Written report

The Science of Scams

Joshua Heng (leader) 3A3, Foo Hai Jang 3A3, Lu Junjie 3A3, and Tan Jun Huan 3P1

Introduction

a. Rationale

Internet scams are when cybercriminals target unsuspecting individuals and deceive or trick them in order to illegally obtain money or steal personal information. According to CNA, S$201,000,000+ was lost to scams with a total of 15756 reported cases by 2021. Internet scams have huge impacts on individuals.

1. Psychological - Some people may be very paranoid and have trust issues. They may also blame themselves and feel guilty for falling victim to scams. In addition to financial losses, some may feel depressed.
2. Emotional - People may feel stressed or may face anxiety as the amount lost is significant.
3. Behavioral - As they are more paranoid, many will avoid doing activities that they once did just to avoid getting scammed again, example, Online shopping.

b. Idea Description

We want to make infographics to show our analysis of the scam data and make them accessible to the public through packaging it in our website that also includes other information or conclusions that we have found.

c. Focus and Significance of Project

As shown in our rationale, scams are a serious problem in the world, thus our focus is to analyse the trends of scams, find more factors, present the data, raise awareness and hopefully reduce scam rates. Our focus for scams and target audience is stated in our project scope below.

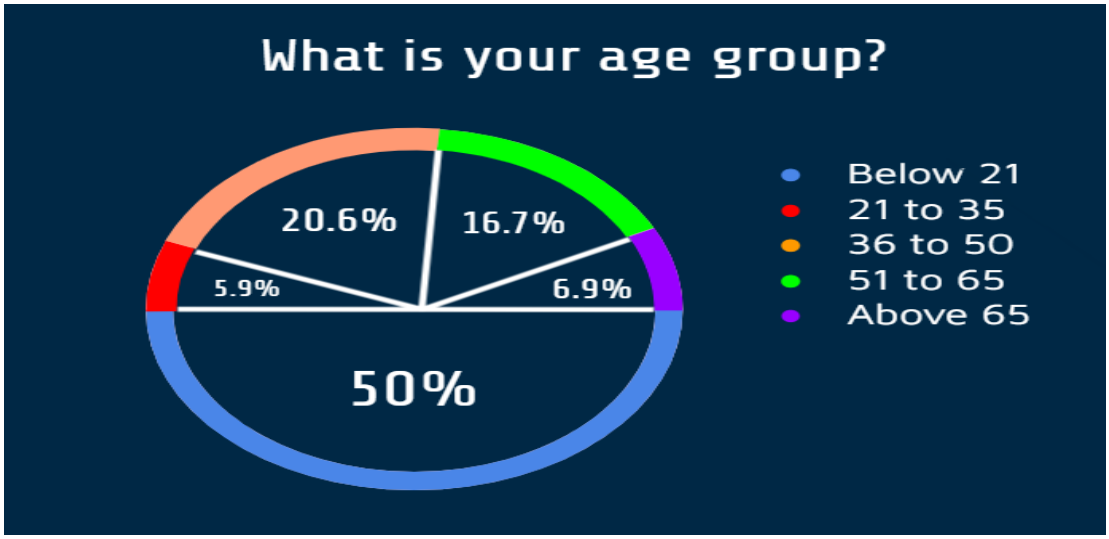
d. Project Scope

Dating and romance, investment, e-commerce and phishing scams. We have no target audience as everyone is vulnerable to scams.

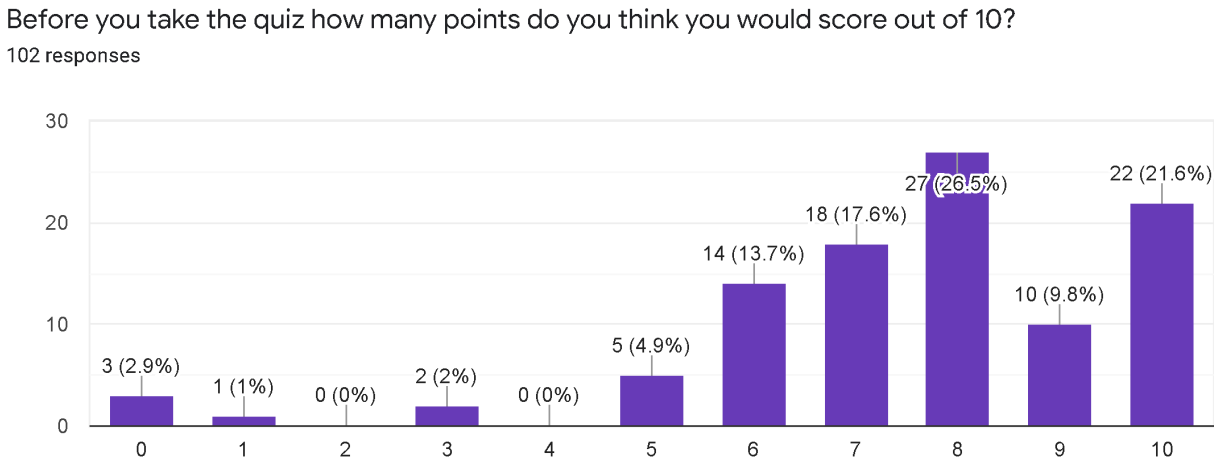
Literature Review

For our literature review, we looked at other websites which feature scam statistics, which were the Australian Competition and Consumer Commission(ACCC) and Scam Alert from Singapore. We also did a survey to ensure the need of our project.

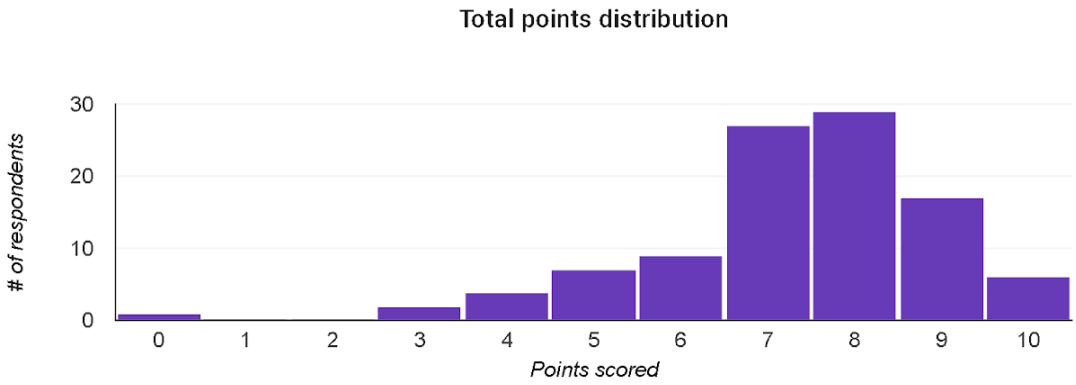
As talked about in the introduction, scams are growing, so we decided to do a survey to confirm the need of our project. Our survey consisted of MCQ questions which put the person in different scenarios, allowing them to choose what they thought was the right choice to not get scammed. The demographics of people who took our survey are shown below.



Below are the main points of the survey that we would be covering.

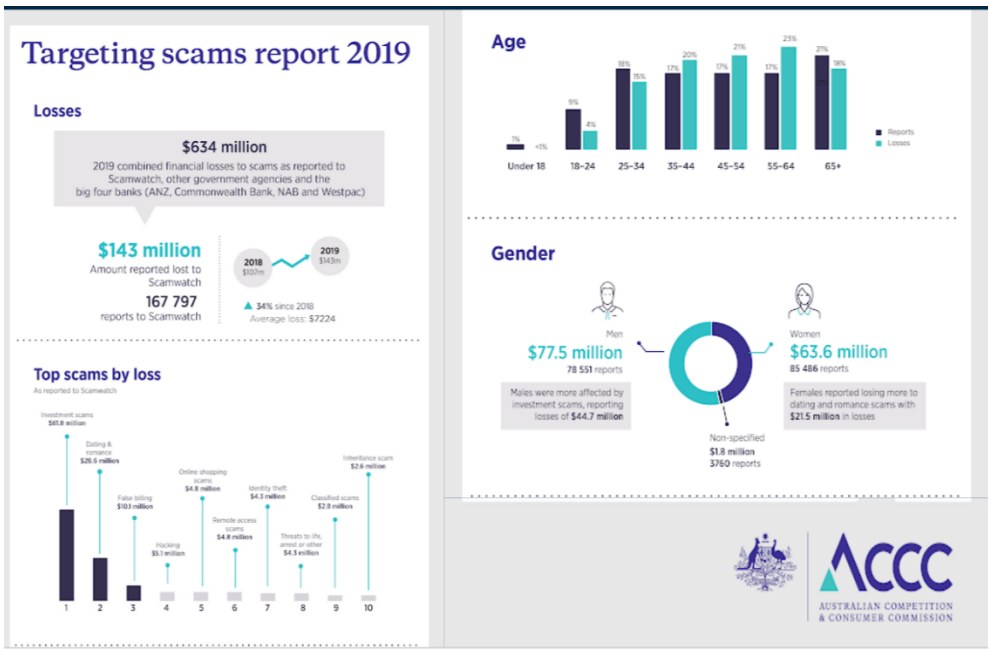


Average	Median	Range
7.3 / 10 points	8 / 10 points	0 - 10 points

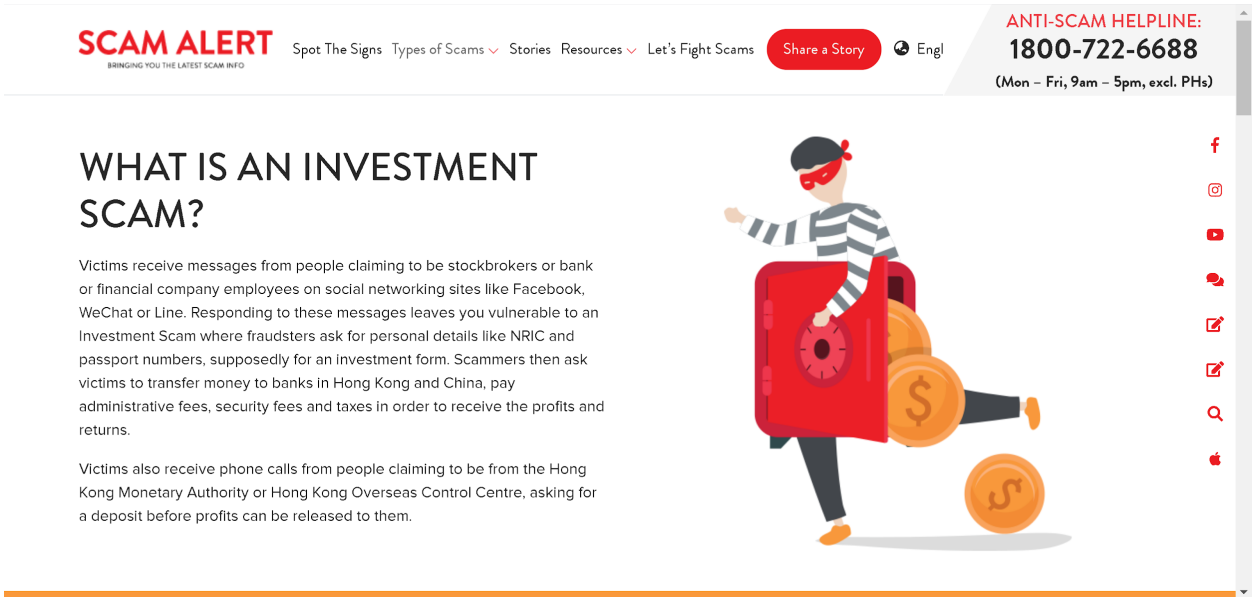


From the first image, we can see that 22 people thought that they would get 10/10 for the survey. However, the second image shows that only 6 people got 10. In total, 22 people overestimated their scores. This shows that people may overestimate their ability to avoid and detect scams, making them more complacent and vulnerable to scams. The quiz consists of only MCQs and some of the answers are easy or quite obvious. If this was translated to real life scenarios, only 6 people will not have been scammed. The rest who did not score 10 could have potentially been scammed. This shows many people are still vulnerable to scams.

Next, we looked at other websites which featured scam statistics to find out the areas of improvements. The first website was the ACCC.



The infographic provided above states the money lost and the number of reports among different age groups and gender in 2019. It shows the scam the genders are most affected by, such as males are more affected by investment scams.



The second website, Scam Alert is a Singapore government website which educates people on scams. It serves as a means for scam victims and others to raise awareness on scams through sharing. However, the demographics are not provided and those who shared their experiences were anonymised.

In general, both websites did not compare age groups to the types of scams, the data provided was too general. The websites also looked at many types of scam which did not allow them to focus and show detail for certain scams. We would like to improve on these areas by showing more comparisons and analysis of scam data and maybe provide a projected or expected trend of scams through data analysis. We also want to narrow the scope to focus on the main scams that people face and provide analysis of them.

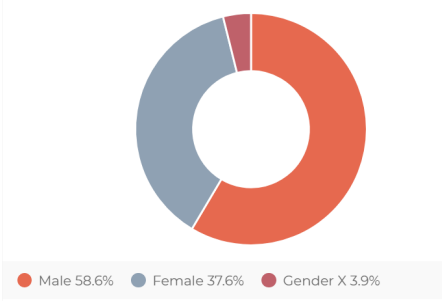
The Study & Methodology

a. Methodology

Our project uses data published by the Australian government's website, Scam Watch, as it provides a comprehensive range of statistics on scams from January 2018 to June 2021. Scam Watch includes data such as the date, and the age and gender of victims, on over 30 different types of scams, including the 4 types of scams that we chose for our scope. As such, this website was suitable as our data source as it is reliable and complete.

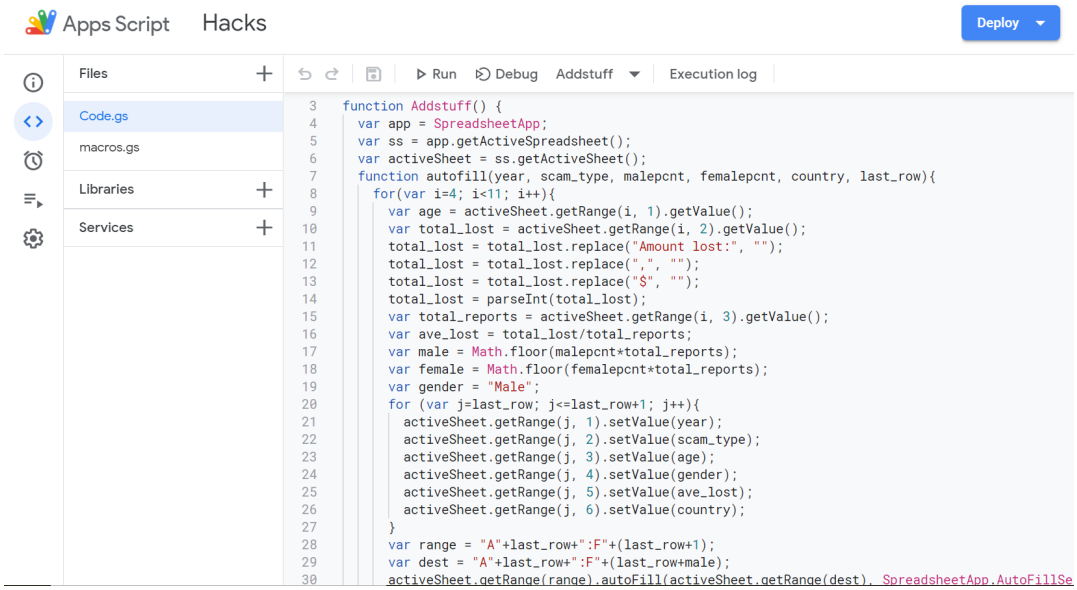
Age	Amount lost	Number of reports
Under 18	Amount lost: $34,068	196
18 to 24	Amount lost: $1,670,171	1,425
25 to 34	Amount lost: $4,274,051	3,918
35 to 44	Amount lost: $4,007,593	3,947
45 to 54	Amount lost: $3,470,773	3,620
55 to 64	Amount lost: $7,213,856	3,570
Over 65	Amount lost: $5,282,412	4,388

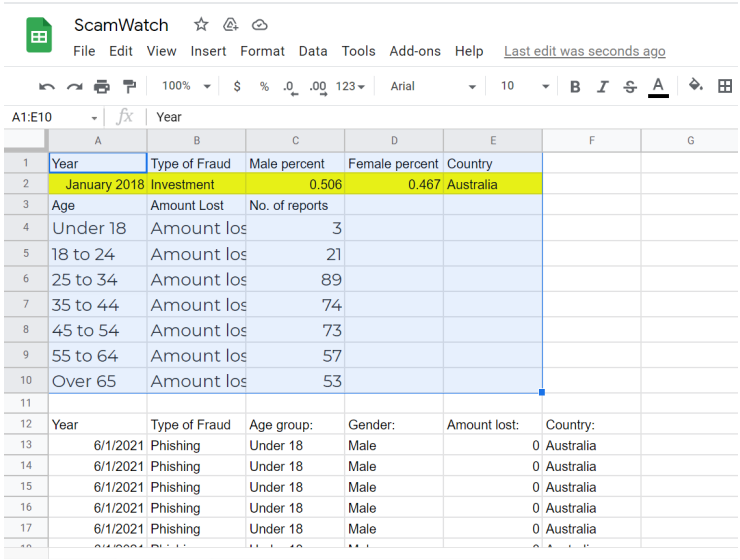
Gender - number of reports



Gender	Number of reports	Percentage
Male	441	58.6%
Female	283	37.6%
Gender X	29	3.9%

However, no raw data was provided and we also could not get the individual cases. As such, we improvised to transform and split the data into individual cases through the use of google sheets' script editor.





	A	B	C	D	E	F	G
1	Year	Type of Fraud	Male percent	Female percent	Country		
2	January 2018	Investment	0.506	0.467	Australia		
3	Age	Amount Lost	No. of reports				
4	Under 18	Amount los	3				
5	18 to 24	Amount los	21				
6	25 to 34	Amount los	89				
7	35 to 44	Amount los	74				
8	45 to 54	Amount los	73				
9	55 to 64	Amount los	57				
10	Over 65	Amount los	53				
11							
12	Year	Type of Fraud	Age group:	Gender:	Amount lost:	Country:	
13	6/1/2021	Phishing	Under 18	Male	0	Australia	
14	6/1/2021	Phishing	Under 18	Male	0	Australia	
15	6/1/2021	Phishing	Under 18	Male	0	Australia	
16	6/1/2021	Phishing	Under 18	Male	0	Australia	
17	6/1/2021	Phishing	Under 18	Male	0	Australia	

By inputting the provided data (as shown previously above) in this format and running the macro, the google sheets will automatically split the data into individual cases using an algorithm and input it into the rows below. As such, this made the data suitable for analysis and representation.

b. Research method

Data source: scamwatch.gov.au
Developmental tools: Wix.com (website), Rstudio (data analysis) and Tableau (representation of data), Google sheets and App Script (Data cleaning)

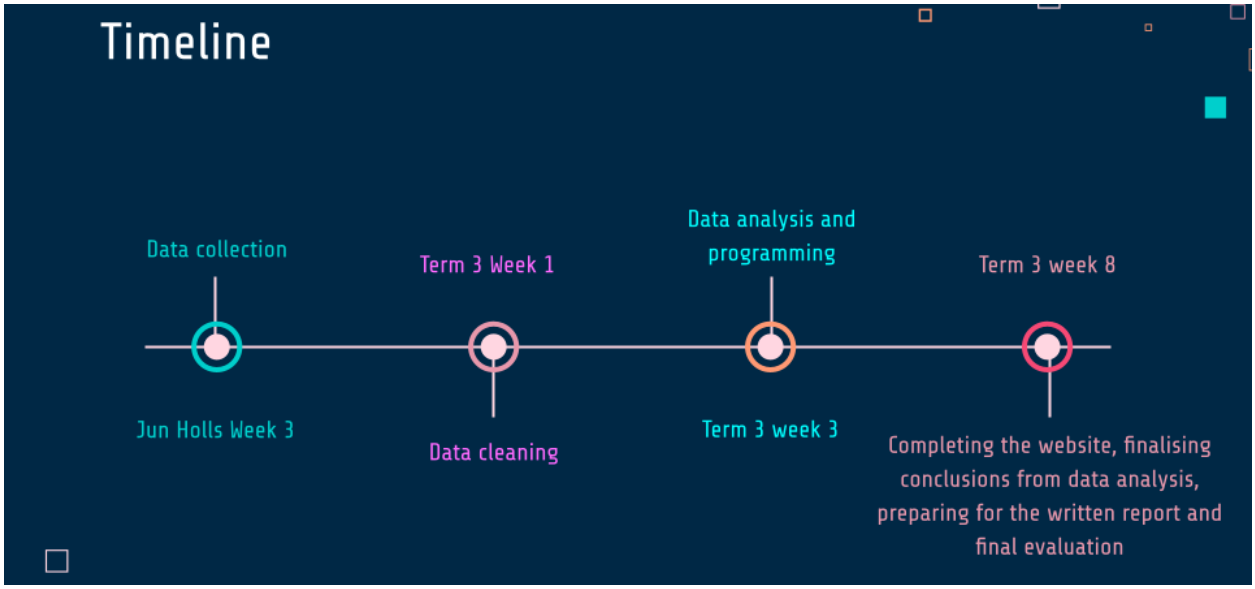
c. Job distributions

Joshua: Rstudio analysis and cleaning of data
Hai Jang: Tableau and finding data
Jun Jie: Tableau and finding data

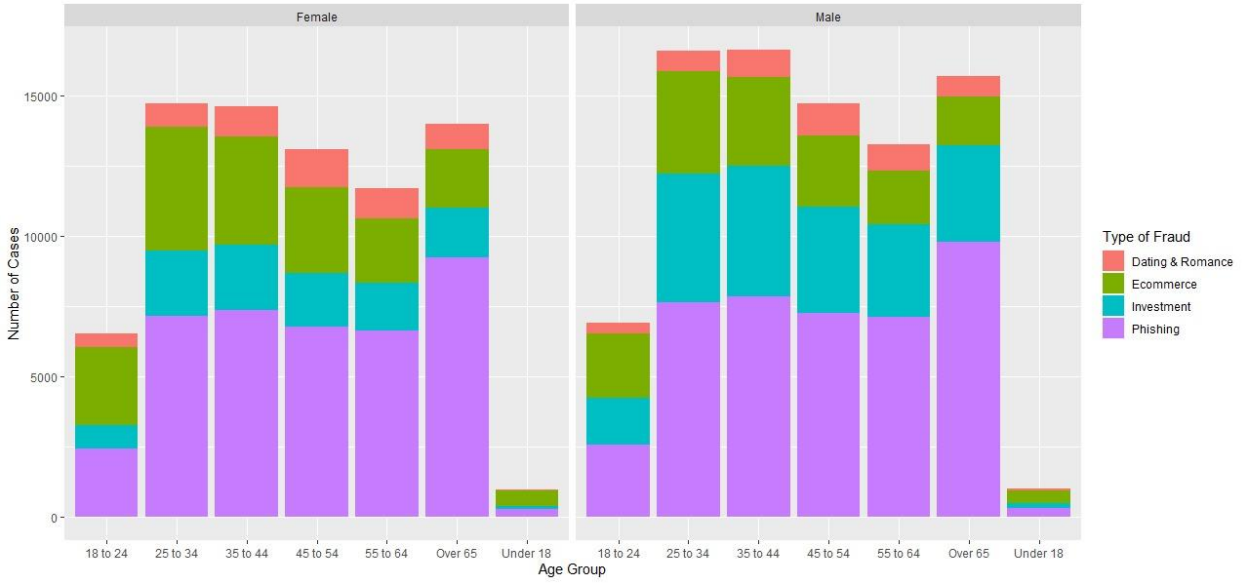
Jun Huan: Website and finding data

d. Timeline

By term 2 week 3, we prepared the slides for our initial project proposal. We decided to collect and begin cleaning up the data in term 2 week 10. Initially, we wanted to complete 70% of the infographic and prepare for the mid-term report by term 3 week 2. However, a problem resulted in us slightly tweaking the topic. By term 3 week 8, we finalised the conclusions of data and the infographic was ready. We also prepared the written report for final evaluation.

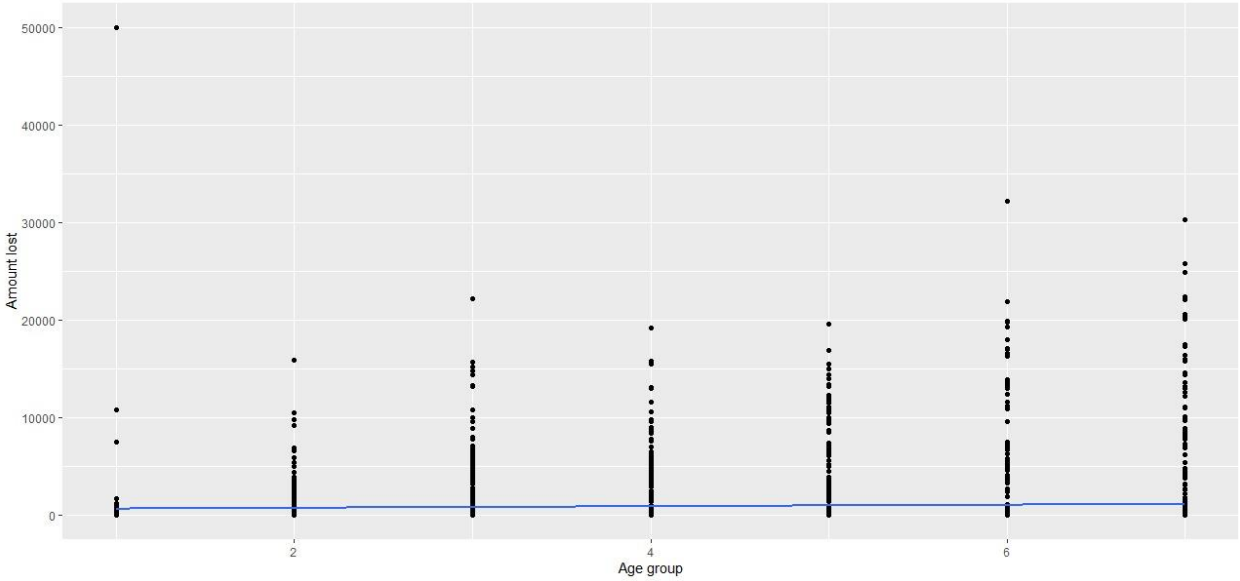


Outcomes, Analysis & Discussions

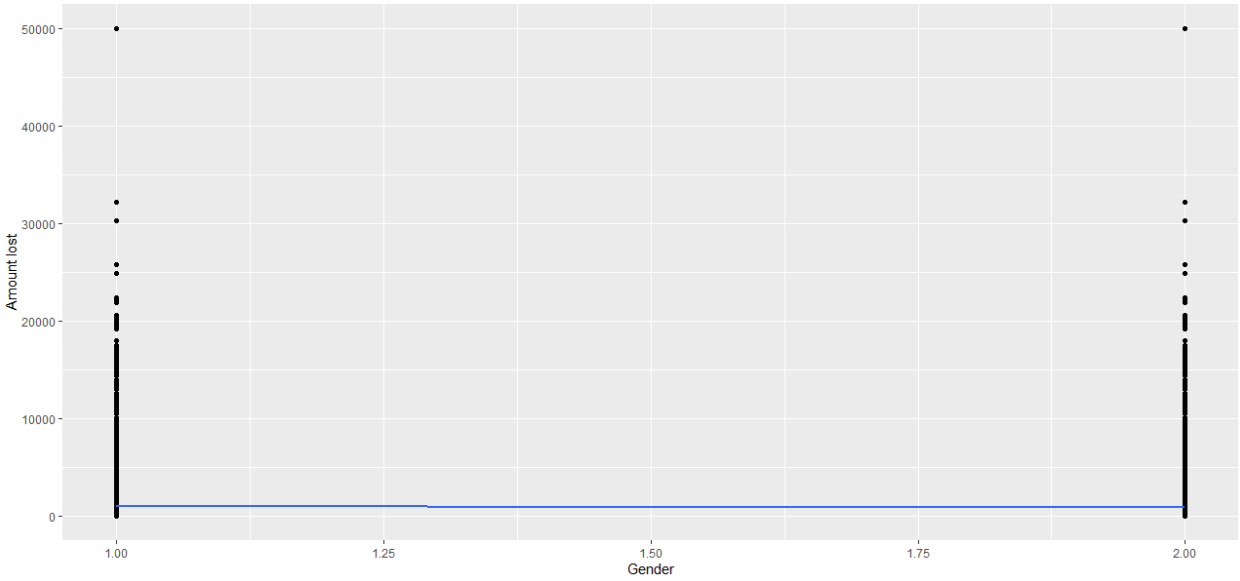


This is a bar graph depicting the number of cases of each type of fraud that people of different ages fall into . From this graph, we can see that phishing scams is the most prevalent category of

scams for people of 25 and above followed by investment and commerce before dating and romance. For people ranging 24 and below, they are more likely to fall for ecommerce scams, followed closely by phishing scams and then dating and romance. The results tend to be similar for both genders under 24 but for above 24, females are more likely to fall for ecommerce scams while men tend to fall for investment. Hence, people should be better educated on phishing and ecommerce scams as they as they are two of the most prevalent scams.

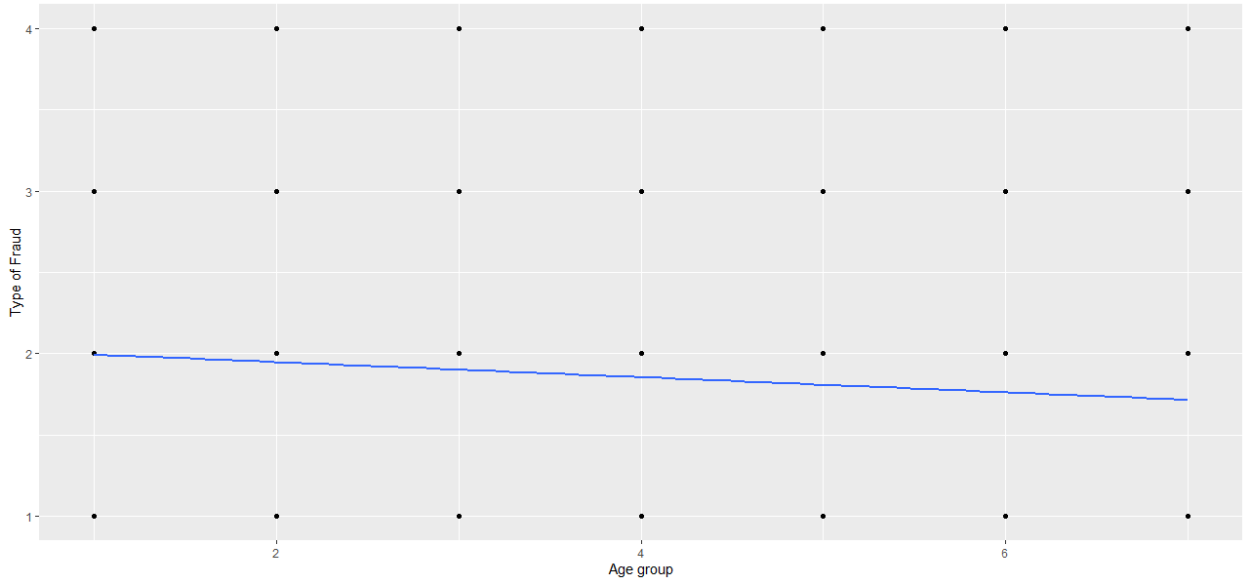


The above is a point graph depicting the losses that people of different age groups are most likely to fall under. The numbers represent the different age groups - 1 represents those under 18, 2 represents those 18 to 24, and so on, with 7 being those over 65. The graph has a best fit line showing the general trend of the amount lost as the age group increases. The best fit line has a steep positive gradient which is not apparent due to the axises. This shows that as the greater the age of an individual, the more money they would lose were they to fall for a scam.

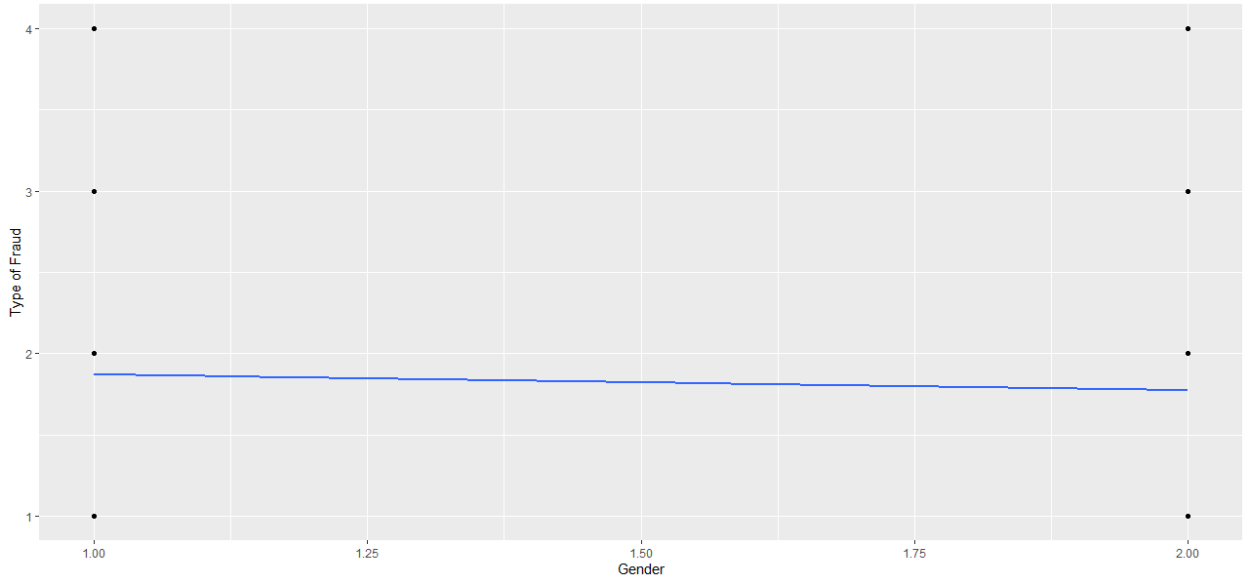


The above is a graph showing the correlation between gender and the amount lost. 1 represents male, while 2 represents female. The graph also has a best fit line with a negative gradient, which

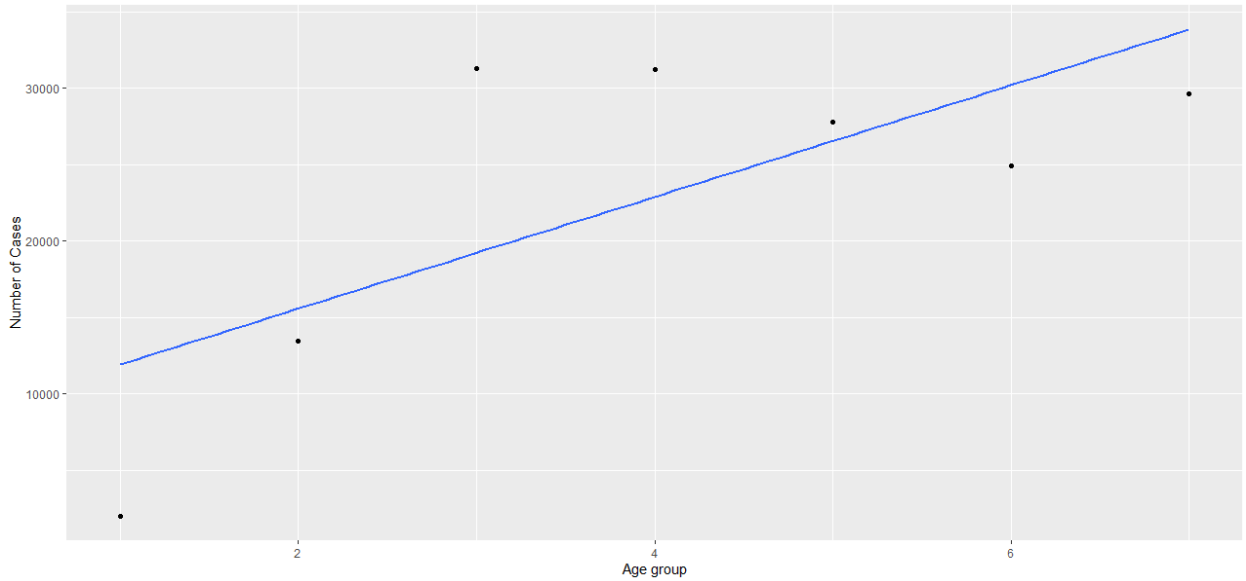
is also hard to see due to the axises of the graph. The graph shows that males tend to lose less money to scams than females.



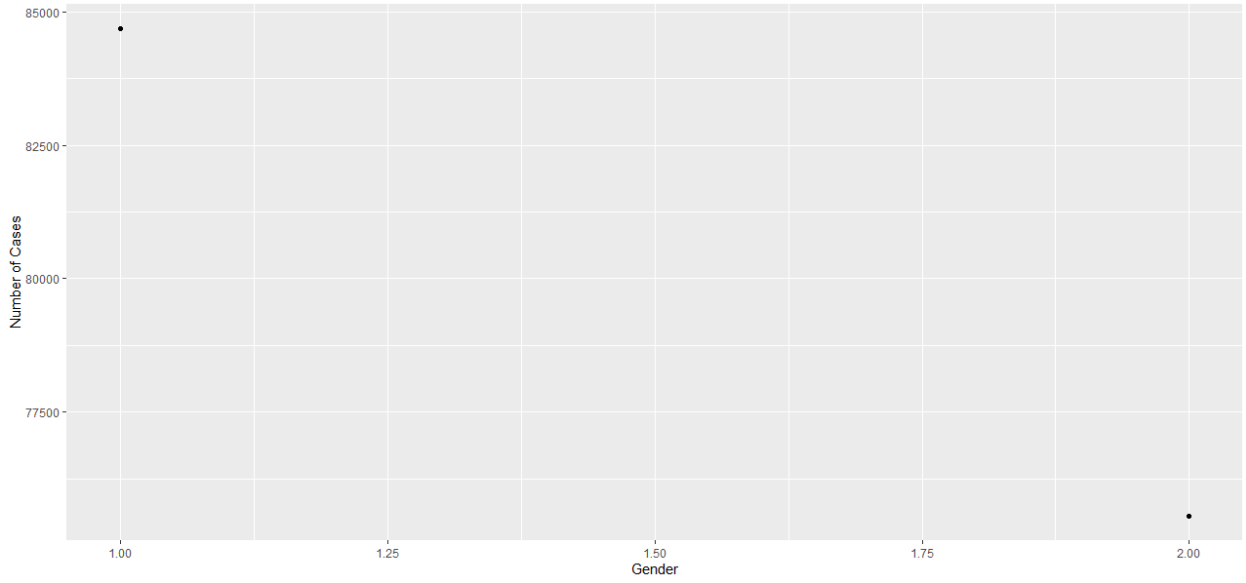
The above graph shows the correlation between the age group and the type of fraud. The type of fraud. 1 is Phishing, 2 is Ecommerce, 3 is Investment and 4 is Dating & Romance scams. The age groups are represented the same as before. The graph has a best fit line with a negative gradient. The graph shows that younger people are more susceptible to Ecommerce scams, while more older people fall for Phishing scams.



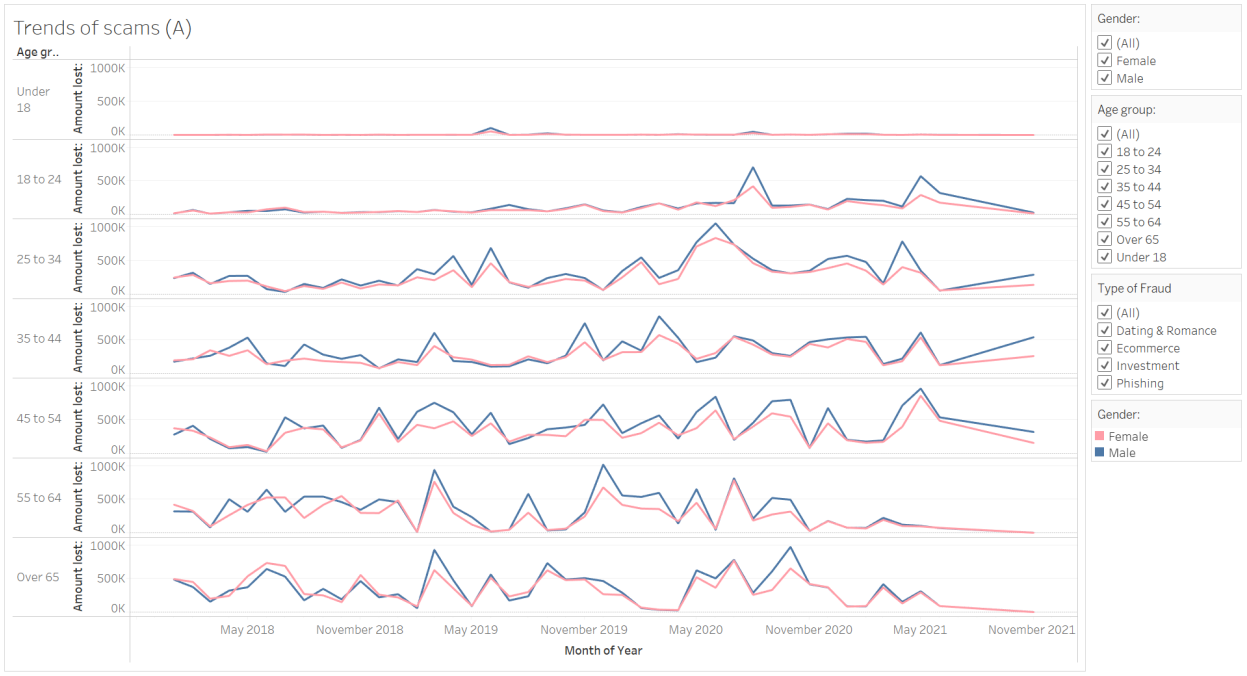
The above graph shows the correlation between the gender of victims and the type of fraud. The graph shows that males are more vulnerable to e-commerce scams than females, and females are more likely to fall for phishing scams than males.

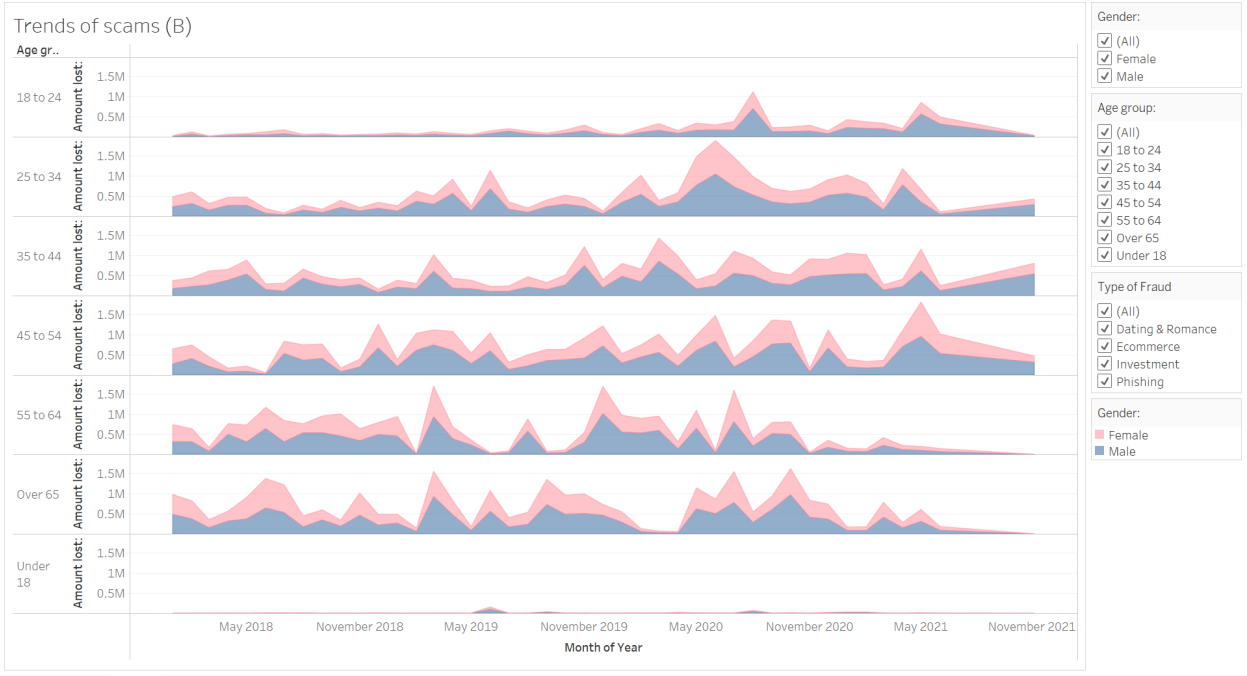


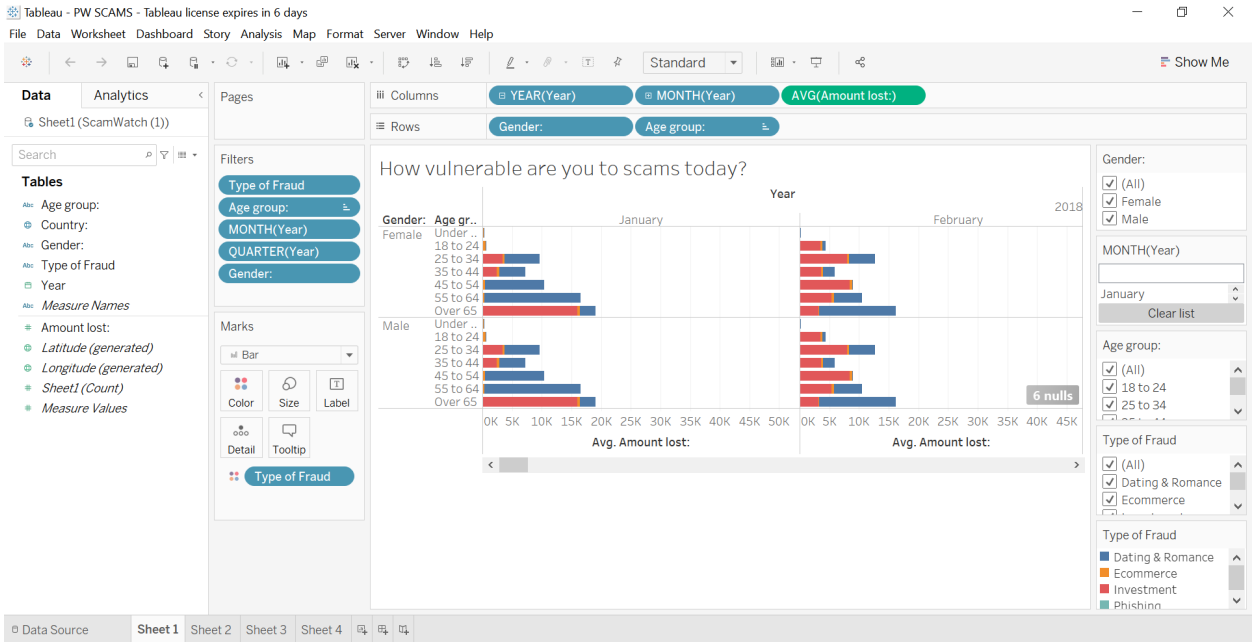
The above graph shows the correlation between the number of cases and the age group of victims. The graph shows a steep upward trend represented by the best fit line. This shows that older people, especially those over 65, are more likely to fall for scams than younger people.



The above graph shows the number of cases of scam reports by both males and females. The graph shows that males are scammed more often than females.

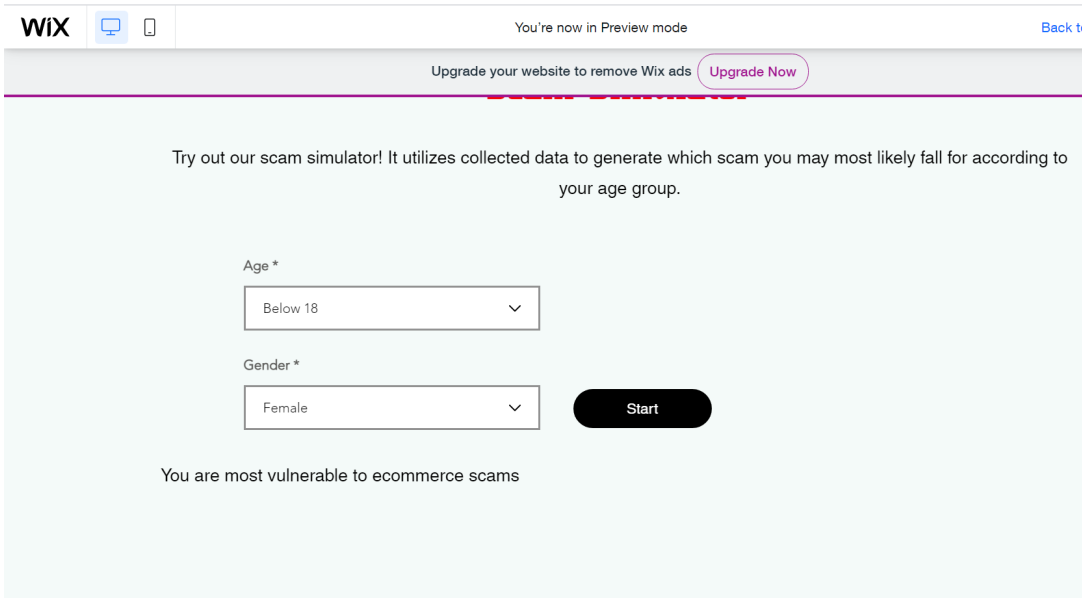

Trends of scams (A)
Age gr..
Under 18
18 to 24
25 to 34
35 to 44
45 to 54
55 to 64
Over 65
Amount lost:
1000K
500K
0K
May 2018
November 2018
May 2019
November 2019
May 2020
November 2020
May 2021
November 2021
Month of Year
Gender:
(All)
Female
Male
Age group:
(All)
18 to 24
25 to 34
35 to 44
45 to 54
55 to 64
Over 65
Under 18
Type of Fraud
(All)
Dating & Romance
Ecommerce
Investment
Phishing
Gender:
Female
Male
Sheet 1
Sheet 2
Sheet 3
Sheet 4

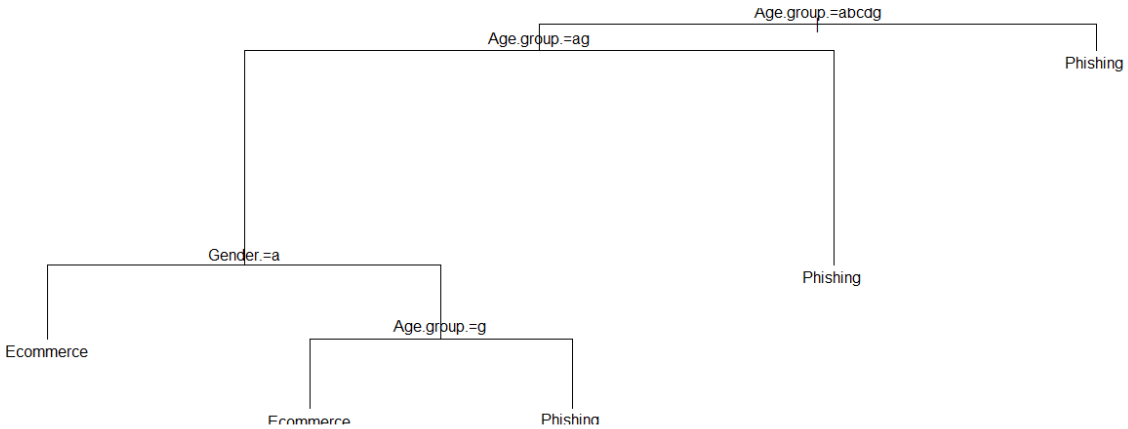

Trends of scams (B)
Age gr..
18 to 24
25 to 34
35 to 44
45 to 54
55 to 64
Over 65
Under 18
Amount lost:
1.5M
1M
0.5M
May 2018
November 2018
May 2019
November 2019
May 2020
November 2020
May 2021
November 2021
Month of Year
Gender:
(All)
Female
Male
Age group:
(All)
18 to 24
25 to 34
35 to 44
45 to 54
55 to 64
Over 65
Under 18
Type of Fraud
(All)
Dating & Romance
Ecommerce
Investment
Phishing
Gender:
Female
Male
Sheet 1
Sheet 2
Sheet 3
Sheet 4



The above are various tableau graphs we used to help people search what scams they may be vulnerable to. Using the bar on the right hand side, users are able to sort for their age and gender and hence use the graph to study the trends of victims of their age and gender group. The colour coded fraud types also allows them to check which fraud type they are most prone to and thus alert them and allow them to be more aware of potential scams and frauds.

This is a decision tree which we used to find the trends of scams and who are most likely to fall for what scam.
This graph is useful for showing what each age group is at most risk to. For example, females under 18 are more likely to fall for ecommerce scams while males below 44 and over 65 are prone to phishing scams. Thus, awareness on the various types of scams should be raised to individuals of different categories in ways such as broadcasting, advertising and education so as to reduce the scam rates.





The above is the interactive element of our webpage which collects the age group and gender of users to find the scam they are most vulnerable to using the decision tree. Age group a represents those under 18, b represents those 18 to 24, and so on. Gender A is female, B is male. The interactive element and decision tree raises awareness, allowing people to be more vigilant when it comes to the scams they are most vulnerable to and thus lowering their chances of getting scammed.

Implications and Recommendations

a. Challenges

We could not find data with enough information that we needed. We even tried reaching out to SPF for data but were rejected. Scraping the data from online was a challenge as we had to find the sources with the information needed. Lastly, analysing and organizing the data was difficult as we had to keep playing around and trying different methods of getting the desired

outcome.

b. Areas for Improvement

Before we begin preparing for the initial project proposal, we should sort out some of the data first so that we do not need to be worried about the inability to obtain adequate data later. We should also ensure that we start slightly earlier so that we have more time to experiment with our data and hopefully bring up better results.

Conclusion

We learnt how to collect the data from different sources such as taking raw data files from websites or scraping the internet for data. We then learnt how to use the different softwares to clean, present or analyze our data. From the various graphs we have created, we can see a recurring trend - The people aged 65 and above are the most prone to scams in general, and adults above the age of 18 all victim to phishing scams more often than any other scam. Young people under the age of 18 are more prone to e-commerce scams. While greater emphasis should be placed on these scams in raising awareness and public education, the other types of scams should not be disregarded as they also have significant impacts on individuals.

Citations

Home | Scamwatch. (2021). Retrieved 7 August 2021, from https://www.scamwatch.gov.au

More than S$201 million cheated in top 10 scam types last year: Police. (2021). Retrieved 7 August 2021, from https://www.channelnewsasia.com/news/singapore/more-than-201-million-cheated-top-10-scam-types-2020-police-14145720

Graham, D. (2021). Employment-Related Scams Are On The Rise: Learn How To Protect Yourself. Retrieved 7 August 2021, from https://www.forbes.com/sites/dawngraham/2020/08/04/employment-related-scams-are-on-the-rise-learn-how-to-protect-yourself/?sh=2e8a357b77e5

(2021). Retrieved 7 August 2021, from https://www.routledge.com/rsc/downloads/9781138931206_-_chapter_4.pdf

The psychology of scams: why do people fall for cyber scams? | Howden Singapore. (2021). Retrieved 7 August 2021, from https://www.howdengroup.com/sg-en/why-phishing-works

Police Warns of WhatsApp Messages from Pretty Ladies from Hong Kong Pretending to be Your Friend. (2021). Retrieved 7 August 2021, from https://goodyfeed.com/whatsapp-lady-scam/

ScamAlert - Bringing you the latest scam info. (2021). Retrieved 7 August 2021, from https://www.scamalert.sg/

Australian Competition and Consumer Commission. (2021). Retrieved 7 August 2021, from https://www.accc.gov.au/

(2021). Retrieved 7 August 2021, from https://www.accc.gov.au/system/files/1657RPT_Targeting%20scams%202019_FA.pdf

RStudio | Open source & professional software for data science teams. (2021). Retrieved 7 August 2021, from https://www.rstudio.com/

Tableau: Business Intelligence and Analytics Software. (2021). Retrieved 7 August 2021, from https://www.tableau.com/

Singapore Police Force (SPF) | Home. (2021). Retrieved 7 August 2021, from https://www.police.gov.sg/