



## **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: \_\_\_\_\_

Programme of Study ☐ PhD in ☒ Master of Science (MSc)

(please tick one): ☐ 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: 31-July-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.*

## RAISED AWARENESS HELPS DETECTING & PREVENTING ONLINE SHOPPING SCAMS

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**

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.

Results in this study provided a review on the effect of training when categorizing deals as fraudulent or legitimate. The study was conducted with 147 participants across different geographies, age-group, professions, and gender. Our results showed that the capability of spotting a fraudulent deal has improved with the 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
Research Theory .....	11
Research Hypothesis .....	13
Online Shopping Frauds .....	14
Methods.....	16
Participants.....	18
Material Gathering .....	20
Scoring .....	21
Pre-Training-Score .....	21
Post-Training-Score .....	21
Survey Tool.....	21
Data clean-up .....	22
Scoring Scenarios.....	23
Result .....	33
Paired Sample T-Test .....	34
Correlation Analysis – Clicks, Time and Score .....	38
Discussion .....	40
Recommendations.....	42
Limitation.....	43
Future work .....	44
Conclusion .....	45
Appendix.....	47
Questionnaire .....	47
SPS Script.....	47
Reference .....	48
Web References .....	49

## Table of Content - Figure

Figure 1 Statista. (2020, March 23). Breakdown of cybercrime cases in Singapore in 2020 [Graph]. Retrieved from <a href="https://www.statista.com/statistics/1270670/singapore-breakdown-of-cybercrime-cases/">https://www.statista.com/statistics/1270670/singapore-breakdown-of-cybercrime-cases/</a> .....	9
Figure 2 Euromonitor. (2022, June 14). E-commerce as a percentage of retail sales continues to grow across regions. [Graph]. Retrieved from <a href="https://www.morganstanley.com/ideas/global-ecommerce-growth-forecast-2022">https://www.morganstanley.com/ideas/global-ecommerce-growth-forecast-2022</a> .....	15
Figure 3 Facebook. (n.d.). Fraudulent Online-Deal Snapshot - Pre-Training [Photo]. Retrieved from <a href="https://www.facebook.com/marketplace/">https://www.facebook.com/marketplace/</a> .....	17
Figure 4 Facebook. (n.d.). Fraudulent Online-Deal Snapshot - Post-Training [Photo]. Retrieved from <a href="https://www.facebook.com/marketplace/">https://www.facebook.com/marketplace/</a> .....	17
Figure 5 Facebook. (n.d.). Fraudulent Online-Deal Snapshot 1 - Pre-Training [Photo]. Retrieved from <a href="https://www.facebook.com/marketplace/">https://www.facebook.com/marketplace/</a> .....	25
Figure 6 Facebook. (n.d.). Fraudulent Online-Deal Snapshot 1, Detailed deal information - Pre-Training [Photo]. Retrieved from <a href="https://www.facebook.com/marketplace/">https://www.facebook.com/marketplace/</a> .....	26
Figure 7 Facebook. (n.d.). Fraudulent Online-Deal Snapshot – Detailed Information on Seller-Pre-Training [Photo]. Retrieved from <a href="https://www.facebook.com/marketplace/">https://www.facebook.com/marketplace/</a> ..	27
Figure 8 Facebook. (n.d.). Fraudulent Online-Deal Snapshot – back to Q1 main [Photo]. Retrieved from <a href="https://www.facebook.com/marketplace/">https://www.facebook.com/marketplace/</a> .....	28
Figure 9 Facebook. (n.d.). Fraudulent Online-Deal Snapshot – Pre-Training – Attributes for fraudulent deal [Photo]. Retrieved from <a href="https://www.facebook.com/marketplace/">https://www.facebook.com/marketplace/</a> .....	29
Figure 10 Boxplot Graph - Outliers Inspection [Graph]. In Boxplot Graph - Outliers Inspection, two outliers line number 52 and 107 highlighted in the graph .....	34
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.....	35
Figure 12 Scatter Plot Graph for checking linearity between time for completing survey vs PostMinusPre Score.....	39
Figure 13 Scatter Plot Graph for checking linearity between number of clicks on the survey vs PostMinusPre Score .....	39

## Table of Content - Table

Table 1 This table elaborates and flow of the survey i.e. pre-training, the training and the post training.....	31
Table 2 Table representing the independent and dependent variables in this research .....	32
Table 3 Paired Samples Statistics, PostTrainingScore mean 5.94 & PreTrainingScore mean 5.43 .....	36
Table 4 Paired Samples Statistics .....	36
Table 5 Paired Samples Statistics .....	37

## **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 report<sup>1</sup> 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-commerce<sup>2</sup> triggered by COVID-19 which encouraged consumers to opt for online transactions.

<sup>1</sup> CSA | Singapore Cyber Landscape 2020. (n.d.). Retrieved July 29, 2022, from

<https://www.csa.gov.sg/News/Publications/singapore-cyber-landscape-2020>

<sup>2</sup> 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 cases numbers shown in the Figure 1 (Kashif et al., 2020).

**Figure 1**

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

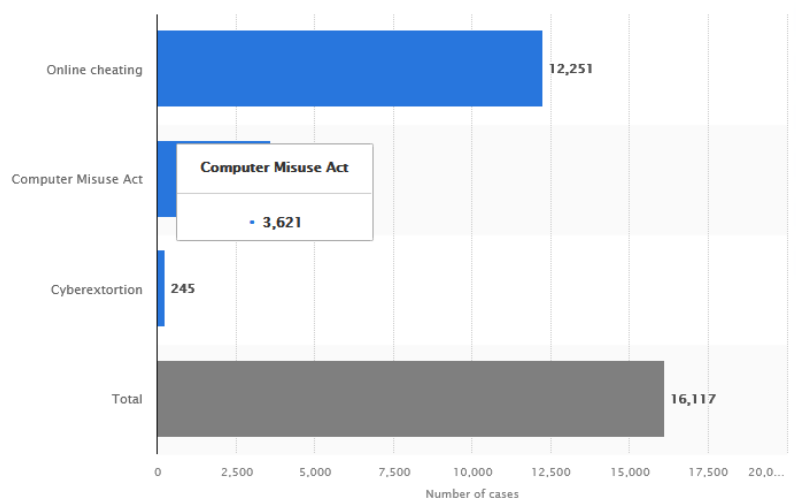


Figure 1 Statista. (2020, March 23). Breakdown of cybercrime cases in Singapore in 2020 [Graph]. Retrieved from <https://www.statista.com/statistics/1270670/singapore-breakdown-of-cybercrime-cases/>

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 Report<sup>1</sup>, cybercrime was ranked by the World Economic Forum as one of the top 5 risks facing the entire world.

<sup>1</sup>The 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

## RAISED AWARENESS HELPS DETECTING & PREVENTING ONLINE SHOPPING SCAMS

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 report<sup>1</sup> 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.

<sup>1</sup>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>

**Figure 2**

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

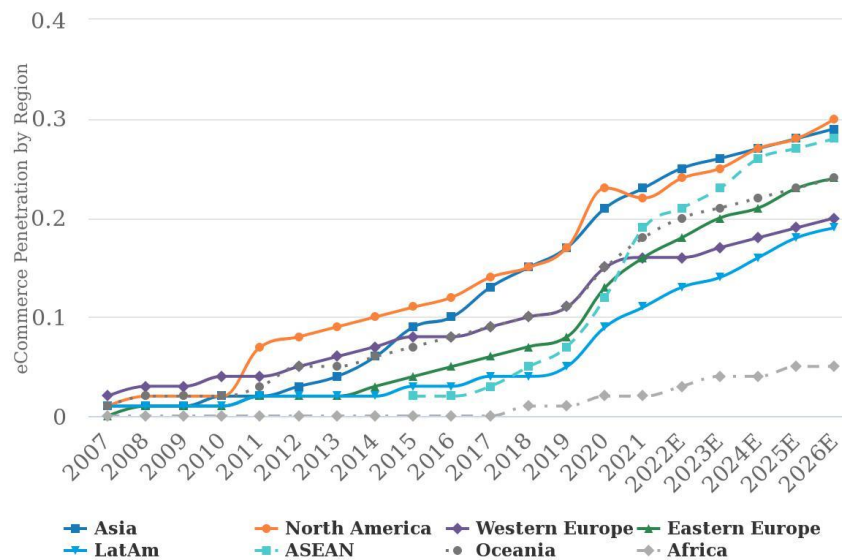


Figure 2 Euromonitor. (2022, June 14). E-commerce as a percentage of retail sales continues to grow across regions.

[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 Typeform<sup>1</sup> 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 Marketplace<sup>2</sup>).

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

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

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



**Figure 3**

*Pre-Training Snapshots*

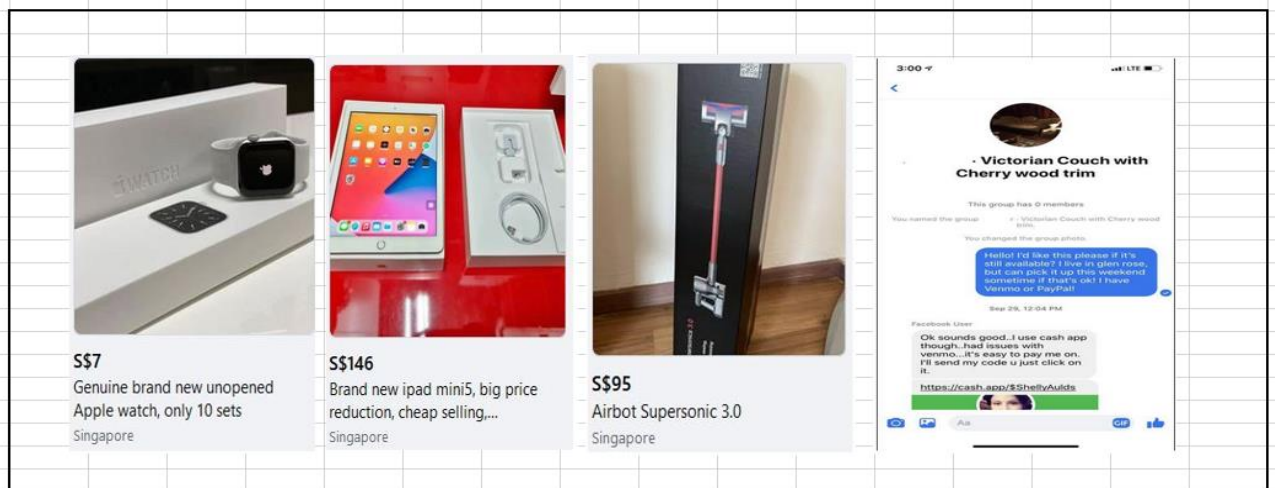


Figure 3 Facebook. (n.d.). Fraudulent Online-Deal Snapshot - Pre-Training [Photo]. Retrieved from <https://www.facebook.com/marketplace/>

**Figure 4**

*Post-Training Snapshots*

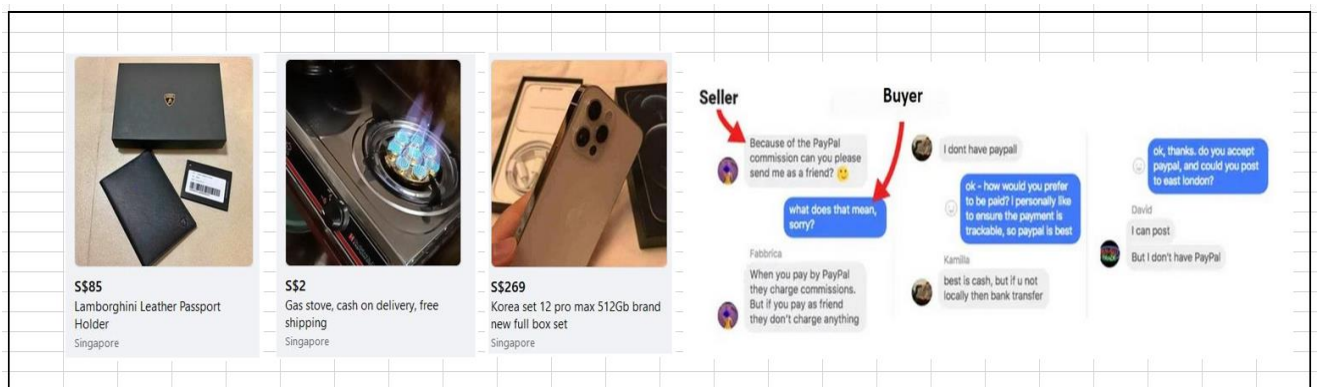


Figure 4 Facebook. (n.d.). Fraudulent Online-Deal Snapshot - Post-Training [Photo]. Retrieved from <https://www.facebook.com/marketplace/>

## **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 of 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

## RAISED AWARENESS HELPS DETECTING & PREVENTING 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 advisories<sup>1</sup> on ecommerce scams & National Crime Prevention Council's scam advisories<sup>2</sup>. 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.

<sup>1</sup> 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](https://www.police.gov.sg/Media-Room/News/20211015_police_advisory_on_e-commerce_scam_inv_sale_of_newly_released_electronic_devices)

<sup>2</sup> 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*

Do you think the deal in the photograph is legitimate or fraudulent?\*

Take a close look at the photograph and click "Need More Info" to get more details about it.

- ☐ A Legitimate
- ☐ B Fraud
- ☐ C Not Sure
- ☐ D Need more Info

[Add choice](#)



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*

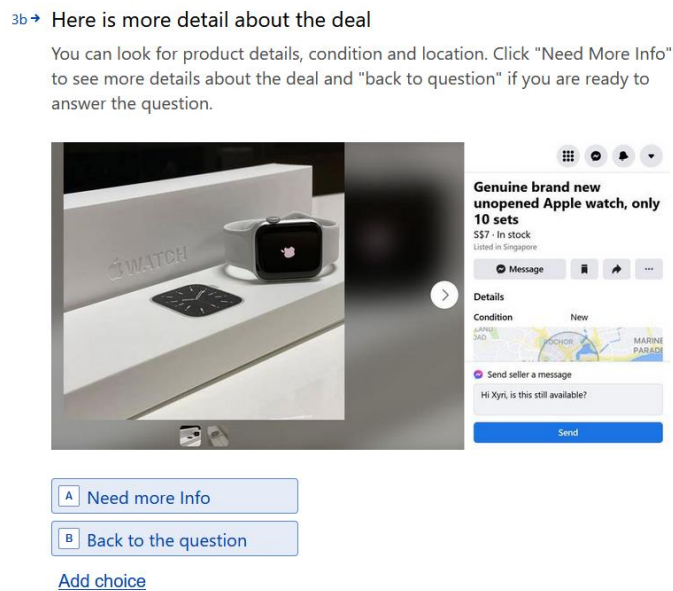


Figure 6 Facebook. (n.d.). Fraudulent Online-Deal Snapshot 1, Detailed deal information - Pre-Training [Photo]. Retrieved from <https://www.facebook.com/marketplace/>

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.

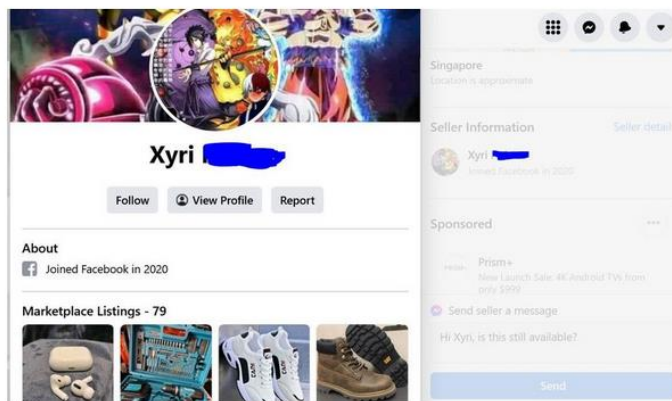
## Figure 7

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

## RAISED AWARENESS HELPS DETECTING & PREVENTING ONLINE SHOPPING SCAMS

3c → Here is more detail about the seller of the deal

You can look for seller's ratings, location and photograph. Click "back to question" if you are ready to answer the question.



[Add choice](#)

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*

3d → Do you think the deal in the photograph is legitimate or fraudulent?\*


Take a close look at the photograph and click "Need More Info" to get more details about it.

☐ A Legitimate

☐ B Fraud

☐ C Not Sure

[Add choice](#)



**S\$7**  
Genuine brand new unopened  
Apple watch, only 10 sets  
Singapore

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

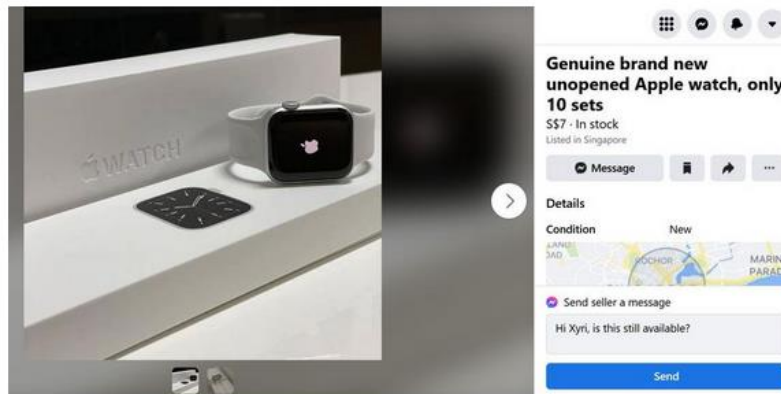
If the participant categorises this fraudulent deal as “Legitimate” or “Not Sure”, they score 0 points and are shown snapshot of question number 2. If the participant correctly categorises this deal as “Fraudulent” they score 1 point and are shown another screen as shown in Figure 9 below.

**Figure 9**

*Pre-Training Snapshot Q1, attributes for fraud*

3e → So you think this online deal is fraudulent, please select the features below which may support your answer:

*Description (optional)*



Make between 1 and 2 choices

- ☐ A Offer price too good to be true
- ☐ B Dubious Seller Contact Information
- ☐ C Inadequate information for product
- ☐ D Absence of seller or product review
- ☐ E Other

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

## RAISED AWARENESS HELPS DETECTING & PREVENTING ONLINE SHOPPING SCAMS

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.

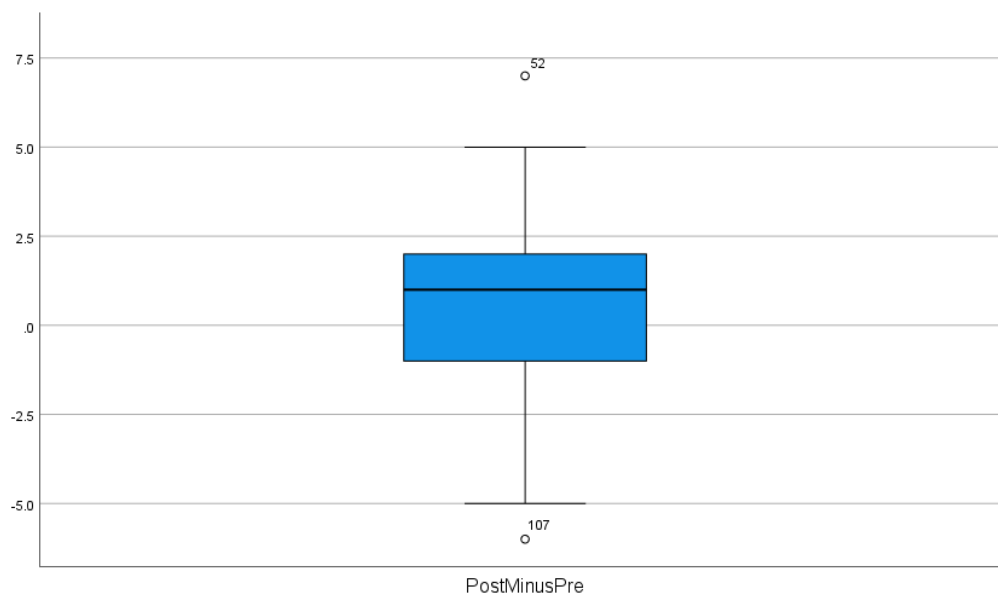
### Paired Sample T-Test

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*

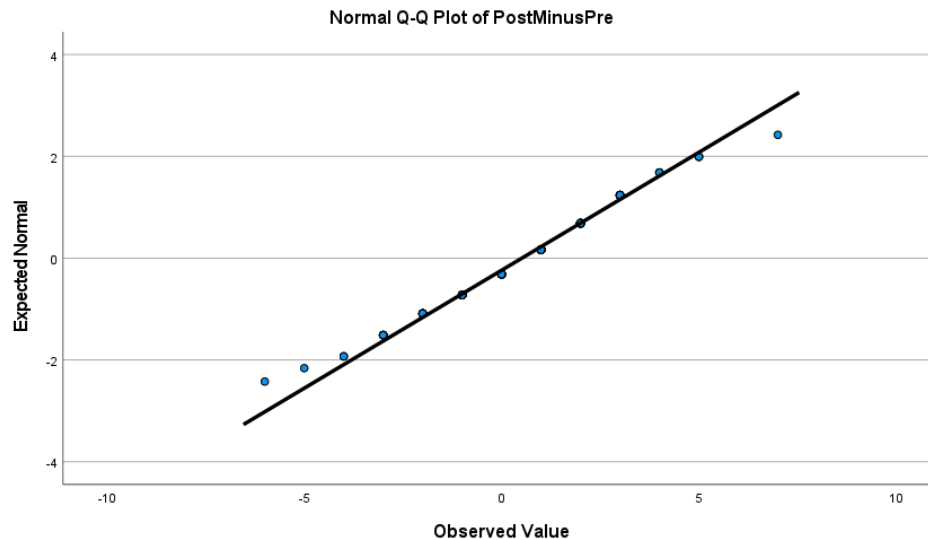


*Figure 10 Boxplot Graph - Outliers Inspection [Graph]. In Boxplot Graph - Outliers Inspection, two outliers line number 52 and 107 highlighted in the graph*

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*

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

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

**Table 5***Paired Samples Test*

		Paired Differences					Significance			
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference		t	df	One- Sided p	Two- Sided p
					Lower	Upper				
Pair 1	PostTraining Score - PreTraining Score	.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 3 and 4 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.

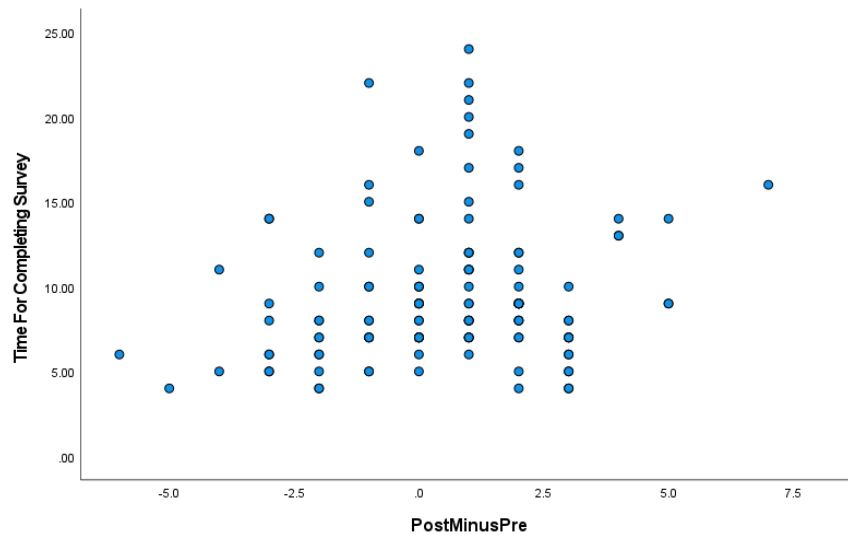
We proceeded to test for linearity with the scatter-plot graph. As shown in the Figure 10 and Figure 11 below, there is no linear relationship between the time for completing survey and the PostMinusPre Score and number of clicks and PostMinusPre score either. The graphs didn't show any monotonic relationship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

Upon visual inspection of the graph, there is no linearity observed between number of clicks, total time spent of the survey and PostMinusPre score, we reject the H3 hypothesis and accept the H4 hypothesis i.e. The time-spent by the participant on the survey and total clicks on the survey form do not influence the participants score.

There is no evidence in the data about relation between two variables, therefore we cannot accept H3 nor the alternative.

**Figure 12**

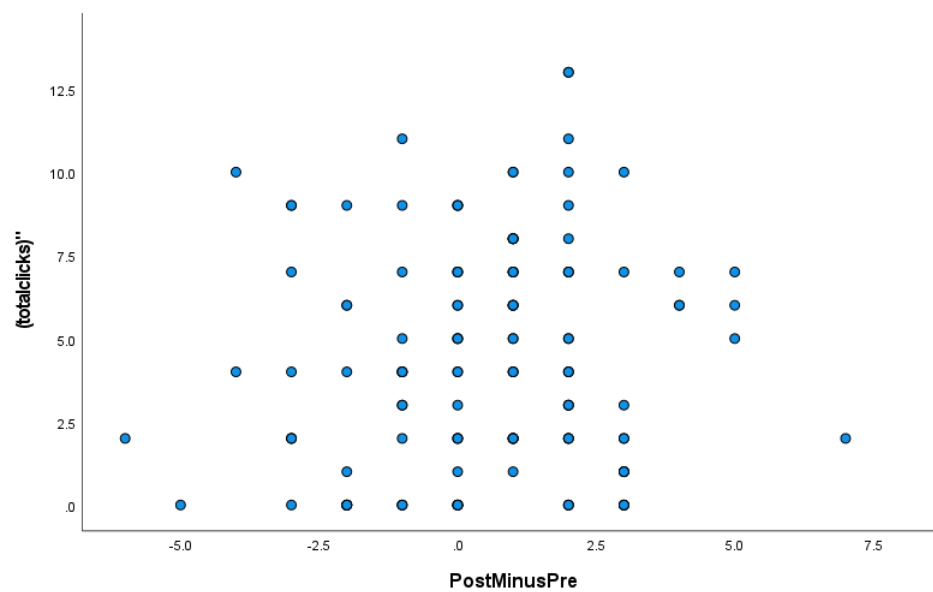
*Scatter Plot Graph Plot for PostMinusPre Score & Time for completing survey*



*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 platforms<sup>1</sup>, the occurrence of online-shopping frauds may increase in future<sup>2</sup>, hence it is important for constantly evolving online-shopping fraud awareness trainings to protect the end-consumer from frauds.

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 theories existing principles.

<sup>1</sup>Ministry 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>

<sup>2</sup>Online 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>

## **Appendix**

### **Questionnaire**

The questionnaire is attached for future researcher's reference



Mayank  
Nauni\_Survey\_Ver3.docx

### **SPS Script**

The SPS Script is attached below for future researcher's reference



31JulCommands\_v1  
1.sps

## 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.
- Compeau, D. R., et al. (1995b). Computer self-efficacy: Development of a measure and initial test. *MIS quarterly*, 189-211.
- 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 & 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](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/>