****

**Raised awareness helps detecting & preventing online shopping scams**

Submitted by

**Mayank Nauni**

Thesis Advisor

**Dr. Pieter Hartel**

**Mr. Jaddoo Yeaz Elias**

**Information Systems Technology and Design**

**(ISTD)**

A thesis submitted to the Singapore University of Technology and Design in fulfilment of the requirement for the degree of Master of Science in Security by Design.

**2022**

**SUBMISSION OF THESIS FOR EXAMINATION**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PART I – TO BE COMPLETED BY STUDENT**  *(After completing Part I of this form, submit it to your main advisor together with your thesis)* | | | | | |
| Name: | Mayank Nauni | | | | |
| Student ID: | 1004741 | | Date of Admission: | | 1st September 2019 |
| Programme of Study  *(please tick one):* | √   |  |  |  |  | | --- | --- | --- | --- | |  | PhD in |  | Master of Science (MSc) |  |  |  | | --- | --- | |  | Architecture and Sustainable Design (ASD) | |  | Engineering Product Development (EPD) | |  | Engineering Systems and Design (ESD) | | √ | Information Systems Technology and Design (ISTD) | | | | | |
| Title of Thesis: | *Raised awareness helps detecting & preventing online shopping scams* | | | | |
|  |  | | | | |
| *(The number of words for Master, PhD thesis and HTC submission should not exceed 40,000, 50,000 and 80,000 respectively)*  I confirm the following:   * I hereby certify the content of this thesis is the result of work done by me and has not been submitted for higher degree to any other University or Institution. * I hereby grant SUTD the permission to reproduce and distribute publicly paper and electronic copies of this thesis document in whole or in part in any medium now known or hereafter created in accordance with Policy on Intellectual Property, clause 4.2.2. * I have fulfilled all requirements as prescribed by the University and provided 1 copy of my thesis in PDF. * The thesis \*does/ does not (\*circle one) contain patentable or confidential information; and that I have not communicated with any examiners on matters related to the thesis examination. * I certify that the thesis has been checked for plagiarism via turnitin/ithenticate. The score is \_\_**7**\_\_\_\_\_%. | | | | | |
| Signature: | |  | Date: | 09-August-2022 | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PART II – TO BE COMPLETED BY MAIN ADVISOR & CO-ADVISOR (IF ANY)**  *(Applicable for Master Programme only)* | | | | | |
|  | I, the main advisor certify that the thesis has been checked for plagiarism via turnitin/iThenticate.  I certify that the thesis is in a form ready and acceptable for examination and confirm the thesis title. The student is to be awarded the Master of Science in Security by Design degree based on the thesis submitted for examination. The student has passed fulfilling the requirements satisfactorily.  I certify that the declaration made by the student is correct.  I certify that the student did not pass. | | | | |
|  |
| Name / Signature of Main Advisor: | | |  | Date\*: |  |
| Name / Signature of Co-Advisor: | | |  | Date\*: |  |
| Name / Signature of Co-Advisor: | | |  | Date\*: |  |
| Name / Signature of Independent Reviewer | | |  | Date\*: |  |

*\*For Master of Engineering (Research) scholarships, the last day of scholarship award will be based on this date.*

|  |
| --- |
| Comments:  *(If the space provided is insufficient, please provide a copy of your comments on a separate piece of paper)* |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PART III – TO BE COMPLETED BY MAIN ADVISOR & CO-ADVISOR (IF ANY)**  *(Applicable for PhD Programme only)* | | | | | |
|  | I certify that the thesis is in a form ready and acceptable for examination and confirm the thesis title. | | | | |
|  |
|  | I, the main advisor certify that the thesis has been checked for plagiarism via turnitin. | | | | |
| Name / Signature of Main Advisor: | | |  | Date: |  |
| Name / Signature of Co-Advisor: | | |  | Date: |  |
| Name / Signature of Co-Advisor: | | |  | Date: |  |
| Name / Signature of Independent Reviewer | | |  | Date: |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PART IV – TO BE COMPLETED BY CHAIR, THESIS ADVISORY COMMITTEE**  *(Applicable for PhD Programme only)* | | | | | | | | | | |
|  | On behalf of the Head of Pillar and Thesis Advisory Committee, I confirm and approve the thesis is acceptable for examination. | | | | | | | | |
|  | Examiners have been appointed as follows: | | | | | | | | |
|  | Name: |  | | Title: |  | | Organisation: | |  |
|  | Name: |  | | Title: |  | | Organisation: | |  |
|  | Name: |  | | Title: |  | | Organisation: | |  |
|  | Name: |  | | Title: |  | | Organisation: | |  |
| Name / Signature: | | | |  | | | Date\*: | |  | |

\**For PhD scholarships, the last day of scholarship award will be based on this date.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PART V – TO BE COMPLETED BY OFFICE OF GRADUATE STUDIES** | | | | | |
|  | Endorsed | | | |
| Comments (if any): | | |  | | |
| Name / Signature: | | |  | Date: |  |

**Abstract**

**Introduction**: Online shopping scams involve scammers impersonating legitimate online merchants, either through a phony website or a phony advertisement on a legitimate ecommerce platform. In this paper, we study the effectiveness of training on the capability of users to identify online-shopping frauds. We hypothesize that post the training on identification of online shopping fraud attributes, an attentive subject would be able to identify a fraud deal online.

**Method**: The study was conducted with 147 participants across different geographies, age-group and gender.

**Result**: Results in this study provided a review on the effect of training when categorizing deals as fraudulent or legitimate. Our results showed that the capability of spotting a fraudulent deal has improved with the training.

**Discussion**: The connectivism theory, on which our research was based, was successful in our study, as evidenced by the participant's score significantly improving after training.

*Keywords*: online shopping, customer, seller, fraud, e-commerce

**Acknowledgment**

The author of this research would like to express my heartfelt gratitude to Professor Pieter Hartel and Mr Jaddoo Yeaz Elias for their constant support, guidance and advises throughout the course of this research.

The author would also like to thank SUTD Institutional Review Board and Ms Jasmine for their support on this project.

Lastly, the author would also like to thank all the participants for the online survey, for taking their time out for participation.

**Table of Content**

[Introduction and Literature Review 8](#_Toc110969844)

[Research Theory 11](#_Toc110969845)

[Research Hypothesis 13](#_Toc110969846)

[Online Shopping Frauds 14](#_Toc110969847)

[Methods 16](#_Toc110969848)

[Participants 18](#_Toc110969849)

[Material Gathering 20](#_Toc110969850)

[Scoring 21](#_Toc110969851)

[Pre-Training-Score 21](#_Toc110969852)

[Post-Training-Score 21](#_Toc110969853)

[Survey Tool 21](#_Toc110969854)

[Data clean-up 22](#_Toc110969855)

[Scoring Scenarios 23](#_Toc110969856)

[Result 33](#_Toc110969857)

[Paired Sample T-Test 34](#_Toc110969858)

[Correlation Analysis – Clicks, Time and Score 38](#_Toc110969859)

[Discussion 40](#_Toc110969860)

[Limitation 43](#_Toc110969861)

[Future work 44](#_Toc110969862)

[Conclusion 45](#_Toc110969863)

[Appendix 47](#_Toc110969864)

[Questionnaire 47](#_Toc110969865)

[SPS Script 49](#_Toc110969866)

[Paper checklist 63](#_Toc110969867)

[Reference 65](#_Toc110969868)

[Web References 66](#_Toc110969869)

**Table of Content - Figure**

Figure 1 Statista. Breakdown of cybercrime cases in Singapore in 2020 9

Figure 2 Euromonitor. E-commerce as a percentage. 15

Figure 3 Facebook. Fraudulent Online-Deal Snapshot - Pre-Training 17

Figure 4 Facebook. Fraudulent Online-Deal Snapshot - Post-Training 17

Figure 5 Facebook. Fraudulent Online-Deal Snapshot 1 - Pre-Training 25

Figure 6 Facebook. Fraudulent Online-Deal Snapshot 1- Detailed deal information - Pre-Training 26

Figure 7 Facebook. Fraudulent Online-Deal Snapshot 1 – Detailed Information on Seller-Pre-Training 27

Figure 8 Facebook. Fraudulent Online-Deal Snapshot – back to Q1 28

Figure 9 Facebook. Fraudulent Online-Deal Snapshot – Pre-Training 29

Figure 10 Boxplot Graph 34

Figure 11 Normal Q-Q Plot. 35

Figure 12 Scatter Plot Graph 1 39

Figure 13 Scatter Plot Graph 2 39

**Table of Content - Table**

Table 1 Flow of the survey. 31

Table 2 Table representing the independent and dependent variables 32

Table 3 Paired Samples Statistics, PostTrainingScore & PreTrainingScore mean 36

Table 4Paired Samples Statistics 36

Table 5 Paired Samples Statistics, Paired Difference Mean 37

Table 6 Questionnaire in the survey. 48

# **Introduction and Literature Review**

With the ease provided by online shopping specially during the pandemic era, transaction fraud is growing seriously. A study on the impact of raised awareness for fraud detection & avoidance is motivating and significant (Lallie et al., 2021).

As per the annual report1 of Cyber Security Agency of Singapore (CSA), Cybercrime made up 43% of overall crime in 2020, from the same report, it is stated that online cheating, which are cheating cases in which victims were approached through the Internet, or which involved e-commerce, is the top category in the cybercrimes. The number of online cheating cases were 12,251 in year 2020 as compared to 7,580 in year 2019 and 4,928 in year 2018. This trend also signifies the growth of e-commerce2 triggered by COVID-19 which encouraged consumers to opt for online transactions.

1 CSA | Singapore Cyber Landscape 2020. (n.d.). Retrieved July 29, 2022, from <https://www.csa.gov.sg/News/Publications/singapore-cyber-landscape-2020>

2 Global e-commerce jumps to $26.7 trillion, COVID-19 boosts online sales. (2021, May 3). Retrieved from <https://unctad.org/news/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-sales>

In general, the ongoing COVID-19 pandemic sparked a global surge in cybercrime since 2019. It was a direct outcome of circuit-breaker (lockdown) regulations enforced by the government, online shopping saw a surge of users during the pandemic. It was mainly triggered by the sense of safety associated with online shopping as compared to shopping malls or shops. This surge in the online shoppers also presented an opportunity to the cybercriminals for committing cybercrimes which is very well represented in the crime casesnumbers shown in the Figure 1 (Kashif et al., 2020).

**Figure 1**

*Breakdown of cybercrime cases in Singapore in 2020, © Statista*

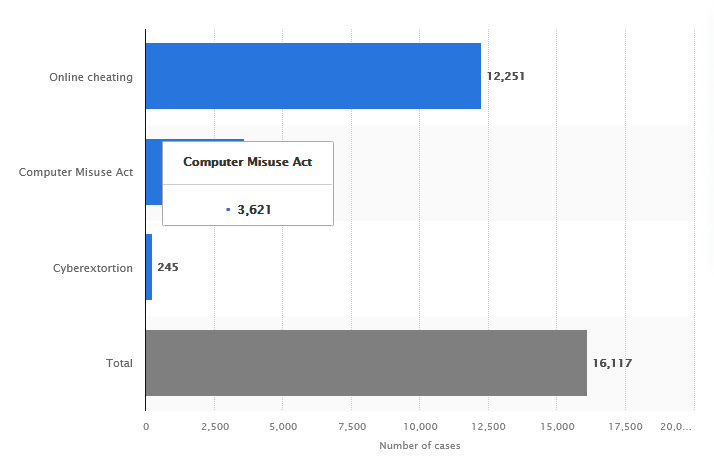


Figure 1 Statista. (2020, March 23). Breakdown of cybercrime cases in Singapore in 2020 [Graph]. Retrieved from <https://www.statista.com/statistics/1270670/singapore-breakdown-of-cybercrime-cases/>

The majority of research papers on ecommerce fraud detection focus on the addressing the issue on the ecommerce hosting platform using various artificial intelligence and machine learning on the ecommerce application itself. In a research conducted on the e-commerce fraud, the researchers studied the impact of knowledge gap between cheater and cheated on the ecommerce platforms and argued that it often leads to e-commerce frauds (Zhang et al., 2018).

In this paper, we study the effectiveness of training on the capability of an online-shopper to identify fraud ecommerce deals. We hypothesize that post the training on identification of online shopping fraud attributes, an attentive subject would be able to identify a fraud deal online.

Data has been collected from 147 participants through a well-designed survey. The participants were selected across different geographies, age-group, education-level and gender. The data collected was analysed to test the hypothesis, that post the training on identification of online shopping fraud attributes, an attentive subject would be able to identify a fraud deal online, and derive other meaningful conclusions.

Cybercrime is still one of the biggest threats to society today, despite the Covid-19 pandemic. The stark evidence demonstrates how devastatingly cybercrime affects society. In 2021, World Economic Forum’s Global Risk Report1, cybercrime was ranked by the World Economic Forum as one of the top 5 risks facing the entire world.

1The Global Risks Report 2021. (2021, January 19). Retrieved from <https://www.weforum.org/reports/the-global-risks-report-2021/>

# **Research Theory**

The theory of Connectivism was referred to for this paper, it describes learning as a process that occurs within an active with everchanging fundamental components that are not under the control of an individual. Connectivism is a learning theory founded by George Siemens and Stephen Downes, who both did considerable work in the areas of network and connectedness of online learning and the interpretative nature of knowledge (Bell, 2009).

In Connectivism, learning is focused on connecting specialized information sets. Connectivism can also be defined as the main platform that encompasses principles of informal learning, network, and complexity - through communities of practice, personal networks, and through the completion of work-related tasks. (Duke et al., 2013).

Connectivism argues that individuals are now able to learn from non-traditional mediums of education, such as internet, and are also capable of making sound decisions given this new climate of thinking. Connectivism is receiving acknowledgement as a fresh way of conceptualising learning in the digital age. The learning theory of connectivism was developed as a result of belief that there was a need for a learning theory, which considered the manner in which society has changed as a result of the new technologies of the digital age. Connectivism seeks to assist in the development of current practice in order that learning design in the future will be developed in such a way that learning through digital means will be an inherent consideration in any learning design.

(Duke et al., 2013).

On the basis of the relevance of connectivism theory to our research, this study is built upon this theory, that predicts that the participants will be able to learn and make sound decisions after going through the training & an online-based remote training model can also bring about a constructive and direct impact on ensuring that subjects can learn how to identify fraudulent online deals and be able to spot common characteristics of a potential fraud online shopping deal.

# **Research Hypothesis**

Training the online-users can increase user’s ability to detect fraudulent ecommerce deals as compared to the group of internet users with no training. Participants who have undergone the training will have higher chances of identifying a fraud online shopping deal as compared to participants who have not received any training. The research theory predicts outcome of this hypothesis.

**H0** = Participants who undergo training on identification of online-shopping fraud will not be able to identify a fraud deal online.

**H1** = Post the training on identification of online shopping fraud, the participant would be able to identify a fraud deal online.

**H2** = The time-spent by the participant on the survey and total clicks on the survey form influence the participants score.

# **Online Shopping Frauds**

Online fraud encompasses a wide range of fraud categories made possible by digital technologies, including online banking fraud, card-not-present fraud on the Internet, fraudulent sales on online retail or auction sites, consumer scams, phishing scams, pharming, and purported "online romance" frauds. Online fraud is a type of cyber-enabled crime, while the other categories all define cyber-dependent crimes. (Buil-Gil et al., 2021).

The lure of what appears to be a fantastic deal for a device, clothing, amusement park, or concert ticket marketed online frequently tempts victims of online shopping scams. The victim buyer send money to the cybercriminal posing as a "seller" after being assured that the item will be delivered. After the initial payment is received, some merchants request additional payments for duties or shipping fees. In the end, the victim never gets the good they paid for.

The extract below is from the report1 by Morgan Stanley, an American multinational investment management and financial services company, global e-commerce growth rose from 15% of total retail sales in 2019 to 21% in 2021. The report also suggested that the growth of digital commerce represents a lasting change in the way people shop. As shown in Figure 2, Morgan Stanley’s commerce model suggests that e-commerce will continue to gain traction, even in countries where online shopping is already prevalent.

1Morgan Stanley. (2022, June 14). The Surprising Case for Stronger E-commerce Growth. Retrieved from <https://www.morganstanley.com/ideas/global-ecommerce-growth-forecast-2022>

**Figure 2**

*E-commerce as a percentage of retail sales continues to grow across regions*

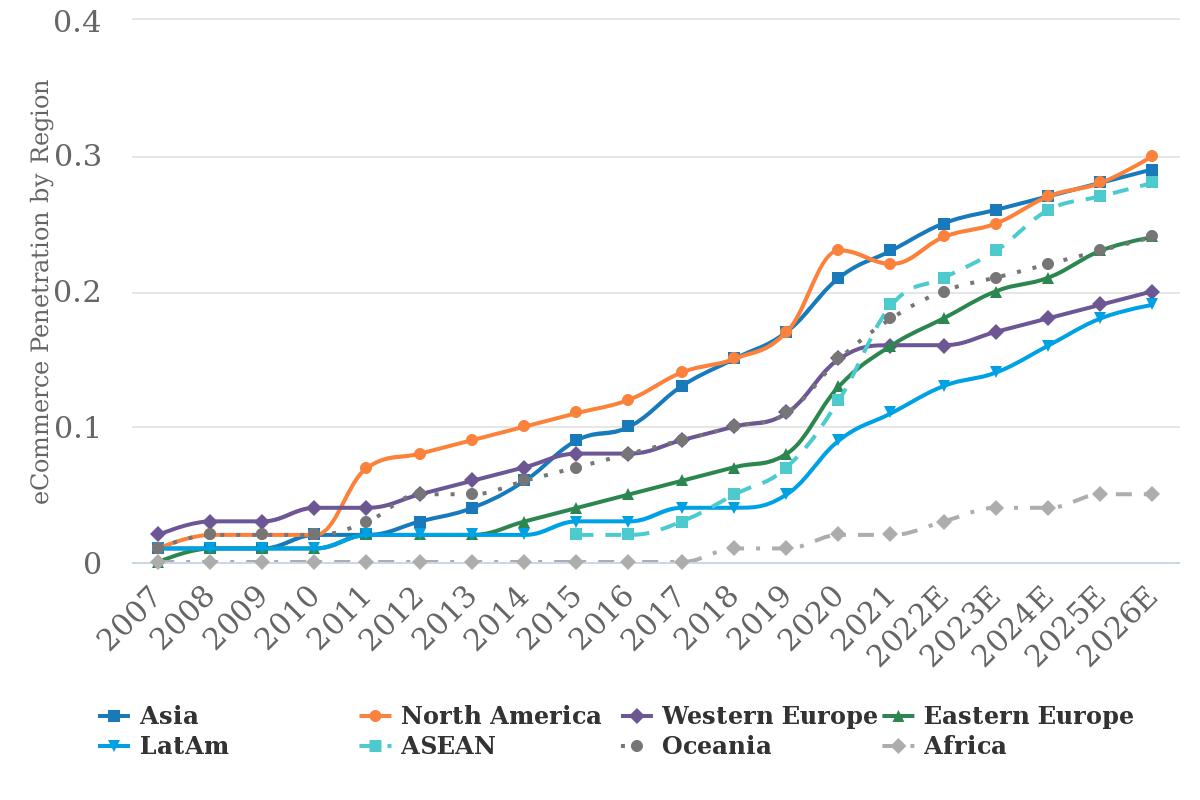


Figure 2 Euromonitor. (2022, June 14). E-commerce as a percentage of retail sales continues to grow across regions. [Graph]. Retrieved from <https://www.morganstanley.com/ideas/global-ecommerce-growth-forecast-2022>

With this considerable growth in the ecommerce space, occurrences of ecommerce frauds are expected & it brings along high risks of victimisation to many online users.(Setiawan et al., 2018)

# **Methods**

An online survey was requested via messages, email and social media platforms; the survey was hosted on a gamification type platform based on Typeform1 that goes through basic information gathering, pre-test, training content and post-test.

Data was collected from 147 participants through a survey. The participants were selected across different geographies, age-group, professions, and gender. The data collected was further analysed.

The participants were presented with a survey link, which constituted of two tests i.e. pre and post training and a training primarily focused on the below pointers to differentiate a legitimate deal from a fraudulent deal:

* Deals that are drastically below market value & are advertised as limited-time offers or flash sales,
* High demand products that are marked down
* Lack of product details or unclear terms and conditions,
* A seller who insists on external bank transfers and refuses to use the ecommerce platform’s payment methods.

The online survey presented the participants snapshots of legitimate and fraud online shopping deals on an e-commerce platform (Facebook Marketplace2).

Figure 3 and 4 shows the snapshot that were used for the research questionnaire.

1Typeform. (n.d.). Typeform: People-Friendly Forms and Surveys. Retrieved July 30, 2022, from <https://www.typeform.com/>

1Facebook - Marketplace. (n.d.). Retrieved July 30, 2022, from <https://www.facebook.com/marketplace/>

**Figure 3**

*Pre-Training Snapshots*

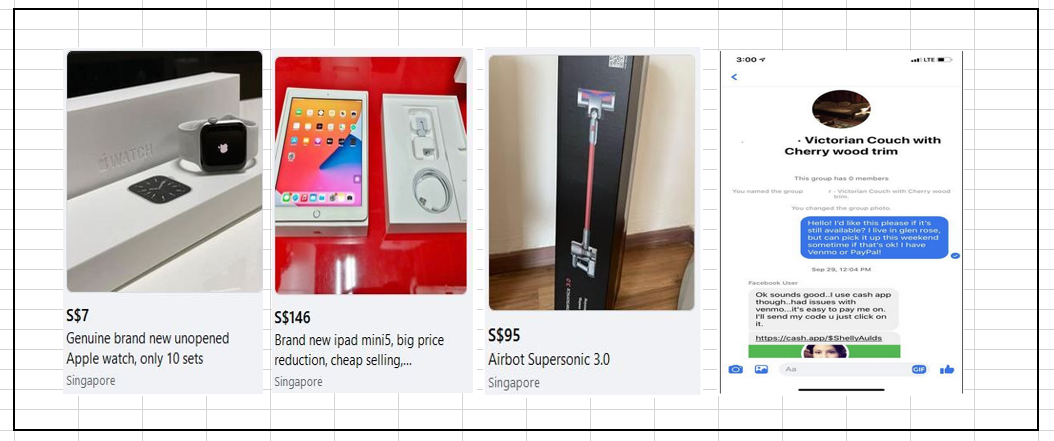


Figure 3 Facebook. (n.d.). Fraudulent Online-Deal Snapshot - Pre-Training [Photo]. Retrieved from <https://www.facebook.com/marketplace/>

**Figure 4**

*Post-Training Snapshots*

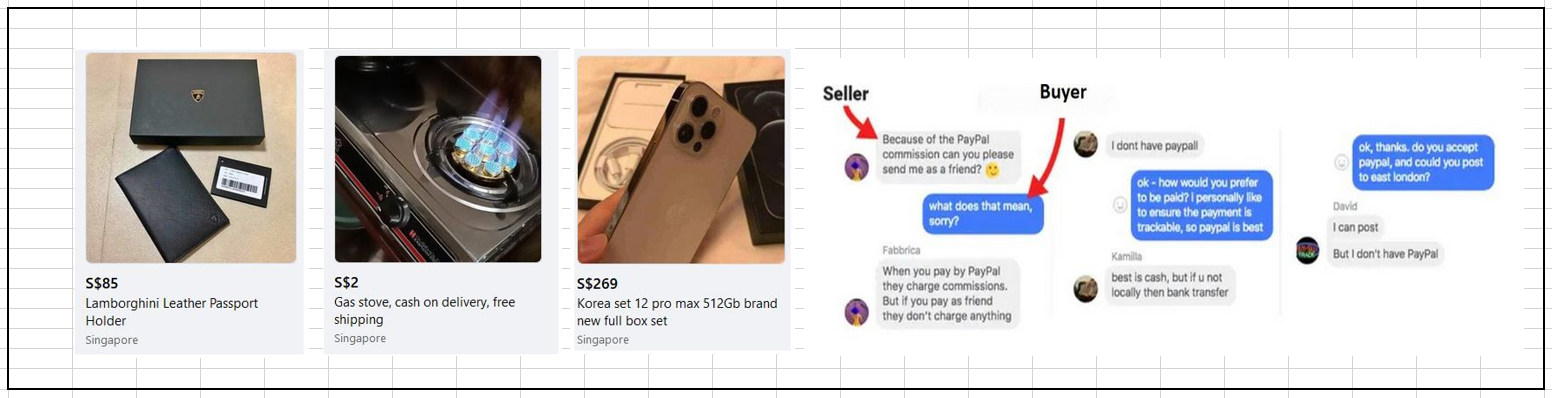


Figure 4 Facebook. (n.d.). Fraudulent Online-Deal Snapshot - Post-Training [Photo]. Retrieved from <https://www.facebook.com/marketplace/>

## **Participants**

The online survey primarily focused on e-shoppers from different age groups, genders, varying education levels, geographically distributed, two-group design of exposed and unexposed users to online shopping frauds. The intent behind having a wide variety of participant choice was to study the effect or training on an audience with diverse background. A survey link was shared with the participants.147 participants participated in the survey, however, the data was cleaned up using IBM SPSS for outliers such as slackers, speedsters, straight-liners, 18 participants who were time-based outliers i.e. participants who took less than 4 minutes and greater than 30 minutes were dropped from the research data reducing the participants from 147 to 129. The survey completion timeframe of minimum four & a maximum of thirty minutes was decided during the initial dry-run of the survey, on the basis of inputs gathered from participating volunteers.

There were 64 participants from Singapore and 51 from India and 14 participants from other countries were combined as RoW (rest of the world). There were 92 male participants and 35 female participants, the skew in the gender-based participation is an impact of researcher’s network’s effect. Other highlights of the participants are as below:

* Average time spent on the survey was 9 minutes 52 seconds
* 49.6% participation were from the age-group of 35-50 years, followed by 49.3% from 25-35 years, 6.2% from 18-25 years and 3.9% for 50 years and above.
* 49.6% participants were from Singapore, 39.5% from India and 10.9% participants were from rest of the world
* 71.3% participants were male & 27.1% were female
* 58.4% participants were graduates followed by 38.4% post-graduates & above and 3.2% were Diploma.
* 97.7% of participants had heard of online-shopping scams
* 19.4% of participants had been victim of online-shopping scams in past while 80.6% were not victims of fraud before.

## **Material Gathering**

The fraud shopping snapshots for the survey were gathered using the Singapore Police Force’s portal and by scrapping the online shopping platform, Facebook marketplace. The intent behind having snapshots instead of links to the online-shopping deals was to ensure consistency in the data collection for the survey, as the fraudulent deals are reported and frequently taken down by the hosting platforms.

We had chosen the online-deals for the test snapshots after researching on the basis of Singapore police advisories1 on ecommerce scams & National Crime Prevention Council’s scam advisories2. The advisories were for alerting the public to the common ecommerce fraud trend where scammers posted fake ecommerce advertisements following the sale of newly released electronic devices or popular apparels etc.

A total of eight deals were chosen i.e. four for pre-training test and four for the post-training test, eight snapshots were chosen to ensure that the average participants could complete the test and the training in a maximum interval of 30 minutes.

1 Singapore Police Force. (2021, October 15). Police Advisory on E-Commerce Scam Involving Sale of Newly Released Electronic Devices. Retrieved from <https://www.police.gov.sg/Media-Room/News/20211015_police_advisory_on_e-commerce_scam_inv_sale_of_newly_released_electronic_devices>

2 National Crime Prevention Council. (n.d.). ScamAlert - Bringing you the latest scam info. Retrieved July 30, 2022, from <https://www.scamalert.sg/>

## **Scoring**

### **Pre-Training-Score**

A sequel of 4 snapshots pointing to fraudulent and legitimate shopping deals were presented to participants asking them to identify snapshot as fraud or legitimate. If classified incorrectly, the test presented them the next snapshot and if participant correctly classification the image, the test further asked them to select a maximum of 2 from 5 options presented which described why the snapshot was classified as fraud or legitimate.

### **Post-Training-Score**

Similar approach and logics were followed as Pre-training-score with different snapshot of same difficulty scale and order of presentation. After the completion of the post-test users were presented with thank you a message with total pre-training and post-training scores.

## **Survey Tool**

We have used the Typeform licensed professional version that provides multiple intuitive templates to choose from option for adding logic jumps, scoring method, and linkage to Google spreadsheet to store data. The platform enabled us by making the survey intuitive and engaging.

## **Data clean-up**

As the survey was hosted on a Software as a Service (SaaS) professional platform, it automatically discarded incomplete surveys and stored data for only completed ones. The research survey was design in such a way that there wasn’t a possibility of getting missing data.

A manual visual inspection of the data was performed together with variance check to check for straight-liners and the data was found to be free from straight-liner.

## **Scoring Scenarios**

The number of questions in the survey were same for all participants. After the declaration of consent and a couple of demographic questions around gender, education, exposure to online shopping fraud, the participants in all groups were presented the first set i.e., pre-test snapshots. Every snapshot carried three marks to one mark i.e., first marks for correctly classifying the snapshot and two marks to spot the attributes that helped the participant to correctly classify the online deal snapshot, one mark was awarded for every correctly spotted attribute and a maximum of two attributes were present in every snapshot. There was a legitimate deal photograph in both sets (pre and post training) which carried only one mark. Every question provided the participants with “need more info” option button that displayed with more information about the product (specifications, condition, location etc) and seller (reviews, rating, location and photograph); the intent of this information was to help the participant with sufficient data to make a justified call on the snapshot’s classification.

There was a logic jump involved in the survey i.e., for every snapshot question wrongly answered, the survey jumped to the next snapshot in question directly without asking the users the attributes that may classify the online deal’s snapshot as a potential fraud or legitimate. Post the first four snapshot-based questionnaire, a training followed with slides illustrating different attributes that can be used to spot the fraudulent online deals. Soon after the training, the users repeated the same step as pre-set but with different four online shopping deal snapshots. The maximum score possible was 9 marks for both phases i.e., 9 from pre-training and 9 from post-training. At the end of the survey, the scores were shared with participants. Scoring Scenarios examples are below:

Scenario one - fraudulent deal; the participant correctly selects the first snapshot’s first question as fraudulent, they are awarded 1 point of it. The survey proceeds to second part of the first question wherein the participant has to select the attributes that influenced their decision to classify the snapshot as fraudulent deal, if the participant selects the two-right attribute, a maximum of two points will be awarded. Hence a participant with all right answers would score a maximum of three points per question (with fraudulent deal snapshot).

Scenario two - fraudulent deal; if the participant selects the snapshot in question as legitimate online deal, they are not presented the second part of the question asking for the attributes and a logic jump takes them to the next question. The participant scores zero points for this question.

Scenario three - fraudulent deal; if the participant selects the snapshot in question as fraudulent deal, they are presented the second part of the question, if they select all wrong attribute out of the presented four options, they get zero for the second part, scoring one point for this question.

Scenario four - legitimate deal; if the participant correctly selects the snapshot in question as legitimate deal, they are not presented the second part of the question, scoring one point for this question.

Scenario five - legitimate deal; if the participant incorrectly selects the snapshot in question as fraudulent deal, they are not presented the second part of the question, scoring zero point for this question.

An elaborated example of the scoring is below, below is the image presented to the user when they have completed the demographic entry. Figure 5, is displaying a deal and asking user for if it is fraudulent or legitimate. The user has an option to “click need more info button” if they need more information about this deal to make an informed call.

**Figure 5**

*Pre-Training Snapshot Q1, first question, main screen*

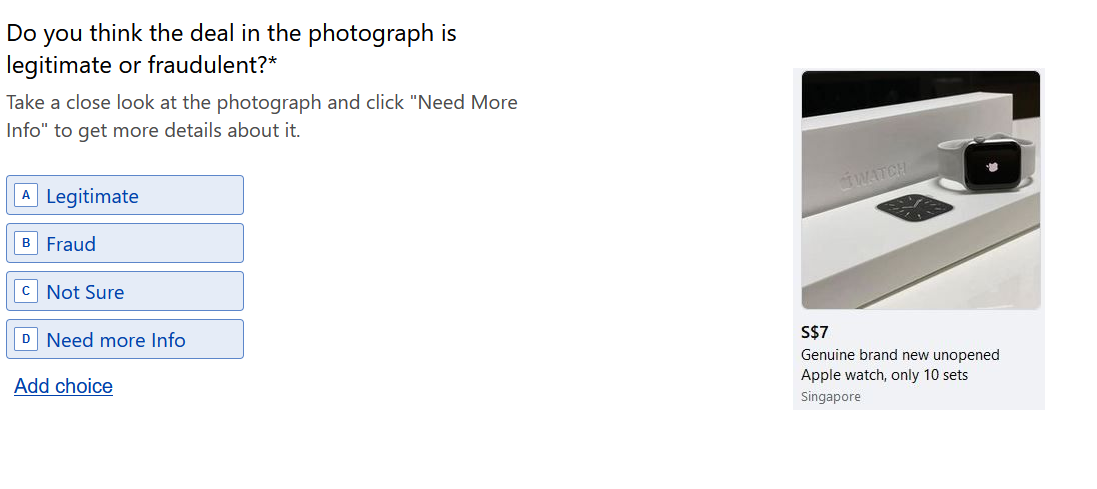


Figure 5 Facebook. (n.d.). Fraudulent Online-Deal Snapshot 1 - Pre-Training [Photo]. Retrieved from <https://www.facebook.com/marketplace/>

If the user selected, “Need more info” in the Q1, main screen, they are presented with more information about the deal details as shown in Figure 6 below, these clicks are counted by the survey platform. These clicks were aggregated on the survey platform throughout the survey and a total count will be displayed to the researcher for the individual participants.

**Figure 6**

*Pre-Training Snapshot 1, need more information, deal details*

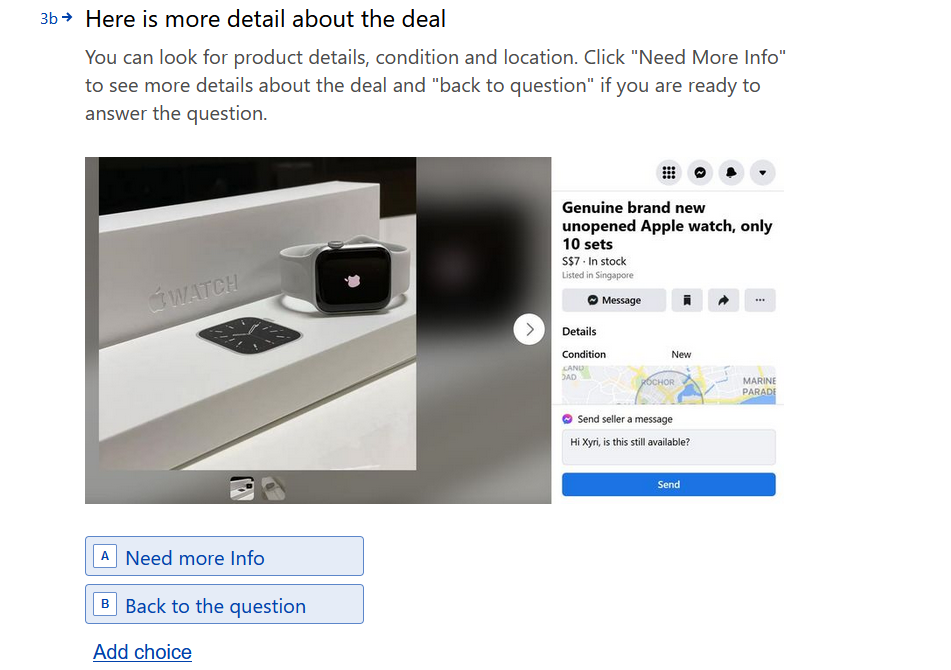


Figure 6 Facebook. (n.d.). Fraudulent Online-Deal Snapshot 1, Detailed deal information - Pre-Training [Photo]. Retrieved from <https://www.facebook.com/marketplace/>

If the user selected, “Need more info” again in the Q1, deal details section in Figure 6, they are presented with more information about the seller as shown in Figure 7 below.

**Figure 7**

*Pre-Training Snapshot 1, need more information, seller details*

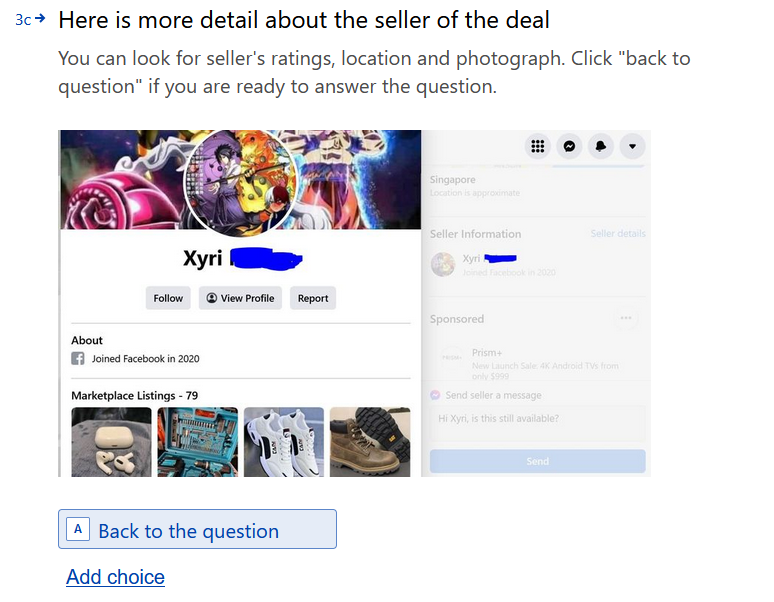


Figure 7 Facebook. (n.d.). Fraudulent Online-Deal Snapshot – Detailed Information on Seller-Pre-Training [Photo]. Retrieved from <https://www.facebook.com/marketplace/>

The user will click, “Back to the question” on the snapshot in Figure 7 above, and will be presented the Q1 main screen as seen in the Figure 8 below.

**Figure 8**

*Pre-Training Snapshot 1, back to Q1 main*

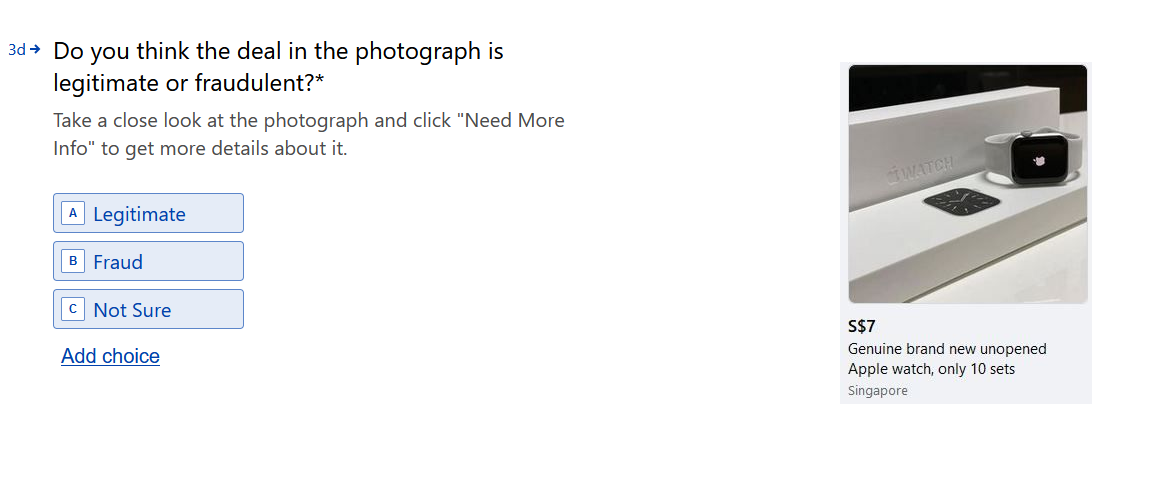


Figure 8 Facebook. (n.d.). Fraudulent Online-Deal Snapshot – back to Q1 main [Photo]. Retrieved from <https://www.facebook.com/marketplace/>

If the participant categorises this fraudulent deal as “Legitimate” or “Not Sure”, they score 0 points and are shown snapshot of question number 2. If the participant correctly categorises this deal as “Fraudulent” they score 1 point and are shown another screen as shown in Figure 9 below.

**Figure 9**

*Pre-Training Snapshot Q1, attributes for fraud*

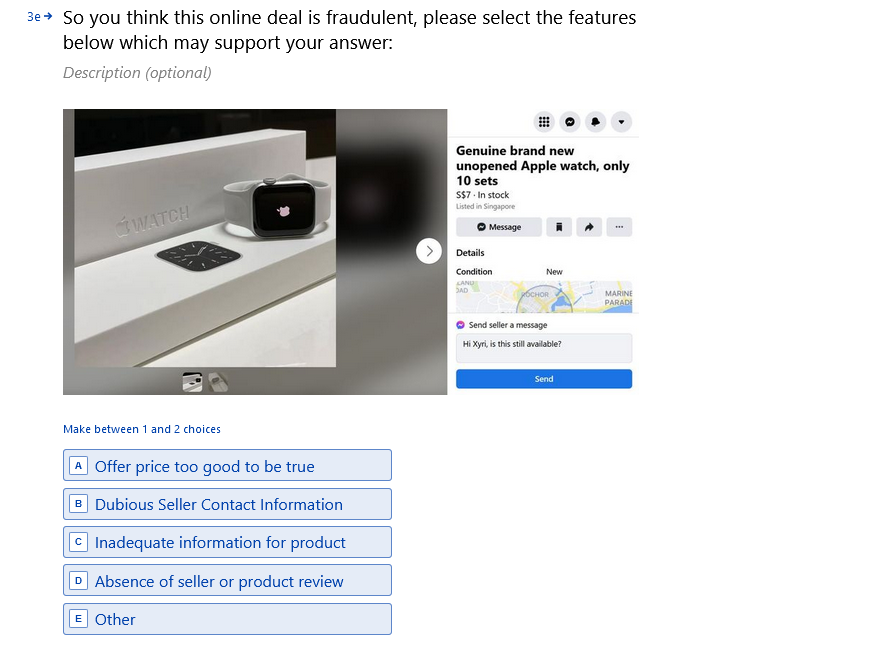


Figure 9 Facebook. (n.d.). Fraudulent Online-Deal Snapshot – Pre-Training – Attributes for fraudulent deal [Photo]. Retrieved from <https://www.facebook.com/marketplace/>

If the participant chooses the correct attributes (maximum of two) in Figure 9 above i.e. “offer price too good to be true” and “Inadequate information for product”, they get 1 point for each selection in this section making the score 3 for them for question 1.

If they select one attribute correctly only, for example “offer price too good to be true”, they score 1 point on this section, making their score 2 for question 1.

**Table 1**

*Questionnaire in the Survey*

|  |  |
| --- | --- |
| Num. | Question |
| 1 | Informed Consent |
| 2 | Please select your age group |
| 3 | Please select your gender |
| 4 | What is your highest formal education? |
| 5 | Where do you live? |
| 6 | Have you heard about online shopping frauds before? |
| 7 | Have you been a victim of online shopping fraud before? |
| 8 | Would you like to share more about your online fraud experience? (optional step) |
|  | Phase 1 (Pre-Training) |
| 10 | What do you think about this deal in the snapshot? (options are fraud, legitimate, not sure and need more info) - score +1 for spotting correctly  If participant clicks on “need more info”, more information is shown about the product, the participant can go back to question and answer it (step 10) or choose to see more information |
| 11 | If participant click on need more info again, they are shown more information about seller’s location, rating and photograph etc. The participant can click go back to answer the question (step 10) |
| 12 | Logic Jump if selected fraud in the step 10 - So you think that this link may be fraudulent, please select the features below which may support your selection: -  Offer price too good to be true  Dubious Seller Contact Information  Inadequate information for product  Absence of seller or product review  Other |
| 13 | [Logic Jump if Selected Legitimate in Step 10] – Next Snapshot. What do you think about this deal in the snapshot? |
| 14 | Step 10 is repeated till 4 snapshots are shown. |
|  | Training Slides |
|  | Phase 2 (Post Training) |
| 15 | What do you think about this deal in the snapshot? (options are fraud, legitimate, not sure and need more info) - score +1 for spotting correctly  If participant clicks on “need more info”, more information is shown about the product, the participant can go back to question and answer it (step 15) or choose to see more information |
| 16 | If participant click on need more info again, they are shown more information about seller’s location, rating and photograph etc. The participant can click go back to answer the question (step 15) |
| 17 | Logic Jump if selected fraud in the step 10 - So you think that this link may be fraudulent, please select the features below which may support your selection: -  Offer price too good to be true  Dubious Seller Contact Information  Inadequate information for product  Absence of seller or product review  Other |
| 18 | [Logic Jump if Selected Legitimate in Step 15] – Next Snapshot. What do you think about this deal in the snapshot? |
| 19 | Step 15 is repeated till 4 snapshots are shown. |
|  | Thank You Page with Score |

Table 1 This table elaborates and flow of the survey i.e. pre-training, the training and the post training.

**Table 2**

*Dependent and Independent Variables*

|  |  |
| --- | --- |
| Independent Variable | Dependent Variable |
| Age | Pre-Score |
| Gender | Post-Score |
| Education | Number of Clicks on Survey |
| Heard about online shopping fraud | Time Spent on Survey |
| Have been a victim of online shopping fraud |  |

Table 2 Table representing the independent and dependent variables in this research

The variables were carefully chosen to test the research hypothesis, for example, the time spent on survey and the number of clicks on the survey form will be able to measure the attentiveness of the participants.

# **Result**

We have performed an analysis to calculate mean pre-scores, mean post-scores.

Result highlights:

* The male participants spent more time on the survey which was average 10.054 minutes with average 4.20 clicks on the survey form and had a better overall (preminuspost) score than females, at average of 0.59.
* The female participants spent an average of 8.171 minutes on the survey with average 4.60 clicks on the survey form and had an overall score (preminuspost) average 0.34.
* The age-group 18-25 years had the highest overall score (preminuspost) 1.75 average followed 35-50 years group who scored 0.61 and 0.23 was the average score for 25-25 years participants.
* Victims of fraud, scored better with overall score (preminuspost) of average 1.24 as compared to the non-victims of fraud who had overall score (preminuspost) of average 0.34. The past experience of victims could have been a factor for helping them to score better.
* RoW based participants scored highest overall score (preminuspost) average 1.14 followed by Singapore’s average overall score 0.66 and India’s average overall score 0.16 respectively.
* The post graduates & above had highest overall score (preminuspost) average 0.63 followed by graduates with an average overall score of .52.
* The effect of training was better for Singapore based participants with an average score of 5.70 for pre-training and 6.33 for post training as compared to India based participants with average score of 5.14 pre-training and 5.06 average score post training.

## **Paired Sample T-Test**

A paired sample T-Test was performed to inspect a significant difference between the mean pre-training & post-training scores. The assumptions for the t-test were also validated. We have continuous dependent variable and the independent variable are categorical with two related groups.

As shown in Figure 10, two outliers were detected that were more than 1.5 box-lengths from the edge of the box in a boxplot. Inspection of their values did not reveal them to be extreme and they were kept in the analysis.

**Figure 10**

*Box Plot Graph Plot for PostMinusPre Score*

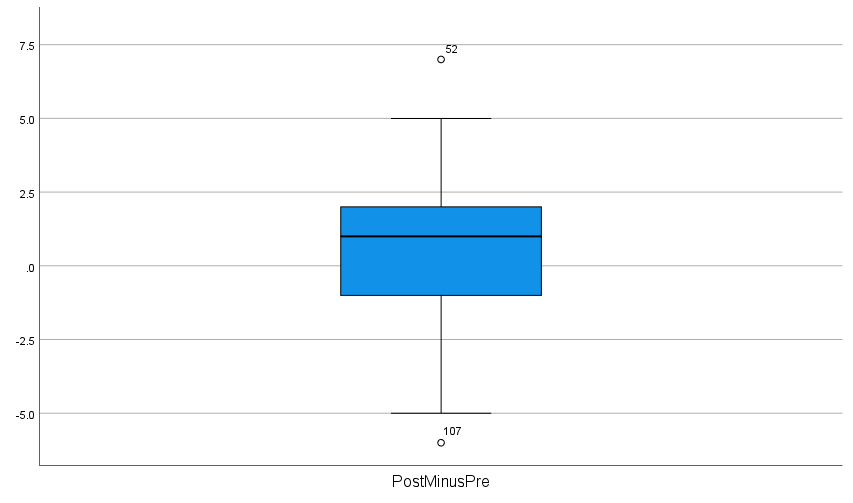
**

Figure 10 Boxplot Graph - Outliers Inspection [Graph]. In Boxplot Graph - Outliers Inspection, two outliers line number 52 and 107 highlighted in the graph

As seen in the Figure 11, the difference scores for the Pre-training Score and PostTrainingScore were normally distributed, as assessed by visual inspection of a Normal Q-Q Plot.

**Figure 11**

*Normal Q-Q Plot for PostMinusPre Score*

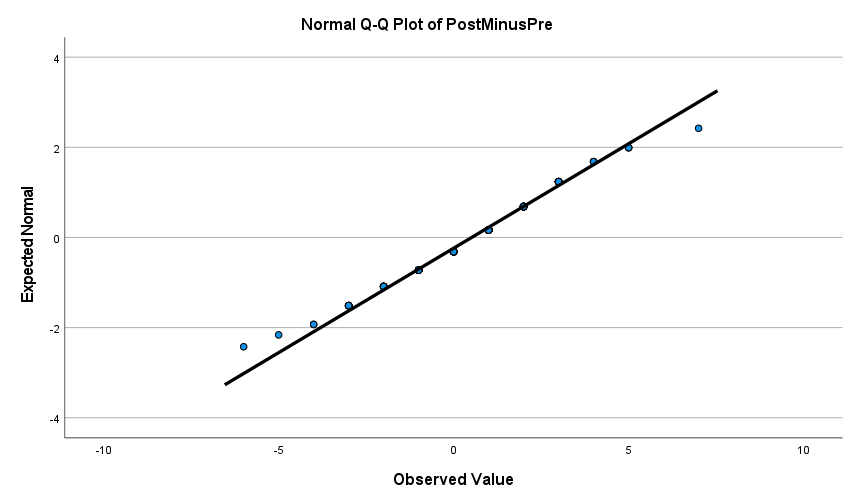


Figure 11 Normal Q-Q Plot – Normally Distributed Data Inspection [Graph]. In Normal Q-Q Plot – Normally Distributed Data Inspection. The visual inspection shows normal data distribution.

In the Table 9, for paired samples statistics, by observing the mean value it can be inferred that when the participants took the test without any training on spotting online-shopping fraud attributes they scored an average of 5.43 comparing with a post-training average score of 5.94. This improvement supports our hypothesis, but to ascertain whether this result is significant or due to change, the Paired Samples Test table must be examined.

The Std. Deviation in Table 9, shows that the spread of scores in the post-training-test is larger than that in the pre-training-test suggesting the absorption level of training is varying due to the involved human factors.

**Table 3**

*Paired Samples Statistics*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
|  | | Mean | N | Std. Deviation | Std. Error Mean |
| Pair 1 | PostTrainingScore | 5.94 | 129 | 2.045 | .180 |
| PreTrainingScore | 5.43 | 129 | 1.624 | .143 |

Table 3 Paired Samples Statistics, PostTrainingScore mean 5.94 & PreTrainingScore mean 5.43

The Paired Samples Correlations table 10, shows the Pre and Post-training scores correlation coefficient and its significance value. From the above table, the correlation of our samples is r = 0.326 and p < 0.001. Our participants are therefore behaving consistently as their scores in the post-training are significantly but correlated low with the pre-training scores.

**Table 4**

*Paired Samples Correlations*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
|  | | N | Correlation | Significance | |
| One-Sided p | Two-Sided p |
| Pair 1 | PostTrainingScore & PreTrainingScore | 129 | .326 | <.001 | <.001 |

Table 4Paired Samples Statistics, r = 0.326 and p < 0.001

**Table 5**

*Paired Samples Test*

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | | |
|  | | Paired Differences | | | | | t | df | Significance | | |
| Mean | Std. Deviation | Std. Error Mean | 95% Confidence Interval of the Difference | | One-Sided p | Two-Sided p |
| Lower | Upper |
| Pair 1 | PostTrainingScore - PreTrainingScore | .512 | 2.158 | .190 | .136 | .888 | 2.692 | 128 | .004 | .008 |

Table 5 Paired Samples Statistics, Paired Difference Mean = 0.512, Std. Dev. = 2.158, t = 2.692, p < 0.05

The results of Paired Sample Test in table 11 revealed that there was a significant improvement from the pre-test score. Paired Difference Mean = 0.512, Std. Dev. = 2.158, t = 2.692, p < 0.05.

These results show that there was an increase in the scores post the training and therefore, we can reject the null hypothesis and accept the alternative hypothesis.

## **Correlation Analysis – Clicks, Time and Score**

In perform further analysis of our hypothesis H2 which draw relationship between the participant’s attentiveness i.e. time spent on the survey and number of clicks on the survey form and eventually the score achieved. Before conducting the right correlation analysis, the prerequisite was to check the linearity of the two variables.

We proceeded to test for linearity with the scatter-plot graph. As shown in the Figure 10 and Figure 11 below, there is no linear relationship between the time for completing survey and the PostMinusPre Score and number of clicks and PostMinusPre score either. The graphs didn’t show any monotonic relationship either.

Upon visual inspection of the graph, there is no linearity observed between number of clicks, total time spent on the survey and PostMinusPre score.

The relationship between PostMinusPre score and number of clicks, total time spent on the survey was not statistically significant. Therefore, we cannot reject the null hypothesis and cannot accept the H2 or the alternative hypothesis.

**Figure 12**

*Scatter Plot Graph Plot for PostMinusPre Score & Time for completing survey*

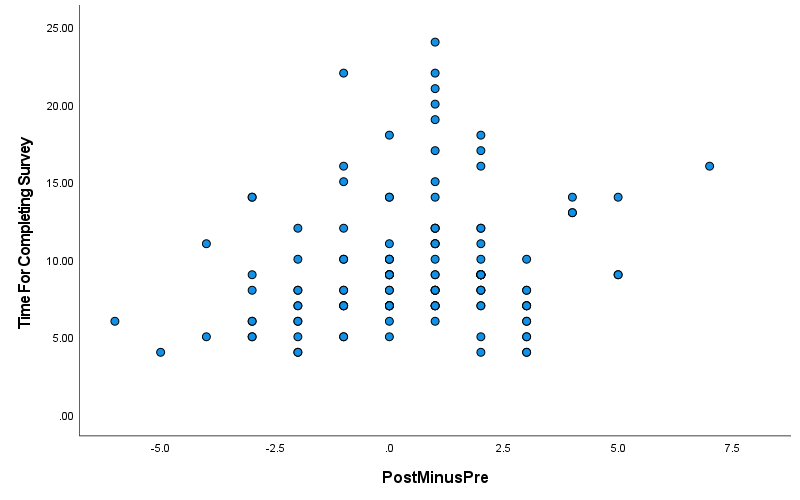


Figure 12 Scatter Plot Graph for checking linearity between time for completing survey vs PostMinusPre Score

**Figure 13**

*Scatter Plot Graph Plot for PostMinusPre Score & number of clicks during the survey*

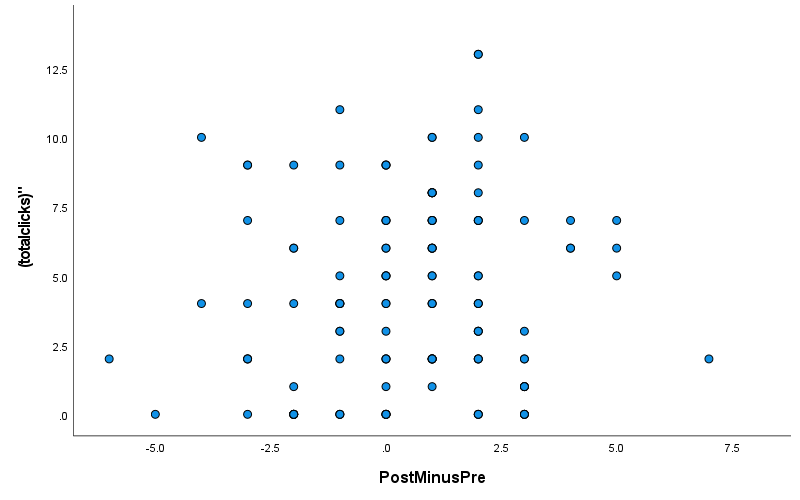


Figure 13 Scatter Plot Graph for checking linearity between number of clicks on the survey vs PostMinusPre Score

# **Discussion**

We had 147 participants in this research from students to professionals, aged between the minimum of 18 years to above 50 years, primarily from Singapore and India. They were from diverse educational background varying from diploma to post-graduate.

The pre-training scores show that majority of the participants were able to identify the online-shopping fraud snapshots even though there was no priming intervention. Most of these participants (126 out of 129) had highlighted in the survey that they had heard about the online-shopping scams and hence they were able to identify some of the online shopping fraud snapshots even before the training.

Twelve participants from India shared that the survey could have been better if the shopping deals would have displayed the currency in INR (Indian Rupee), as they had to invest some time in converting the amount displayed in the snapshot, which was in Singapore Dollar, to Indian Rupee. For future studies, it is recommended to design tests with country specific / regional attributes (local currency and local shopping portals) for a better training effect.

Seventeen participants, who were victim of online-shopping scams in past, shared their experience on the survey form. Seven participants mentioned buying the articles online, and not receiving them. Two participants highlighted receiving a sub quality product and not the displayed product on the online shopping deal. One participant admitted buying a product online despite of vague product information and not receiving it late.

To elaborate the role of the training content and hence the scores we had referred to previous studies by Bramley, which suggests the factors for the training to be effective, the training program should be administered in a similar environment to actual work conditions i.e. an online survey platform is conducive to simulate an online-shopping environment, for example, the seller’s profile and detailed disruption of the item were available to the participants by clicking on the relevant buttons of the survey. Bramley went on to mention that when users can see that they can apply the content of training into real environment, it increases the effectiveness of the training (Bramley, 1991).

Another probable reason for the good post-training scores in our research could be that the survey platform offered a gamification-based questionnaire, twenty-three of the participants conveyed to the researchers that they found the survey method interesting and they felt like participating in a quiz. Thirty participants had reached out to the researcher mentioning that they thoroughly enjoyed the survey and found the learnings practically applicable.

The connectivism theory did work for our training wherein a substantial improvement in the participant’s score was observed. However, there are some principles of connectivism which were not evaluated in our research due to the time constraints, such as “learning is a process of connecting” & “nurturing and maintaining connections are needed for continual learning”.

Connectivism is one of the most prominent of the learning theories which have been developed for e-learning environments. While connectivism offers a beneficial perspective for better understanding and managing teaching and learning utilizing digital technology, further research and testing are still recommended as it is improbable that a single theory will adequately account for learning in technologically evolving ecommerce scams. The researchers thus highly recommend evaluating other theories for the future experiments (Goldie, 2016).

**Recommendations**

We recommend that online shopping platforms should increase customer’s awareness about cybercrime to help educate them and conduct periodic mandatory surveys and trainings to enforce the awareness and thus reduce the occurrence of online shopping scams. Apart from the trainings, we would also recommend that Online stores should also use security certificates and safe payment options to increase the sense of their websites' credibility.

Given the online shopping fraud strategies are evolving rapidly, the training attributes are to be revised frequently to deliver similar (or better) results. The future researcher should constantly look-out for new attributes published by local scam-awareness bodies such as police force & security advisory section of online-shopping portals.

Based on the feedback received during the survey, the survey should be targeting specific regions (such as a country) and the attributes used i.e. currency and products should be local as well, it helps the participants to better understand the deals and make a well-informed decision. Thus, a global survey has a limitation in terms of consistent outcome across different geography due to the changing attributes as mentioned above.

Another feedback received was from the female participants to include apparel related deal snapshot in future research as majority of them had experienced fraud while buying clothes online.

# **Limitation**

Due to the network effect of researcher, there was a disproportionate participation from one gender, the outcomes could have been more interesting if there was a proportionate participation.

Extracting the snapshots of fraudulent deal was a rough process, given the dynamic nature of cyber-crime prevention constantly taking them down and when researcher needed to get additional attributes for training purposes that wasn’t captured before, the deal would be taken down. This resulted in constantly changing the deals till a final attribute list was established.

The researcher intended to have global participation for a bigger sample size but the local geographic attributes such as currency, popular articles & scam tactics couldn’t be standardized for a wider global participation, this also surfaced in feedback from participants in India requesting for snapshots in local currency for future similar surveys.

The connectivism theory did work for our training wherein a substantial improvement in the participant’s score was observed. However, there are some principles of connectivism which were not evaluated in our research due to the time constraints, such as “learning is a process of connecting” & “nurturing and maintaining connections are needed for continual learning”. The researcher would recommend testing these principles of connectivism by connecting the learners together for a duration for learning purposes and re-evaluate their network-based learning after a period.

# **Future work**

For future experiments, researchers could look at expanding this survey to focused geographies & snapshots can be extracted from multiple online shopping platforms based on the popularity of the target region. For the online-shopping snapshots, researchers can refer to common / popular scam alerts from the local scam alerting bodies.

By expanding the survey outside the current scope, researchers could collect more information on the demographic of the people who do fall prey to online-shopping frauds and observe which groups of individuals are more vulnerable to frauds.

With higher participation from 50 years and above, the future researcher may also study the effect of digital divide.

The future researchers may also try to study relationship between time spent on the survey and the clicks on the survey form for a bigger participation sample to draw relationship between time spent & clicks on the form attributes and participant’s attentiveness during the survey.

# **Conclusion**

In this study, we tried to improve the ability of an individual to spot fraudulent online shopping deals. According to our participant demographics, most of them were young adults, with graduation and post-graduation-level education with adequate experience as an internet user – both for personal and professional nature. As such, this group would be one of the most well-suited demographics for learning the techniques of identifying fraudulent online-shopping deals.

As reflected in the scores, before our training, most of the participants missed the attributes in the snapshots. Statistical evidence from our experiments suggests that without adequate exposure or training, people are more likely to be misled or fooled by fraudulent online shopping deals.

With increasing ecommerce adoption for both consumer and sellers, and unavailability of robust anti-scam measures on prominent online shopping platforms1, the occurrence of online-shopping frauds may increase in future2, hence it is important for constantly evolving online-shopping fraud awareness trainings to protect the end-consumer from frauds.

1Ministry of Home Affairs, Singapore. (n.d.). E-Commerce Marketplace Transaction Safety Ratings. Retrieved July 30, 2022, from <https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings>

2Online Payment Fraud Losses to Exceed $206 Billion Over the Next Five Years. (2021, July 5). Retrieved from <https://www.juniperresearch.com/press/online-payment-fraud-losses-exceed-206-bn>

The researcher felt the need of an element of “attentiveness” in the theory. The connectivity theory doesn’t argue about the impact of participant’s “attentiveness” on their score and hence it is not as complete as it could be. Adding the element of attentiveness on the training outcome would complement the theory’s existing principles.

# **Appendix**

## **Questionnaire**

**Table 1**

*Questionnaire in the Survey*

|  |  |
| --- | --- |
| Num. | Question |
| 1 | Informed Consent |
| 2 | Please select your age group |
| 3 | Please select your gender |
| 4 | What is your highest formal education? |
| 5 | Where do you live? |
| 6 | Have you heard about online shopping frauds before? |
| 7 | Have you been a victim of online shopping fraud before? |
| 8 | Would you like to share more about your online fraud experience? (optional step) |
|  | Phase 1 (Pre-Training) |
| 10 | What do you think about this deal in the snapshot? (options are fraud, legitimate, not sure and need more info)  If participant clicks on “need more info”, more information is shown about the product, the participant can go back to question and answer it (step 10) or choose to see more information |
| 11 | If participant click on need more info again, they are shown more information about seller’s location, rating and photograph etc. The participant can click go back to answer the question (step 10) |
| 12 | Logic Jump if selected fraud in the step 10 - So you think that this link may be fraudulent, please select the features below which may support your selection: -  Offer price too good to be true  Dubious Seller Contact Information  Inadequate information for product  Absence of seller or product review  Other |
| 13 | [Logic Jump if Selected Legitimate in Step 10] – Next Snapshot. What do you think about this deal in the snapshot? |
| 14 | Step 10 is repeated till 4 snapshots are shown. |
|  | **Training** |
|  | Phase 2 (Post Training) |
| 15 | What do you think about this deal in the snapshot? (options are fraud, legitimate, not sure and need more info)  If participant clicks on “need more info”, more information is shown about the product, the participant can go back to question and answer it (step 15) or choose to see more information |

Table 6 This table elaborates the questionnaire in the survey i.e. pre-training and the post training.

## **SPS Script**

|  |
| --- |
| \* Encoding: UTF-8.  /\* **Author**: Mayank Nauni – 1004741  /\* **Research Title**: *Raised awareness helps detecting & preventing online shopping scams*  **/\*Upload Data**    GET DATA  /TYPE=XLSX  /FILE='C:\Users\nauni\Documents\CyberCrime Thesis\Experiment '+  'Results\19-Jun\Experiment\_Latest\responses-export.xlsx'  /SHEET=name 'responses-export'  /CELLRANGE=FULL  /READNAMES=ON  /DATATYPEMIN PERCENTAGE=95.0  /HIDDEN IGNORE=YES.  EXECUTE.  DATASET NAME DataSet1 WINDOW=FRONT.  **/\* Sanitize the raw data**  \* Recode the string variable Age .  RECODE Age ("18-25 Yrs"=1) ("25 - 35 Yrs"=2) ("35 - 50 Yrs"=3) ("50 & above"=4) INTO Age\_num .  VARIABLE LABELS Age\_num "Age (numeric)" .  FORMATS Age\_num (F1.0) .  ADD VALUE LABELS Age\_num  1 "18-25 Yrs"  2 "25 - 35 Yrs"  3 "35 - 50 Yrs"  4 "50 & above" .  EXECUTE.  \* Recode the string variable Gender .  RECODE Gender ("Female"=1) ("Male"=2) ("Prefer not to answer"=3) INTO Gender\_num .  VARIABLE LABELS Gender\_num " Gender (numeric)" .  FORMATS Gender\_num (F1.0) .  ADD VALUE LABELS Gender\_num  1 "Female"  2 "Male"  3 "Prefer not to answer" .  EXECUTE.  \* Recode the string variable Country .  RECODE Country ('Singapore'=1) ('India'=2) (ELSE=3) INTO Country\_num.  VARIABLE LABELS Country\_Num 'Country (numeric)'.  FORMATS Country\_Num (F1.0) .  ADD VALUE LABELS Country\_Num  1 "Singapore"  2 "India"  3 "RoW" .  EXECUTE.  \* Recode the string variable Education .  RECODE Education ('Graduate'=1) ('Post Graduate'=2) ('Diploma'=3) ('Doctorate '=2) ('Prefer not '+  'to answer'=4) INTO Education\_num.  FORMATS Education\_num (F1.0) .  VARIABLE LABELS Education\_num 'Education (numeric)'.  ADD VALUE LABELS Education\_Num  1 "Graduate"  2 "Post Graduate & Above"  3 "Diploma"  4 "Prefer not to answer" .  EXECUTE.  \* Recode the string variable Heard Fraud .  RECODE HeardShoppingFraud (1=1) (0=0) INTO HeardShoppingFraud\_num.  FORMATS HeardShoppingFraud\_num (F1.0) .  VARIABLE LABELS HeardShoppingFraud\_num 'HeardShoppingFraud (numeric)'.  ADD VALUE LABELS HeardShoppingFraud\_num  1 "Yes"  0 "No" .  EXECUTE.  \* Recode the string variable VictimOfFraud .  RECODE VictimOfFraud (1=1) (0=0) INTO VictimOfFraud\_num.  FORMATS VictimOfFraud\_num (F1.0) .  VARIABLE LABELS VictimOfFraud\_num 'VictimOfFraud (numeric)'.  ADD VALUE LABELS VictimOfFraud\_num  1 "Yes"  0 "No" .  EXECUTE.  \* Recode the string variable SharedExperience .  RECODE SharedExperience (1=1) (ELSE=2) INTO SharedExperience\_num.  VARIABLE LABELS SharedExperience\_num 'SharedExperience (numeric)'.  FORMATS SharedExperience\_num (F1.0) .  ADD VALUE LABELS SharedExperience\_num  1 "Yes"  2 "No" .  EXECUTE.  **/\* RECODING RESPONSE VALUES /\***    \* PreQ1  RECODE PreQ1First ("Fraud"=1) ("Legitimate"=2) ("Need more Info"=3) ("Not Sure"=4) INTO PreQ1First\_num.  VARIABLE LABELS PreQ1First\_num 'PreQ1First (numeric)'.  FORMATS PreQ1First\_num (F1.0) .  ADD VALUE LABELS PreQ1First\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure" .  EXECUTE.  RECODE PreQ1Final ("Fraud"=1) ("Legitimate"=2) ("Need more Info"=3) ("Not Sure"=4) (ELSE=0) INTO PreQ1Final\_num.  VARIABLE LABELS PreQ1Final\_num 'PreQ1Final (numeric)'.  FORMATS PreQ1Final\_num (F1.0) .  ADD VALUE LABELS PreQ1Final\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure"  0 "AnsweredAlready" .  EXECUTE.  RECODE PreQ1DealInfo ("Back to the question"=1) ("Need more Info"=2) (ELSE=0) INTO PreQ1DealInfo\_num.  EXECUTE.  VARIABLE LABELS PreQ1DealInfo\_num 'PreQ1DealInfo (numeric)'.  FORMATS PreQ1DealInfo\_num (F1.0) .  ADD VALUE LABELS PreQ1DealInfo\_num  1 "Back to the question"  2 "Need more Info"  0 "NotVisted" .  EXECUTE.  RECODE PreQ1DealSeller ("Back to the question"=1) (ELSE=0) INTO PreQ1DealSeller\_num.  EXECUTE.  VARIABLE LABELS PreQ1DealSeller\_num 'PreQ1DealSeller (numeric)'.  FORMATS PreQ1DealSeller\_num (F1.0) .  ADD VALUE LABELS PreQ1DealSeller\_num  1 "Back to the question"  0 "NotVisted" .  EXECUTE.  RECODE PreQ1OfferPrice ("Offer price too good to be true"=1) (ELSE=0) INTO PreQ1OfferPrice\_num.  EXECUTE.  VARIABLE LABELS PreQ1OfferPrice\_num 'PreQ1OfferPrice (numeric)'.  FORMATS PreQ1OfferPrice\_num (F1.0) .  ADD VALUE LABELS PreQ1OfferPrice\_num  1 "Offer price too good to be true"  0 "NotSelected" .  EXECUTE.  RECODE PreQ1DubiousSeller ("Dubious Seller Contact Information"=1) (ELSE=0) INTO PreQ1DubiousSeller\_num.  EXECUTE.  VARIABLE LABELS PreQ1DubiousSeller\_num 'PreQ1DealSeller (numeric)'.  FORMATS PreQ1DubiousSeller\_num (F1.0) .  ADD VALUE LABELS PreQ1DubiousSeller\_num  1 "Dubious Seller Contact Information"  0 "NotSelected" .  EXECUTE.  RECODE PreQ1InadequateInfo ("Inadequate information for product"=1) (ELSE=0) INTO PreQ1InadequateInfo\_num.  EXECUTE.  VARIABLE LABELS PreQ1InadequateInfo\_num 'PreQ1InadequateInfo (numeric)'.  FORMATS PreQ1InadequateInfo\_num (F1.0) .  ADD VALUE LABELS PreQ1InadequateInfo\_num  1 "Inadequate information for product"  0 "NotSelected" .  EXECUTE.  RECODE PreQ1AbsenceofReview ("Absence of seller or product review"=1) (ELSE=0) INTO PreQ1AbsenceofReview\_num.  EXECUTE.  VARIABLE LABELS PreQ1AbsenceofReview\_num 'PreQ1AbsenceofReview (numeric)'.  FORMATS PreQ1AbsenceofReview\_num (F1.0) .  ADD VALUE LABELS PreQ1AbsenceofReview\_num  1 "Absence of seller or product review"  0 "NotSelected" .  EXECUTE.  \* PreQ2  RECODE PreQ2First ("Fraud"=1) ("Legitimate"=2) ("Need more Info"=3) ("Not Sure"=4) INTO PreQ2First\_num.  VARIABLE LABELS PreQ2First\_num 'PreQ2First (numeric)'.  FORMATS PreQ2First\_num (F1.0) .  ADD VALUE LABELS PreQ2First\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure" .  EXECUTE.  RECODE PreQ2Final ("Fraud"=1) ("Legitimate"=2) ("Need more Info"=3) ("Not Sure"=4) (ELSE=0) INTO PreQ2Final\_num.  VARIABLE LABELS PreQ2Final\_num 'PreQ2Final (numeric)'.  FORMATS PreQ2Final\_num (F1.0) .  ADD VALUE LABELS PreQ2Final\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure"  0 "AnsweredAlready" .  EXECUTE.  RECODE PreQ2DealInfo ("Back to the question"=1) ("Need more Info"=2) (ELSE=0) INTO PreQ2DealInfo\_num.  EXECUTE.  VARIABLE LABELS PreQ2DealInfo\_num 'PreQ2DealInfo (numeric)'.  FORMATS PreQ2DealInfo\_num (F1.0) .  ADD VALUE LABELS PreQ2DealInfo\_num  1 "Back to the question"  2 "Need more Info"  0 "NotVisted" .  EXECUTE.  RECODE PreQ2DealSeller ("Back to the question"=1) (ELSE=0) INTO PreQ2DealSeller\_num.  EXECUTE.  VARIABLE LABELS PreQ2DealSeller\_num 'PreQ2DealSeller (numeric)'.  FORMATS PreQ2DealSeller\_num (F1.0) .  ADD VALUE LABELS PreQ2DealSeller\_num  1 "Back to the question"  0 "NotVisted" .  EXECUTE.  RECODE PreQ2OfferPrice ("Offer price too good to be true"=1) (ELSE=0) INTO PreQ2OfferPrice\_num.  EXECUTE.  VARIABLE LABELS PreQ2OfferPrice\_num 'PreQ2OfferPrice (numeric)'.  FORMATS PreQ2OfferPrice\_num (F1.0) .  ADD VALUE LABELS PreQ2OfferPrice\_num  1 "Offer price too good to be true"  0 "NotSelected" .  EXECUTE.  RECODE PreQ2DubiousSeller ("Dubious Seller Contact Information"=1) (ELSE=0) INTO PreQ2DubiousSeller\_num.  EXECUTE.  VARIABLE LABELS PreQ2DubiousSeller\_num 'PreQ2DealSeller (numeric)'.  FORMATS PreQ2DubiousSeller\_num (F1.0) .  ADD VALUE LABELS PreQ2DubiousSeller\_num  1 "Dubious Seller Contact Information"  0 "NotSelected" .  EXECUTE.  RECODE PreQ2InadequateInfo ("Inadequate information for product"=1) (ELSE=0) INTO PreQ2InadequateInfo\_num.  EXECUTE.  VARIABLE LABELS PreQ2InadequateInfo\_num 'PreQ2InadequateInfo (numeric)'.  FORMATS PreQ2InadequateInfo\_num (F1.0) .  ADD VALUE LABELS PreQ2InadequateInfo\_num  1 "Inadequate information for product"  0 "NotSelected" .  EXECUTE.  RECODE PreQ2AbsenceofReview ("Seller or product review"=1) (ELSE=0) INTO PreQ2AbsenceofReview\_num.  EXECUTE.  VARIABLE LABELS PreQ2AbsenceofReview\_num 'PreQ2AbsenceofReview (numeric)'.  FORMATS PreQ2AbsenceofReview\_num (F1.0) .  ADD VALUE LABELS PreQ2AbsenceofReview\_num  1 "Absence of seller or product review"  0 "NotSelected" .  EXECUTE.  \* PreQ3  RECODE PreQ3First ("Fraud"=1) ("Legitimate"=2) ("More Info"=3) ("Not Sure"=4) INTO PreQ3First\_num.  VARIABLE LABELS PreQ3First\_num 'PreQ3First (numeric)'.  FORMATS PreQ3First\_num (F1.0) .  ADD VALUE LABELS PreQ3First\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure" .  EXECUTE.  RECODE PreQ3Final ("Fraud"=1) ("Legitimate"=2) ("Need more Info"=3) ("Not Sure"=4) (ELSE=0) INTO PreQ3Final\_num.  VARIABLE LABELS PreQ3Final\_num 'PreQ3Final (numeric)'.  FORMATS PreQ3Final\_num (F1.0) .  ADD VALUE LABELS PreQ3Final\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure"  0 "AnsweredAlready" .  EXECUTE.  RECODE PreQ3Chat ("Back to the question"=1) (ELSE=0) INTO PreQ3Chat\_num.  EXECUTE.  VARIABLE LABELS PreQ3Chat\_num 'PreQ3Chat (numeric)'.  FORMATS PreQ3Chat\_num (F1.0) .  ADD VALUE LABELS PreQ3Chat\_num  1 "Back to the question"  0 "NotVisted" .  EXECUTE.  RECODE PreQ3OfferPrice ("Offer price too good to be true"=1) (ELSE=0) INTO PreQ3OfferPrice\_num.  EXECUTE.  VARIABLE LABELS PreQ3OfferPrice\_num 'PreQ3OfferPrice (numeric)'.  FORMATS PreQ3OfferPrice\_num (F1.0) .  ADD VALUE LABELS PreQ3OfferPrice\_num  1 "Offer price too good to be true"  0 "NotSelected" .  EXECUTE.  RECODE PreQ3DubiousSeller ("Dubious Seller Contact Information"=1) (ELSE=0) INTO PreQ3DubiousSeller\_num.  EXECUTE.  VARIABLE LABELS PreQ3DubiousSeller\_num 'PreQ3DealSeller (numeric)'.  FORMATS PreQ3DubiousSeller\_num (F1.0) .  ADD VALUE LABELS PreQ3DubiousSeller\_num  1 "Dubious Seller Contact Information"  0 "NotVisted" .  EXECUTE.  RECODE PreQ3ExternalPayment ("Seller is asking for external payment"=1) (ELSE=0) INTO PreQ3ExternalPayment\_num.  EXECUTE.  VARIABLE LABELS PreQ3ExternalPayment\_num 'PreQ3ExternalPayment (numeric)'.  FORMATS PreQ3ExternalPayment\_num (F1.0) .  ADD VALUE LABELS PreQ3ExternalPayment\_num  1 "Seller is asking for external payment"  0 "NotVisted" .  EXECUTE.  RECODE PreQ3AbsenceofReview ("Seller or product review"=1) (ELSE=0) INTO PreQ3AbsenceofReview\_num.  EXECUTE.  VARIABLE LABELS PreQ3AbsenceofReview\_num 'PreQ3AbsenceofReview (numeric)'.  FORMATS PreQ3AbsenceofReview\_num (F1.0) .  ADD VALUE LABELS PreQ3AbsenceofReview\_num  1 "Seller or product review"  0 "NotVisted" .  EXECUTE.  \*Pre Q4  RECODE PreQ4First ("Fraud"=1) ("Legitimate"=2) ("Need More Info"=3) ("Not Sure"=4) INTO PreQ4First\_num.  VARIABLE LABELS PreQ4First\_num 'PreQ4First (numeric)'.  FORMATS PreQ4First\_num (F1.0) .  ADD VALUE LABELS PreQ4First\_num  1 "Fraud"  2 "Legitimate"  3 "Need More Info"  4 "Not Sure" .  EXECUTE.  RECODE PreQ4Final ("Fraud"=1) ("Legitimate"=2) ("Need More Info"=3) ("Not Sure"=4) (ELSE=0) INTO PreQ4Final\_num.  VARIABLE LABELS PreQ4Final\_num 'PreQ4Final (numeric)'.  FORMATS PreQ4Final\_num (F1.0) .  ADD VALUE LABELS PreQ4Final\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure"  0 "AnsweredAlready" .  EXECUTE.  RECODE PreQ4DealInfo ("Back to the question"=1) ("Need more Info"=2) (ELSE=0) INTO PreQ4DealInfo\_num.  EXECUTE.  VARIABLE LABELS PreQ4DealInfo\_num 'PreQ4DealInfo (numeric)'.  FORMATS PreQ4DealInfo\_num (F1.0) .  ADD VALUE LABELS PreQ4DealInfo\_num  1 "Back to the question"  2 "Need more Info"  0 "NotVisted" .  EXECUTE.  RECODE PreQ4DealSeller ("Back to the question"=1) (ELSE=0) INTO PreQ4DealSeller\_num.  EXECUTE.  VARIABLE LABELS PreQ4DealSeller\_num 'PreQ4DealSeller (numeric)'.  FORMATS PreQ4DealSeller\_num (F1.0) .  ADD VALUE LABELS PreQ4DealSeller\_num  1 "Back to the question"  0 "NotVisted" .  EXECUTE.  \* POST Q1  RECODE PostQ1First ("Fraud"=1) ("Legitimate"=2) ("Need more Info"=3) ("Not Sure"=4) INTO PostQ1First\_num.  VARIABLE LABELS PostQ1First\_num 'PostQ1First (numeric)'.  FORMATS PostQ1First\_num (F1.0) .  ADD VALUE LABELS PostQ1First\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure" .  EXECUTE.  RECODE PostQ1Final ("Fraud"=1) ("Legitimate"=2) ("Need more Info"=3) ("Not Sure"=4) (ELSE=0) INTO PostQ1Final\_num.  VARIABLE LABELS PostQ1Final\_num 'PostQ1Final (numeric)'.  FORMATS PostQ1Final\_num (F1.0) .  ADD VALUE LABELS PostQ1Final\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure"  0 "AnsweredAlready" .  EXECUTE.  RECODE PostQ1DealInfo ("Back to the question"=1) ("Need more Info"=2) (ELSE=0) INTO PostQ1DealInfo\_num.  EXECUTE.  VARIABLE LABELS PostQ1DealInfo\_num 'PostQ1DealInfo (numeric)'.  FORMATS PostQ1DealInfo\_num (F1.0) .  ADD VALUE LABELS PostQ1DealInfo\_num  1 "Back to the question"  2 "Need more Info"  0 "NotVisted" .  EXECUTE.  RECODE PostQ1DealSeller ("Back to the question"=1) (ELSE=0) INTO PostQ1DealSeller\_num.  EXECUTE.  VARIABLE LABELS PostQ1DealSeller\_num 'PostQ1DealSeller (numeric)'.  FORMATS PostQ1DealSeller\_num (F1.0) .  ADD VALUE LABELS PostQ1DealSeller\_num  1 "Back to the question"  0 "NotVisted" .  EXECUTE.  \* POST Q2  RECODE PostQ2First ("Fraud"=1) ("Legitimate"=2) ("Need more info"=3) ("Not Sure"=4) INTO PostQ2First\_num.  VARIABLE LABELS PostQ2First\_num 'PostQ2First (numeric)'.  FORMATS PostQ2First\_num (F1.0) .  ADD VALUE LABELS PostQ2First\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure" .  EXECUTE.  RECODE PostQ2Final ("Fraud"=1) ("Legitimate"=2) ("Need more info"=3) ("Not Sure"=4) (ELSE=0) INTO PostQ2Final\_num.  VARIABLE LABELS PostQ2Final\_num 'PostQ2Final (numeric)'.  FORMATS PostQ2Final\_num (F1.0) .  ADD VALUE LABELS PostQ2Final\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure"  0 "AnsweredAlready" .  EXECUTE.  RECODE PostQ2DealInfo ("Back to the question"=1) ("Need more Info"=2) (ELSE=0) INTO PostQ2DealInfo\_num.  EXECUTE.  VARIABLE LABELS PostQ2DealInfo\_num 'PostQ2DealInfo (numeric)'.  FORMATS PostQ2DealInfo\_num (F1.0) .  ADD VALUE LABELS PostQ2DealInfo\_num  1 "Back to the question"  2 "Need more Info"  0 "NotVisted" .  EXECUTE.  RECODE PostQ2DealSeller ("Back to the question"=1) (ELSE=0) INTO PostQ2DealSeller\_num.  EXECUTE.  VARIABLE LABELS PostQ2DealSeller\_num 'PostQ2DealSeller (numeric)'.  FORMATS PostQ2DealSeller\_num (F1.0) .  ADD VALUE LABELS PostQ2DealSeller\_num  1 "Back to the question"  0 "NotVisted" .  EXECUTE.  RECODE PostQ2OfferPrice ("Offer price too good to be true"=1) (ELSE=0) INTO PostQ2OfferPrice\_num.  EXECUTE.  VARIABLE LABELS PostQ2OfferPrice\_num 'PostQ2OfferPrice (numeric)'.  FORMATS PostQ2OfferPrice\_num (F1.0) .  ADD VALUE LABELS PostQ2OfferPrice\_num  1 "Dubious Seller Contact Information"  0 "NotSelected" .  EXECUTE.  RECODE PostQ2DubiousSeller ("Dubious Seller Contact Information"=1) (ELSE=0) INTO PostQ2DubiousSeller\_num.  EXECUTE.  VARIABLE LABELS PostQ2DubiousSeller\_num 'PostQ2DealSeller (numeric)'.  FORMATS PostQ2DubiousSeller\_num (F1.0) .  ADD VALUE LABELS PostQ2DubiousSeller\_num  1 "Dubious Seller Contact Information"  0 "NotSelected" .  EXECUTE.  RECODE PostQ2InadequateInfo ("Inadequate information for product"=1) (ELSE=0) INTO PostQ2InadequateInfo\_num.  EXECUTE.  VARIABLE LABELS PostQ2InadequateInfo\_num 'PostQ2InadequateInfo (numeric)'.  FORMATS PostQ2InadequateInfo\_num (F1.0) .  ADD VALUE LABELS PostQ2InadequateInfo\_num  1 "Inadequate information for product"  0 "NotSelected" .  EXECUTE.  RECODE PostQ2AbsenceofReview ("Seller or product review"=1) (ELSE=0) INTO PostQ2AbsenceofReview\_num.  EXECUTE.  VARIABLE LABELS PostQ2AbsenceofReview\_num 'PostQ2AbsenceofReview (numeric)'.  FORMATS PostQ2AbsenceofReview\_num (F1.0) .  ADD VALUE LABELS PostQ2AbsenceofReview\_num  1 "Seller or product review"  0 "NotSelected" .  EXECUTE.  \* POST Q3  RECODE PostQ3First ("Fraud"=1) ("Legitimate"=2) ("Need more Info"=3) ("Not Sure"=4) INTO PostQ3First\_num.  VARIABLE LABELS PostQ3First\_num 'PostQ3First (numeric)'.  FORMATS PostQ3First\_num (F1.0) .  ADD VALUE LABELS PostQ3First\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure" .  EXECUTE.  RECODE PostQ3Final ("Fraud"=1) ("Legitimate"=2) ("Need more Info"=3) ("Not Sure"=4) (ELSE=0) INTO PostQ3Final\_num.  VARIABLE LABELS PostQ3Final\_num 'PostQ3Final (numeric)'.  FORMATS PostQ3Final\_num (F1.0) .  ADD VALUE LABELS PostQ3Final\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure"  0 "AnsweredAlready" .  EXECUTE.  RECODE PostQ3DealInfo ("Back to the question"=1) ("Need more Info"=2) (ELSE=0) INTO PostQ3DealInfo\_num.  EXECUTE.  VARIABLE LABELS PostQ3DealInfo\_num 'PostQ3DealInfo (numeric)'.  FORMATS PostQ3DealInfo\_num (F1.0) .  ADD VALUE LABELS PostQ3DealInfo\_num  1 "Back to the question"  2 "Need more Info"  0 "NotVisted" .  EXECUTE.  RECODE PostQ3DealSeller ("Back to the question"=1) (ELSE=0) INTO PostQ3DealSeller\_num.  EXECUTE.  VARIABLE LABELS PostQ3DealSeller\_num 'PostQ3DealSeller (numeric)'.  FORMATS PostQ3DealSeller\_num (F1.0) .  ADD VALUE LABELS PostQ3DealSeller\_num  1 "Back to the question"  0 "NotVisted" .  EXECUTE.  RECODE PostQ3OfferPrice ("Offer price too good to be true"=1) (ELSE=0) INTO PostQ3OfferPrice\_num.  EXECUTE.  VARIABLE LABELS PostQ3OfferPrice\_num 'PostQ3OfferPrice (numeric)'.  FORMATS PostQ3OfferPrice\_num (F1.0) .  ADD VALUE LABELS PostQ3OfferPrice\_num  1 "Dubious Seller Contact Information"  0 "NotSelected" .  EXECUTE.  RECODE PostQ3DubiousSeller ("Dubious Seller Contact Information"=1) (ELSE=0) INTO PostQ3DubiousSeller\_num.  EXECUTE.  VARIABLE LABELS PostQ3DubiousSeller\_num 'PostQ3DealSeller (numeric)'.  FORMATS PostQ3DubiousSeller\_num (F1.0) .  ADD VALUE LABELS PostQ3DubiousSeller\_num  1 "Dubious Seller Contact Information"  0 "NotSelected" .  EXECUTE.  RECODE PostQ3InadequateInfo ("Inadequate information for product"=1) (ELSE=0) INTO PostQ3InadequateInfo\_num.  EXECUTE.  VARIABLE LABELS PostQ3InadequateInfo\_num 'PostQ3InadequateInfo (numeric)'.  FORMATS PostQ3InadequateInfo\_num (F1.0) .  ADD VALUE LABELS PostQ3InadequateInfo\_num  1 "Inadequate information for product"  0 "NotSelected" .  EXECUTE.  RECODE PostQ3AbsenceofReview ("Seller or product review"=1) (ELSE=0) INTO PostQ3AbsenceofReview\_num.  EXECUTE.  VARIABLE LABELS PostQ3AbsenceofReview\_num 'PostQ3AbsenceofReview (numeric)'.  FORMATS PostQ3AbsenceofReview\_num (F1.0) .  ADD VALUE LABELS PostQ3AbsenceofReview\_num  1 "Inadequate information for product"  0 "NotSelected" .  EXECUTE.  \* POST Q4  RECODE PostQ4Final ("Fraud"=1) ("Legitimate"=2) ("Need more info"=3) ("Not Sure"=4) (ELSE=0) INTO PostQ4Final\_num.  VARIABLE LABELS PostQ4Final\_num 'PostQ4Final (numeric)'.  FORMATS PostQ4Final\_num (F1.0) .  ADD VALUE LABELS PostQ4Final\_num  1 "Fraud"  2 "Legitimate"  3 "Need more Info"  4 "Not Sure"  0 "AnsweredAlready" .  EXECUTE.  RECODE PostQ4OfferPrice ("Offer price too good to be true"=1) (ELSE=0) INTO PostQ4OfferPrice\_num.  EXECUTE.  VARIABLE LABELS PostQ4OfferPrice\_num 'PostQ4OfferPrice (numeric)'.  FORMATS PostQ4OfferPrice\_num (F1.0) .  ADD VALUE LABELS PostQ4OfferPrice\_num  1 "Dubious Seller Contact Information"  0 "NotSelected" .  EXECUTE.  RECODE PostQ4DubiousSeller ("Dubious Seller Contact Information"=1) (ELSE=0) INTO PostQ4DubiousSeller\_num.  EXECUTE.  VARIABLE LABELS PostQ4DubiousSeller\_num 'PostQ4DealSeller (numeric)'.  FORMATS PostQ4DubiousSeller\_num (F1.0) .  ADD VALUE LABELS PostQ4DubiousSeller\_num  1 "Dubious Seller Contact Information"  0 "NotSelected" .  EXECUTE.  RECODE PostQ4InadequateInfo ("Inadequate information for product"=1) (ELSE=0) INTO PostQ4InadequateInfo\_num.  EXECUTE.  VARIABLE LABELS PostQ4InadequateInfo\_num 'PostQ4InadequateInfo (numeric)'.  FORMATS PostQ4InadequateInfo\_num (F1.0) .  ADD VALUE LABELS PostQ4InadequateInfo\_num  1 "Inadequate information for product"  0 "NotSelected" .  EXECUTE.  RECODE PostQ4ExternalPayment ("Seller is asking for external payment"=1) (ELSE=0) INTO PostQ4ExternalPayment\_num.  EXECUTE.  VARIABLE LABELS PostQ4ExternalPayment\_num 'PostQ4ExternalPayment (numeric)'.  FORMATS PostQ4ExternalPayment\_num (F1.0) .  ADD VALUE LABELS PostQ4ExternalPayment\_num  1 "Inadequate information for product"  0 "NotSelected" .  EXECUTE.  \* Encoding: UTF-8.  /\* PRE TRAINING SCORING /\*  /\* Q1 add first and final to all variables/\*  RECODE PreQ1First\_num (1=1) (ELSE=0) INTO PreQ1A1.  VARIABLE LABELS PreQ1A1 'PreQ1A1 First '.  EXECUTE.  RECODE PreQ1Final\_num (1=1) (ELSE=0) INTO PreQ1A2.  VARIABLE LABELS PreQ1A2 'Pre Q1A2 Final '.  EXECUTE.  RECODE PreQ1OfferPrice\_num (1=1) (ELSE=0) INTO PreQ1A3.  VARIABLE LABELS PreQ1A3 'PreQ1A3 Price'.  EXECUTE.  RECODE PreQ1InadequateInfo\_num (1=1) (ELSE=0) INTO PreQ1A4.  VARIABLE LABELS PreQ1A4 'PreQ1A4 Info'.  EXECUTE.  RECODE PreQ1AbsenceofReview\_num (1=1) (ELSE=0) INTO PreQ1A5.  VARIABLE LABELS PreQ1A5 'PreQ1A5 Review'.  EXECUTE.  COMPUTE PreQ1Total=PreQ1A1 + PreQ1A2 + PreQ1A3 + PreQ1A4 + PreQ1A5.  EXECUTE.  /\* Q2 /\*  RECODE PreQ2First\_num (1=1) (ELSE=0) INTO PreQ2A1.  VARIABLE LABELS PreQ2A1 'PreQ2A1'.  EXECUTE.  RECODE PreQ2Final\_num (1=1) (ELSE=0) INTO PreQ2A2.  VARIABLE LABELS PreQ2A2 'PreQ2A2'.  EXECUTE.  RECODE PreQ2OfferPrice\_num (1=1) (ELSE=0) INTO PreQ2A3.  VARIABLE LABELS PreQ2A3 'PreQ2A3'.  EXECUTE.  RECODE PreQ2AbsenceofReview\_num (1=1) (ELSE=0) INTO PreQ2A5.  VARIABLE LABELS PreQ2A5 'PreQ2A5'.  EXECUTE.  COMPUTE PreQ2Total=PreQ2A1 + PreQ2A2 + PreQ2A3 + PreQ2A5.  EXECUTE.  /\* Q3 /\*  RECODE PreQ3First\_num (1=1) (ELSE=0) INTO PreQ3A1.  VARIABLE LABELS PreQ3A1 'PreQ3A1'.  EXECUTE.  RECODE PreQ3Final\_num (1=1) (ELSE=0) INTO PreQ3A2.  VARIABLE LABELS PreQ3A2 'PreQ3A2'.  EXECUTE.  RECODE PreQ3ExternalPayment\_num (1=1) (ELSE=0) INTO PreQ3A3.  VARIABLE LABELS PreQ3A3 'PreQ3A3'.  EXECUTE.  COMPUTE PreQ3Total=PreQ3A1 + PreQ3A2 + PreQ3A3.  EXECUTE.  /\* Q4 /\*  RECODE PreQ4First\_num (2=1) (ELSE=0) INTO PreQ4A1.  VARIABLE LABELS PreQ4A1 'PreQ4A1'.  EXECUTE.  RECODE PreQ4Final\_num (2=1) (ELSE=0) INTO PreQ4A2.  VARIABLE LABELS PreQ4A2 'PreQ4A2'.  EXECUTE.  COMPUTE PreQ4Total=PreQ4A1 + PreQ4A2.  EXECUTE.  **/\* Total Score Pre-test /\***  COMPUTE PreTrainingScore=PreQ1Total+PreQ2Total + PreQ3Total + PreQ4Total.  FORMATS PreTrainingScore (F1.0) .  EXECUTE.  **/\* POST TRAINING SCORING /\***    /\* Q1 /\*  RECODE PostQ1First\_num (2=1) (ELSE=0) INTO PostQ1A1.  VARIABLE LABELS PostQ1A1 'PostQ1A1'.  EXECUTE.  RECODE PostQ1Final\_num (2=1) (ELSE=0) INTO PostQ1A2.  VARIABLE LABELS PostQ1A2 'PostQ1A2'.  EXECUTE.  COMPUTE PostQ1Total=PostQ1A1 + PostQ1A2.  EXECUTE.  /\* Q2 /\*  RECODE PostQ2First\_num (1=1) (ELSE=0) INTO PostQ2A1.  VARIABLE LABELS PostQ2A1 'PostQ2A1'.  EXECUTE.  RECODE PostQ2Final\_num (1=1) (ELSE=0) INTO PostQ2A2.  VARIABLE LABELS PostQ2A2 'PostQ2A2'.  EXECUTE.  RECODE PostQ2OfferPrice\_num (1=1) (ELSE=0) INTO PostQ2A3.  VARIABLE LABELS PostQ2A3 'PostQ2A3'.  EXECUTE.  RECODE PostQ2AbsenceofReview\_num (1=1) (ELSE=0) INTO PostQ2A5.  VARIABLE LABELS PostQ2A5 'PostQ2A5'.  EXECUTE.  RECODE PostQ2DubiousSeller\_num (1=1) (ELSE=0) INTO PostQ2A6.  VARIABLE LABELS PostQ2A6 'PostQ2A6'.  EXECUTE.  COMPUTE PostQ2Total=PostQ2A1 + PostQ2A2 + PostQ2A3 + PostQ2A5 + PostQ2A6.  EXECUTE.  /\* Q3 /\*  RECODE PostQ3First\_num (1=1) (ELSE=0) INTO PostQ3A1.  VARIABLE LABELS PostQ3A1 'PostQ3A1'.  EXECUTE.  RECODE PostQ3Final\_num (1=1) (ELSE=0) INTO PostQ3A2.  VARIABLE LABELS PostQ3A2 'PostQ3A2'.  EXECUTE.  RECODE PostQ3OfferPrice\_num (1=1) (ELSE=0) INTO PostQ3A3.  VARIABLE LABELS PostQ3A3 'PostQ3A3'.  EXECUTE.  RECODE PostQ3AbsenceofReview\_num (1=1) (ELSE=0) INTO PostQ3A4.  VARIABLE LABELS PostQ3A4 'PostQ3A4'.  EXECUTE.  RECODE PostQ3DubiousSeller\_num (1=1) (ELSE=0) INTO PostQ3A5.  VARIABLE LABELS PostQ3A5 'PostQ3A5'.  EXECUTE.  COMPUTE PostQ3Total=PostQ3A1 + PostQ3A2 + PostQ3A3 + PostQ3A4 + PostQ3A5.  EXECUTE.  /\* Q4 /\*  RECODE PostQ4Final\_num (1=1) (ELSE=0) INTO PostQ4A2.  VARIABLE LABELS PostQ4A2 'PostQ4A2'.  EXECUTE.  RECODE PostQ4ExternalPayment\_num (1=1) (ELSE=0) INTO PostQ4A3.  VARIABLE LABELS PostQ4A3 'PostQ4A3'.  EXECUTE.  COMPUTE PostQ4Total= PostQ4A2 + PostQ4A3.  EXECUTE.  **/\* Total Score Post-test /\***  COMPUTE PostTrainingScore=PostQ1Total+PostQ2Total + PostQ3Total + PostQ4Total.  FORMATS PostTrainingScore (F1.0) .  EXECUTE.  **/\* Time Taken**  COMPUTE time\_for\_completion=(SubmitDateUTC - StartDateUTC) / 60.  VARIABLE LABELS time\_for\_completion "Time For Completing Survey".  VARIABLE LEVEL time\_for\_completion (SCALE).  FORMATS time\_for\_completion (F8.2).  VARIABLE WIDTH time\_for\_completion(8).  EXECUTE.  **/\* Score**  COMPUTE PostMinusPre=PostTrainingScore - PreTrainingScore.  FORMATS PostMinusPre (F1.0) .  EXECUTE.  **/\* Analysis**    \* Encoding: UTF-8.  MISSING VALUES Gender\_num SharedExperience\_num ( 3 ).  EXECUTE.  MISSING VALUES Education\_num ( 4 ).  EXECUTE.  VARIABLE LABELS totalclicks (totalclicks)" .  ADD VALUE LABELS totalclicks  0 "low"  1 "low"  2 "low"  3 "low"  4 "low"  5 "high"  6 "medium"  7 "medium"  8 "medium"  9 "medium"  10"high"  11 "high"  12 "high"  13 "high" .  EXECUTE.  **/\* for discarding time based outliers i.e. participants who took less than 4 minutes and greater than 30 minutes**  COMPUTE Is\_selected = ( time\_for\_completion > 4.00 AND time\_for\_completion < 30.00) .  FREQUENCIES VARIABLES=Is\_selected .  SELECT IF Is\_selected .  EXECUTE.  **/\* Straightliners identification and elimination**  COMPUTE answer\_variation=VARIANCE(PreQ1First\_num,PreQ1Final\_num,PreQ2First\_num,PreQ2Final\_num,  PreQ3First\_num,PreQ3Final\_num, PreQ4First\_num,PreQ4Final\_num,PostQ1First\_num,PostQ1Final\_num,  PostQ2First\_num,PostQ2Final\_num,PostQ3First\_num,PostQ3Final\_num,PostQ4Final\_num).  EXECUTE.  SELECT IF ( answer\_variation = 0).  EXECUTE.  **\* Frequency Analysis**  FREQUENCIES VARIABLES= Age\_num time\_for\_completion.  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=PreQ1Total  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=PreQ2Total  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=PreQ3Total  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=PreQ4Total  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=PostQ1Total  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=PostQ2Total  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=PostQ3Total  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=PostQ4Total  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=PreTrainingScore  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=PostTrainingScore  /ORDER=ANALYSIS.  FREQUENCIES  VARIABLES=PreTrainingScore  /HIST=NORMAL .  FREQUENCIES  VARIABLES=PostTrainingScore  /HIST=NORMAL .  FREQUENCIES VARIABLES=Country\_num  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=Gender\_num  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=Education\_num  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=VictimOfFraud\_num  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=time\_for\_completion  /ORDER=ANALYSIS.  FREQUENCIES  VARIABLES=time\_for\_completion  /HIST=NORMAL .  FREQUENCIES VARIABLES=Age PostMinusPre  /ORDER=ANALYSIS.  FREQUENCIES VARIABLES=time\_for\_completion PostMinusPre  /ORDER=ANALYSIS.  /\* Particpants Education Level /\*  GRAPH  /BAR(SIMPLE)=COUNT BY Education\_num.  /\* Particpants Gender /\*  GRAPH  /BAR(SIMPLE)=COUNT BY Gender\_num.  /\* Particpants Age /\*  GRAPH  /BAR(SIMPLE)=COUNT BY Age\_num.  /\* Particpants heard online shopping fraud /\*  GRAPH  /BAR(SIMPLE)=COUNT BY HeardShoppingFraud\_num.  /\* Victim of online shopping fraud /\*  GRAPH  /BAR(SIMPLE)=COUNT BY VictimOfFraud\_num.  /\* Particpants by Country /\*  GRAPH  /BAR(SIMPLE)=COUNT BY Country\_Num.  /\* Particpants by Gender and Education Stacked Graph /\*  GRAPH  /BAR(GROUPED)=COUNT BY Gender\_num BY Education\_num.  /\* Particpants by Age and Education Stacked Graph /\*  GRAPH  /BAR(GROUPED)=COUNT BY Age\_num BY Education\_num.  **/\* Means Calcuation by Demographics \*/**  MEANS TABLES=PostTrainingScore PreTrainingScore PostMinusPre BY Age\_num  /CELLS=MEAN COUNT STDDEV.  MEANS TABLES=PostTrainingScore PreTrainingScore PostMinusPre BY Country\_num  /CELLS=MEAN COUNT STDDEV.  MEANS TABLES=PostTrainingScore PreTrainingScore PostMinusPre BY Gender\_num  /CELLS=MEAN COUNT STDDEV.  MEANS TABLES=PostTrainingScore PreTrainingScore PostMinusPre BY Education\_num  /CELLS=MEAN COUNT STDDEV.  MEANS TABLES=PostTrainingScore PreTrainingScore PostMinusPre BY HeardShoppingFraud\_num  /CELLS=MEAN COUNT STDDEV.  MEANS TABLES=PostTrainingScore PreTrainingScore PostMinusPre BY VictimOfFraud\_num  /CELLS=MEAN COUNT STDDEV.  MEANS TABLES=PostTrainingScore PreTrainingScore PostMinusPre BY time\_for\_completion  /CELLS=MEAN COUNT STDDEV.  MEANS TABLES=PostTrainingScore PreTrainingScore PostMinusPre BY totalclicks  /CELLS=MEAN COUNT STDDEV.  **/\* Paired T-test for null hyphothesis /\***  EXAMINE VARIABLES=PostMinusPre  /PLOT BOXPLOT NPPLOT  /COMPARE GROUPS  /STATISTICS DESCRIPTIVES  /CINTERVAL 95  /MISSING LISTWISE  /NOTOTAL.  T-TEST PAIRS=PostTrainingScore WITH PreTrainingScore (PAIRED)  /ES DISPLAY(TRUE) STANDARDIZER(SD)  /CRITERIA=CI(.9500)  /MISSING=ANALYSIS.  **/\* Linear Correlation Test H3 hyphothesis /\***    GRAPH  /SCATTERPLOT(BIVAR)=PostMinusPre WITH totalclicks  /MISSING=LISTWISE.  GRAPH  /SCATTERPLOT(BIVAR)=PostMinusPre WITH time\_for\_completion  /MISSING=LISTWISE.  **/\* Particpants Performance between SG and IN - Independent Sample T-Test /\***    T-TEST GROUPS=Country\_num(1 2)  /MISSING=ANALYSIS  /VARIABLES=PostMinusPre  /ES DISPLAY(TRUE)  /CRITERIA=CI(.95).  /\*An independent samples t-test was conducted to see if subjects from both India and Singapore performed well with no significant difference and both groups positively benefitted from the intervention.  /\* Per the statistics below, the effect of training was more visible on Singapore participants and had less impact on India’s participant./\*  /\*This may be caused by the factor that in the training content prices were represented in Singapore Dollar ( SGD ) which might have resulted in erroneous evaluation.  /\*Tests designed with country specific / regional attributes ( local currency and local shopping portals) would have been more effective – for future studies.  **/\* Independent samples T-test by Gender, Score and TimeTaken**    T-TEST GROUPS=Gender\_num(1 2)  /MISSING=ANALYSIS  /VARIABLES=TotalClicks time\_for\_completion PostTrainingScore  /ES DISPLAY(TRUE)  /CRITERIA=CI(.95).  /\*Inference:  /\*Female participants spent more time to finish the survey, had more number of clicks on “need more info” than male counterparts and have also scored well ( PostMinusPreScore).  /\* Education vs Time Spent ( for non-linear ) : Scatter Plot  GRAPH  /SCATTERPLOT(BIVAR)=time\_for\_completion WITH Education\_num  /MISSING=LISTWISE.  /\*Mean: Age-group and Score  MEANS TABLES=PostMinusPre BY Age\_num  /CELLS=MEAN COUNT STDDEV.  /\* Inference:  /\*Participants in the age group of 35-50 years had better scores after the training as compared to other participant age-groups  MEANS TABLES=PostMinusPre BY Gender\_num  /CELLS=MEAN COUNT STDDEV.  MEANS TABLES=PostMinusPre BY VictimOfFraud\_num  /CELLS=MEAN COUNT STDDEV.  /\* Even though the number of participants who were a victim of online-shopping fraud was smaller as compared for those who weren’t victim of an online shopping fraud,  /\* the victim of fraud had better score as compared to the participants who weren’t victim of online shopping fraud.  /\* Female participants had better scores as compared to the male participants  /\* Individual Gender T Test to calculate effect size  T-TEST GROUPS=Gender\_num(1 2)  /MISSING=ANALYSIS  /VARIABLES=PostTrainingScore PreTrainingScore  /ES DISPLAY(TRUE)  /CRITERIA=CI(.95).  /\* Effect size on Countries  T-TEST GROUPS=Country\_num(1 2)  /MISSING=ANALYSIS  /VARIABLES=Post\_Training Pre\_Training  /ES DISPLAY(TRUE)  /CRITERIA=CI(.95).  /\*Digital Divide Study  MEANS TABLES=PostMinusPre BY Age\_num  /CELLS=MEAN COUNT STDDEV.  MEANS TABLES=Post\_Training Pre\_Training BY Age\_num  /CELLS=MEAN COUNT STDDEV. |

## **Paper checklist**

Abstract

1. Have you written the abstract with at least one sentence on the Background, Method and Results, and does it mention N?

*Yes, the abstract has the IMRAD structure.*

Background

1. Have you described the problem that led to your research?

*Yes, we were interested in problem posed by online-shopping fraud and were motivated by the same to initiate a research on the topic.*

1. Have you described the background, and the key references from the peer reviewed literature in APA format on which your work is built?

*Yes, we describe the essence of related research, 12 peer-reviewed papers are cited in APA format.*

1. Have you listed a research question?

*Yes, we have listed the research questions.*

Method

1. Have you added a picture to summarise how the different groups are treated?

*We had only one group in the experiment, so no picture has been added.*

1. Have you described how you recruited your subjects and the number of participants?

*Yes. Our subjects are 147 participants from two countries majorly i.e. India and Singapore, they were recruited via online social media platforms such as LinkedIn, Facebook and an email was sent to SUTD students as well.*

1. Have you described what you asked your subjects to do?

*Yes, we asked our participants to complete a pre-training questionnaire followed by a training and a post-training questionnaire.*

1. Have you described how the control group was created, and how big it is?

*No control group was created in this experiment.*

1. Have you described **all** the dependent and independent variables and how they are coded?

*Yes, all dependent and independent variables are described.*

Results

1. Have you described how you analysed your data?

*Yes, we have described the data analysis.*

1. Have you described which statistical tests you applied to the data, and what the outcome of those tests is?

*Yes, it has been described in the result section.*

Discussion

1. Have you summarised the background and purpose of your research?

*Yes.*

1. Have you described to what extent the research question has been answered?

*Yes, the research had form-based questions.*

Limitations

1. Have you discussed the limitations of your research?

*Yes.*

Conclusions

1. Have you provided conclusions that reflect the key findings?

*Yes.*

1. Have you put your work in perspective as provided by the literature?

*Yes*

Appendices

1. Have you included this completed paper checklist, any questionnaire(s), and the SPSS syntax file as appendices?

*Yes.*

# **Reference**

Bell, F. (2009). Connectivism: a network theory for teaching and learning in a connected world. *Educational Developments, The Magazine of the Staff and Educational Development Association, 10*(3). Retrieved from <http://usir.salford.ac.uk/id/eprint/2569/>

Bramley, P. (1991). *Evaluating training effectiveness: Translating theory into practice*: McGraw-Hill Companies.

Buil-Gil, D., et al. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies, 23*(sup1), S47-S59. doi:10.1080/14616696.2020.1804973

Compeau, D. R., et al. (1995a). Application of social cognitive theory to training for computer skills. *Information systems research, 6*(2), 118-143.

Daft, R. L., et al. (1986). Organizational information requirements, media richness and structural design. *Management science, 32*(5), 554-571.

Duke, B., et al. (2013). Connectivism as a digital age learning theory. *The International HETL Review, 2013*(Special Issue), 4-13.

Goldie, J. G. S. (2016). Connectivism: A knowledge learning theory for the digital age? *Medical teacher, 38*(10), 1064-1069.

Kashif, M., et al. (2020). A surge in cyber-crime during COVID-19. *Indonesian Journal of Social and Environmental Issues (IJSEI), 1*(2), 48-52.

Lallie, H. S., et al. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers &amp; Security, 105*, 102248. doi:10.1016/j.cose.2021.102248

Setiawan, N., et al. (2018). Impact Of Cybercrime In E-Business And Trust. *Int. J. Civ. Eng. Technol, 9*(7), 652-656.

Zhang, X., et al. (2018). Fraud, economic versus social-psychological losses, and sustainable e-auction. *Sustainability, 10*(9), 3130.

# **Web References**

CSA | Singapore Cyber Landscape 2020. (n.d.). Retrieved July 29, 2022, from <https://www.csa.gov.sg/News/Publications/singapore-cyber-landscape-2020>

Global e-commerce jumps to $26.7 trillion, COVID-19 boosts online sales. (2021, May 3). Retrieved from <https://unctad.org/news/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-sales>

The Global Risks Report 2021. (2021, January 19). Retrieved from <https://www.weforum.org/reports/the-global-risks-report-2021/>

Morgan Stanley. (2022, June 14). The Surprising Case for Stronger E-commerce Growth. Retrieved from <https://www.morganstanley.com/ideas/global-ecommerce-growth-forecast-2022>

Typeform. (n.d.). Typeform: People-Friendly Forms and Surveys. Retrieved July 30, 2022, from <https://www.typeform.com/>

Facebook - Marketplace. (n.d.). Retrieved July 30, 2022, from <https://www.facebook.com/marketplace/>

Singapore Police Force. (2021, October 15). Police Advisory on E-Commerce Scam Involving Sale of Newly Released Electronic Devices. Retrieved from <https://www.police.gov.sg/Media-Room/News/20211015_police_advisory_on_e-commerce_scam_inv_sale_of_newly_released_electronic_devices>

National Crime Prevention Council. (n.d.). ScamAlert - Bringing you the latest scam info. Retrieved July 30, 2022, from <https://www.scamalert.sg/>