

Google Tag Manager (GTM) is a free tool offered by Google that allows you to easily add and manage marketing and analytics tags on your website without the need for code changes. It allows you to add and manage various tags such as Google Analytics, Google Ads conversion tracking, and more. GTM also provides a user-friendly interface that allows you to manage your tags and triggers in one place, making it easier to keep track of what tags are on your site and when they are firing.

With GTM, you can create tags, triggers, and variables, and use them to track events, such as clicks, form submissions, and pageviews. It also allows you to create and use the Data Layer, a JavaScript object that can be used to store and pass information to GTM, which can then be used to populate variables in your tags. This allows you to track and analyse user behaviour on your website more effectively.

GTM also provides detailed reporting and debugging features, which help you understand how your tags are behaving and troubleshoot any issues that may arise. It also has built-in security features to ensure that your data is safe and that only authorized users have access to your tags. Overall, GTM is a powerful tool that can help you improve your website's performance and gain valuable insights about your visitors.

Google Analytics:

Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. It allows you to gather data about your website's visitors, including information about their demographics, behaviour, and conversions. With Google Analytics, you can track metrics such as pageviews, bounce rate, and sessions, as well as more advanced metrics such as e-commerce transactions and user engagement.

One of the key features of Google Analytics is its ability to segment your data and create custom reports. This allows you to analyse the behaviour of specific groups of users, such as those who have visited a certain page or completed a specific goal. Additionally, Google Analytics also allows you to track user behaviour across different devices and platforms, giving you a comprehensive view of your website's performance.

Google Analytics also integrates with other Google tools such as Google Ads and Tag Manager. This allows you to track and analyse user behaviour on your website more effectively, and also make better-informed decisions about your marketing and advertising strategy. Overall, Google Analytics is a powerful tool that can help you gain valuable insights about your website's visitors, improve your website's performance, and make data-driven decisions.

Data Transfer from website to Google Tag Manager:

Data is transferred from a website to the Data Layer and then to Google Tag Manager (GTM) through a process called data-pushing. This process involves the use of JavaScript code that is added to the website's source code.

The JavaScript code creates a Data Layer object on the website and populates it with data. This data can be pulled from various sources, such as form submissions, clicks, and pageviews, and can include information such as user behaviour, product information, and transaction data.

Once the Data Layer is populated with data, it can then be passed to GTM through a process called data-pulling. GTM is able to access the Data Layer and retrieve the data through a series of triggers and variables that are set up within the GTM container. The data can then be used to trigger events, such as form submissions, clicks, and pageviews, and to populate variables in your tags, such as Google Analytics.

Once the data is passed to GTM, it can be used to track and analyse user behaviour on the website and also passed to other tools and platforms, such as Google Analytics providing an even more comprehensive view of website's performance.

Data Layer Push JavaScript Sample Code:

```
<script type="text/javascript">
  document.getElementById("myButton").onclick = function () {
    location.href = "mainpage.html";
    var email = document.getElementById("Email");
    dataLayer.push({
      'event': 'login',
      'user_id': email
    });
  };
</script>
```

Figure 12: DataPush code

Email of the user is referred by JavaScript variable “email” which is assigned to dataLayer variable user_id and event name “login”. Those two data are pushed to DataLayer.

How Data Received by Google tag manager:

In Google tag Manager create user defined variable with same variable name mentioned in JavaScript(user_id).

1. Variables -> User-Defined Variables->create variable name same as in JavaScript.

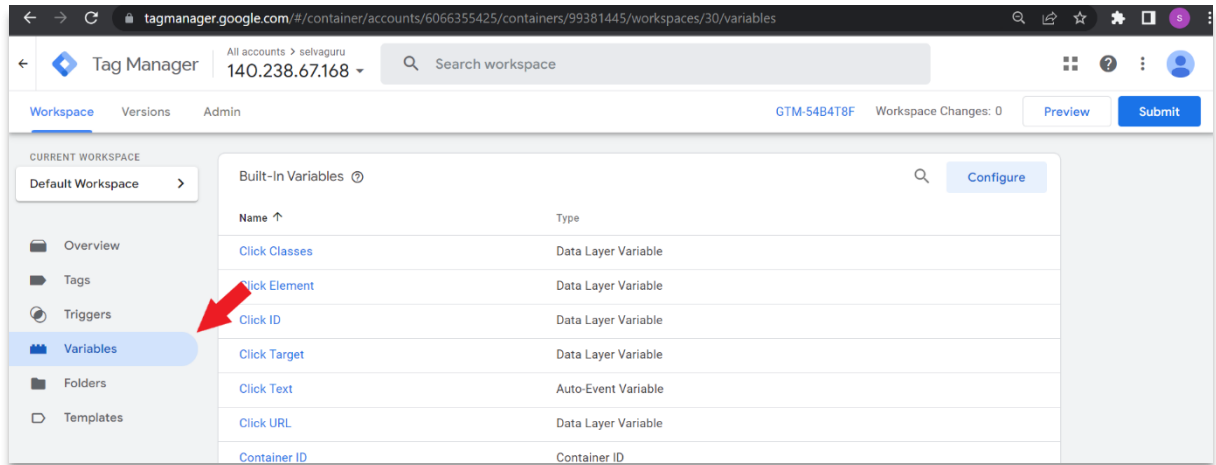


Figure 13: GTM Variable

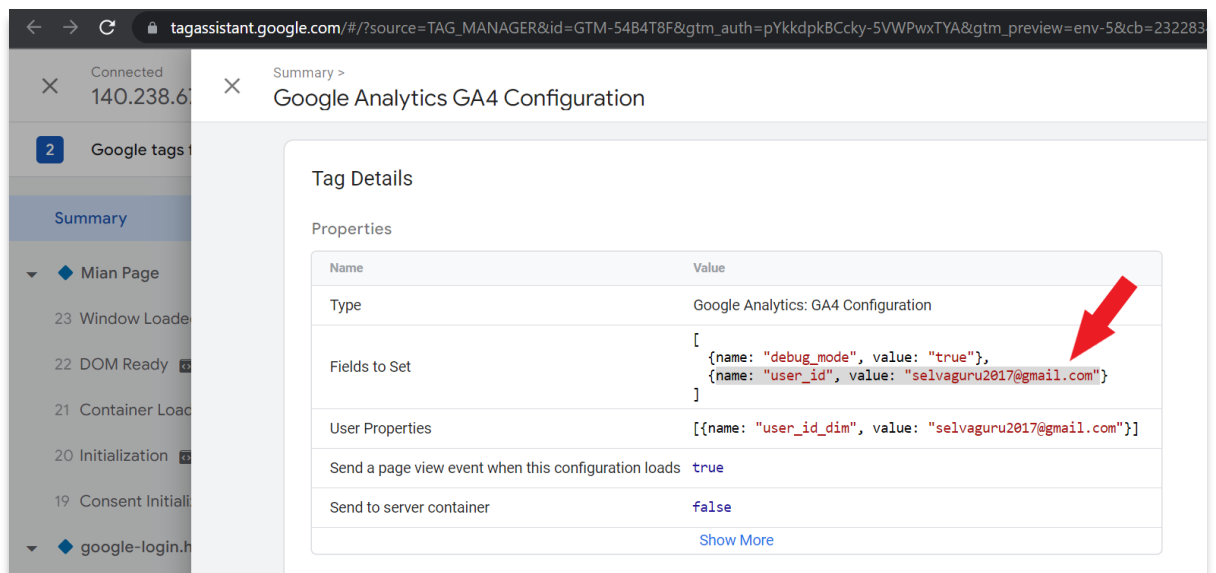


Figure 14: GTM Variable

The above Fig 14 show how data received by Google Tag manager from datalayer.

Data Transfer form Google Tag manger to Google Analytic:

Google Tag Manager Variable:

Google Tag Manager is a tag management system created by Google to manage JavaScript and HTML tags used for tracking and analytics on websites. It allows users to update tracking codes and related code fragments collectively known quickly and easily as tags on their website or mobile app. GTM allows users to create and update tags for conversion tracking, site analytics.

Google Tag manager Tags:

Google Tag Manager (GTM) is a free tool that allows you to quickly and easily add and manage tags on your website. Tags are snippets of code that are used to measure site traffic, track conversions. With GTM, you can easily add, remove, and update tags without having to manually edit your website code. Additionally, GTM makes it easy to control when and where tags fire, which helps ensure that you are collecting accurate data.

Google tag manager Trigger.

Google Tag Manager (GTM) triggers are an integral part of the tag-management system. They are used to fire tags in response to specific user interactions or events. Triggers are made up of conditions that must be true for a tag to fire. These conditions can be based on page URLs, page elements, user interactions, and more. GTM triggers are used to ensure that tags are fired accurately and only when necessary.

Triggers	Tags
➤ Triggers are used to determine when a tag should fire.	➤ Tags are used to collect data or perform actions.
➤ Triggers are used to define the conditions for when a tag is fired.	➤ Tags are used to send data to analytics tools, marketing platforms, or other systems.
➤ Triggers are used to specify when a tag should fire, such as when a button is clicked or a page is viewed.	➤ Tags are used to collect data such as page views, clicks, and form submissions.
➤ Triggers are used to specify when a tag should fire, such as when a button is clicked or a page is viewed.	➤ Tags are used to perform actions such as tracking conversions, setting cookies, and triggering pop-ups.
➤ Triggers can be created and managed in the GTM interface	➤ Tags are created and managed in the GTM interface.
➤ Triggers are reusable and can be shared across multiple tags	➤ Tags are specific to the task they are performing.

Table 1: Trigger vs Tag

How data send to Google analytics:

```

325 MenuItems.style.maxHeight = '0px';
326
327 function menutoggle() {
328   if (MenuItems.style.maxHeight == '0px') {
329     MenuItems.style.maxHeight = '200px';
330   } else {
331     MenuItems.style.maxHeight = '0px';
332   }
333 }
334
335
336 <script src="mainpage-script.js"></script>
337 <div class="popup">
338
339   <div class="fab fa-youtube icon1"></div>
340   <!-- cancel button -->
341   <button id="close">&times;</button>
342
343   <h2>safenet extension </h2>
344   <p>This extension will allow you to be safe on internet via our network</p>
345   <a id="extension_Accepted_to_install" href="permission.html" class="a-class"> <strong>Accept</strong></a>
346
347 </div>
348
349
350
351 </body>
352 </html>

```

Figure 15: ID refer

Fig 15 show that that anchor tag with Id “extension_Accepted_to_install” let’s see how to track that anchor tag with google tag manager.

First Create Trigger.

Triggers -> New -> Just Links-> Create Trigger based on the needs.

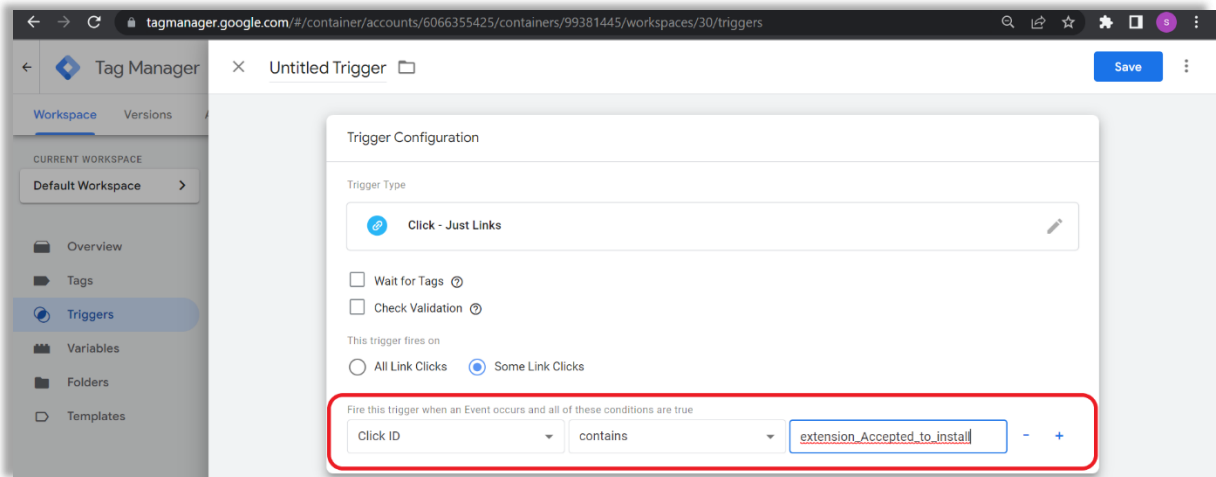


Figure 16: config Trigger

In Fig 16 it shows trigger created with Link click function. And tracking the particular anchor Tag ID is performed by assigning ID value to Pre-defined GTM variable “click ID”. This how each and every Trigger is defined.

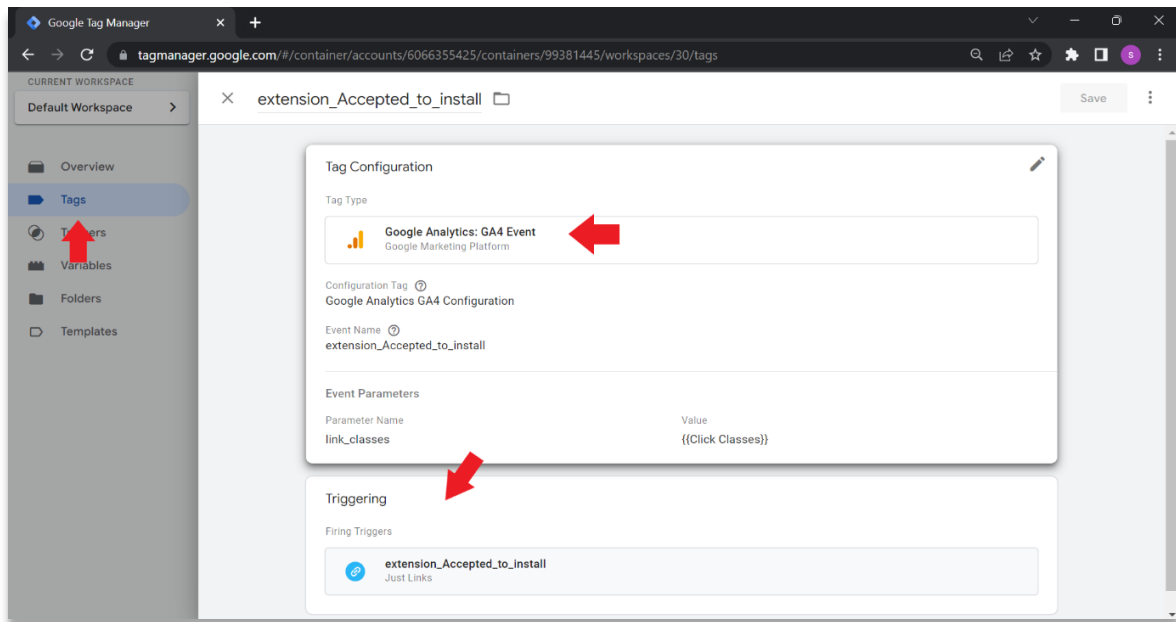


Figure 17: config Tag

Fig 17 show how triggers linked with Tag. In Tag Configuration add Google analytics account with Measurement ID, Event Name as our wish. Whenever Trigger get Triggered Corresponding Linked Tag get fired and Events values send to linked google analytics.

7.Realtime Deploy for user evaluation:

To work with Google Tag manager and with Google Analytics Website must be hosted not in local. For that, this cyber awareness model simulation website is hosted in Oracle Cloud server.

System Configuration:

OS Type : Ubuntu server 22.04,
Architecture : x64,
CPU : 4,
RAM : 12,
Hosting Server : Apache2,
IP : 140.238.67.168,
Access Via : SSH with Private and Private Key Protection.

Here are the general steps to connect website to Google Tag Manager:

- Create a Google Tag Manager account and container by giving IP address or domain name of the website hosted.

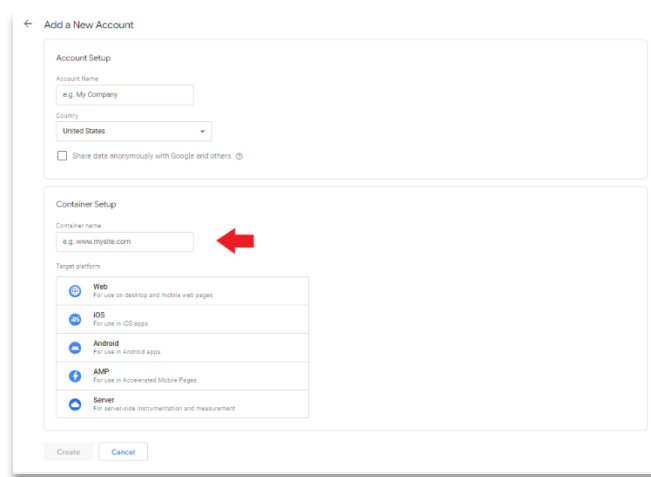
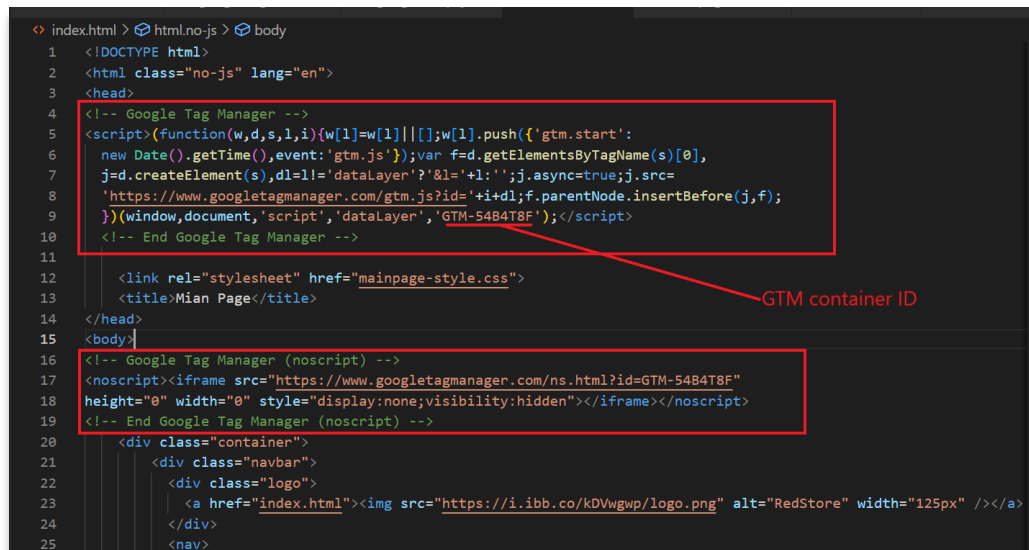


Figure 18: GTM setup

- Add the Google Tag Manager code snippet to the each and every page of head and body section in website's HTML. This code connects website to the Google Tag Manager container created.

NOTE: Google tag manager Script must be added to every HTML page. Those script will be generated by GTM once container created.



```
<!-- Google Tag Manager -->
<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
  new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
  j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
  'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
  })(window,document,'script','dataLayer','GTM-5484T8F');
<!-- End Google Tag Manager -->

<link rel="stylesheet" href="mainpage-style.css">
<title>Mian Page</title>
</head>
<body>
  <!-- Google Tag Manager (noscript) -->
  <noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-5484T8F"
    height="0" width="0" style="display:none;visibility:hidden"></iframe></noscript>
  <!-- End Google Tag Manager (noscript) -->
  <div class="container">
    <div class="navbar">
      <div class="logo">
        <a href="index.html"></a>
      </div>
    </div>
  </div>
```

Figure 19 : GTM script to code

- Verify that your website is properly connected to the container by checking the Google Tag Manager preview and debug mode.

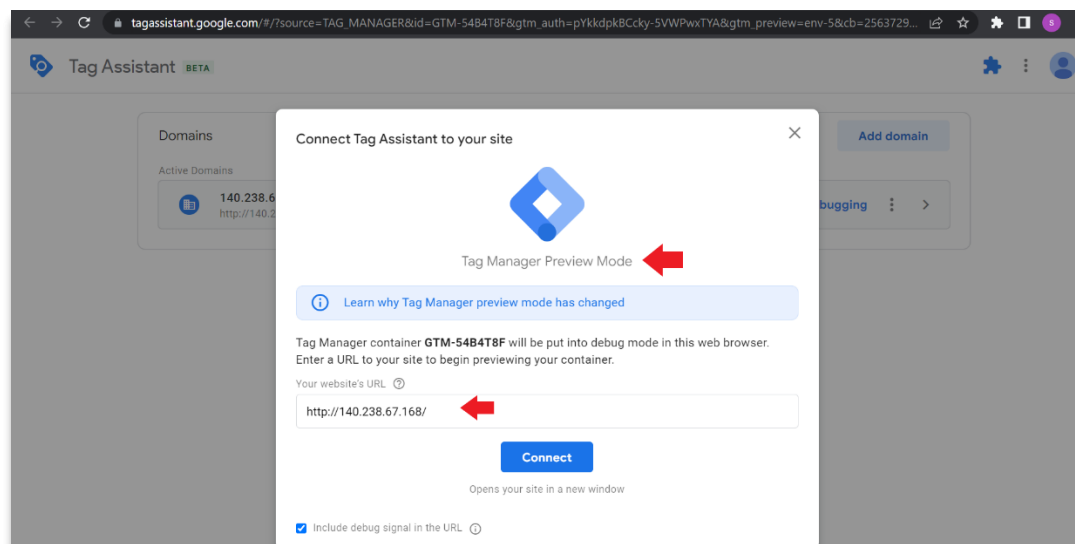


Figure 20: GTM preview

- Create and publish tags in Google Tag Manager. These tags allow you to track specific events on your website, such as button clicks or page views which mentioned above in Fig 15, 16, 17.

- Test your tags to ensure that they are firing correctly on your website.

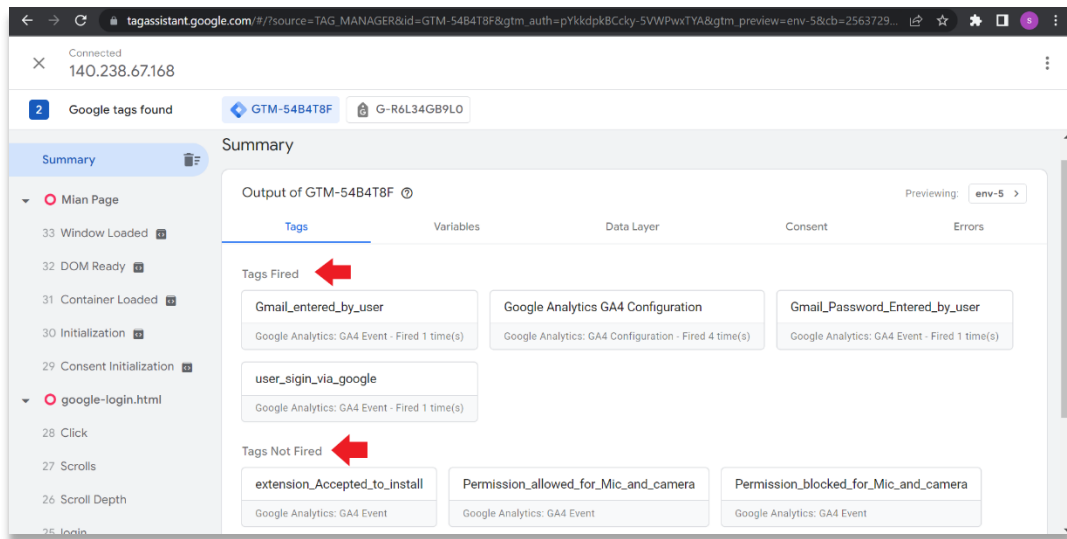


Figure 21: Tag firing

- After deploying your website, double check the GTM connection by visiting your website and verify if the GTM tracking code is firing correctly.
- Once everything is working, go to live website to some activity and start using Google Tag Manager to track and analyse user behaviour.
- In this Project there is number of triggers and Tags which is quite difficult to show in this report. For that Whole trigger and Tag configuration file is Export and attached in Source code Zip file.
- Next, create a Google Analytics account and create property with website IP or Domain name.
- Note the Measurement ID.
- In the Google tag Manager, configure the tag to send data to your Google Analytics property by entering your Measurement ID.

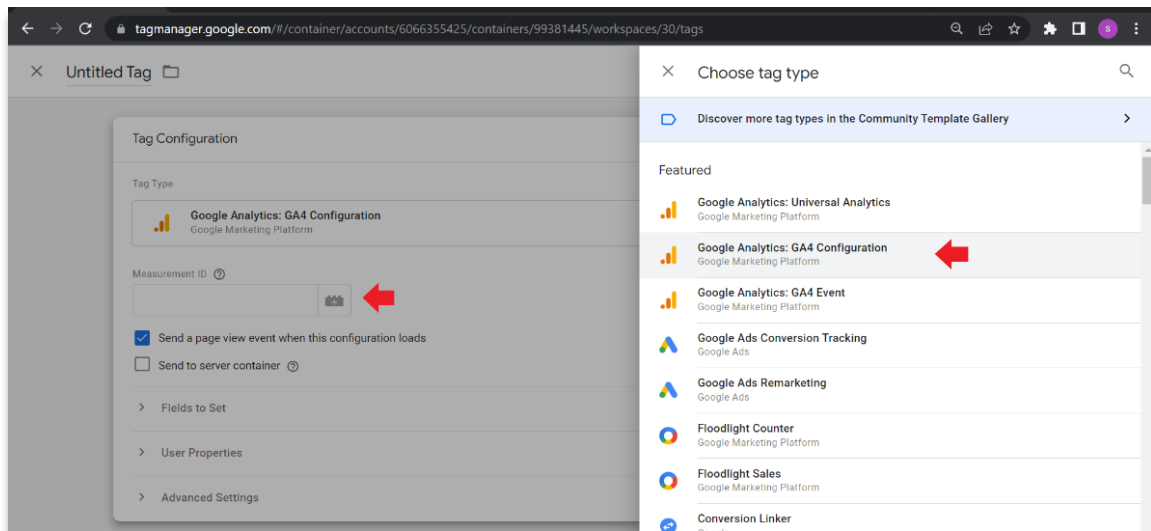


Figure 22: GTM configuration

- Verify that data is being sent to your Google Analytics property by checking the real-time report in Google Analytics.

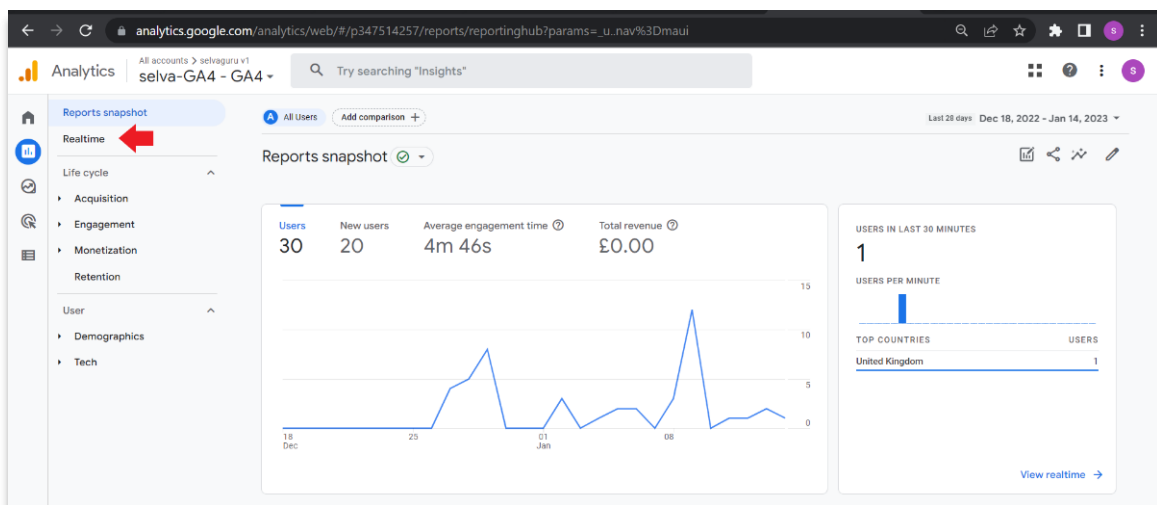


Figure 23 : GA Realtime

Once data is being sent to Google Analytics, start using Google Analytics to track user behaviour based on trigger and tag created in GTM.

General steps to create account and properties in Google Tag manager and Google Analytics. (Different Way used this project but it is genera step to work with).

Step	Google Tag Manager	Google Analytics
1	Go to tagmanager.google.com	Go to analytics.google.com
2	Click on "Create Account" button	Click on "Start for free" button
3	Fill in account details and accept terms of service	Fill in account details and accept terms of service
4	Create a container for your website	Create a property for your website
5	Install the Google Tag Manager container snippet on your website	Install the Google Analytics tracking code on your website
6	Add and configure tags (e.g. Google Analytics) in the Google Tag Manager interface	Set up goals and other settings in the Google Analytics interface

Table 2: GTM vs GA

8.Steps to Third Person Redeploy this cyber awareness Model:

- Host the website simulation in dedicated server or any hosting providers as your wise.
- Create a Google Analytics account and property for your website.
- Create a Google Analytics tag in Google Tag Manager and create container in it with IP or Domain of the hosted website.

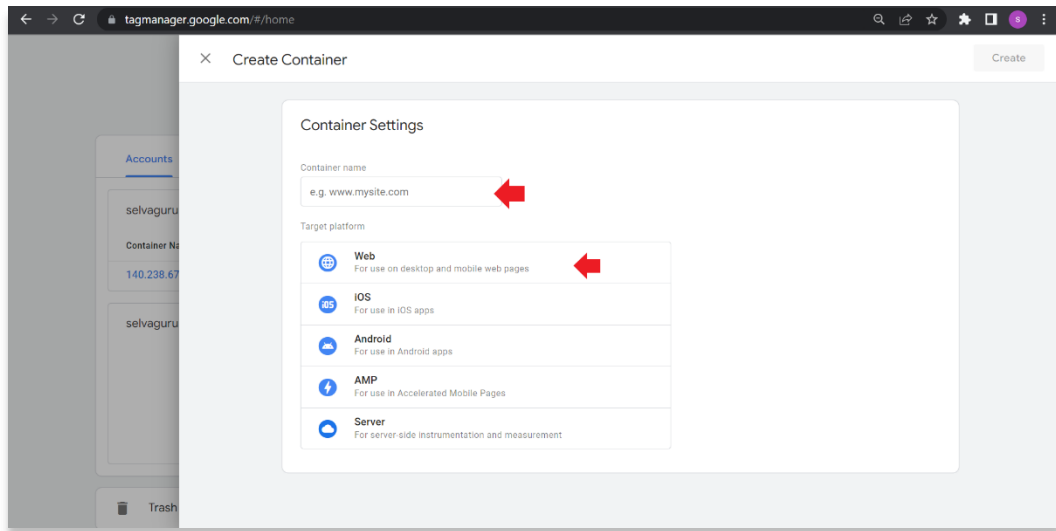


Figure 24: GTM setup

- And next import the Tag configuration file to Google Tag Manger which is attached in source code zip file.

Open container-> Admin->Import Container.

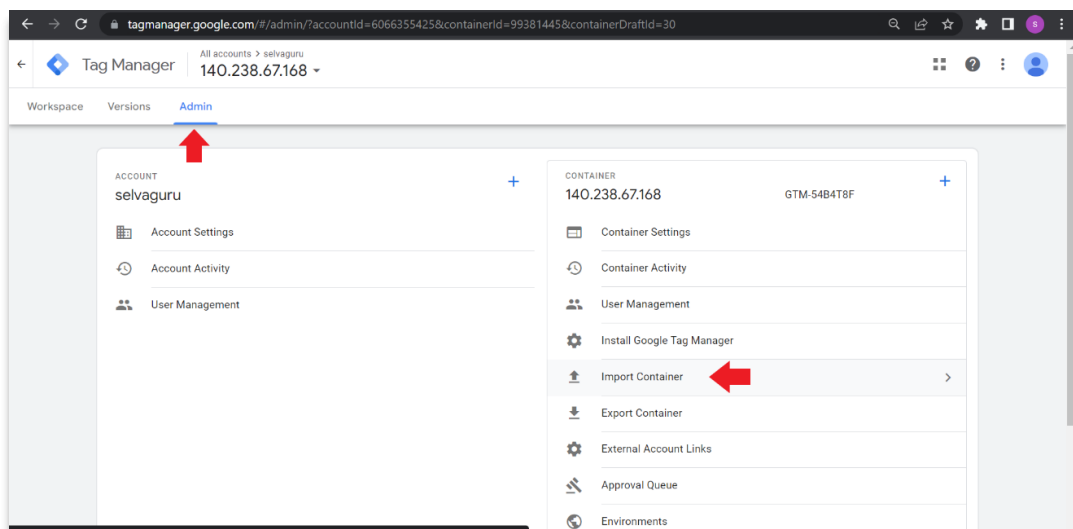


Figure 25: GTM admin view

- Now all configurations are imported to Tag manager. Final step to complete the setup is change the measurement ID with your Google Analytics Measurement ID.

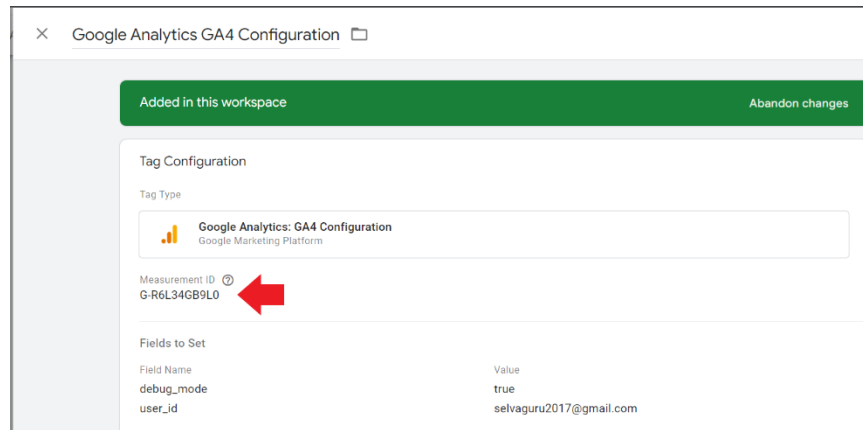


Figure 26: GA Measurement ID

Note: Measurement ID must replace with yours google analytics measurement ID.

Steps to get measurement ID in google analytics:

- Sign into your Google Analytics account.
- Under the "Account" column, select "Create Property."
- Fill in the details for the property you wish to create, including the website name, website URL, and industry category.
- Select the data sharing settings that you prefer.
- Click on the "Create" button to create the property.
- Now Select the website property that created now to get the measurement ID for.
- Click on "Admin" in the bottom left corner of the screen.
- Under the "Property" column, click on "Data stream" and click on property name snow.
- The measurement ID will be listed. It will be a string of letters and numbers in the format "UA-XXXXX-Y."

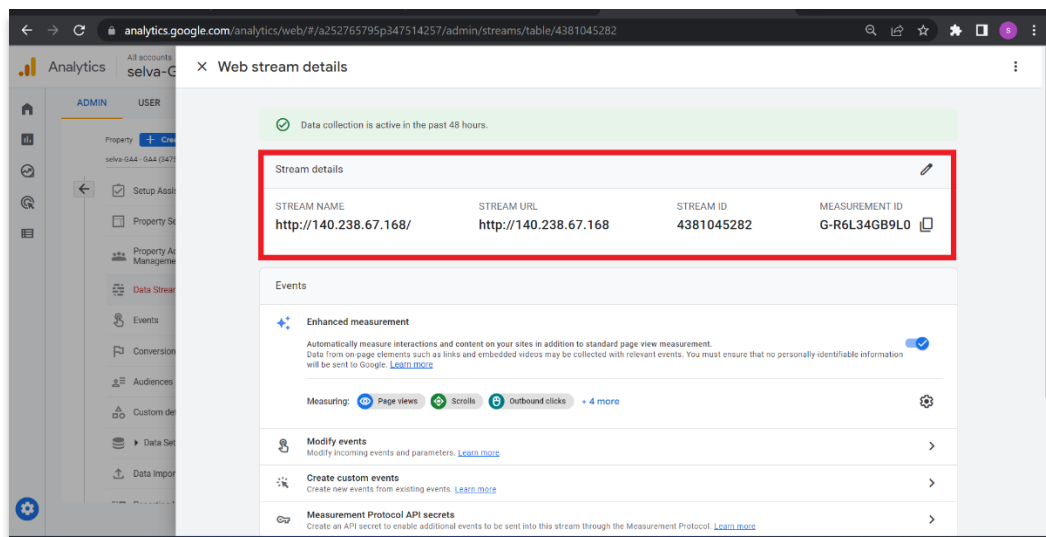


Figure 27: GA Measurement ID

9. Why Google Analytics is used over dedicated cyber threats protection software:

Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. It is primarily used to track website usage, user behaviour, and conversion rates. It helps website owners understand how users interact with their website and tracking every move of the users by make triggers and Tags.

On the other hand, cyber threat protection software is used to track and detect malicious activity on a website or network. It is designed to detect and prevent cyber-attacks, such as malware, phishing, and other types of cybercrime. It does this by monitoring network traffic, identifying suspicious behaviour, and alerting administrators to potential threats.

This project simulated with web platform and Google analytics is light weight to install and configure with host, but on the other side cyber threat protection tools needs to be install on the user side, occupies more resources and it won't be realistic for user evaluation. That the main reason to go with Google analytics.

10. Product Testing before deploying:

Here are some steps for web product testing before deploying:

- Test environment setup: Set up the testing environment, including the necessary hardware and software, and configure any test data that will be needed.

- **System Configuration:**

- OS Type : Ubuntu server 22.04,
- Architecture : x64,
- CPU : 4,
- RAM : 12,
- Hosting Server : Apache2,
- IP : 140.238.67.168,
- Access Via : SSH with Private and Private Key Protection.
- Install necessary software: Once the VPS is set up, Install necessary software on the instance. This may include web server software like Apache or Nginx.
- Configure the web server: Configure the web server to serve the web application. This will typically involve specifying the document root,

creating virtual hosts, and configuring the server to use the appropriate web framework.

- In advantage of Cloud Server, real time production stage testing is done easily with Docker or any other image Containers like Kubernetes.
- It is better to test this cyber awareness model in virtual host address. If any testing crash occurs that can be easily removed without affecting actual deploy.

web unit testing:

Web unit testing is the process of testing individual units of code for a web application to ensure that they are functioning correctly. These units of code can include individual functions, methods, or classes. The goal of web unit testing is to identify and fix any bugs or errors in the code before the application is deployed to production. Web unit testing can be done manually by a developer, but it is more commonly automated using a testing framework. Automated web unit testing allows developers to run a large number of tests quickly and easily, and to easily repeat tests as needed. Overall, web unit testing is an important part of the web development process, as it helps to ensure the quality and reliability of web applications. By identifying and fixing bugs and errors early on, web unit testing can help to save time and money and improve the user experience.

Web integration testing:

Web integration testing is the process of testing the interactions and interfaces between different components of a web application. This type of testing is designed to ensure that different components and systems within the application are working together correctly and as expected. It helps to identify any issues that may arise when different parts of the application are combined, and it is a critical step in the overall quality assurance process. Web integration testing typically includes a range of different tests, including functional tests, performance tests, and security tests. The goal of these tests is to ensure that the application is functioning correctly, is performing well under load, and is secure against potential threats. Web integration testing is typically done after web unit testing, which focuses on testing individual units of code. It is an important step in the overall web development process, as it helps to ensure that the application is stable, reliable, and ready for deployment. In this test web application and Google Tag manager and Google Analytics are integrated properly or not.

web End-to-end tests:

Web end-to-end (E2E) tests are a type of testing that is used to validate the functionality of a web application by simulating real-world scenarios. These tests are designed to ensure that the application behaves as expected and meets the user's needs by testing the entire system, including all its components, dependencies (Java Scripts), and external systems. Web E2E tests are important because they help to ensure that the web application is working correctly and meets the user's needs by testing the entire system from end to end. They can also help to identify and fix bugs and issues before the application is released to the public.

- Plan the test: Define the scope of the test, including the features and functionality to be tested.
 - Basic functionality: Testing the core functionality of the web application, such as login, registration, and data entry forms.
 - Navigation: Testing the navigation of the web application, including the menu and links, to ensure they are working correctly.
 - Compatibility: Testing the web application on different browsers, devices, and screen sizes to ensure it is compatible with a range of environments.
 - Usability: Testing the usability of the web application, such as ease of use and user experience, to ensure that it is user-friendly to use.
 - Integration: Testing the integration of the web application with other systems, such as third-party gateways and APIs, to ensure that it works seamlessly with these systems.
- Create test cases: Develop a set of test cases that cover all the functionality of the website or web application.
 - Consider you as user and explore each page, functionality of the website
- Execute the test: Run the test cases and document any issues or bugs that are found.
 - Like, button function are working or not, ID tracking working or not with Google Tag manager, Trigger and Tag are fired or not,

- Analyse the results: Review the test results and identify any areas of improvement or issues that need to be noted
- Fix bugs: Fix any bugs that were identified during testing.
 - Like, Tag configuration, web functionality (Button Onclick, Broken Link, All screen resolution responsive, etc).
- Retest: Retest the website or web application to ensure that the bugs have been fixed and the website or web application is working as expected.
- Deploy: Once testing is completed and all bugs have been fixed, deploy the website or web application to the production environment.
- Monitor: Monitor the website or web application after deployment to ensure it is working properly and note any issues to fix.

11.Perform Result Analysis:

Evaluating the results from Google Analytics can provide valuable insights into the performance of a website or web application. Some key areas to consider when evaluating the results include.

Traffic: Analyse the overall traffic to the website, including the number of visitors, page views, and bounce rate. This will give you an idea of how many people are visiting the site and how engaged they are with the content.

Audience: Look at the demographics of the visitors, such as their location, age, and gender. This information can help you understand who your target audience is.

Acquisition: Analyse how visitors are finding your website, including the sources of traffic such as organic search, referral, social media and direct. This information can help you understand which ways users used most to visit website.

Behaviour: Analyse the behaviour of visitors on the website, including the pages they visit, the duration of their stay, and the actions they take. This information can help you understand how users interact with the website and identify their intentions.

Conversion: Analyse the conversion rate of the website, which is the percentage of visitors who complete a desired action such as filling out a form. This information can help you understand how well the website is performing in terms of conversion.

Goal: Analyse the goals that you have set up in Google analytics, such as a form submission, Page Visit, event set by Tag Manager, etc. This will give you an idea of how well the website is performing in terms of achieving your business objectives.

Realtime Report:

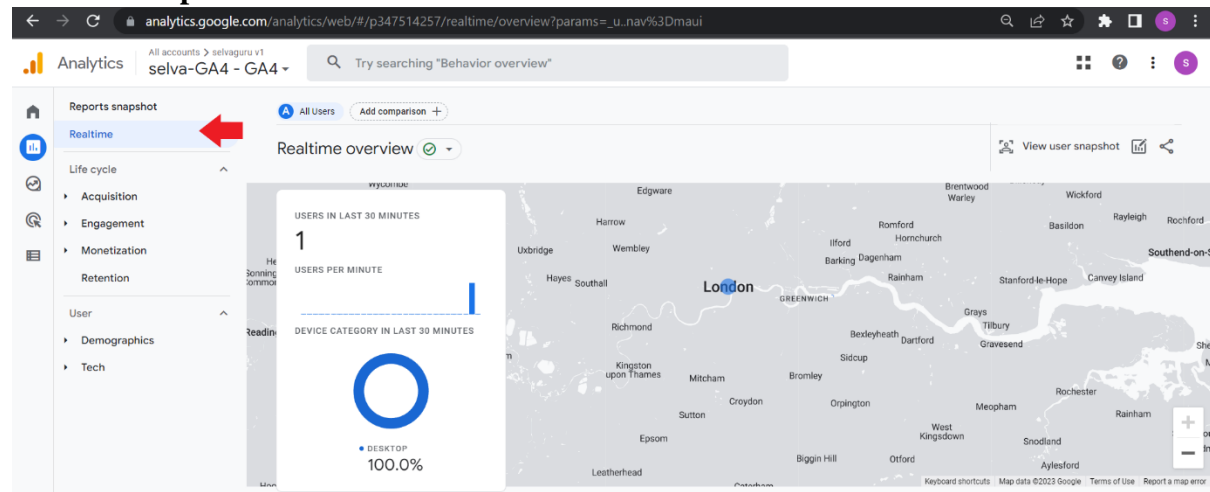


Figure 28: GA Realtime Report

Google Analytics Real-Time reports allow you to see data about your website as it happens. This can include information on the number of active users on your site, the pages they are viewing, the geographic location of the users, and the sources of traffic to your site. Real-time reports can be used to monitor website traffic and engagement in real time, identify and troubleshoot issues as they arise, and measure the effectiveness of marketing and advertising campaigns in real-time. Additionally, you can segment the data by different dimensions such as location, traffic source, and user behaviour, to gain deeper insights into your audience.

This feature allows to help for real time user monitoring in this cyber awareness module.

Google analytics Acquisition:

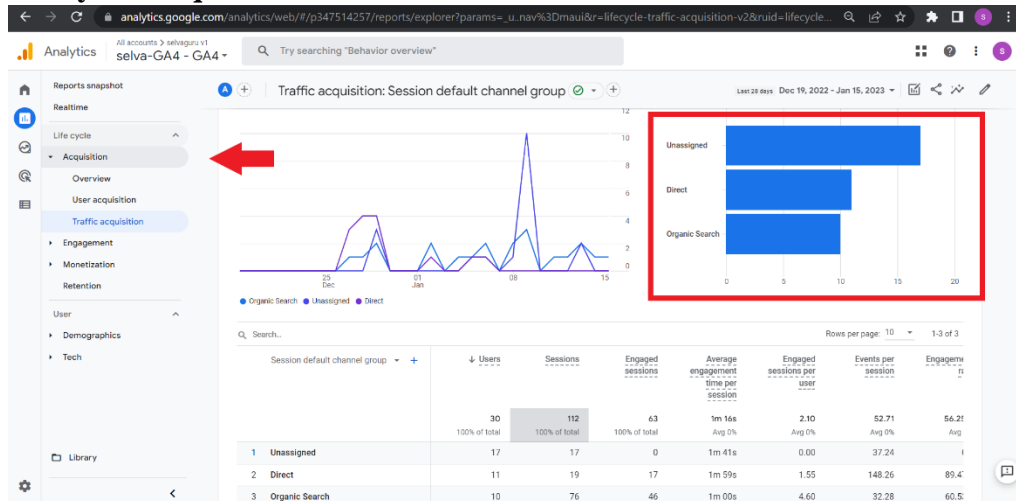


Figure 29 : GA acquisition

The Acquisition section in Google Analytics provides information on how users are finding your website. It includes data on the sources of traffic to your site, such as search engines, referral sites, social media, and direct traffic.

The Overview report in the Acquisition section shows the number of users, sessions, and bounce rate for each traffic source. The All-Traffic report provides a breakdown of the different sources of traffic to your site, including search engines, referral sites, social media, and direct traffic.

Direct Traffic: Visitors who come to a website by typing the URL directly into their browser or by clicking on a link from a bookmarked page. This traffic is considered direct because the visitor has a direct connection to the website.

Organic Search Traffic: Visitors who come to a website by clicking on a link from a search engine results page (SERP). This traffic is considered organic because it is generated by users searching for a specific keyword or phrase.

Google analytics engagement:

In Google Analytics, engagement refers to the actions and interactions that visitors have with a website. Some examples of engagement metrics that can be tracked in Google Analytics include:

- Bounce rate: The percentage of visitors who leave a website after only viewing one page. A high bounce rate indicates that visitors are not engaging with the website.
- Session duration: The average amount of time that a visitor spends on a website. A longer session duration indicates that visitors are engaging with the website for a longer period of time.
- Pages per session: The average number of pages that a visitor views during a session. A higher number of pages per session indicates that visitors are engaging with more content on the website.
- Events: Custom interactions that you can track on your website, such as clicks on a button or link, or video plays.
- Goals: pre-defined actions that you want your visitors to take on your website, such as filling out a contact form.

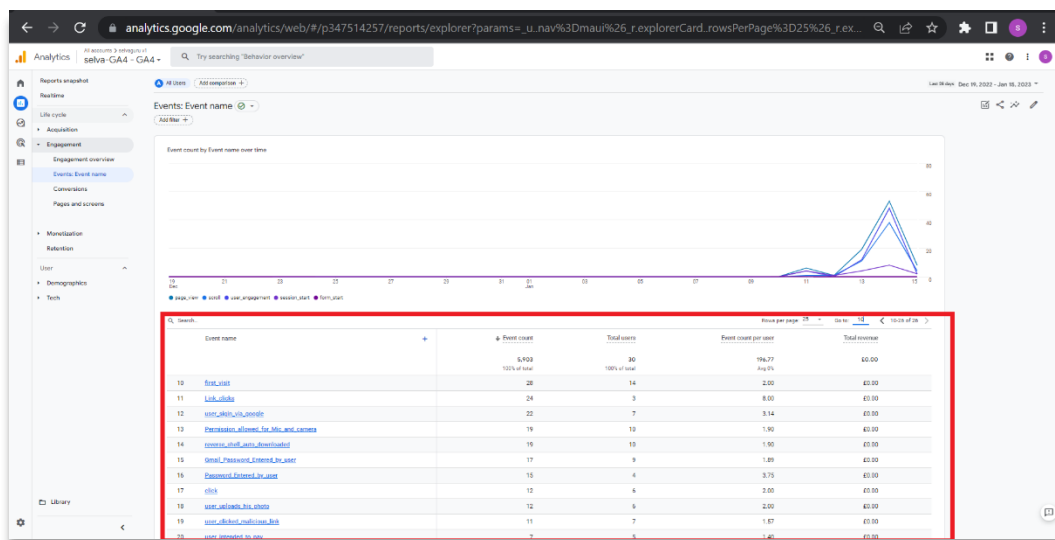


Figure 30: GA events

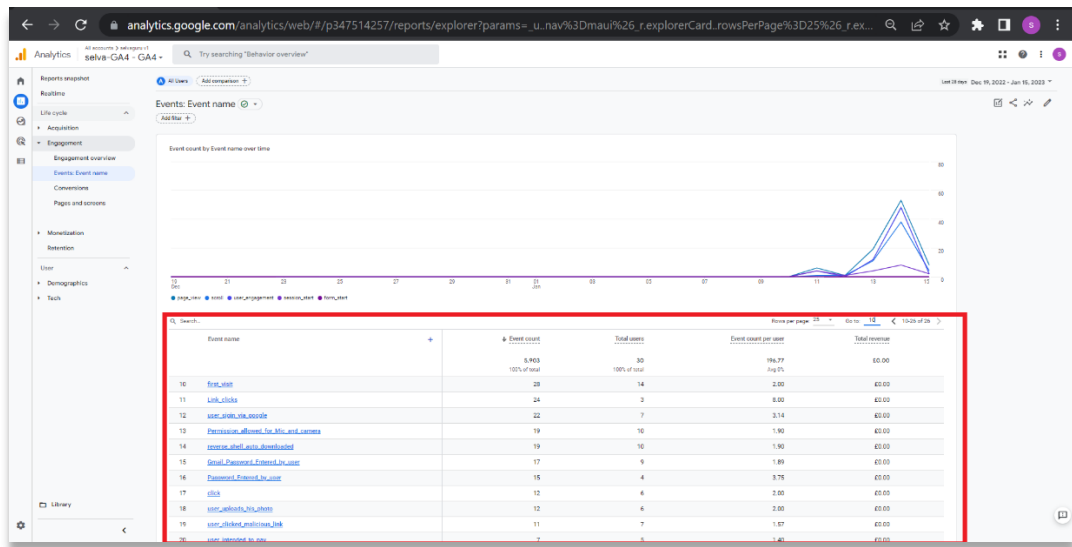


Figure 31: GA events

Google analytics Demographic details: Country:

Google Analytics provides demographic details such as countries for users who have enabled the Demographics and Interests Reports in their Analytics settings. This information includes the percentage of visitors from each country and the total number of visitors from each country. This information can be used to gain insights into user behaviour and target specific audiences. You can use this data to better understand who is visiting your site and how they are engaging with your content. The Country use in tracking report shows you which countries your visitors are coming from. You can use this data to see which countries are driving the most traffic to your site and to identify user from which location most.

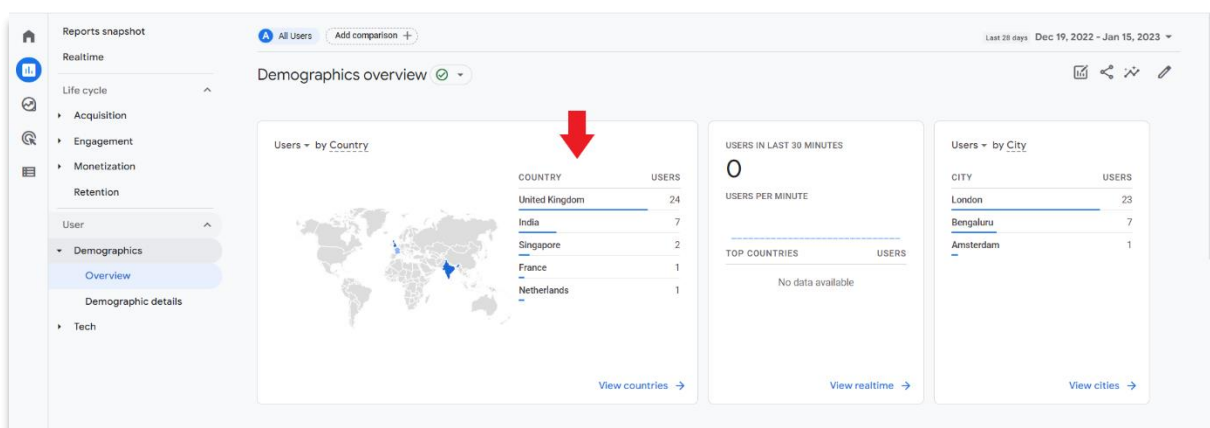


Figure 32: Country view

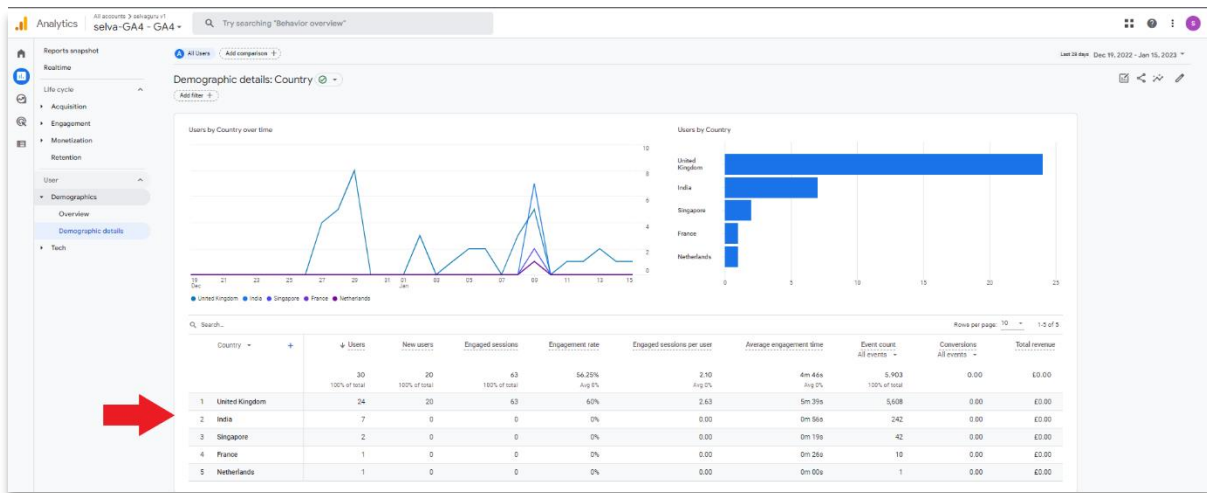


Figure 33: country View

Google analytics-Tech:

Tech Report provides platform used, operating system used by users, device category, Browser used by users and screen resolution of the user's phone, device model, and platform and browser versions.

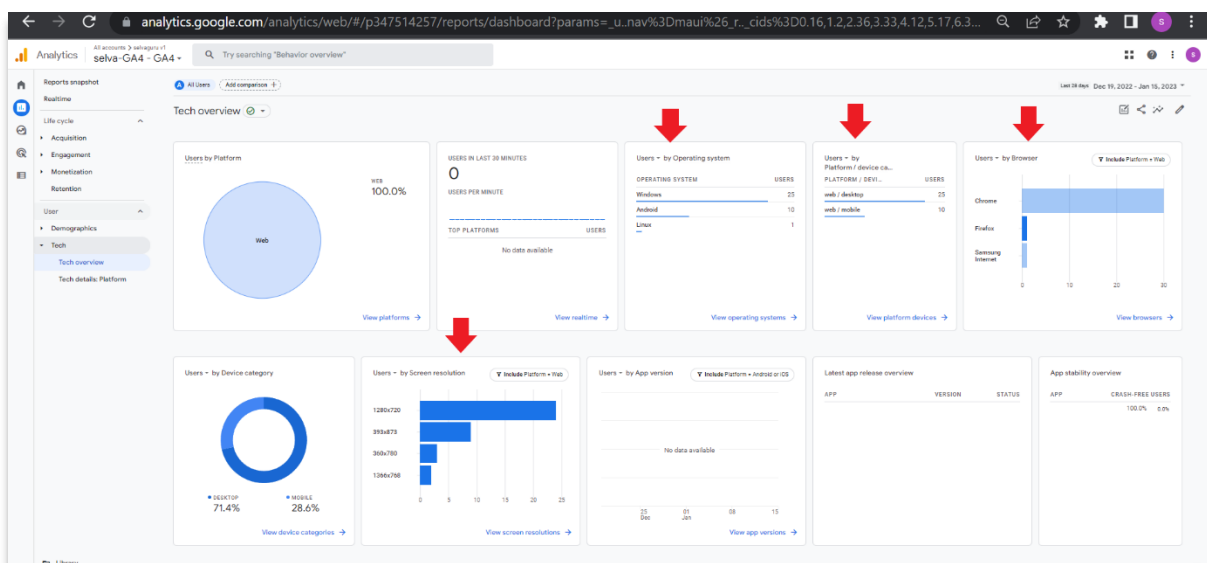


Figure 34: Tech details

Google analytics user exploration:

Google Analytics User Exploration refers to the process of analysing user behaviour on a website using Google Analytics. This includes tracking user interactions, such as page views, clicks, and conversions, as well as user demographics, such as location, age, and gender. Additionally, user exploration can help identify trends in user behaviour over time, which can be used to track individual users.

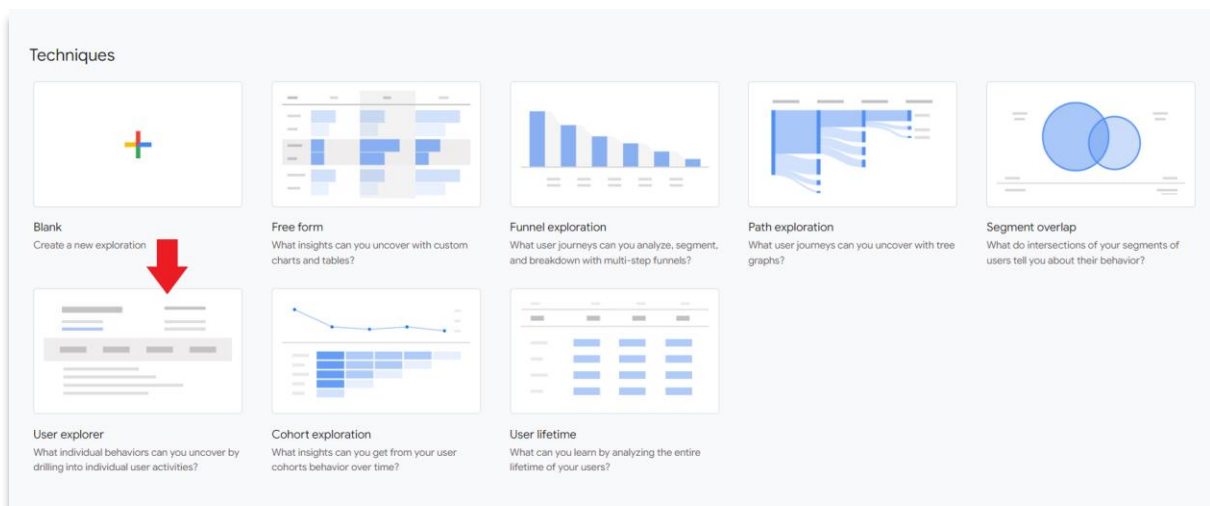


Figure 35: user explorer

Figure 36 shows the Google Analytics User Explorer interface. The table displays user details for the selected exploration. The table is outlined with a red border.

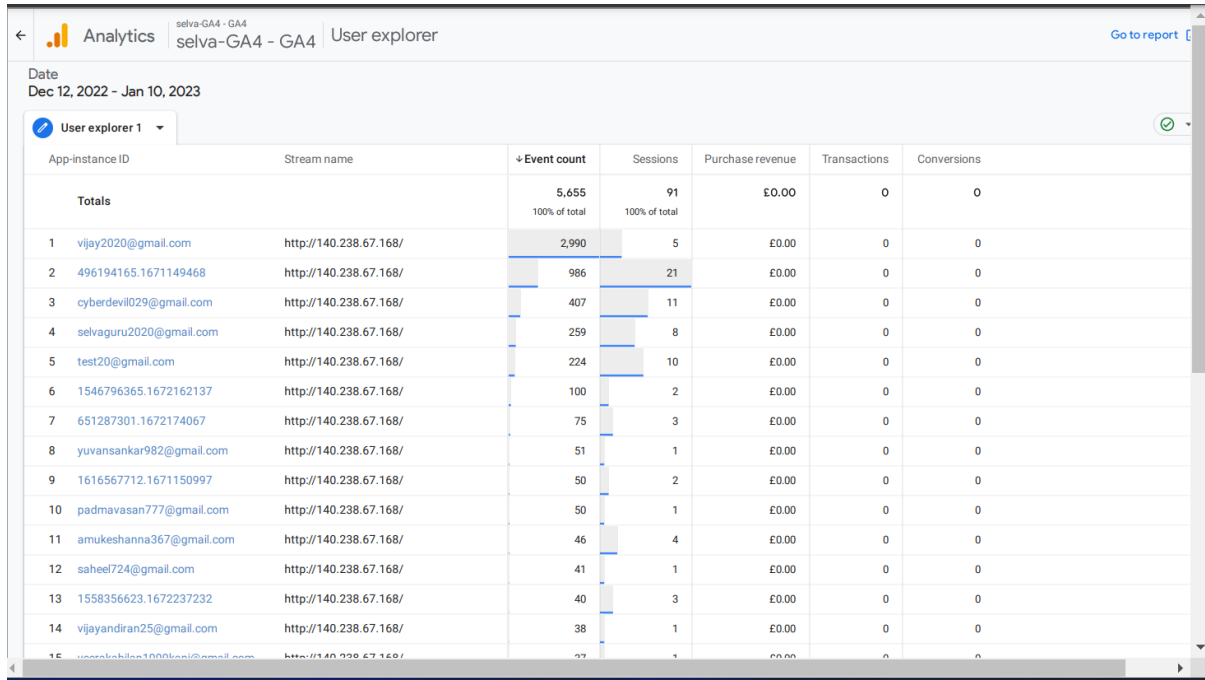
App-instance ID	Stream name	+ Event count	Sessions	Purchase revenue	Transactions	Conversions
Totals		5,903 100.0% of total	112 100.0% of total	£0.00	0	0
1 vijay2020@gmail.com	http://140.238.67.168/	2,990	5	£0.00	0	0
2 496194165.1671149468	http://140.238.67.168/	986	21	£0.00	0	0
3 cyberdevil029@gmail...	http://140.238.67.168/	407	11	£0.00	0	0
4 selvaguru2020@gmail...	http://140.238.67.168/	299	8	£0.00	0	0
5 test20@gmail.com	http://140.238.67.168/	224	10	£0.00	0	0
6 selvaguru2017@gmail...	http://140.238.67.168/	216	13	£0.00	0	0
7 1546796365.1672162...	http://140.238.67.168/	100	2	£0.00	0	0
8 amukeshanna367@gma...	http://140.238.67.168/	78	12	£0.00	0	0
9 651287301.1672174067	http://140.238.67.168/	75	3	£0.00	0	0
10 yuvansankar982@gmai...	http://140.238.67.168/	51	1	£0.00	0	0

Figure 36: All user details

The above Figure show all Individual users and to see their activity click on their mail ID.

12. User Evaluation:

This Cyber Awareness simulated website is tested with some of my friends. And here we see have to analysis the results of their and how they aware about cyber threats.



The screenshot displays the Google Analytics 'User explorer' interface. At the top, it shows the date range 'Dec 12, 2022 - Jan 10, 2023' and the property 'selva-GA4 - GA4'. The report is titled 'User explorer 1'. The table lists individual users with columns for App-instance ID, Stream name, Event count, Sessions, Purchase revenue, Transactions, and Conversions. The first row shows a total of 5,655 events and 91 sessions. Subsequent rows list individual users, such as vijay2020@gmail.com, with their respective event counts and sessions. The Stream name for all users is http://140.238.67.168/.

App-instance ID	Stream name	Event count	Sessions	Purchase revenue	Transactions	Conversions
Totals		5,655 100% of total	91 100% of total	£0.00	0	0
1 vijay2020@gmail.com	http://140.238.67.168/	2,990	5	£0.00	0	0
2 496194165.1671149468	http://140.238.67.168/	986	21	£0.00	0	0
3 cyberdevil029@gmail.com	http://140.238.67.168/	407	11	£0.00	0	0
4 selvaguru2020@gmail.com	http://140.238.67.168/	259	8	£0.00	0	0
5 test20@gmail.com	http://140.238.67.168/	224	10	£0.00	0	0
6 1546796365.1672162137	http://140.238.67.168/	100	2	£0.00	0	0
7 651287301.1672174067	http://140.238.67.168/	75	3	£0.00	0	0
8 yuvansankar982@gmail.com	http://140.238.67.168/	51	1	£0.00	0	0
9 1616567712.1671150997	http://140.238.67.168/	50	2	£0.00	0	0
10 padmavasan777@gmail.com	http://140.238.67.168/	50	1	£0.00	0	0
11 amukeshanna367@gmail.com	http://140.238.67.168/	46	4	£0.00	0	0
12 saheel724@gmail.com	http://140.238.67.168/	41	1	£0.00	0	0
13 1558356623.1672237232	http://140.238.67.168/	40	3	£0.00	0	0
14 vijayandiran25@gmail.com	http://140.238.67.168/	38	1	£0.00	0	0
15 userkshilpa100kni@gmail.com	http://140.238.67.168/	37	1	£0.00	0	0

Figure 37: All users Details

The above figure show how may individual users visits this simulated website hosted in <http://140.238.67.168/> .

Users who Logged-in are tracked with their mail id's.

Users who are not logged-in are tracked with random numeric value assigned by google analytics automatically.

Analysing some user's evaluation report:

User:1

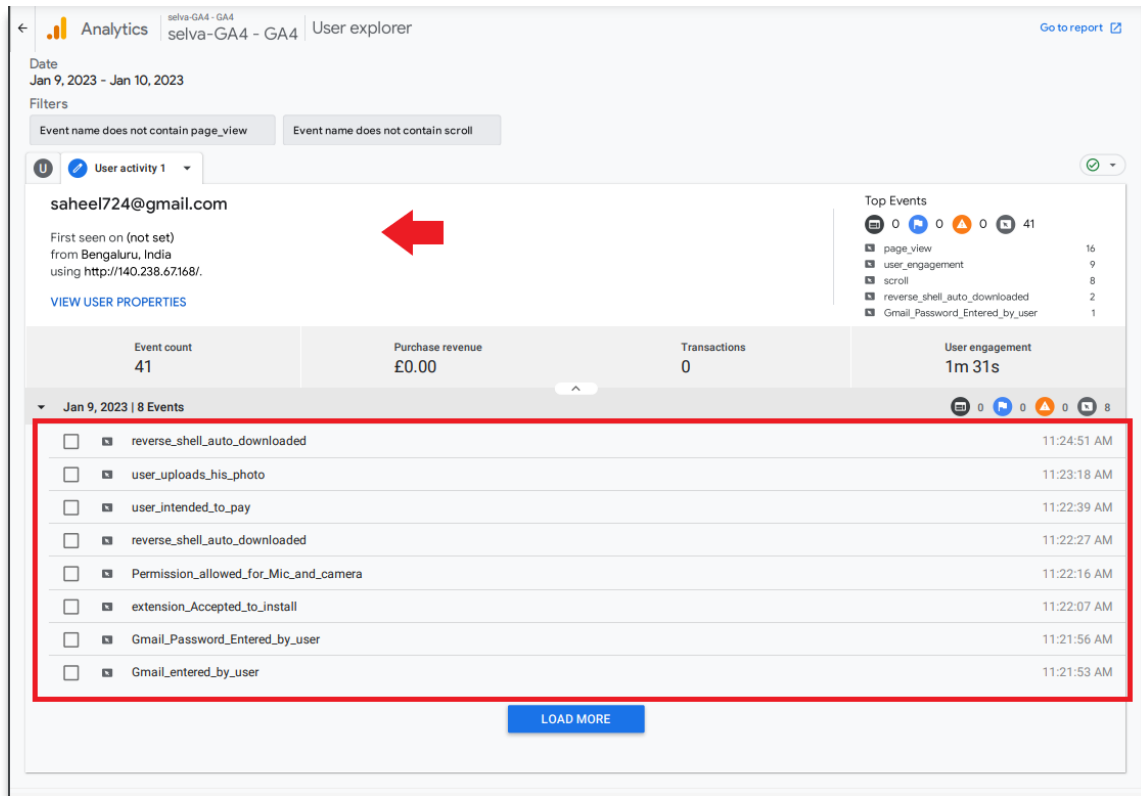


Figure 38: user activity

- Unsafe browser extension install,
- Phishing page asking for Gmail username and password,
- Accessing Camera and Mic without user knowledge,
- Sensitive Information asked by chatbot by user manipulation questions,
- Malicious link clicks,
- Reverse shell install, user intention to pay to untrusted source,
- Uploading personal profiles to untrusted source.

From the above mentioned threats here with this report we see how this user behaved to those threats.

Name: saheel,

Country: India,

This user not aware about google login URL he doesn't has basic knowledge about login mechanism of Google Account he entered his Password in password file that is tracked with

Button ID by google Tag Manger and passwords is not collect form the user. He accepts install browser extension form untrusted source which make series of impacts to his security concern. Permission for mic and camera access is accepted by him in inappropriate scenario which make attacker to spy him. Reverse shell is auto download which show he is not using upgrade browser version, now a days browser are preventing form auto download. This user fall on user manipulation because he intended to pay via bitcoin or PayPal, he has no idea about how trusted payment works. And also he upload he profile photo to untrusted source which is not mandatory, photo can be used to fraud by attackers.

User:2

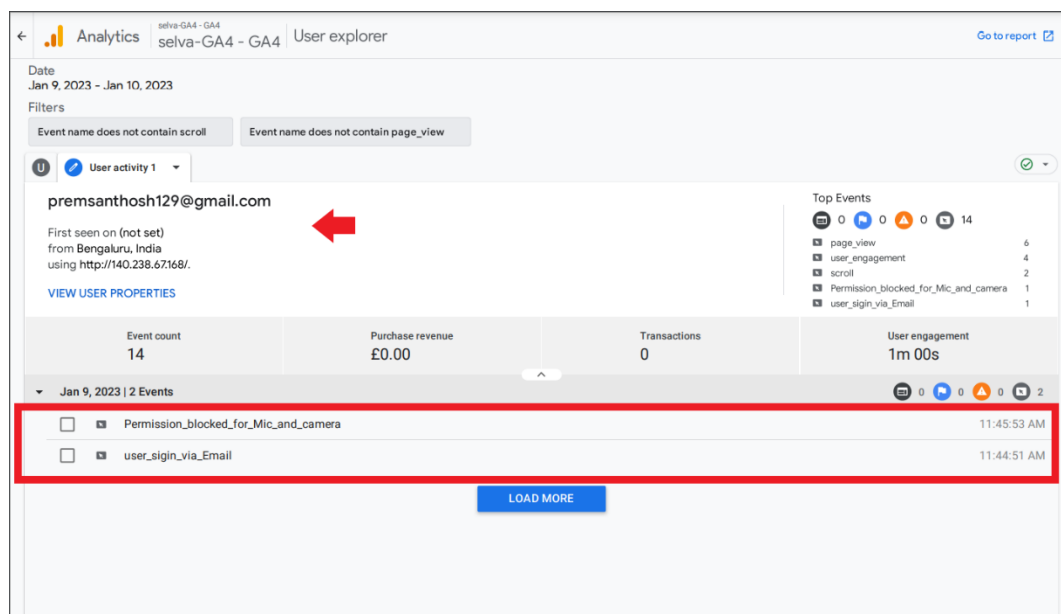


Figure 39: 2nd user Activity

- Unsafe browser extension install,
- Phishing page asking for Gmail username and password,
- Accessing Camera and Mic without user knowledge,
- Sensitive Information asked by chatbot by user manipulation questions,
- Malicious link clicks,
- Reverse shell install, user intension to pay to untrusted source,
- Uploading personal profiles to untrusted source.

From the above-mentioned threats here with this report we see how this user behaved to those threats.

Name: prem Santhosh,

Country: India,

This user is more aware of cyber threats he never falls in any catch in website one best example is he blocked mic and camera access and never accepted browser extension and don't have intension to pay and using updated browser version proven by browser prevented auto download reverse shell.

Note: As for now in this report every individual user result can't analysed. But all the individual users report are attached in source code Zip file.

And after real time evaluation with user, 2 day later feedback is taken from user which is attached below in form of spreadsheet.

<https://docs.google.com/spreadsheets/d/117JZ-WBRLOnPIxT821K0OYpVsfe7p7LAnycggNrHhqzs/edit?usp=sharing>

13.conclusion.

Assessing user's susceptibility and awareness of cybersecurity threats is crucial for ensuring the security and integrity of information systems. In this project, user is evaluated with cyber awareness Realtime model. Here this model is designed in simulated website which is with some common and some uncommon cyber threats which make feel Realtime to the users.

Using Google Tag manager and Google Analytics to track individual user activity in simulated website how they behave to cyber threats, what are actions they are doing, analysing some real time user actions, Application, browser, mobile version and are model are gathered as much not forced to users. Lot of user reports are gathered form Google Analytics with that information users are evaluated. The main moto of this project is to assess the user's cyber awareness about real world cyber threats and based on the evaluation result of individual user, cyber awareness training is given to them. For Example: consider an organisation with certain number of staffs, head of the organisation wants to test their staff's cyber awareness, for that they are planning to deploy real time simulation to test cyber awareness. In this case this project is perfectly suitable to fit in that simulation that organisation expected. With the help of this Project's report each and individual users of the organisation are assessed and based on their activity they are marked with some levels. With those levels, staffs got trained. Level like Low, Medium, High. Low represents staff need less cyber awareness training sessions, for High staff need more cyber awareness training session likewise for medium. This level is set by organisation based on their needs. But the goal of the Project is fulfilled. In future this model will get upgraded by UI, better functionally, even more specify tracking and including more cyber threats loopholes.

References:

1. Kankanhalli, A., Teo, H.H., Tan, B.C. and Wei, K.K., 2003. An integrative study of information systems security effectiveness. *International journal of information management*, 23(2), pp.139-154.
2. Kwak, Y., Lee, S., Damiano, A. and Vishwanath, A., 2020. Why do users not report spear phishing emails. *Telematics and Informatics*, 48, p.101343.
3. Arachchilage, N.A.G. and Love, S., 2014. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behaviour*, 38, pp.304-312.
4. Ikhaila, E., 2017. *A malware threat avoidance model for online social network users* (Doctoral dissertation, Brunel University London).
5. Gupta, B.B., Tewari, A, (2016). Fighting Against Phishing Attacks: State of the Art and Future Challenges.
6. Dhamija, R., Tygar, J.D., Hearst, M.(2006) Why Phishing Works. In Proceedings of ACM Conference on Human Factors in Computing Systems (CHI2006), pp. 581-590.
7. Banday, M.T., Qadri, J.A. (2007) Phishing - A Growing Threat to ECommerce. *The Business Review*,12(2), pp. 76-83.
8. Kirda, E. & Kruegel, C. (2005) Protecting Users against Phishing Attacks with AntiPhish. Available at: http://cs.ucsb.edu/~chris/research/doc/compsac05_antiphish.pdf (Accessed 18 May, 2016).
9. Banday, M.T., Qadri, J.A. (2007) Phishing - A Growing Threat to ECommerce. *The Business Review*,12(2), pp. 76-83.
10. Athulya, A. A., and K. Praveen(2020). "Towards the Detection of Phishing Attacks." 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184). IEEE,.
11. Aleroud, A. and Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, 68, pp.160–196.
12. Carroll, F., Adejobi, J.A. and Montasari, R. (2022). How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society. *SN Computer Science*, 3(2).
13. Marriott, C. (2018). Through the Net: Investigating How User Characteristics Influence Susceptibility to Phishing. [online] www.semanticscholar.org. Available at:

<https://www.semanticscholar.org/paper/Through-the-Net%3A-Investigating-How-User-Influence-Marriott/ff48d13ac16f6f542527a5b355bf02c153338b3c> .

14. Alsufyani, A., Alotaibi, Y., Almagrabi, A.O., Alghamdi, S.A. and Alsufyani, N., 2021. Optimized intelligent data management framework for a cyber-physical system for computational applications. *Complex & Intelligent Systems*, pp.1-13.
15. Li, Y. and Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, [online] 7(7), pp.8176–8186.
16. Kshetri, N. (2018). Cybersecurity and privacy challenges in big data analytics. *Computer*, 51(3), 32-40.
17. Wang, L., Li, X., Li, L., & Lu, J. (2018). A security awareness assessment model based on phishing simulation. *Journal of Network and Computer Applications*, 104, 1-11.
18. Alhabash, S., Chen, Y., & Wise, K. (2018). Social media use, cyber security behavior, and susceptibility to cyber-attacks: An empirical study. *Computers in Human Behavior*, 80, 1-12.
19. Kotzé, P., & Zinn, J. (2016). Cyber security awareness and susceptibility to social engineering attacks: An exploratory study. *Journal of Information Security and Applications*, 26, 1-8.
20. Wang, Q., Liang, Y., Chen, W., & Wang, X. (2018). Investigating the factors influencing individuals' susceptibility to phishing attacks. *Journal of Computer Information Systems*, 58(4), 1-12.

Appendix:

ID and Classess used by Google Tag manager:

google-login.html:

id="Gmail_entered_by_user"

class="btn Password_Entered_by_user"

mainpage.html:

id="extension_Accepted_to_install"

permission.html

id="Permission_allowed_for_Mic_and_camera"

id="Permission_blocked_for_Mic_and_camera"

chatbot.html

id="Sensitive_information_entered_by_user_to_chatbot"

offers.html

id="user_intended_to_pay"

login-option.html

class="social-button user_signin_via_google"

class="social-button user_signin_via_Email"

chechout.html

id="user_clicked_malicious_link"

index.html

id="reverse_shell_auto_downloaded"

3d.html

id="user_uploads_his_photo"

Steps for Deploying this project:

Note : Please refer topic “Steps to Third Person Redeploy this cyber awareness Model” in report for deploying this project with screenshot references.

- ☐ Host the website simulation in dedicated server or any hosting providers as your wise.
- ☐ Create a Google Analytics account and property for your website.
- ☐ Create a Google Analytics tag in Google Tag Manager and create container in it with IP or Domain of the hosted website.

☐ And next import the Tag configuration file to Google Tag Manger which is attached in source code zip file.

1. Open container-> Admin->Import Container.

☐ Now all configurations are imported to Tag manager. Final step to complete the setup is change the measurement ID with your Google Analytics Measurement ID.

Note: Measurement ID must replace with yours google analytics measurement ID.

Steps to get measurement ID in google analytics:\

☐ Sign into your Google Analytics account.

☐ Under the "Account" column, select "Create Property."

☐ Fill in the details for the property you wish to create, including the website name, website URL, and industry category.

☐ Select the data sharing settings that you prefer.

☐ Click on the "Create" button to create the property.

☐ Now Select the website property that created now to get the measurement ID for.

☐ Click on "Admin" in the bottom left corner of the screen.

☐ Under the "Property" column, click on "Data stream" and click on property name snow.

☐ The measurement ID will be listed. It will be a string of letters and numbers in the format "UA-XXXXX-Y."

India:

sahil- saheel724@gmail.com

padmavasan- padmavasan777@gmail.com

shanmuga - shanmugapriyandlite@gmail.com

mukesh - amukeshanna367@gmail.com

prem santhosh - premsanthosh129@gmail.com

yuvan - yuvansankar982@gmail.com

Singapore

veera kabilan- veerakabilan1999kani@gmail.com

UK

vijayandiran - vijayandiran25@gmail.com

yugesh - ykmi1427@gmail.com

gowtham - gowthamd95@gmail.com

← → ↻ tagassistant.google.com/#/?source=TAG_MANAGER&id=GTM-54B4T8F>m_auth=pYkkdpkBCcky-5VWPwxTYA>m_preview=env-5&cb=232283

Connected 140.238.67.100

Summary > Google Analytics GA4 Configuration

2 Google tags

Summary

▼ Mian Page

23 Window Loaded

22 DOM Ready

21 Container Load

20 Initialization

19 Consent Initiali

▼ google-login.h

Tag Details

Properties

Name	Value
Type	Google Analytics: GA4 Configuration
Fields to Set	<pre>[{name: "debug_mode", value: "true"}, {name: "user_id", value: "selvaguru2017@gmail.com"}]</pre>
User Properties	<pre>[{name: "user_id_dim", value: "selvaguru2017@gmail.com"}]</pre>
Send a page view event when this configuration loads	true
Send to server container	false
	Show More

← → ↻ tagassistant.google.com/#/?source=TAG_MANAGER&id=GTM-54B4T8F>m_auth=pYkkdpkBCcky-5VWPwxTYA>m_preview=env-5&cb=232283

Connected 140.238.67.100

Summary > Google Analytics GA4 Configuration

2 Google tags

Summary

▼ Mian Page

23 Window Loaded

22 DOM Ready

21 Container Load

20 Initialization

19 Consent Initiali

▼ google-login.h

Tag Details

Properties

Name	Value
Type	Google Analytics: GA4 Configuration
Fields to Set	<pre>[{name: "debug_mode", value: "true"}, {name: "user_id", value: "selvaguru2017@gmail.com"}]</pre>
User Properties	<pre>[{name: "user_id_dim", value: "selvaguru2017@gmail.com"}]</pre>
Send a page view event when this configuration loads	true
Send to server container	false
	Show More


← → ↻ Not secure | 140.238.67.168/index.html

REDSTORE


Products category Offers Customer services Account

All Products


Default Shorting




Red Printed T-shirt
₹,500.00



Red Printed T-shirt
₹,500.00



Red Printed T-shirt
₹,500.00



Red Printed T-shirt
₹,500.00

+

← → ↻ Not secure | 140.238.67.168/product-autodownload.html

NIKE SHOES

[VISIT NIKE STORE](#)

4.7(21)

Old Price: \$267.00
New Price: \$249.00 (5%)

About This Item:


Lorem ipsum dolor sit amet consectetur adipisicing elit. Illo eveniet veniam tempora fuga tenetur placeat sapiente architecto illum soluta consequuntur, aspernatur quidem at sequi ipsa!

Lorem ipsum dolor sit amet consectetur adipisicing elit. Consequatur, perferendis eius. Dignissimos, labore suscipit. Unde.

- ✓ **Color:** Black
- ✓ **Available:** in stock
- ✓ **Category:** Shoes
- ✓ **Shipping Area:** All over the world
- ✓ **Shipping Fee:** Free

1 [Add to Cart](#) [Compare](#)

Share At: ○ ○ ○ ○ ○ ○



reverse-shell (1).exe

← → ↻ tagmanager.google.com/#/container/accounts/6066355425/containers/99381445/workspaces/30/triggers

Tag Manager

Workspace Versions

CURRENT WORKSPACE

Default Workspace

- Overview
- Tags
- Triggers
- Variables
- Folders
- Templates

Untitled Trigger

[Save](#)

Trigger Configuration

Trigger Type

☒ Click - Just Links

☐ Wait for Tags

☐ Check Validation

This trigger fires on

☐ All Link Clicks ☒ Some Link Clicks

Fire this trigger when an Event occurs and all of these conditions are true

Click ID	contains	extension_Accepted_to_install	-	+
----------	----------	-------------------------------	---	---