UNIVERSITY OF TURKU

A Study of Scams and Frauds using Social Engineering in "The Kathmandu Valley" of Nepal

Cyber Security

Master's Degree Programme in Information and Communication Technology

Department of Computing, Faculty of Technology

Master of Science in Technology Thesis

Author:

Amit Maharjan

Supervisors:

Professor Jouni Isoaho

Dr. Ali Farooq

June 2023

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Amit Maharjan
Title: Title
Number of pages: 54 pages, 5 appendix pages
Date: June 2023

Abstract.

Social Engineering scams are common in Nepal. Coupled with inability of government to enforce policies over technology giants and large swaths of population that are uneducated, social engineering scams and frauds are a real issue. The purpose of the thesis is to find out the extent and impact of social engineering attacks in "The Kathmandu valley" of Nepal. The Kathmandu valley consists of 3 cities including the capital city of Nepal.

To conduct the research, the newspaper "The Kathmandu Post" from the year 2019 to 2022 was downloaded and searched for keywords "scam" and "fraud". After which the results were manually examined to separate news reports of social engineering attacks in Nepal and other countries. Also, a survey was conducted by visiting parks in the Kathmandu valley. A total of 149 people were interviewed to collect data by asking 21 questions regarding social engineering attack faced by the interviewee. Further, literature review of the research papers published related to social engineering and phishing was conducted.

The main finding of the thesis was that public awareness program are effective reducing the extent and impact of social engineering attacks in Nepal. The survey suggests large percentage of population have become victims of social engineering attack attempts. More than 70 percent have received messages on WhatsApp regarding fake lottery wins.

Keywords: social engineering, phishing, scams and fraud survey, newspaper report analysis.

Table of contents

Table of Figures

List of tables

List of Abbreviations

BFPT - Big Five Personality Traits

SE – Social Engineering

PF – Psychological Factors

EU – European Union

DNS – Domain Naming System

MFA – Multi Factor Authentication

1 Introduction

Technology has become ubiquitous throughout the society [1]. It has become nearly impossible to live without using technology. Technology be it communication through a simple phone call or availability of all human knowledge on internet has been a great equalizer [2]. We can all reach each other and be more educated more on various topics. However, with the ability to communicate anyone and information from lots of different content creators, it has become possible for bad actors to scam and fraud large swaths of population. As the cost of communication drops it becomes possible for criminals to spam large number of people [3] and make money from small number of people who fall for their scam.

The tools and techniques used to scam and fraud people fall under social engineering [4]. It is well known that humans are a weak link in security [5]. Add to that the fact that education in developing countries is not good and large percentage of people only attend school level education [6], social engineering to scam and fraud the population becomes appealing to criminals.

It is believed that phishing attacks which are a part of social engineering attacks are common in developing countries. For e.g., during the research of newspaper reports about such incidents in Nepal through “The Kathmandu Post” lottery scam report was reported two separate occasions. Also, 84% of the survey participants reported receiving fake lottery win messages.

It is believed that these types of attacks are very hard to mitigate. Couple that with low levels of education, it becomes very hard to mitigate the attacks. The government is only left with choice of holding back the technologies and making them unavailable. For e.g., Nepali debit and credit cards are only usable in few countries like Nepal, Bhutan, India, and recurring charges are not allowed. This hold back of technology impacts entrepreneurs as they cannot develop products that require recurring payments cause the entire country to lag behind in technology.

1.1 Research Objectives

The objective of the thesis is to understand the different types of social engineering attacks prevalent in Nepal. This is done to generate awareness so that people are able to detect social

engineering attacks on them. Generating awareness is expected to make people less susceptible to social engineering attacks.

1.2 Research Questions

The research questions are as follows:

1. What are the different types of social engineering attacks that are most common in Nepal and how can they be mitigated?
2. What are the characteristics of victims or those exposed to scams?
3. What channels of fraud exposure exist?
4. Have people been informed or warned about fraud through awareness campaigns?

1.3 Overview of Research

The scope of research in this thesis is twofold. Firstly, Newspaper reports about various scams reported in "The Kathmandu Post" from 2019 to 2022 have been researched due to easy availability of the newspaper. However, not studying scam in other newspapers has created limitations in the research done for the thesis.

Secondly, for the data collection from the survey, the data collection was limited to certain places in the Kathmandu Valley. The number of surveys was limited to 149 people. These constraints mean that only information about people living in Kathmandu Valley or who visited Kathmandu Valley during the data collection was able to be collected.

1.4 Structure of the Thesis

The rest of the thesis is organized into 5 chapters. Chapter 2 – Literature review, reviews the past and current literature related to this thesis. Chapter 3 – Methodology, describes the methodology of survey and newspaper report research in detail. Chapter 4 – Findings, describes the findings from both survey and newspaper reports research. Chapter 5 – Discussion, describes the implications of findings, limitation of research and future research that can be conducted. Chapter 6 – Conclusion, summarizes the thesis.

2 Literature Review

2.1 Social Engineering

2.1.1 Taxonomy of Social Engineering Attacks

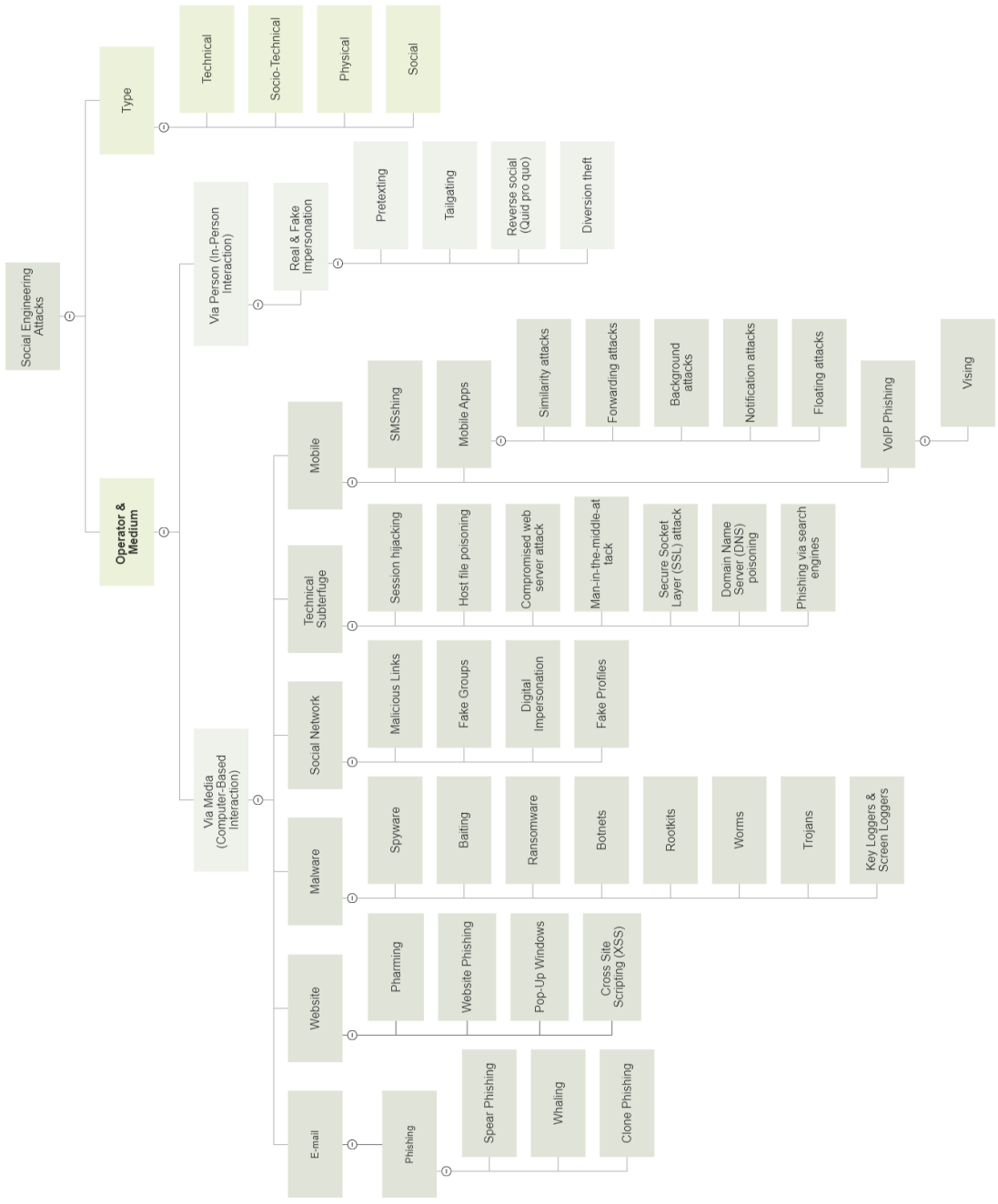

Figure 1 Social Engineering Taxonomy Part 1 [4]

Figures 1 shows the taxonomy of social engineering attacks. As evident from the figure, there are various types of social engineering attacks and various mediums of social engineering attacks such as in-person interaction and computer-based interaction. Under computer-based

interaction there are many subcategories such as E-mail, Website, Malware, Social Network, Technical subterfuge and Mobile.

2.1.1.1 Types of Social Engineering Attacks

There are 4 main types of SE attacks which are as follows:

Social

This type of SE attack uses the techniques of manipulation and persuasion [7]. Psychological skills are used to gain sensitive and confidential information. This method depends highly on the relationship between the attacker and victim [8]. In the second stage of the attack relationship is established with the victim to become trustworthy. Therefore, this method is based on that particular stage.

Technical

In this method of SE attack sophisticated technical tools are used to obtain sensitive information [9]. Since most people use same passwords in many websites, attackers target less secure social networking sites to gain access to their passwords and use it to gain access to other sites [8] [10]. Tools used in this type of attack are email attachments, popup windows, or websites [11].

Socio-Technical

For a social engineering attack to be success, a combination of different approaches is often required. Therefore, some combination of social and technical method are used in SE attacks [8] [10]. Some examples of this type of attacks are Baiting attack, and spear-phishing [7].

Physical

Physical actions of the attacker are required for successful social engineering attack [8]. The most popular example of physical SE is dumpster diving. Extortion or theft are other examples [12].

2.1.1.2 In Person Interaction

Certain principles are used in this approach such as: scarcity, distraction, authority, curiosity, liking and similarity, deception, social proof, fear, commitment, lying, dishonesty, reciprocation, trust, laziness, human need and greed, time pressure, friendship, diffusion of

responsibility, and natural inclination to help [13]. Following are the types of in person interaction attacks:

Impersonation

In this type of attack, attacker present themselves as other people and then gain access to the information they target which may be secured, confidential and private [4]. A go to method of impersonation is pretending to be from helpdesk [14]. Attacker pretends to be from helpdesk department to provide help and get access to the information they want [4].

Pretexting

Pretexting is a technique in which a fake situation is created in order to force the target to act urgently to find a solution. This raises the possibility that the victim will perform certain action or giveaway the information the attacker is after [4]. The situation is designed in such a way that the victim contacts the designer of the attack. Reverse SE is an example of pretexting [14].

Tailgating

The attacker depends on trust or deception in this type of attack. To access secured area the attacker simply walks behind an authorized person. The authorized person will hold the door open following common courtesy. Additionally, using deception the attacker may also pretend to present an identity token [4].

Quid Pro Quo

In this type of attack, random number are dialled pretending to be from technical support. This works because eventually, the attacker hits a person with a genuine problem and glad that someone called. During the process of solving problem, the attacker gets the victim to type commands that give them access or infect with malware [15].

Diversion Theft

In this type of attack, attackers misguide a target who delivers something genuine in another place than the genuine place. The objective is to get the package delivered in an easy to access place [16].

2.1.1.3 Technology-Based Interaction Via Media

In these types of attacks, deceiving events are carried out through various devices and the internet. Devices such as: computer, mobile, tablet, etc which are connected to internet are used. Emails, websites, malware, social networks, etc are used to carry out attacks.

Email

There are various techniques used to conduct SE attacks using email. Phishing is the method of making the messages look genuine to the recipient [17]. It usually contains deceiving information and a link leading to malicious content. Spear-phishing targets specific individual. Whaling targets "whales" in the target organization for e.g., business owners and CEO, CFO, etc. Clone-Phishing uses the legitimate email then replaces links and attachments with fake version [4].

Website

Websites can be used as medium of attack by social engineers in various ways. Pharming is a method in which victim gets redirected to a malware site which then gives access to all the passwords entered into the fake website. Website Phishing is a technique in which a victim is led to believe that they are accessing is a legitimate website. The purpose is to get credentials of the victim. Pop-Up Windows show alerts that cause panic. The victims click on the link to solve the issue which results in attack. Cross Site Scripting (XSS) the attacker is able to appear as victim to a system and then get access to all the information and details [4].

Malware

There are many types of malware SE attacks. Spyware technique uses a special software installed on the devices used by the victim which allows access to personal details, passwords, etc [18] [19]. Baiting technique uses a malware infected physical media left near the victim in the hopes that someone will pick it up and insert into a computer. This allows the attacker to access confidential information. Ransomware is a common SE attack in which the victim gets locked out of their device after visiting infected websites or responding to phishing email. In Botnets devices used by the victim are connected to a compromised network of the attacker. This gives backdoor access to the device. Other types of malware-based attacks are rootkits, worms, trojans, keyloggers and screen loggers, etc [4].

Social Network

In social networks there are various types of social engineering attacks. Attackers send malicious links by impersonating someone of authority or other fake profile. The attackers try to get victims to click on the links and redirect to infected site. Fake groups can be created on social networking sites like Facebook without verification. Hence, attackers might attract victims using fake groups [20] [21]. Digital Impersonation attack is when attacker pretends to be some trusted authority. Attackers often fake their identities by spoofing other users' identity. Fake profiles attack is when attackers create fake identities in social media to gain trust with individual's friend and deceive them later [4].

2.1.1.4 Technical Subterfuge

There are various SE attacks that fall under Technical Subterfuge. They are discussed in 2.2.1.2.

2.1.1.5 Mobile

Apps that are malware infected are easily found on the web. Installing them on smartphones can lead to backdoor access for attackers [22] . This category consists of various attacks which are as follow: In Similarity attacks, apps infected by malware which have fake icons as well as interfaces of login are advertised. Thus, fake apps that look similar to genuine apps might be installed leading to infection from malicious files [23] . In Forwarding Attacks, the attacker uses few smartphone apps to send on important information to different social networking platforms [22] [24]. In Background Attacks, background running apps infected with malware are run which record details of other apps [22]. In Notification Attacks, false notification windows are built which look like genuine notification windows. Thus, information is derived through filling in pop-up notification windows [22]. Floating Attacks often occur in android through background apps. The floating app is not visible, and the perpetrator is provided with information through it [22]. In Voice over Internet Protocol (VoIP) Phishing, attackers hack user devices and steal personal information [25]. In Vishing, attacker use audio conversation to manipulate the victim and get information that is confidential to the victim. Tools that allow faking caller ID and voice modulation are used [4].

2.1.2 What makes social engineering work?

There are many psychological factors and techniques that make social engineering work. The basics of psychological background knowledge are following two concepts.

Firstly, Big Five Personality Traits (BFPT) which are: Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism [26]. BFPT personality traits remain the same throughout the whole life, they can forecast success in career, divorce probability, life expectancy, etc [27].

Secondly, Cialdini's Principles of Persuasion are strategies that can be implemented to so that targets behave in a way that is desired. They are derived from the field of sales and marketing [26]. The seven main principles of which are as follows; (I) LIKING means that person is easily influenced by someone who the person likes or people who have similar beliefs; (II) RECIPROCIATION is a feeling that compels people to giveback the favours; (III) SOCIAL PROOF means copying other people's behaviours; (IV) CONSISTENCY which means similar behaviour or keeping a promise; (V) AUTHORITY, which means following the opinion of experts or following the orders of superiors or other people with authority; (VI) SCARCITY which means valuing the things that are in shortage more than others; [28] When persuasion goes unnoticed, it inspires the use of heuristic reasoning. However, when the target becomes aware of it, response regarding the message becomes unfavourable [26] .

Cognitive Psychological Factors that make social engineering work are Cognitive Miser, Expertise, Overconfidence, and Absentmindedness.

1. **Cognitive Miser** is the process of decision-making using shortcuts [29]. People in general are cognitive misers and make decisions by using heuristic-based processing [30]. McAlaney and Hills suggest that people will use this process of decision making depending on less time availability, perception of importance, and difficulty of situation [31].

2. **Expertise** means the knowledge a person has in a specific field. Qualitatively speaking, a person does become less susceptible to social engineering attack because of expertise [32];[33]. Quantitatively speaking individual does not become more able to cope with social engineering attacks (i.e., decrease in ability to tell if a genuine action or conversation is flagged as social engineering attack or classify an attack as not an attack)[34]

3. **Over Confidence** means the quality of individual in having too much confidence in themselves [35], especially the individual's ability to identify phishing [36] which can be improved through education and training [37].

4. **Absentmindedness** means the amount to which a person's attention is diverted from a singular task. Absentminded people tend to click more on phishing links as they lack attention on their task [38] [39].

Emotional Psychological factors are Greed, Fear, Sympathy, Empathy, and Loneliness.

1. **Greed** as a psychological factor is well recognized by many scholars [26]. It describes a person's strong and selfish desire for things like money, power, or edibles. It is used in phishing attacks to persuade a victim [40] and is frequently paired with what the victim needs (i.e., armed with the knowledge of what the victim needs, it is presented as bait) [41]. The greedier a person more possibility of the person falling victim to social engineering attacks [26].

2. **Fear** describes a person's belief that something which causes pain, is a danger or a threat to oneself may be present. Fear strongly makes people want to avoid the thing in terms of action and thoughts. [42]. Algarni et al. [43] found that social engineering attacks have higher probability of success against people who are fearful. [40]recognize fear as one of the persuasion techniques in phishing.

3. **Sympathy** is an emotional state in which a person understands another's state of mind or emotion without really feeling it [26]. It is a quality present in all individuals which might make them vulnerable to social engineering attacks [44]. This is the reason why attackers often manage to get people's sympathy [26] .

4. **Empathy** is a state in which a person relates state of mind and state of emotion of somebody else based on their own experience [26]. Scammers exploit empathy as a natural behaviour [45]or a persuasion technique [40] to get what they want from victims [46] [45].

5. **Loneliness** is perceived as lack of actual companionship of friends, connectedness in social life, or intimacy compared to what is desired [47]. It is exploited by attackers as perceived loneliness makes them vulnerable [46] [48].

The are 8 **Social psychological factors**. Out of the 8 social psychological factors, 6 are the same as Cialdini's principles of persuasion which have been discussed in 2.1.2. The remaining 2 are: Disobedience and Respect.

1. **Disobedience** is the tendency of an individual to refuse to follow hierarchy of power or rules established by people with authority. Having this quality can make a person open to social engineering attacks [39]. Having employees with this quality can also make the company more vulnerable to SE attacks. [49].

2. **Respect** shows and individual's esteem for another [43]. For example, a person may choose to ignore signs of dubious request from their friend out of respect for their friendship. This PF can go together with Authority [45] [32].

There are 18 **Psychological factors** that impact Personality and Individual Difference which are discussed below.

1. **Disorganization:** This PF describes a person's inclination to act with no pre-planning or to complicate their environment. This condition may make it difficult to notice peculiarity or signs of SE attacks [39].

2. **Freewheeling:** This PF describes tendency of a person to not follow established rules or conventions. This PF makes one more susceptible to SE attacks [39].

3. **Individual Indifference:** This PF describes an individual's disinterest in doing task assigned to them or a necessary task not assigned to them. A culture which promotes risky behaviour can result from long-term indifference toward security. This can be exploited by SE attacks [50].

4. **Negligence:** This PF describes a person's failure to conduct a particular task carefully. It is one of the important reasons for security breaches. Reports show that 27% of data breaches are caused by negligent employees with remote access to organisation's network [26].

5. **Trust:** This PF describes a person's inclination to believe in others. Trusting people are more open to SE attacks [51].

6. **Self-Control:** This PF describes a person's ability to make good decision even when faced with strong emotions and desires. People with less self-control tend to become

victim of online scams [35]. People with low self-control become risk takers and careless concerning cybersecurity principles [50] [52] [53].

7. **Vulnerability:** This PF describes the special needs required because of age of a person, disability that a person suffers from, etc. In case of organization, it was found that employees with only 1 year or under of service are almost twice as vulnerable to spear phishing as employees with eight years of service [54].

8. **Impatience:** This PF describes frustration one experiences while waiting for some something to happen or time required to complete a task. Impatient individual may fall prey to SE attacks as they do not look at things in detail or clues of SE attacks. [53]

9. **Impulsivity:** This PF describes the inclination to act without putting much thought into the action. It was found that people who are after sensation are more likely to fall for scams [26].

10. **Submissiveness:** This PF describe an individual's readiness to follow authority or commands from others. People who are highly submissive are more susceptible to phishing email [55].

11. **Curiosity:** This PF describes an individual's desire to gain knowledge about something. Scammers operating online exploit an individual's curiosity to increase the likelihood of errors in judgement and decision making [35]. They may also use it as bait [26].

12. **Laziness:** This PF describes an individual's inability to complete a task voluntarily. Laziness makes individuals hesitant to do their work or perform tasks that reduce risk thus making them more vulnerable to SE attacks [56] .

13. **Vigilance:** This PF describes the extent to which an individual is observant of possible risks and anomalies. Vigilance decreases the likelihood of becoming victim to social engineering attacks [26].

14. **Openness:** This PF relates to imagination and insight of an individual. Higher openness corelates to higher susceptibility to phishing attacks[57].

15. **Conscientiousness:** This PF relates to careful thought, control of impulse and goal-oriented behaviours. It was found that people who are highly conscientious are less susceptible to spear phishing attacks [26].

16. **Extraversion:** This PF relates to the level to which an individual is sociable, talkative, etc. It was found that extraversion increases the chances of falling for phishing emails [55].

17. **Agreeableness:** This PF relates to attributes like trust, altruism, kindness, etc and other prosocial behaviours [58]. It was found that higher level of agreeableness corelates with higher susceptibility to phishing attacks [59].

18. **Neuroticism:** This PF relates to individual's tendency to be moody and have an instability of emotion. Individuals with higher neuroticism might fall more often to phishing attacks [59].

There are many **Psychological Techniques** that make social engineering work**.** Only the techniques relevant to this thesis are discussed here: **Urgency**, **Incentive and Motivator, Persuasion**, **Trusted Relationship**, **Affection trust** [26].

Urgency

A circumstance which requires instant action or lack of time impacts cybersecurity by creating sense of urgency[50]. This leads to decreased ability to detect deceptive elements in information delivered [60]. Scareware attacks urging installation of software to avoid threats or missing plugin that prevents viewing of desired content are implementation of this tactic [26] .

Incentive and Motivator

This technique makes the victim want to perform desired behaviour or comply with a request. Incentive gives external reward and motivator gives internal reward to the individual. Psychological factors used in this technique are sympathy, empathy, loneliness and disobedience [26].

Persuasion

This technique compels the victim to take particular action by exploiting many PFs. The success of this technique depends on other things like age[61] and request type[22]. Email based attacks for e.g., phishing use persuasion [26].

Trusted Relationship

In this technique, a relationship that the perpetrator already has with a potential victim is exploited by taking advantage of various PFs [62]. An example of use of this type of attack is Business Email Compromise in which a trusted relationship between senior and subordinate staff is exploited [26].

Affection Trust

In this technique, a relationship that is affectionate is established with victim. Affection makes the victim a greater risk taker but does not decrease perception of risk or cause rise in trust [63].

2.2 Phishing

2.2.1 Phishing Techniques and Tactics

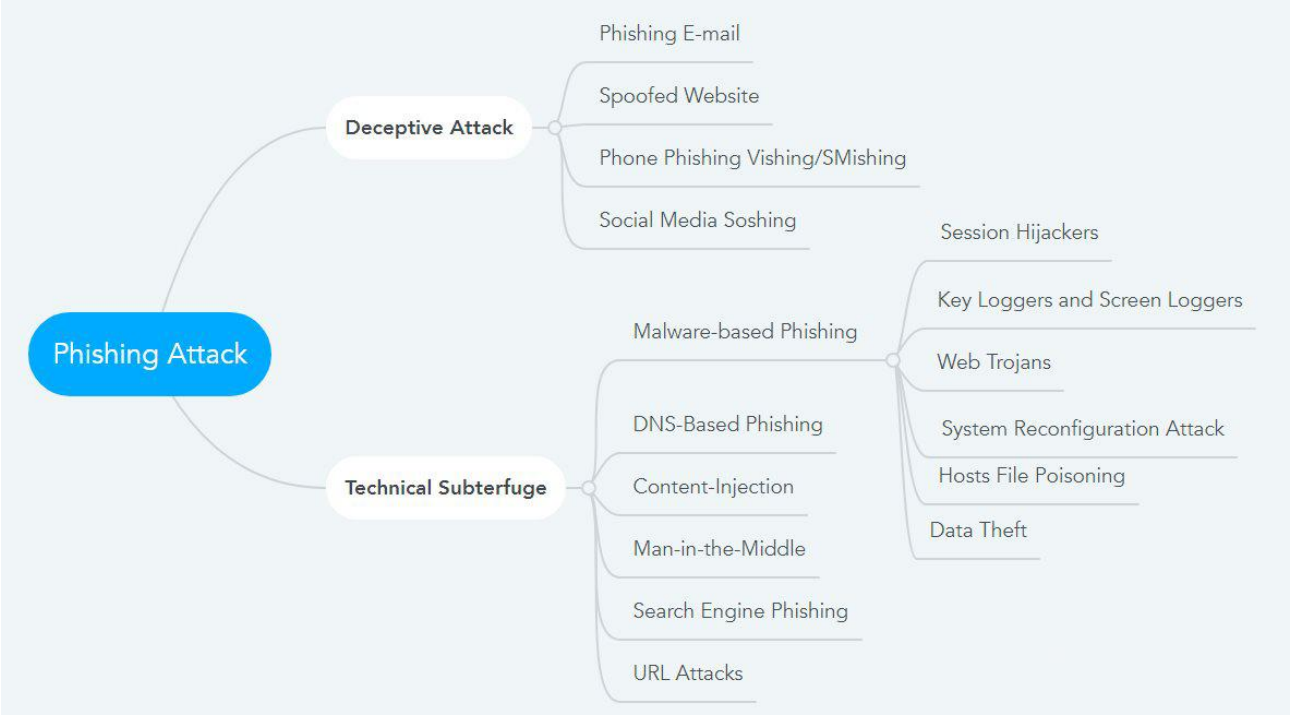

Figure 2 Phishing Techniques and Attacks [64]

As shown in the figure 2 there are many types and techniques of Phishing Attacks. Let us discuss them in detail below.

2.2.1.1 Deceptive Attack

Deceptive phishing is the phishing attack which occurs most often. Social engineering tricks or technical methods are used to lure and convince victims [65]. The victims fall prey by believing in the techniques used.

Phishing e-Mail

Deceiving people through email is the most popular phishing type. An attacker creates a spoofed email and sends it to thousands of victims randomly. The recipient believes the spoofed email to be genuine which leads to the victim giving sensitive information. Spear phishing occurs when a group of people within the same organization are targeted [66].

Spoofed Website

Also known as a phishing website, in this type of attack, a website that looks genuine is created by the attacker. If the target interacts with the spoofed website and enters information, the attacker gains sensitive information [67].

Phone Phishing (Vishing and Smishing)

Phone calls or text messages are used by attackers pretending to be someone familiar to a victim or a source trusted by the victim. Targets get a convincing message pretending to be from banks asking for passwords or PINs. An attacker may also redirect the user to click on a hyperlink sent with a text message. The phisher can gather sensitive information [64].

Social Media Attack (Soshing, Social Media Phishing)

It is the new medium of attack making possible various types of attacks such as account hijacking, impersonation attacks, etc. But detecting and mitigating such attacks is time-consuming because social media is not inside the network that is controlled by organisation [64].

2.2.1.2 Technical Subterfuge

It is the method of getting individuals to disclose delicate information through technical subterfuge by compromising the victim's system through malicious code downloaded in it. There are many types of technical subterfuge which are as follows [64]:

Malware-Based Phishing

Like the name, this type of attack is performed through malicious software run on the user's system. Malware gets injected in the target's computer through SE tricks or by exploitation of system vulnerabilities [65].

Key Loggers and Screen Loggers

Either email attachments that seem genuine but are actually harmful or direct download of malware into target's system is completed. Keystrokes are monitored and recorded which are then forwarded to the attacker.

Viruses and Worms

Viruses transfer between computers through the documents by attaching themselves to the documents while infected host file are the medium of transfer for worms. Both can damage data and software or even cause Denial-of-Service conditions [64].

Spyware

Spyware is malicious software that tracks users through websites and steal delicate information while performing a phishing attack. Email is used to deliver spyware, once installed it takes control of the device and changes settings or gathers delicate information such as passwords, credit card numbers, etc [65]

Adware

Adware shows endless pop-up windows harming the performance of the device. It is mostly safe but may be annoying. Some adware can track the user through websites or even record keystrokes [68].

Ransomware

A malware which encrypts the data in a user's device due to running an executable program is call Ransomware. The malicious attacker then holds the decryption keys for ransom until the user pays [68].

Rootkits

A malicious software that allows access to a computer or network of computers is called rootkit. It is used so that intruders can hide the actions they have taken from system administrators. This is achieved by changing code or modifying functionality [69].

Session Hijackers

In session hijacking, the user's activities are monitored by the attacker through attaching malicious software in the browser or by sniffing the network. The attacker's goal is to hijack the session which allows him to perform act as the genuine user e.g., the attacker is able to transfer money without permission [65].

Web Trojans

Web Trojans collects users' login details by propping up a hidden interface over the genuine login screen. The credentials entered by the users are captured and transmitted directly to the attacker [70].

Hosts File Poisoning

Here, the attacker modifies the hosts file which contains the DNS cache. The result is that the user is taken to a completely different website. This is possible by sending a different IP address when the victim enters a domain name into the browser. It is difficult to detect this type of attack [64].

System Reconfiguration Attack

In this type of attack, the phisher changes the computer settings to compromise the information on the computer through malicious activities. System reconfiguration can be changed through operating system reconfiguration or modification of the DNS server address [65].

Data Theft

Data theft is stealing or accessing delicate information from businesses or individuals without authorization. It can be performed using email. The email contains malicious code which after being downloaded into the target's computer steals delicate information within the computer [65]. Sensitive information that are stolen are as follows: login credentials, government identification numbers, credit card information, etc.

Domain Name System based Phishing (Pharming)

In this type of attack, DNS Server is compromised so the user is sent to malicious website no matter how the user accesses the website. Even hyperlink click will result in redirection to the attacker's website. Pharming is different from Host file Poisoning where host file in the victim's computer is modified [65][71].

Content Injection Phishing

This type of attack fake content is injected into genuine websites. The injected content may redirect users to fake websites, which might lead the victim to disclose their sensitive information or download malware [65] [72].

Man-In-The-Middle Phishing

In this type of attack, the phisher inserts communication between two parties and tries to gain access to messages from both communicators by intercepting the victim's communication. Techniques used for this type of attack are Address Resolution Protocol (ARP) poisoning, DNS spoofing, etc [65]. The culprit may also position himself between a user and an application [73] [74].

Search Engine Phishing

Also known as black hat SEO, malicious websites with enticing offers are created as well as using Search Engine Optimization (SEO). These websites legitimately rank on Search Engines and appear to people searching for products or services [65]. Some of the black hat SEO techniques are keyword stuffing i.e., mentioning the words that they want to rank for many times, Link farm under which a large number of websites link to the website that they want to rank and cloaking under which different content is served to search engine and visitor [75].

URL and HTML Obfuscation Attacks

This is the most popular technique used by phishers today. The real link is obfuscated, and the user is redirected to the phisher's malicious server. Bad Domain Names and Host Name Obfuscation are often used by attackers [64].

2.2.2 What makes phishing work?

There are many factors that make people fall for phishing attacks. Most of them are similar to what makes social engineering works. The factors such as: Reciprocity, Scarcity, Authority, Liking and Social Proof are the same as Cialdini's principles discussed in 2.1.2 "What makes social engineering work". Emotional factors that make social engineering work are Fear and Empathy. They have been discussed under Emotion Psychological Factors. Besides these two more factors make phishing work which are: Curiosity and Contrast [76].

Curiosity: In this method, hackers convince victims by talking about trending topics or facts that are interesting to targets which they might find in social media [76].

Contrast: In this method, two opposite options are given in a manipulative email which forces the victim to pick on option or the other. However, the choice is just a façade because all options are maliciously contaminated [76].

2.2.3 Protection against phishing

There are many protections against phishing attacks. These are discussed below.

2.2.3.1 User Education Approaches

The weakest factor in Internet Security is 'human'[77]. What's more, cybercriminals continue to formulate new attacking techniques depending on human infirmity. To counter this, governments and various organization are providing cybersecurity awareness programs and their prevention [64].[78]

Phishing avoidance by a security warning

The browser plug-in is used to detect phishing by most phishing detection tools. These plugins can instantly recognize phishing instances and warn the user about them. If the warning is ignored, it may lead to adverse outcomes. According to Yang et al., security indicator training makes warning messages more effective [64].

2.2.3.2 Machine learning-based approaches

For Machine learning techniques, learning algorithms are trained based on data representing phishing and non-phishing features. Website parts such as Uniform Resource Locator, HTML content, etc are used to extract features. Machine learning algorithm performs depending on (i) a large number of features, (ii) approach of feature selection, (iii) selected features inconsistency with different selection algorithms [64]. Machine learning techniques can detect attacks more accurately with artificial neural networks [79].

2.2.3.3 Search Engine based techniques

Popular search engines like Google return the brand's domain when searching for a brand name. However, most search engines recognize phishing websites and do not index them. Also, the false alarm rate in this method is very high due to new websites as well as unpopular websites [64].[72]

2.2.3.4 List Based on anti-phishing solutions.

A list of genuine websites is called whitelist and a list of malicious websites is called Blacklist. Websites frequently visited by people are listed in the whitelist. Maintaining a blacklist takes resources such as a system to report the malicious URL [64] [78].

2.2.3.5 Mobile phishing detection approaches

Detecting mobile malicious web page detection is challenging because of the small screen size of smartphones as a user cannot see the full URL [64][78].

2.3 Scams and Frauds

Many types of SE scams exist. Following are the various types of social engineering scams with covid related scams removed from the listing such as: Gift Card Scam, Romance Scam, IRS Scam, Check Scam, Mortgage Scam, Recruitment Scam, Technical Support Scam, Law Firm Scam, Cat Scam and Landlord Rental Scam [80]

2.3.1 Gift Card Scam

In this type so scam, the victim is promised financial help in return for buying gift cards for the scammer from Walmart, target, CVS, etc. However, once the scammer gets gift cards, they sever their contact with the victim. The scammer may then use the gift card to buy things

for themselves or use a mule to do so. Tracking scammers is very difficult in this case as cooperation from multiple parties is required. [80]

2.3.2 Romance Scam

Online Romance scams one of the most prevalent and profitable crimes made possible by internet. Criminals create fake profiles in dating or social networking sites and make the targets fall for them and then ask for money. The double loss of relationship and money is sometimes hard on victims [81].

2.3.3 IRS Scam

IRS Scam are based on technique known as phishing. Pretending to be a legitimate source in emails and phone calls then collecting this information into a database which is then used to scam individuals to give large amounts of money. [82]

2.3.4 Check Scam

In this type of scam, the scammer exploits a loophole the banking system i.e., it takes a few days to process checks. The criminals send a fake overpaid check and ask for the overpaid money to be returned in genuine check. They then cash the genuine check. The victim loses money as well as is exposed to judicial proceedings. [83]

2.3.5 Mortgage Scam

In this type of scam, the scammers sell federally insured homes which are often in need of huge repairs. Unable to pay for repairs the victim family would lose everything they invested in the home. [84]

2.3.6 Recruitment Scam

In this type of scam, scammer get access to sensitive information which they later use to blackmail the person or applicant. The applicants often resign from their current position leading to loss of job and becoming a victim of blackmail. [85]

2.3.7 Technical Support Scam

In this type of scam, a popup shows up asking to contact the given phone number immediately in order to solve the errors. If the person calls the number, the scammer will ask

to fix their computer performance issues or computer virus issue. If the user is unable to identify the scam, the follow the instructions it may lead to malware infection by scammer. The scammer then asks for money, or they ask for money for fixing the issues. If the money is transferred, the scammer disappears immediately. [86]

2.3.8 Law Firm Scam

In this type of scam, the scammer impersonates attorneys and collect money on behalf of attorneys. For e.g., scammers send emails to a large number of people in a county raising money for a good cause. If normal people think a respected attorney is raising the money, they may donate money. [80]

2.3.9 Pet Scam

In this type of scam, the scammers get a pet adoption website up and running. They use various techniques and tactics to get a victim emotionally invested with the fictious pet. The unaware victim might order the pet online and pay for the pet and shipping. Once the scammers get the money, they switch to other tactics to get more money from emotionally and financially invested victim. [87]

2.3.10 Landlord Scam/ Rental Scam

There are 2 types of scams in this category. The scammers post fake house renting post in social media or paper ads; getting victims to pay in advance for rental confirmation. Once the money is transferred, the scammer won't respond.[80]

The other type of scam in this category is one in which the scammer pretends to be a renter. They give the check of more than the due amount and ask for the higher amount to be returned. If the landlord falls for it, they scammer withdraws from the landlord's contact. [80]

Other types of scams are Ewhoring Scam, Craigslist Scam [80].

2.4 Information Technology in Context of Nepal

Nepal is one of the least developed countries as classified by United Nations. However, it enjoys access to products from India and China. Concerning the situation of Information Technology in Nepal; Nepal had first computers in 1971 which were used for conducting the census. Even so personal computers first appeared in the marketplace in 1985. Every year

about 5,500 Nepalese graduates enter the IT sector. There are about 500 IT companies in Nepal among which few companies have more than 300 employees [88].

In terms of number of websites and registered domains, Table 1 shows the information.

S.No.	Domain Category	Total Domain
1.	Com.np	10820
2.	Org.np	2505
3.	Edu.np	1312
4.	Net.np	480
5.	Gov.np	376
6.	Mil.np	1

Table 1Registered Domain in Nepal [89]

Nepal has a sizeable population for a country of its size at about 30 million. Furthermore, the population is young of which half of the population are under 30. So, it can be assumed that the population is more tech savvy compared to similar countries with older population. There are many ecommerce websites in Nepal which has benefited from presence of digital payment mechanisms. Social media sites like Facebook and Instagram are also very popular in Nepal. The most popular e-commerce site is daraz.com.np which was launched in 2014. [90]

In terms of connectivity, as of January 2022 Nepal has 11.51 million internet users. 38.4 percent of the population is connected to the internet. Connectivity and delivery of products is difficult in Nepal due to 80% of people living in rural areas [90]. Various broadband technologies are used to connect people to internet in Nepal. 4G Services has been introduced in 72 out of 77 districts headquarters in Nepal [88].

The GDP per capita of Nepal is USD 1208.2 as of 2021 [91]. This means personal computers are out of reach of most people in rural areas. However, according to Nepal census data 2022, the smart phone penetration in Nepal is 73% [92].

In terms of datacentres, Nepal has about a dozen data centre [93].

2.5 Similar Studies and Comparison

In their research [94], they conducted a study of impact of scam education in the form of tips in a market where phone scams were highly prevalent. Their study found that there was no significant impact of tips on Scam Identification Ability. On further analysis, they found that

non-scam communication from organization banks contained markers of scam communication. If such communication could be distinguished from scam messages, people's ability to detect scams would be clearly improved. Furthermore, they show that tips lead to increased confidence but not overly confident in detecting scam. [94]

The survey conducted for the thesis has revealed that awareness raising program do make a difference in people falling for social engineering scams. These awareness raising messages are distinct from regular communication from banks which is critical for their success.

In their research [95], found that risk factors such as characteristics of society and economy, delicate state of finances, lack of social company, and competence in financial matters vary by the category scam and being aware of exact scam is helpful in protection against the scam. They also conclude, that having a widespread consumer awareness campaign from various organizations such as government, non-profit, and private sector stakeholders would benefit the consumers. [95]

The survey also revealed that the single most important factor in preventing people from becoming victims was education and second factor was exposure to messages from awareness raising programs.

In their research [96], any program that is aimed at keeping people from becoming victims needs to consider: social conditions, demographic data, qualities of the people, and activities that happen routinely and that considering just routine activity or personality does not work. Websites like e-commerce sites, dating sites, etc need to give advice upfront in an easily accessible way and the information should be useful and correct advice. [96]

The findings of [96], are like those found during this thesis, in that many victims were found to have suffered from e-commerce websites. Hence, identifying trustworthy e-commerce websites is key to protect from e-commerce fraud. Other services such as dating sites are not popular in Nepal.

In their research [97], suggest that in Ghana, even with work on managing cyber fraud, it will remain a necessary evil and a threat as long as online shopping exists. It cannot be eradicated. Online systems in Ghana lack trust because of issues in online information security. [97]

In case of Nepal, it was found that ecommerce fraud is much less pronounced in trusted e-commerce websites such as: daraz.com.np, and sastodeal.com. This is due to the requirement

for vendors to be registered as shops or vendors in the government registration service. This is different from problems faced and accepted as necessary evil in Ghana.

In their research [98], fraud of elders in USA is widespread. These frauds are conducted through voice calls, E-mail, Short Message Service, pop-ups, and letters. Probability of being defrauded decreases with simple prevention and mitigation strategies such as use of strong passwords, MFA, anti-virus software, pop-up blockers, no-caller ID applications, Federal Trade Commission blacklists. [98]

In case of Nepal, it was found that frauds were present in the form of WhatsApp messages and calls. However, few people fell for the bait. The high financial loss occurred in fraud that happened in person. While ecommerce fraud was second leading factor.

In their research [99] found that people who are less agreeable and more extravert have higher chance of becoming victims of identity theft. People who are neurotic and work in the field outside of their studies may face more harassment. Men who are working fulltime outside their field of study have higher probability of becoming victims of scam. Men working in their field of study have higher probability of becoming victim of phishing [99].

The personality type and their impact were not studied during the thesis. Hence, comparisons cannot be drawn between the research conducted and [99].

In their research [100], found that in Malaysia online review of products are the most important consideration for people buying products and that Malaysians should not believe the online review of products so much or only believe reviews provided by authentic users. [100]

During the research, 30% of the people were found to check customers reviews and ratings before buying from an e-commerce website. This means that ratings and reviews are not a very important factor during purchase for participants.

In their research [101], where a total of 1710 people participated, 223 were victims but only 20 reported to the police. The financial impact was the most important factor for reporting to the police. [101]

People who suffered a high financial loss went to police or other official authority for help. This is like what was found during the thesis and is what is expected.

3 Methodology (Newspaper Reports & Survey)

In this section, the methods used to conduct the research, and analysis of data to arrive at conclusions are described. There are two research methods employed: a face-to-face survey of 149 people and newspaper research of the daily newspaper "The Kathmandu Post" spanning 4 years and totalling 1460 newspapers.

3.1 Instrument Development

Nepal is a multicultural nation with most people speaking several languages. Students are taught in English in private schools starting in childhood. Also, the Nepali language has failed to keep up with modern technology and science leading to the language being ineffective in discussions surrounding rapidly changing information technology.

Coupled with the technical nature of social engineering, it is very difficult to collect data through other forms of data collection such as interviews and focus groups. Furthermore, when using survey in Nepali language, people might misinterpret the questions and lie as they might not want to show their ignorance.

Taking above factors into consideration as well as considering the report for EU Survey On "Scams and Fraud Experienced by Consumers" [102] on which the research of this thesis is based, the author decided to create a questionnaire so that the difficult task of building the questionnaire was simplified by basing the questions on the EU survey to some degree. The questionnaire is attached in the appendix chapter named "Survey Questionnaire". Furthermore, conducting survey allowed the author to explain each question to the participant where not understood. This ensured that questions in the survey were properly understood by the participant.

The objectives of the survey are as follows [102]:

- Understand the frequent and common type of fraud/scam.
- Understand the most frequent channels used by fraudsters.
- Identify financial as well as non-financial impact of the frauds/scam.
- To measure if consumers are aware of awareness raising programs about scams and frauds and protect themselves.
- To measure the extent to which scams and frauds effect online behaviour.

3.2 Survey Participants

To get variety of participants and decrease bias in the collected data, the survey was conducted in public places where a good mix of people from different age groups, ethnicities, and professions could participate. The survey was done in Jawalakhel Park, Basantapur, and Patan Durbar Square and a total of 149 respondents were surveyed.

The limited number of respondents and locations might skew the data from the study.

Therefore, the survey method was chosen to collect the data. The survey was inspired by Survey on "Scams and Fraud Experienced by Consumers" of the European Union [102]. This is so that the hard part of designing a good survey does not fall on the shoulders of the author.

3.3 Newspaper Research

For research of newspaper reports of scams and frauds, "The Kathmandu Post" was chosen. The Kathmandu Post is the largest-selling English daily newspaper in Nepal making it a reliable source of scam and fraud reports.

Also, the daily newspaper is available in text searchable PDF format going back 5 years. However, only 4 years' worth of newspapers were studied. This availability made it possible to quickly search the archive of about 1460 newspapers for reports of scams and frauds.

First, all the newspapers were downloaded into a local hard drive. Then," Foxit PDF Reader" software was used to search the archive for keywords "scam" and "fraud". The resulting search results were then manually studied one by one to qualify for social engineering or information technology-related reports of scams and fraud. All corruption-related reports were ignored as they as not closely related to the subject of research but to politics.

The search resulted in national and international scam and fraud reports, corruption reports, bribery reports, etc. Clearly, not all the reports in the newspaper were social engineering related.

The date and page number of the qualifying newspaper reports were recorded. Then, the reports were used to draw a summary of national and international scam reports in the newspaper.

4 Scams & Frauds Reported in “The Kathmandu Post” and Survey Research

This section describes the scams and frauds reported in “The Kathmandu Post” newspaper from 2019 to 2022. It also summarizes and draws parallels between the survey and the reports.

4.1 Findings from Scam & Fraud Reports in “The Kathmandu Post”

This section describes the scam and fraud reports related to social engineering in “The Kathmandu Post” from 2019 to 2022. Each subsection is divided by year and then is described by month.

4.1.1 2019

In March 2019, there was 1 scam report. On 9 March 2019, there was a report from the Australian watchdog suspending two cryptocurrency exchanges. A study revealed that the value of stolen cryptocurrency surged over 400 percent to about $1.7 billion in 2018.

In April 2019, there was 1 scam report. On 24 April 2019, there was a report of Indian and Chinese nationals conning Nepalis through a lottery scam with a Nigerian national. The group had frauded Rs 4,039,419 in total. They used Facebook, Viber, WhatsApp, and IMO to contact victims.

In July 2019, there was 1 scam report. On 24 July 2019, there was a report of fake opportunities to buy Libra, Facebook’s currency. The fraudsters used the official Facebook logo and photos of Facebook CEO Mark Zuckerberg.

In December 2019, there was 1 scam report. On 12 December 2019, there was a report of the arrest of three men who defrauded Rs 150 million through lottery scams.

4.1.2 2020

In January 2020, there were 1 scam reports. On 11 January 2020, there was a report of police arresting five persons including two foreigners over an online parcel scam. The victims were told to deposit money in bank accounts which were supposedly for parcel clearance at the airport.

In February 2020, there was 1 scam report. The report was about malicious files disguised as popular award-winning movies. The report says Kaspersky Company found over 20 phishing websites and 925 disguised files.

In March 2020, there was 1 scam report. On 18 March 2020, there was a report of scammers pretending to be from a bank who were authorized to collect Covid contaminated bank notes and gave fake receipts. The victims were told that receipts were tradable for clean banknotes.

During April 2020, there was 1 scam report. On 28 April 2020, there was a report of an increase in the number of cybercrimes which grew from 4 per day to 6 per day. The report mentions an ISP in Nepal suffering from a data breach that leaked over 170,000 customer data.

In June 2020, there was 1 scam report. On 26 June 2020, there was a report of people running a lottery scam. The arrestees had swindled over Rs 10 million from the victims. According to the database of Nepal police headquarters, fraud cases are steadily increasing with 627 cases in 2018/19.

4.1.3 2021

In February 2021, there was 1 scam report. On 4 February, there was a report of foreign nationals collecting money promising jobs in foreign countries. One of the companies was demanding INR 8,000 for filling out the application and Rs100,000 when the offer letter would arrive. It is suspected that the foreign employment sector has become a playground for foreign scammers.

In July 2021, there was 1 scam report. On 21 July 2021, there was a report of 577 fraud cases filed in the country regarding foreign employment. One solution suggested was verifying the job demand letter with the concerned embassy.

4.1.4 2022

In January 2022, there was 1 scam report. On 10 January 2022, there was a report of a manuscript theft scam. The perpetrator would pretend to be a legitimate person trying to get hold of manuscripts. The perpetrator was accused of registering more than 160 fraudulent domains. However, the financial benefit of the perpetrator was not clear.

In March 2022, there were 2 scam reports. On 08 March 2022, there was a report of informal money transfer scams hitting such heights that many embassies stopped labelling them as informal money transfer scams. On 15 March 2022, there were reports of consumers being defrauded in price, quantity, and quality of goods. The government does seem to be able to do much about it.

In July 2022, there was 1 scam report. The report was about a call centre running scams to dupe people. It was run by a Chinese national, 2 Indians, and 33 Nepalis.

In October 2022, there was 1 scam report. The report was about Indian tech workers lured into various countries by promising them high salaries but then forced to commit a cybercrime once they reach there. A total of 130 people were rescued.

In November 2022, there was 1 scam report. On 3 November 2022, there was a report of cyber criminals holding Asian tech workers captive in scam factories. The report says it took 15 days of building a relationship with the target to get them to invest in a bogus cryptocurrency.

4.1.5 Summary Findings of Newspapers Analysis

The following figure 3 are a mind map of the scams reported in “The Kathmandu Post” newspaper from year 2019 to 2022. The scams are divided by the location of their occurrence for e.g., Nepal means that scams occurred in Nepal and “international” means scam occurred outside Nepal.

In the survey, lottery scam was found to be the most pervasive type of scam with 84% participants reporting that they got messages saying they were winners of lottery but only few fell for it. Similarly, in the newspaper reports, lottery scam is reported in 2019 and 2020. This shows that lottery scam is indeed a pervasive type of social engineering scam in Nepal.

During the survey, I met a participant who was lured into what seems to be a good job in India but then it turned out to be a criminal operation where the victims were forced to work under unfavourable conditions. Similarly, this type of crime is reported in Nepal in 2021 Foreign Employment scam as well as in 2022 international cases were reported: Tech worker scam in India and Asia.

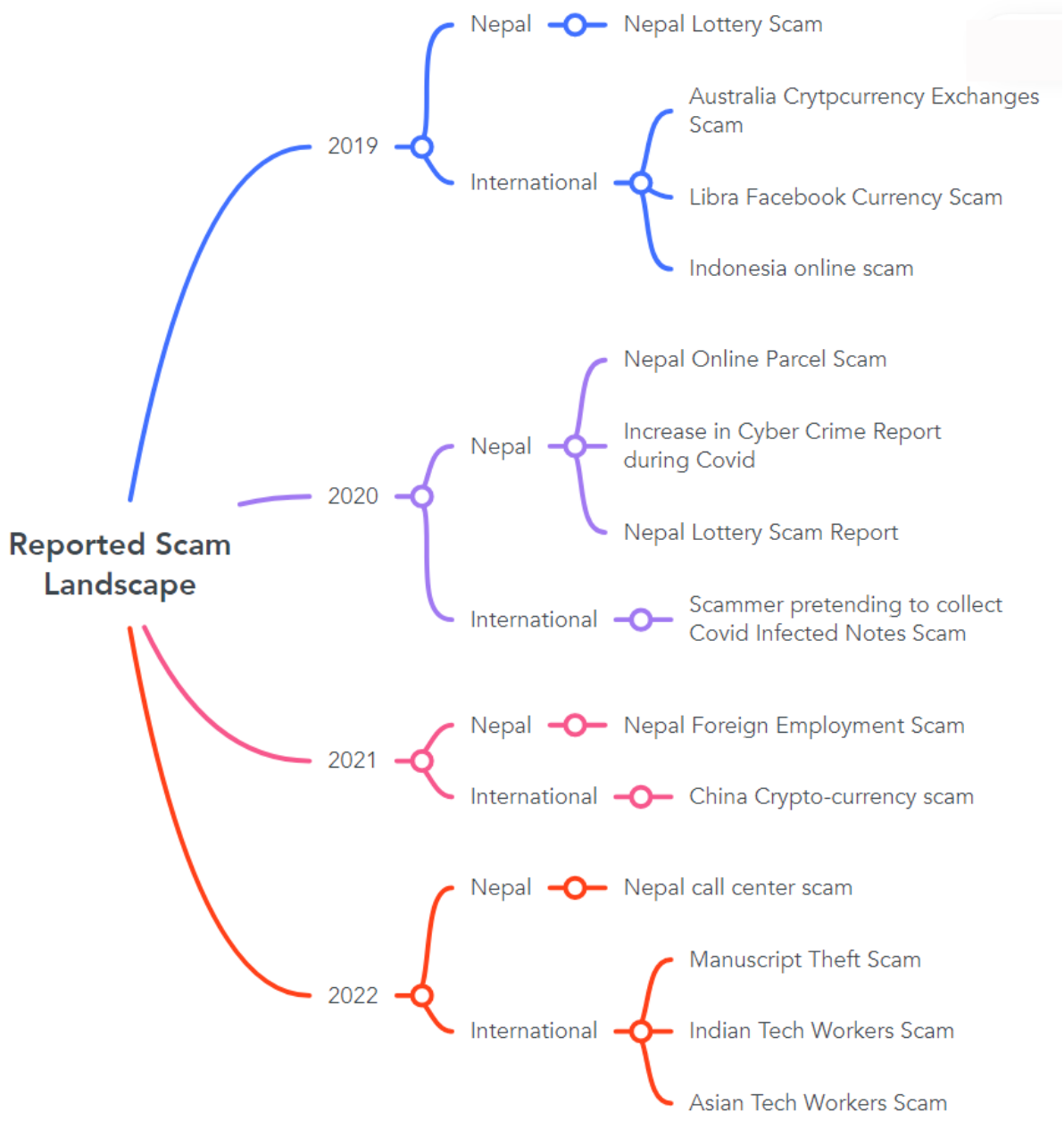

Figure 3 Scams & Frauds (Social Engineering Attacks) Reported in "The Kathmandu Post" 2019 to 2022

4.2 Findings of Survey

4.2.1 Gender

Figure 4 shows that out of the survey participants, about 83.11 percent were male and 16.89 percent were female.

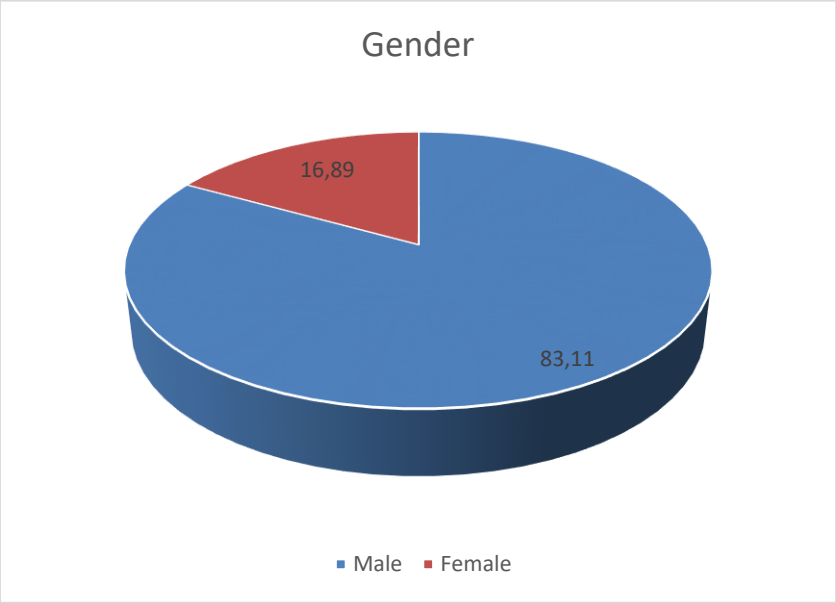

Figure 4 Gender

Upon detailed observation, it is evident that men suffer in multiple ways while women suffer in linear ways. 15% of men suffered both emotionally and financially while 28% of women suffered emotionally only. This is in contrary to popular belief that men are not emotional.

Men were twice as likely to fall for a chance to invest or receive a good, a service or rebate than women.

The data shows that 52.9% of women receive lottery win notification, 23.5% suffered from lottery win notification as well as they fell for product that seemed like a good deal, but the product turned out to be fake or non-existent. 11.7% fell for a fake good deal and another 11.7% fell for fake investment opportunity. On average, salary of men is higher than women across all categories [103].

Men were 20% more likely to buy or not buy goods online for "other" reason. While women were twice as likely to be not interested in buying goods online.

It is interesting to note that top two channels used for reporting are opposite for male and female. In first position, 47% of the men reported to friends and family while only 34% of

female reported to them. In second position, 43% of men did not report to anyone while 47% of women reported to no one. About half of the population don't report to anyone.

4.2.2 Education Level

Figure 5 shows that out of the participants, 30 had completed school level, 32 had completed High School Level, 63 had completed college studies and 23 had completed Master's or higher studies.

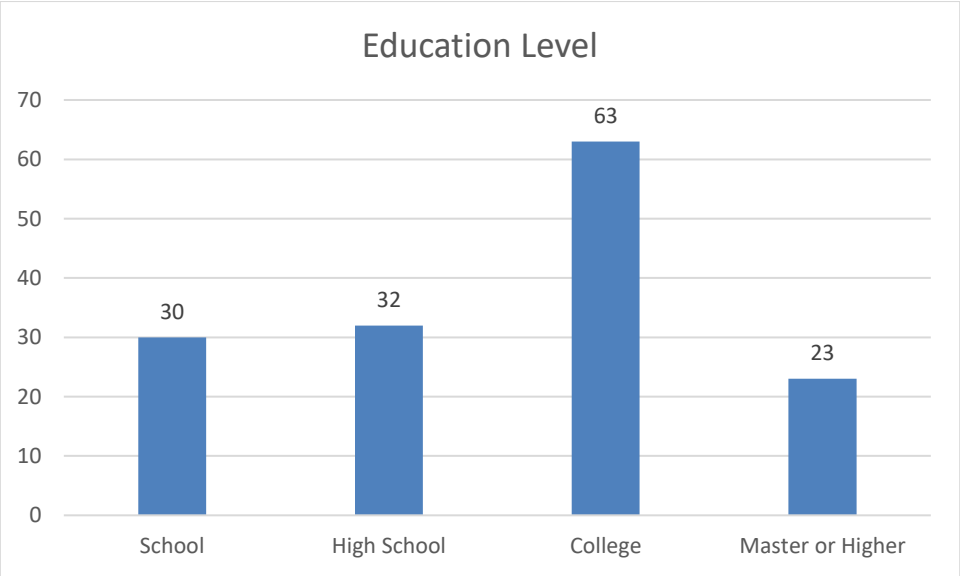

Figure 5 Education Level

On close observation, it can be seen that in all cases of education level about 70% of participants did not suffer any loss. Surprisingly, loss of more than 20,000 can be seen as the second most prevalent amount of financial loss except for education level of college in which financial loss of NPR 500 to 5,000 is more prevalent.

Data also shows that people with only school level education are almost twice as likely to suffer from financial loss of over 20,000 than other groups.

78% master = seen awareness program, 68% of higher education = seen awareness program, 58% college = seen awareness program, 56% school = seen awareness program (school level = lowest seen awareness program and highest %financial loss of more than 20,000).

The observation is that awareness messages are mostly presented inside apps of different banks which are in English leading to people who know English to be the ones who see such messages.

Experienced fraud more than 2 years ago is the least popular choice except for school attendees among whom option 2 “experienced fraud within 2 years” was the least popular choice. The data varies widely for other options.

4.2.3 Internet Use Frequency

Figure 6 shows that out of the participants, 96.62 percent used the internet at least once a week, and 3.38 percent used the internet hardly or never. It is notable that nobody i.e., 0.00% of the participants choose the option “Once a month or less”.

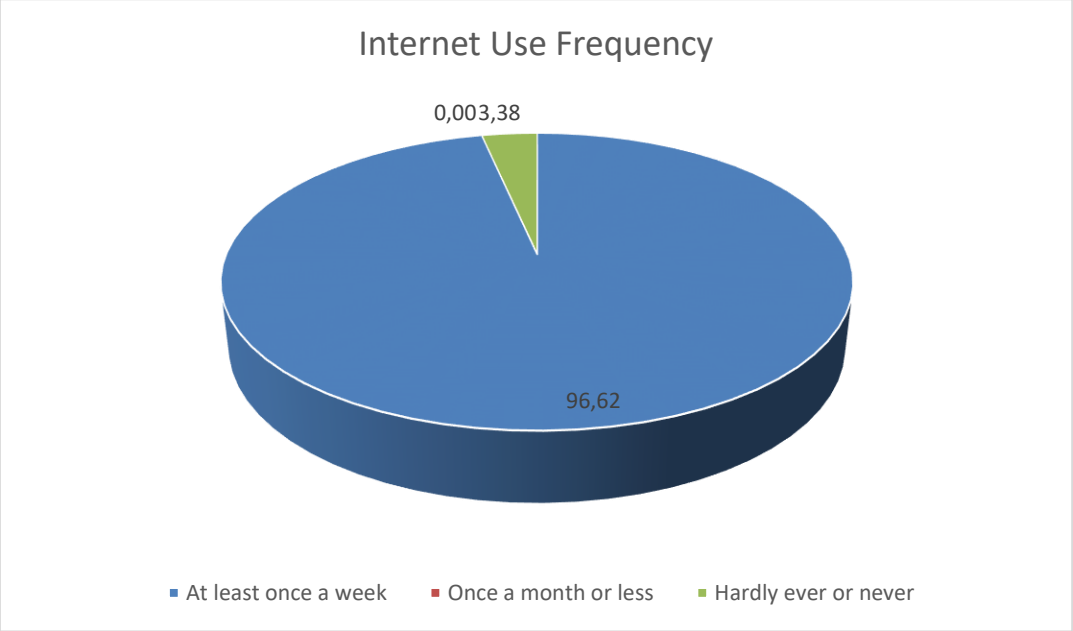

Figure 6 Internet Use Frequency

People who used internet only once a month were 4 times more likely to lose more than 20,000 NRS than people who used internet at least once a week. This shows that people who are not tech savvy are the ones who fall for scams and frauds that cost the victim a lot of money.

Figure 7 shows the number of male participants in each category of education level. It is evident that among male participants the number of participants that have studied up to high school is significant with 58 out of 123 i.e., 47.15% of the participants.

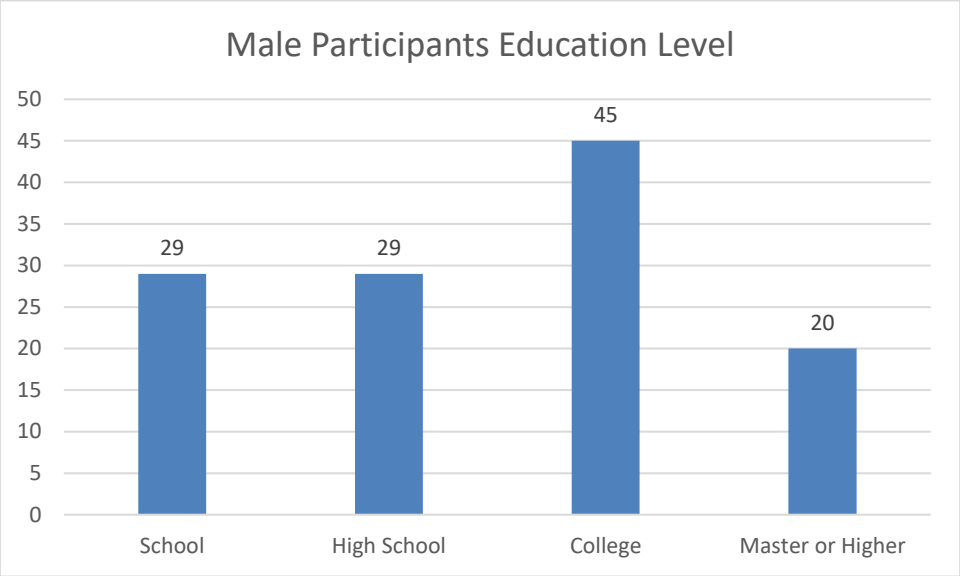

Figure 7 Male Education

Figure 8 shows the number of female participants in each category of education level. Although the number of female participants is significantly less with a total of 26 participants, it is evident that most of the female participants have studied at college level i.e.,73.07% have studied at college level.

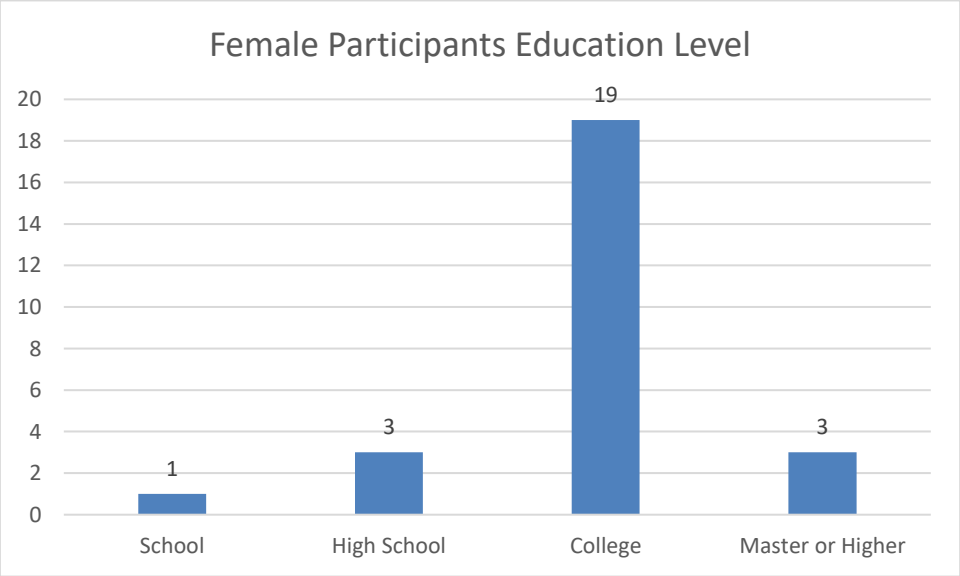

Figure 8 Female Education

4.2.4 Address Urbanity

Figure 9 shows that in terms of participants living in urban areas, 66.89 percent live in Large towns, 27.03 percent live in Small or Mid-size towns and 6.08 percent live in Rural areas or villages.

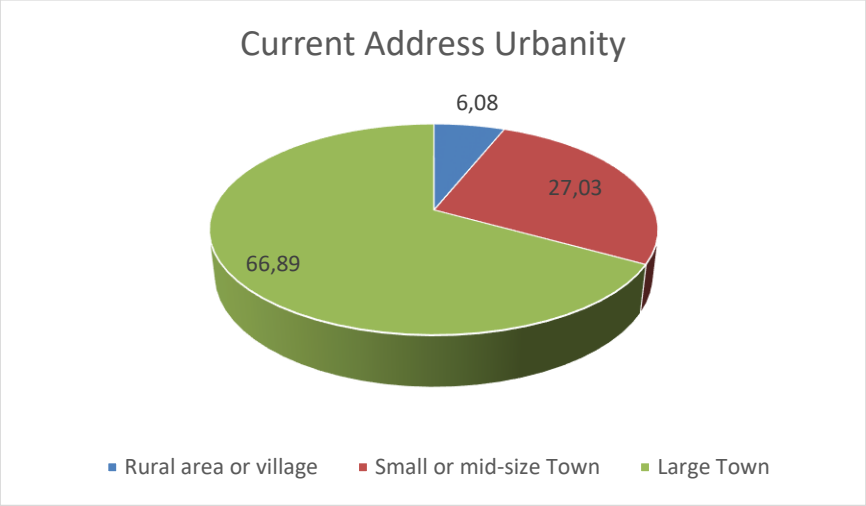

Figure 9 Current Address Urbanity

The use of internet varies little based on the urbanity of the participants' current address. More than 95% of participants use the internet at least once a week no matter the urbanity of their current address.

Over 60% of the participants had seen awareness raising messages no matter the urbanity and About 20% could not remember seeing such message no matter the urbanity. About 10% did not see awareness raising messages in Rural and Small town while 20% did not see such message in large towns. It is well known that people in rural areas have better relationship with their surrounding people than people in cities. This might contribute to discussion between people in rural communities about awareness raising programs. Hence, increasing their effectiveness through word of mouth.

In all 3 types of area by urbanity, the top 3 types of financial loss were Nothing, NPR 500 – NPR 5,000 and over 20,000. People living in large towns were 10% more likely experience no financial loss. This means people living in large towns fall less for scams. Interestingly, the variety of financial loss rises from 3 to 4 to 5 consecutively as urbanization rises.

Data shows that 44.4% of people in rural areas had only completed School level education and another 44.4% had completed college education and only 11.1% had completed master or higher education.

Top 3 channels used for reporting in rural and small towns are the same i.e. about 50% did not report to anyone, about 30% reported to friends/family and **about 10% reported to officials such as police.** While in large towns 51% reported to friends and family, 41% did not report.

Top 3 types of scams in rural in mid-sized towns were same accounting for about 80% of scams. While in large town, 51% fell for a fake product. 42% reported ordering a cheap product but were **charged monthly fees**. As far as I know it is not possible to charge a monthly recurring fee on credit or debit card in Nepal so either the participants lied or did not understand the option.

Reason for buying not buying was the same across all areas. Noticeably, in midsize towns 56% of participants choose other which is 20% less than other groups. 18% more participants from midsize town were not interested in general.

4.2.5 Address Province

Figure 10 shows that 128 participants were from Province No 3 while 20 were from other provinces.

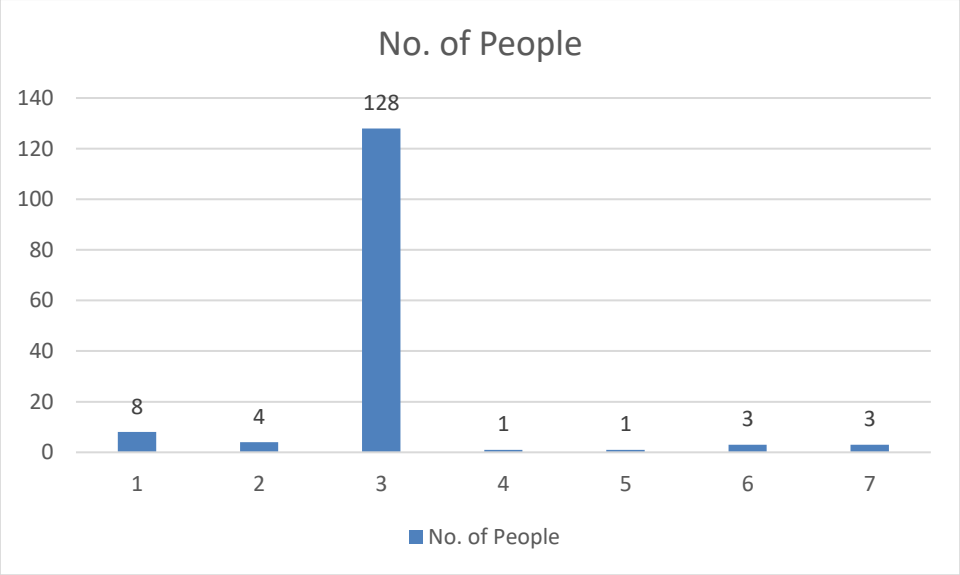

Figure 10 Province of Address

4.2.6 Financial Loss

Figure 11 shows that out of the participants, 74% did not suffer financially. 11% suffered more than Rs20,000 or higher, 5% suffered between Rs 5,000 and Rs20,000, 8.2% lost Rs 500 to Rs5,000, and lastly, 2.0 suffered less than Rs 500. At the time of writing, 1 euro is equal to 141.71 Nepali Rupee (NPR). The average salary in Nepal varies according to jobs for

e.g. in mangers category men earn Rs32,000 per month, the pay for women averages Rs25,500 [103].

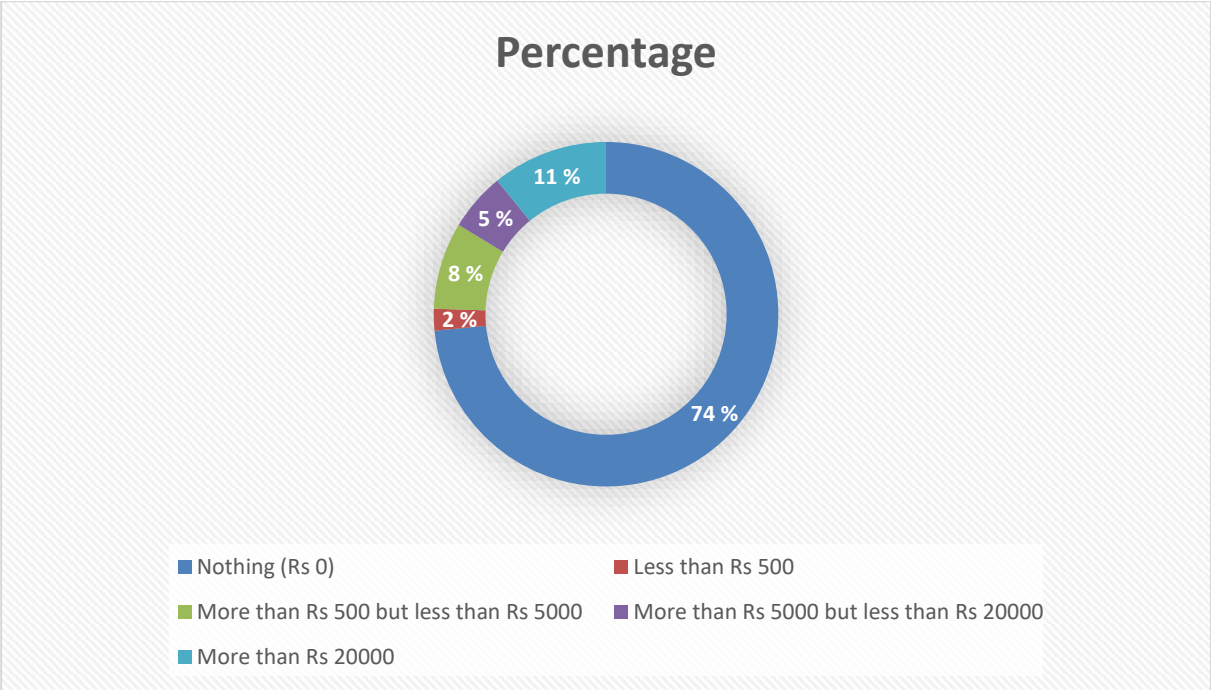

Figure 11 Financial Loss

Channels used for reporting according to financial loss varies widely. The participants who did not suffer financial loss: 52% of them did not report while only 44% reported to friends and family. Both people who suffered more than 20,000 in loses and between 500 and 5,000 NPR: 50% reported to friends and family.

All age groups suffer from financial loss of over 20,000 NRS. The top 2 types of financial loss are nothing at number 1 and that of over 20,000 NRS at number 2 except for the age group 20 to 30 for which over 20,000 NRS is ranked no 4.

Only 31% of the people who suffered more than 20,000 NPR in losses complained to the police while 33% of 500 to 5,000 loss group reported to friends and family. The low percentage of about 30% who report to police means that people don't want to report to police even though they suffer large financial loss. This maybe due to it not being worth the hassle of going to court or taking perpetrator who might be a person close to the victim to the court might be seen as shameful.

The youngest age group might not have lots of money in the first place to spend so naturally few of them suffer from financial loss of over 20,000 NRS.

4.2.7 Awareness Program

Figure 12 shows that out of the participants, 63.51% had seen awareness-raising programs, 19.59 could not remember if they saw one, and 16.89 had not come across any awareness-raising programs.

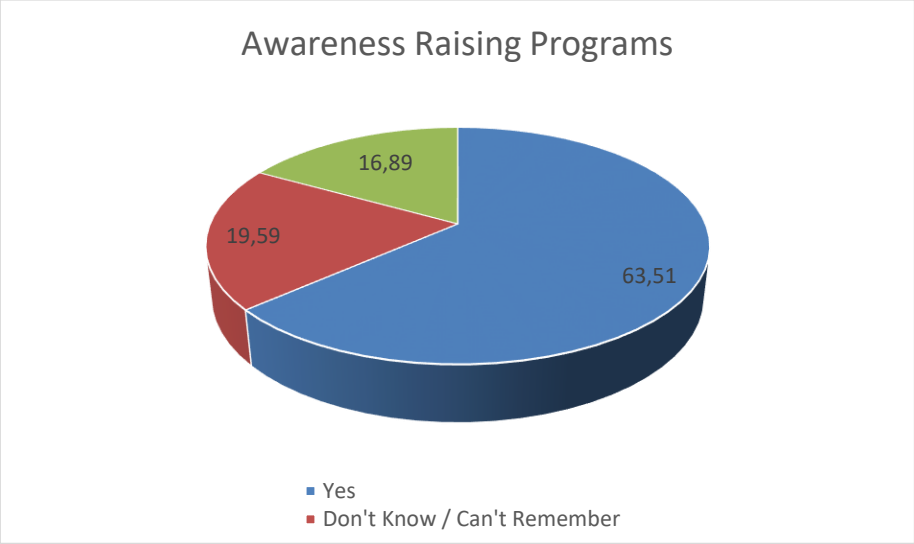

Figure 12 Awareness Raising Programs

Among all age groups, over 60% had seen the message from awareness raising programs. While the others either did not see the message or couldn't remember.

Among the people who saw awareness raising program only 19% indicated financial loss. While among the participants who had not seen the awareness raising program 44% had indicated financial loss. And, among the people who could not remember such a message, 38% of the people indicated financial loss. This shows that people who saw such message where twice as likely to not suffer financially. Hence, the importance of awareness programs cannot be stated enough.

The top three scams indicated in survey across all categories of people seeing an awareness message is the same which are lottery win notification, investment opportunity and fake or non-existent product. However, the percentage of people who got lottery win notification differs considerably. Among people who saw awareness program message 64% indicated seeing lottery win notification while people who did not see the message 33% indicated the same and for participants who could not remember 47% indicated the same. Hence, it seems that even though people saw awareness programs, more people of them indicated such

message. It maybe that people who saw awareness programs are more awareness of lottery win notification and fall less for other types of attacks too.

4.2.8 Reporting Channels

Figure 13 shows that out of the participants 45.59% had reported to friends/family and 44.12% had not reported at all. 5.15% had reported to the police, 3.68% had reported to the vendor and 1.47% had reported to both friends and family as well as the vendor.

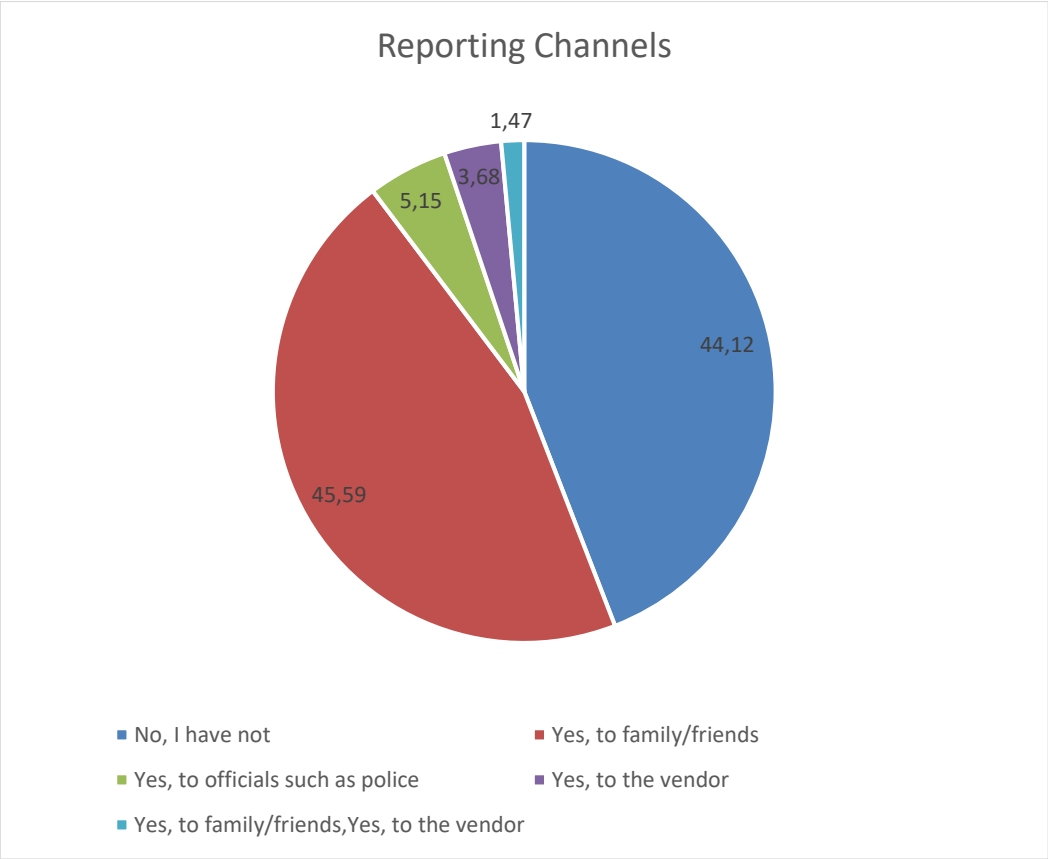

Figure 13 Reporting Channels

4.2.9 Type of Suffering

Table 2 shows that according to the survey data, 65.9 percent of the participants did not suffer in any way emotionally, financially, or physically; 12.9 percent of the participants suffered emotionally and financially; 10.2 percent of the people suffered emotionally only, and 10.2 percent of the people suffered financially only. Less than 1 percent of the people suffered in all three ways.

The comma separated values in Table 2 represent multiple choices of the participants.

Choices	Percentages
4	65.99
1, 2	12.92
1	10.20
2	10.20
1, 2, 3	0.68

Legend

1 = Suffered emotionally,

2 = Suffered financially,

3= Suffered Physically,

4 = Did not suffer

Table 2 Type of Suffering

4.2.10 Subjective Income

Table 3 shows that according to the survey data, 41.8 percent of the participants find earning money to be fairly easy, 36.4 percent find earning money to be fairly difficult, 12.8 percent find earning to be very easy or do not work or are students and 8.7 percent of the participants find earning money to be very difficult.

On closer examination we can see that, financial loss of nothing is the number one type of financial loss across all categories of subjective income. The second highest type of financial loss is that of more than 20,000 NRS except for "Fairly difficult" for which 500 to 5,000 NRS is the second highest financial loss.

This shows that people either lose nothing or lose a lot of money due to scams and frauds regardless of their income level.

Choices	Percentages
3	41.89
2	36.49
4	12.84
1	8.78

Legend

1 = Very difficult,

2 = Fairly difficult,

3 = Fairly Easy,

4 = Very Easy

Table 3 Subjective Income

4.2.11 Online Buying Behaviour Change

Table 4 shows the before and after online buying behaviour after suffering from an SE attack. Table 4 shows that About 85 percent of the participants did not change their behaviour that is if they were frequent buyers, they remained frequent buyers; if they were occasional buyers, they remained occasional buyers; and if they never bought online, they never bought. About 7 percent of participants did not answer if they changed their behaviour. About 2 percent of the participants changed their online behaviour.

8.7% of the participants changed their online behaviour i.e., from occasional buyers to never. Out of the 8.7% of the participants who changed their behaviour from "occasional" buyers to "Never" buying, surprisingly only 26 percent had incurred financial loss and majority 73% marked their online behaviour change without any financial loss. The reason behind this is not obvious.

The comma separated values in table 4 are before and after behaviours. The value before comma represents their normal behaviour and the value after the comma represents their behaviour after encountering scam or fraud.

Behavior Change	Percentage
2,2	42.57
3,3	39.19
2,3	8.78
1,1	3.38
3	2.70
1,2	1.35
2	1.35
2,1	0.68

Legend

1 = Frequent,

2 = Occasional,

3 = Never

Table 4 Behaviour Change

4.2.12 Reason for buying or not

Table 5 shows that by far the highest percentage of participants reasons for buying or not was "Other" with 72 percent choosing this option. 3 reasons totalling 23.8 percent of people who did not buy online were options 1,2 and 3. The only option given for choosing to buy i.e., products being cheap was chosen by 2 percent of the population. More detailed analysis could not be done as participants were not asked if they bought things online or not.

The comma separated values in table 5 are multiple choices of the participants.

Reason for buying or not	Percentages
5	72.79
1	14.96
2	5.44
3	3.40
4	2.04
1, 5	0.68
2, 3	0.68

Legend

1 = I am not interested in general,

2 = Victim of Scam or Fraud,

3 = Too Expensive,

4 = Too Cheap,

5 = Other

Table 5 Reason for buying online or not

4.2.13 Time of Fraud Experienced

Table 6 shows that out of the respondents, 51 percent had experienced fraud within the past 2 years, 19 percent had experienced fraud more than 2 years ago and about 30 percent of people had not experienced fraud.

The channels used for reporting varies widely based on the time of fraud experienced. Among the participants who experienced fraud within 2 years from the time of data collection, the most popular channel of reporting is “Friends and Family” at 60% and “not reporting” at 32%. The same for people who experienced fraud more than 2 years ago is “Friends and family” at 57%, at second is “Officials” such as police at 21.4% and “did not report” at 14%.

Options/Choices	Percentages
2	51.02
1	29.93
3	19.04

Legend

1 = No, I have not

2 = Yes, I have – in the past 2 years ago

3 = Yes, I have – more than 2 years ago

Table 6 Time Past since fraud experienced

4.2.14 Reason for not reporting

Table 7 shows that of the participants, 40 percent thought that filing a complaint would not make a difference, 28 percent did not report because there was no financial harm, 13 percent did not have time, and 3.5 percent were unclear on the reporting authority. Rest had multiple reasons. About 2.35 percent didn’t know how to report and another 2.35 percent felt embarrassed and did not report.

Among the people who felt reporting would not make a difference; 83% were male and only 16% were female, 42% had completed college education, 21% had completed high school, 20% had completed only school level and 15% had completed Master or higher education; 66% of the participants lived in large towns, 27% lived in small or mid-size towns and 6% lived in rural areas or villages.

The comma separated values in table 7 are multiple choices of the participants.

Choices	Percentages
7	40.00
8	28.24
4	12.94
6	3.53
7, 8	2.35
1	2.35
2	2.35
Scolded the messenger	1.18
1, 6, 8	1.18
Stopped calling after a few calls	1.18
1, 4	1.18
3, 7	1.18
1, 7	1.18
3	1.18

Legend

1 = I didn't know how to report

2 = I was Embarrassed

3 = I Couldn't work on the device anymore

4 = I didn't have Time

5 = I didn't want to give out ID Details

6 = I was unclear about reporting authority

7 = I felt it would not make a difference

8 = There was no Financial Harm

Table 7 Reason for not reporting

4.2.15 Reporting Preference (how want to report in general and combine things)

Table 8 shows that given the choice, 75.4 percent of the citizen of Nepal would like to report in a booth located nearby. 14.5 percent of the people would like to call on a dedicated phone number. 3.5 percent would like to report through a website. 2.75 percent would like to call NGO-operated phone numbers. 2 percent would like to email.

The most popular reporting preference is "a booth that is centrally located" across all age groups of 20 to 30, 31 to 40, 41 to 50 and 51 to 60. The second most popular reporting preference across as ages is "a phone number". The Top 3 preferences for reporting which account for over 70% of all participants are the same across all areas categorized by urbanisation which are reporting booth, phone number, government website.

The comma separated values in table 8 are multiple choices of the participants.

Choices	Percentages
4	74.48
1	14.48
2	3.45
5	2.76
3	2.07
1, 2	1.38
6	0.69
1, 3	0.69

Legend

1 = A dedicated free phone number operated by the government

2 = A dedicated governmental website

3 = A dedicated helpdesk via email

4 = A booth in a central location in my country

5 = A dedicated free phone number operated by a non-governmental organization

6 = A dedicated non-governmental website

Table 8 Reporting Preference

4.2.16 Fraud Type and Financial Loss

The financial loss varies widely according to the type of scam people became victim of. People who reported as not suffering any financial loss from fraud i.e., 84% were victims of "notification of lottery win or that they need to pay a fee to collect prize won".

The participants who reported more than NRS 20,000 lost to fraud were victims of just one type of scam that is option number 6 to question no 8 i.e., they were promised goods or services or investment opportunities.

The participant who reported loss of money between NRS 500 to NRS 5,000 were victims of buying an unsatisfactory ecommerce product and receiving a notification about winning a lottery.

5 Discussion

This section gives in depth analysis of findings that became apparent during the thesis. Common scam threads found in the survey, newspaper reports and literature review are discussed here. Future research to address issues that could not addressed, and limitations of the thesis are also discussed here.

5.1 Main Findings

As far as the author knows collection of data regarding social engineering has not been done in Nepal. The survey has revealed several interesting pieces of information.

Through survey, it was found that lottery scams through WhatsApp are very common in Nepal. Most people are aware of this type of scam message. They generally block the number and ignore it. The reason behind this is that most people think reporting it would not make a difference and most people do not suffer in any way. Nepal not being the place of origin of social media and many technologies like WhatsApp make it very difficult for the government to implement policies. Lottery Scams are also reported twice in the newspaper during 2019 and 2020. This shows that lottery scams are indeed a problem for Nepal. Since government cannot implement policies to prevent such attack or provide a good policing service, it should focus on increasing awareness among people. Also, people should not be greedy and fall for such scams. Since, the lottery scam targets people who have not participated in any kind of lottery, it is an easily solvable by avoiding such messages.

Surveys also revealed that most victims who suffer financially and/or emotionally do not suffer through the internet but through meeting the person in real life. The person is usually an acquittance with some level of trust. The scammer pretends to be in trouble and in need of money. They then get the money without any kind of legal proceeding or collateral. After getting the money, the perpetrator severs the relationship with the person. Most people who get scammed and suffer financially are scammed by the people they know who ask for help and later don’t give back the money. This leads to a situation where the victim does not want to go after the perpetrator legally.

Foreign employment scam was also found in both the survey, the newspaper reports, and the literature review. Victims are lured into a lucrative job which then turns out to be non-existent or a criminal operation where they are forced to work under unfavourable conditions. Since,

these operations happen in foreign countries, there is little the government can do once victims leave the country for their job. This type of scam is easily prevented by asking for proper documentation before going after the job. Public awareness can be an effective tool against such scams as well.

The scam and fraud reports in newspapers have revealed the following information:
In general, less than a dozen scams and frauds at the national level and international levels are reported every year. Since there is no dedicated magazines or websites that discuss scams and frauds and national newspapers do not cover smaller stories, many more scam reports may go unreported. A portal where grievances of victims can be anonymously posted and visible to the public would be a low-cost solution to both gather the reports as well as generate public awareness.

The variety of reports is wide ranging from simple lottery messages to cross border employment scams. However, in many cases the law enforcement can do little once the crime has occurred. This is due to international nature of the crime as well as the platforms like WhatsApp being not based in Nepal.

Perpetrators of some scams were found to be from both India and China. These countries being much larger and powerful, Nepal does not have the resources to pursue the criminals once they escape to their home country.

In many situations, public awareness programs are the only option Nepal must fight against scams and frauds in the country. Since, public awareness programs have been found to be effective, it should be given priority.

5.2 Future Research

This study was limited to a survey of 149 participants and 4 years of newspaper reports in "The Kathmandu Post". Time and financial resources were also limited. However, there have been many relevant findings such as a large percentage of participants getting WhatsApp scam messages among others. The findings of the survey can be used to inform future research in information technology policy for Nepal.

It is recommended that other newspapers in Nepali be researched to get a better view of the scam and fraud reports in Nepal. There are thousands of registered newspapers in Nepal.

Covering as much of newspapers as possible will give a much more accurate picture of the scams and frauds reported in Nepal.

The survey spanning the entire country could be conducted so that more granular data is available for research. The urbanity and living situation of Nepal varies widely from very rural villages to metropolitan areas like the capital city of Nepal. Getting the data will make it possible to the detailed research for each district or province of Nepal.

Based on similar research, similarity between communication used by banks and scammers can be compared so as general population are not fooled by scammers. Impact of governmental and e-commerce sites policies can be measured. Effectiveness of advice given on e-commerce, dating websites, etc so that such information can be required by the government policy. Impact reviews and ratings on e-commerce sites can be measured and appropriate policies can be implemented to make them effective. Research on personality types and their impact on social engineering victims can be studied.

5.3 Limitations

The thesis was conducted in a limited amount of time with limited financial resources. Hence, the data collection of only 149 people was possible. Data collected from about 20 people were discarded because the answers provided were given to be socially acceptable rather than being truthful. The limiting factor in conducting surveys was time. As the entire survey was done in about 2 months. The number of participants had to be limited to not disturb the people in public spaces where the survey was conducted. Also, finding people who are willing to participate was not easy.

In the case of newspapers, the PDF versions of newspapers were available going back 5 years. However, due to the limitation of time only 4 years' worth of newspaper reports were researched. Spotting the newspaper reports worth considering in the thesis was a tricky process. Many scam and fraud reports were related to corruption. Some were followed-up of stories in several newspapers. Considering such stories was complicated and left out.

In case of literature review, only some of the available literature about half a dozen were considered. This is due to the time limit.

6 Conclusion

Social engineering is a branch of Cybersecurity which concerns human element in security. It is difficult to protect against due to rapidly changing threat environment, myriad of techniques, tactics available and the human nature of trusting people.

The thesis was approached with scientific research papers, “The Kathmandu Post” newspapers 4 years’ worth 2019 to 2022 and surveys. The thesis investigated the prevalence and impact of social engineering attacks on citizens of Nepal especially the region of “Kathmandu Valley” where the capital of Nepal is located. Survey of about 150 people, research of 4 years’ worth of daily newspaper “The Kathmandu Post” and literature review of similar studies in various countries was conducted.

Through the survey, it was found that scam messages through WhatsApp are the most prevalent and law enforcement are not able to do much about it. This is because the technologies that facilitate these services are not based in Nepal. Hence, if Nepal truly wants to control scams and frauds it needs to be able to enforce laws through the international companies that provide services or facilitate its own technology companies. Furthermore, it was found that people who had seen the public awareness program about social engineering attacks were only half as likely to suffer from financial loss due to such attacks. Also, the people who lose more than 20,000 NRS was the second highest amount of financial loss after no financial loss for 3 out of 4 groups of income distribution. This shows successful social engineering attacks are prevalent in Nepal and are having financial impact on the population.

It was surprising to find that most people i.e. Over 80% did not change their online behaviour and of the people who changed their behaviour only 26% suffered from financial loss. Unsurprisingly, it was also found that people who report to the police are once’s who have suffered from large financial loss.

Through the reports in newspapers, it was found that about a dozen scams and fraud reports are presented in newspapers annually. The scams and frauds concerning only cybersecurity are far fewer in number. The scams and frauds are not only through Nepalese but also through Indian, Chinese, and even Nigerian nationals.

The scam and frauds reported in the newspapers ranged from fraud spanning many companies and personnel in helicopter rescue scams to lottery scam. Some interesting reports were call centres trying to dupe people, Indian tech workers lured with promise of high salaries and

forced to commit cybercrime such as: establishing relationship with a target and getting them to invest in bogus cryptocurrency, bad advertisement showing on good websites due to automated nature of advertising, people smuggling gold through Nepalese airports, fraudulent foreign employment, scammers collecting bank notes by pretending to exchange covid infected cash.

Through comparing various research papers in literature review, it was found that in USA the communication used by banks is hard to distinguish from the social engineering attacks. While, in Nepal exposure to awareness raising programs made a significant impact on people not falling for these types of scams and frauds. E-commerce sites, dating sites need to give advice upfront and easily accessible way. In the survey, it was found that identifying trustworthy e-commerce websites are key to protect fraud. In Ghana, e-commerce fraud is considered as a necessary evil. However, in Nepal sellers in e-commerce sites must be a registered shop so fraudulent activity is significantly less. Communication mediums such as voice calls, email, SMS, pop-ups, and letters are used for frauds. While in the survey, it was found that WhatsApp was the most prevalent communication medium. Fake reviews and rating are problem in Malaysia. In the survey, it was found that only 30% of participants checked customer reviews. Financial impact was important factor in reporting to the police. In the survey, the same was found to be true.

It can also be concluded that public awareness programs are effective in reducing the victims of social engineering attacks that are most prevalent. People who are not tech savvy are the ones who fall for scams. Mindful policies from the government are also effective in reducing e-commerce frauds. Nepal being is small country locked between India and China, it needs to cooperate with these countries to catch fraudsters. The ability to enforce national policies on tech companies from abroad is an important factor in controlling widespread scam channels like WhatsApp.

7 References

[1] I. F. Akyildiz and A. Kak, “The Internet of Space Things/CubeSats: A ubiquitous cyber-physical system for the connected world,” *Computer Networks*, vol. 150, pp. 134–149, Feb. 2019, doi: 10.1016/J.COMNET.2018.12.017.

[2] J. E. Berry, “The Internet: An Educational System for Equalizing Educational Opportunity,” in *Handbook on Promoting Social Justice in Education*, Springer Nature Switzerland, 2020, pp. 1587–1607. doi: 10.1007/978-3-030-14625-2_74.

[3] M. Wang and L. Song, “Efficient defense strategy against spam and phishing email: An evolutionary game model,” *Journal of Information Security and Applications*, vol. 61, p. 102947, Sep. 2021, doi: 10.1016/J.JISA.2021.102947.

[4] H. Aldawood, G. Skinner, and G. Skinner, “An Advanced Taxonomy for Social Engineering Attacks,” *Article in International Journal of Computer Applications*, vol. 177, no. 30, pp. 975–8887, 2020, doi: 10.5120/ijca2020919744.

[5] K. Hughes-Lartey, M. Li, F. E. Botchey, and Z. Qin, “Human factor, a critical weak point in the information security of an organization’s Internet of things,” *Heliyon*, vol. 7, no. 3, p. e06522, Mar. 2021, doi: 10.1016/J.HELIYON.2021.E06522.

[6] E. by, S. Hickey, and N. Hossain, *The Politics of Education in Developing Countries: From Schooling to Learning*, Online Edition. Oxford : Oxford University Press, 2019.

[7] A. O. Imaji, “Ransomware Attacks: Critical Analysis, Threats, and Prevention methods,” Fort Hays State University, 2019. Accessed: May 26, 2023. [Online]. Available: https://www.researchgate.net/publication/332551447_Ransomware_Attacks_Critical_Analysis_Threats_and_Prevention_methods

[8] F. Salahdine and N. Kaabouch, “Social Engineering Attacks: A Survey,” *Future Internet 2019, Vol. 11, Page 89*, vol. 11, no. 4, p. 89, Apr. 2019, doi: 10.3390/FI11040089.

[9] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks *,” *Journal of Information Security and Applications*, vol. 22, pp. 113–122, Jun. 2015, doi: 10.1016/j.jisa.2014.09.005.

[10] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Social Engineering Attacks on the Knowledge Worker,” in *Proceedings of the 6th International Conference on Security of Information and Networks*, 2013, pp. 28–35.

[11] A. E. Mohamed, “Complete Cross-site Scripting Walkthrough.” Accessed: May 26, 2023. [Online]. Available: https://www.exploit-db.com/docs/english/18895-complete-cross-site-scripting-walkthrough.pdf

[12] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks,” *Journal of Information Security and Applications*, vol. 22, pp. 113–122, Jun. 2015, doi: 10.1016/J.JISA.2014.09.005.

[13] M. T. Banday, J. A. Qadri, and N. A. Shah, “Study of Botnets and Their Threats to Internet Security,” *All Sprouts Content*, vol. 9, no. 24, Jun. 2009, Accessed: May 26, 2023. [Online]. Available: https://aisel.aisnet.org/sprouts_all/279

[14] T. R. Peltier, “Social Engineering: Concepts and Solutions,” *Information Systems Security*, vol. 15, no. 5, pp. 13–21, 2007, doi: 10.1201/1086.1065898X/46353.15.4.20060901/95427.3.

[15] A. Shah and J. Giffin, “Analysis of Rootkits: Attack Approaches and Detection Mechanisms”, Accessed: May 26, 2023. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=dee1f56f8ec7d08674ed35d5d8d1394c51ba39a1

[16] A. Koyun and E. Al Janabi, “Social Engineering Attacks,” *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, vol. 4, pp. 2458–9403, 2017, Accessed: May 26, 2023. [Online]. Available: https://www.jmest.org/wp-content/uploads/JMESTN42352270.pdf

[17] R. B, J. R. Y R, and R. B. Dillip Kumar, “A Survey Paper on Malicious Computer Worms,” *International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)*, Apr. 2015. https://docplayer.net/4045934-A-survey-paper-on-malicious-computer-worms.html (accessed May 26, 2023).

[18] M. Hasan, N. Prajapati, and S. Vohara, “Case Study On Social Engineering Techniques for Persuasion,” *International Journal on Applications of Graph Theory In wireless Ad Hoc Networks And sensor Networks*, vol. 2, no. 2, pp. 17–23, Jun. 2010, doi: 10.5121/jgraphoc.2010.2202.

[19] T. F. Stafford and A. Urbaczewski, “Spyware: The Ghost in the Machine,” *Communications of the Association for Information Systems*, vol. 14, no. 1, p. 15, Sep. 2004, doi: 10.17705/1CAIS.01415.

[20] G. Katz and M. Fire, “Strangers Intrusion Detection - Detecting Spammers and Fake Profiles in Social Networks Based on Topology Anomalies,” *ASE Human Journal*, Jan. 2012, Accessed: May 26, 2023. [Online]. Available: https://www.academia.edu/1518357/Strangers_Intrusion_Detection_Detecting_Spammers_and_Fake_Profiles_in_Social_Networks_Based_on_Topology_Anomalies

[21] Q. Cao, X. Yang, J. Yu, and C. Palow, “Uncovering large groups of active malicious accounts in online social networks,” *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 477–488, Nov. 2014, doi: 10.1145/2660267.2660269.

[22] D. Goel and A. K. Jain, “Mobile phishing attacks and defence mechanisms: State of art and open research challenges,” *Comput Secur*, vol. 73, pp. 519–544, Mar. 2018, doi: 10.1016/J.COSE.2017.12.006.

[23] O. T. and S.-M. Yoo, “An Approach against a Computer Worm Attack,” *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 1, no. 2, Aug. 2009, doi: 10.17762/ijcnis.v1i2.14.

[24] Y. Cho and G. Qu, “Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs,” *Int J Distrib Sens Netw*, vol. 2013, p. 16, 2013, doi: 10.1155/2013/205920.

[25] J. Shukla and B. Sahni, “A Survey on VoIP Security Attacks and their Proposed Solutions,” *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, vol. 2, no. 3, Mar. 2013, Accessed: May 28, 2023. [Online]. Available: https://www.ijaiem.org/Volume2Issue3/IJAIEM-2013-03-15-032.pdf

[26] T. Longtchi, R. M. Rodriguez, L. Al-Shawaf, A. Atyabi, and S. Xu, “Internet-based Social Engineering Attacks, Defenses and Psychology: A Survey,” Mar. 2022, doi: 10.48550/arXiv.2203.08302.

[27] G. J. Boyle, G. Matthews, and D. H. Saklofske, “The SAGE Handbook of Personality Theory and Assessment: Volume 2 — Personality Measurement and Testing,” *The SAGE Handbook of Personality Theory and Assessment: Volume 2 - Personality Measurement and Testing*, pp. 1–717, Jan. 2008, doi: 10.4135/9781849200479.

[28] Cialdini B Robert and Lloyd James, *Influence: Science and practice*, vol. 4. Boston MA: Pearson education, 2009. Accessed: Jun. 21, 2023. [Online]. Available: https://www.researchgate.net/publication/229067982_Influence_Science_and_Practice

[29] J. McAlaney and V. Benson, “Cybersecurity as a social phenomenon,” in *Cyber Influence and Cognitive Threats*, Elsevier, 2020, pp. 1–8. doi: 10.1016/B978-0-12-819204-7.00001-4.

[30] Y. Kim and H. Lee, “Towards a Sustainable News Business: Understanding Readers’ Perceptions of Algorithm-Generated News Based on Cultural Conditioning,” *Sustainability 2021, Vol. 13, Page 3728*, vol. 13, no. 7, p. 3728, Mar. 2021, doi: 10.3390/SU13073728.

[31] J. McAlaney and P. J. Hills, “Understanding Phishing Email Processing and Perceived Trustworthiness Through Eye Tracking,” *Front Psychol*, vol. 11, p. 1756, Jul. 2020, doi: 10.3389/fpsyg.2020.01756.

[32] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, “Social engineering attack strategies and defence approaches,” *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, pp. 145–149, Sep. 2016, doi: 10.1109/FICLOUD.2016.28.

[33] S. Das, A. Kim, Z. Tingle, and C. Nippert-Eng, “All About Phishing: Exploring User Research through a Systematic Literature Review,” Aug. 2019, doi: 10.48550/arXiv.1908.05897.

[34] D. Henshel, M. G. Cains, B. Hoffman, and T. Kelley, “Trust as a Human Factor in Holistic Cyber Security Risk Assessment,” *Procedia Manuf*, vol. 3, pp. 1117–1124, Jan. 2015, doi: 10.1016/J.PROMFG.2015.07.186.

[35] E. J. Williams, A. Beardmore, and A. N. Joinson, “Individual differences in susceptibility to online influence: A theoretical review,” *Comput Human Behav*, vol. 72, pp. 412–421, Jul. 2017, doi: 10.1016/J.CHB.2017.03.002.

[36] R. Chen, J. Gaia, and H. R. Rao, “An examination of the effect of recent phishing encounters on phishing susceptibility,” *Decis Support Syst*, vol. 133, p. 113287, Jun. 2020, doi: 10.1016/J.DSS.2020.113287.

[37] G. D. Moody, D. F. Galletta, and B. K. Dunn, “Which phish get caught? An exploratory study of individuals′ susceptibility to phishing,” *European Journal of Information Systems*, vol. 26, no. 6, pp. 564–584, Nov. 2017, doi: 10.1057/S41303-017-0058-X.

[38] H. Zafar, A. Randolph, S. Gupta, and C. Hollingsworth, “Traditional SETA No More: Investigating the Intersection Between Cybersecurity and Cognitive Neuroscience,” *Proceedings of the Annual Hawaii International Conference on System Sciences*, vol. 2019-January, pp. 4914–4923, Jan. 2019, doi: 10.24251/HICSS.2019.591.

[39] H. Collier, A. Collier, and A. C. Henry Collier, “The Port Z3R0 Effect! Human Behaviors Related to Susceptibility,” *Computer Science & Information Technology (CS & IT) Vol.10, No.4*, vol. 10, no. 4, p. 47, Apr. 2020, doi: 10.5121/CSIT.2020.100404.

[40] H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, and N. Memon, “Mind your SMSes: Mitigating Social Engineering in Second Factor Authentication,” *Comput Secur*, vol. 65, pp. 14–28, 2017, doi: 10.1016/j.cose.2016.09.009.

[41] A. Ferreira, “Why Ransomware Needs A Human Touch,” in *International Carnahan Conference on Security Technology*, Institute of Electrical and Electronics Engineers Inc., Dec. 2018, pp. 1–5. doi: 10.1109/CCST.2018.8585650.

[42] A. M. Ness *et al.*, “Reactions to ideological websites: The impact of emotional appeals, credibility, and pre-existing attitudes,” *Comput Human Behav*, vol. 72, pp. 496–511, Jul. 2017, doi: 10.1016/J.CHB.2017.02.061.

[43] A. Algarni, Y. Xu, and T. Chan, “An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook,” *European Journal of Information Systems*, vol. 26, no. 6, pp. 661–687, Nov. 2018, doi: 10.1057/S41303-017-0057-Y.

[44] Z. Wang, H. Zhu, and L. Sun, “Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods,” *IEEE Access*, vol. 9, pp. 11895–11910, 2021, doi: 10.1109/ACCESS.2021.3051633.

[45] N. Abe and M. Soltys, “Deploying Health Campaign Strategies to Defend Against Social Engineering Threats,” *Procedia Comput Sci*, vol. 159, pp. 824–831, Jan. 2019, doi: 10.1016/J.PROCS.2019.09.241.

[46] S. Goel, K. Williams, and E. Dincelli, “Got Phished? Internet Security and Human Vulnerability,” *J Assoc Inf Syst*, vol. 18, no. 1, p. 2, Jan. 2017, doi: 10.17705/1jais.00447.

[47] S. Buecker, M. Maes, J. J. A. Denissen, and M. Luhmann, “Loneliness and the Big Five Personality Traits: A Meta-analysis,” *Eur J Pers*, vol. 34, no. 1, pp. 8–28, Jan. 2020, doi: 10.1002/per.2229.

[48] C. Lekati, “Complexities in Investigating Cases of Social Engineering: How Reverse Engineering and Profiling can Assist in the Collection of Evidence,” *Proceedings - 11th International Conference on IT Security Incident Management and IT Forensics, IMF 2018*, pp. 107–109, Oct. 2018, doi: 10.1109/IMF.2018.00015.

[49] I. Kirlappos, S. Parkin, and M. A. Sasse, “Learning from ‘Shadow Security:’ Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security,” in *Workshop on Usable Security*, Internet Society, May 2014. doi: 10.14722/usec.2014.23007.

[50] N. H. Chowdhury, M. T. P. Adam, and G. Skinner, “The impact of time pressure on cybersecurity behaviour: a systematic literature review,” *BEHAVIOUR & INFORMATION TECHNOLOGY*, vol. 38, no. 12, pp. 1290–1308, Dec. 2019, doi: 10.1080/0144929X.2019.1583769.

[51] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, “Don’t click: towards an effective anti-phishing training. A comparative literature review,” *Human-centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1–41, Dec. 2020, doi: 10.1186/s13673-020-00237-7.

[52] S. G. A. Van De Weijer and E. R. Leukfeldt, “Big Five Personality Traits of Cybercrime Victims,” *Cyberpsychol Behav Soc Netw .*, vol. 20, no. 7, pp. 407–412, Jul. 2017, doi: 10.1089/CYBER.2017.0028.

[53] T. J. Holt, J. van Wilsem, S. van de Weijer, and R. Leukfeldt, “Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization,” *Soc Sci Comput Rev*, vol. 38, no. 2, pp. 187–206, Apr. 2020, doi: 10.1177/0894439318805067.

[54] J. W. Bullee, L. Montoya, M. Junger, and P. Hartel, “Spear phishing in organisations explained,” *Information and Computer Security*, vol. 25, no. 5, pp. 593–613, 2017, doi: 10.1108/ICS-03-2017-0009.

[55] I. Alseadoon, T. Chan, E. Foo, and J. G. Nieto, “Who is more susceptible to phishing emails?: A Saudi Arabian study,” in *ACIS 2012 Proceedings*, Jan. 2012.

[56] P. Wang, X. Liao, Y. Qin, and X. Wang, “Into the Deep Web: Understanding E-commerce Fraud from Autonomous Chat with Cybercriminals.” doi: 10.14722/ndss.2020.23071.

[57] A. Das, S. Baki, A. El Aassal, R. Verma, and A. Dunbar, “SOK: A Comprehensive Reexamination of Phishing Research from the Security Perspective,” *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 671–708, Nov. 2019, doi: 10.1109/COMST.2019.2957750.

[58] K. Cherry, “The Big Five Personality Dimensions 5 Major Factors of Personality”.

[59] D. Yuan *et al.*, “Detecting fake accounts in online social networks at the time of registrations,” *Proceedings of the ACM Conference on Computer and Communications Security*, vol. 16, pp. 1423–1438, Nov. 2019, doi: 10.1145/3319535.3363198.

[60] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, “Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model,” *Decis Support Syst*, vol. 51, no. 3, pp. 576–586, Jun. 2011, doi: 10.1016/J.DSS.2011.03.002.

[61] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, “Preventing the attempts of abusing cheap-hosting Web-servers for monetization attacks,” *CoRR*, vol. abs/1903.05470, Mar. 2019, doi: 10.48550/arXiv.1903.05470.

[62] A. Van Der Heijden and L. Allodi, “Cognitive Triaging of Phishing Attacks”, Accessed: May 29, 2023. [Online]. Available: www.usenix.org/conference/usenixsecurity19/presentation/van-der-heijden

[63] D. J. McAllister, “Affect- and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations,” *Academy of Management Journal*, vol. 38, no. 1, pp. 24–59, Nov. 2017, Accessed: May 29, 2023. [Online]. Available: https://journals.aom.org/doi/abs/10.5465/256727

[64] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” *Front Comput Sci*, vol. 3, p. 6, Mar. 2021, doi: 10.3389/fcomp.2021.563060.

[65] Markus. Jakobsson and S. Myers, *Phishing and countermeasures : understanding the increasing problem of electronic identity theft*. Wiley-Interscience, 2007.

[66] X. Wang, R. Zhang, X. Yang, X. Jiang, and D. Wijesekera, “Voice pharming attack and the trust of VoIP,” *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, SecureComm’08*, 2008, doi: 10.1145/1460877.1460908.

[67] CSI Onsite, “Phishing,” *CSI Onsite*, Mar. 12, 2012. http://csionsite.com/2012/phishing/ (accessed Jun. 21, 2023).

[68] Cisco, “What Is the Difference: Viruses, Worms, Trojans, and Bots?,” *Cisco*, Jun. 14, 2018. https://sec.cloudapps.cisco.com/security/center/resources/virus_differences (accessed Jun. 21, 2023).

[69] Burdova Carly, “What is a Rootkit & How to Remove it? | Avast,” *Avast*, Jul. 22, 2021. https://www.avast.com/c-rootkit (accessed Apr. 28, 2023).

[70] Markus. Jakobsson and S. Myers, *Phishing and countermeasures : understanding the increasing problem of electronic identity theft*. Wiley-Interscience, 2007.

[71] F. Alharbi, Y. Zhou, F. Qian, Z. Qian, and N. Abu-Ghazaleh, “DNS Poisoning of Operating System Caches: Attacks and Mitigations,” *IEEE Trans Dependable Secure Comput*, vol. 19, no. 4, pp. 2851–2863, 2022, doi: 10.1109/TDSC.2022.3142331.

[72] A. K. Jain and B. B. Gupta, “A survey of phishing attack techniques, defence mechanisms and open research challenges,” *https://doi.org/10.1080/17517575.2021.1896786*, vol. 16, no. 4, pp. 527–565, 2021, doi: 10.1080/17517575.2021.1896786.

[73] A. Mallik, “MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS,” *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, vol. 2, no. 2, pp. 109–134, Jan. 2019.

[74] A. Sadiq *et al.*, “A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0,” *Hum Behav Emerg Technol*, vol. 3, no. 5, pp. 854–864, Dec. 2021, doi: 10.1002/HBE2.301.

[75] R. Yang *et al.*, “Scalable Detection of Promotional Website Defacements in Black Hat SEO Campaigns”, Accessed: Jun. 02, 2023. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/yang-ronghai

[76] R. Karamagi, “A Review of Factors Affecting the Effectiveness of Phishing,” *Computer and Information Science*, vol. 15, no. 1, p. 2022, doi: 10.5539/cis.v15n1p20.

[77] N. A. G. Arachchilage, S. Love, and K. Beznosov, “Phishing threat avoidance behaviour: An empirical investigation,” *Comput Human Behav*, vol. 60, pp. 185–197, Jul. 2016, doi: 10.1016/J.CHB.2016.02.065.

[78] A. K. Jain and B. B. Gupta, “A survey of phishing attack techniques, defence mechanisms and open research challenges,” *Enterp Inf Syst*, vol. 16, no. 4, pp. 527–565, 2021, doi: 10.1080/17517575.2021.1896786.

[79] F. Salahdine, Z. El Mrabet, and N. Kaabouch, “Phishing Attacks Detection A Machine Learning-Based Approach,” *CoRR*, vol. abs/2201.10752, 2022, doi: 10.48550/arXiv.2201.10752.

[80] R. Chaganti, B. Bhushan, A. Nayyar, and A. Mourade, “Recent trends in Social Engineering Scams and Case study of Gift Card Scam,” *CoRR*, vol. abs/2110.06487, Oct. 2021, doi: 10.48550/arXiv.2110.06487.

[81] M. T. Whitty, “Who can spot an online romance scam?,” *J Financ Crime*, vol. 26, no. 2, pp. 623–633, 2019, doi: 10.1108/JFC-06-2018-0053.

[82] K. Tzani *et al.*, “Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics,” *Journal of Forensic and Investigative Accounting*, vol. 12, no. 1, pp. 163–178, 2020, Accessed: May 21, 2023. [Online]. Available: http://web.nacva.com/JFIA/Issues/JFIA-2020-No1-10.pdf

[83] B. HAMMI, Y. C. E. Adja, and B. H. and Y. C. E. Adja, “Fake Check Scams: A Block Chain Based Detection Solution,” *Computer Science & Information Technology (CS & IT) 2019,Vol.9*, vol. 9, no. 8, p. 81, Jun. 2019, doi: 10.5121/CSIT.2019.90808.

[84] M. Hernandez, “‘We Are without God Now’: Benign Neglect and Planned Destruction of Brooklyn’s Bushwick Neighborhood,” *J Urban Hist*, vol. 49, no. 2, pp. 411–429, Mar. 2023, doi: 10.1177/00961442211008852.

[85] I. Nessa *et al.*, "Recruitment Scam Detection Using Gated Recurrent Unit," *IEEE Region 10 Humanitarian Technology Conference, R10-HTC*, vol. 2022-September, pp. 445–449, 2022, doi: 10.1109/R10-HTC54060.2022.9929928.

[86] Y. C. Chen, J. L. Chen, and Y. W. Ma, "AI@TSS- Intelligent technical support scam detection system," *Journal of Information Security and Applications*, vol. 61, p. 102921, Sep. 2021, doi: 10.1016/J.JISA.2021.102921.

[87] B. Price and M. Edwards, "Resource Networks of Pet Scam Websites," *eCrime Researchers Summit, eCrime*, vol. 2021-November, Nov. 2020, doi: 10.1109/ECRIME51433.2020.9493253.

[88] GOVERNMENT OF NEPAL MINISTRY OF INDUSTRY and GOVERNMENT OF NEPAL OFFICE OF THE INVESTMENT BOARD, "ICT Sector Profile", Accessed: Apr. 29, 2023. [Online]. Available: https://ibn.gov.np/wp-content/uploads/2020/04/ICT-Sector-Profile.pdf

[89] R. K. Eswari Prasad Sharma, "Internet Security Training for ccTLD managers," Sep. 15, 2008. https://nsrc.org/workshops/2008/cctld-ams/Slides/day1/countries/np-cctld.pdf (accessed Jun. 21, 2023).

[90] Timilsina Prafulla, "E-commerce in Nepal: Does it have a hopeful future? - OnlineKhabar English News," Jan. 31, 2023. https://english.onlinekhabar.com/e-commerce-in-nepal-future.html (accessed Apr. 30, 2023).

[91] "GDP per capita (current US$) - Nepal | Data." https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=NP (accessed Apr. 30, 2023).

[92] Republica, "Over 73 percent of Nepalis use smartphones - myRepublica - The New York Times Partner, Latest news of Nepal in English, Latest News Articles," Mar. 25, 2023. https://myrepublica.nagariknetwork.com/news/over-73-percent-of-nepalis-use-smartphones-1/?categoryId=81 (accessed Apr. 30, 2023).

[93] Poudel Diwas, "Data Center in Nepal," Nov. 19, 2022. https://ourtechroom.com/fitness/data-center-in-nepal/ (accessed Apr. 30, 2023).

[94] E. Kubilay, E. Raiber, L. Spantig, J. Cahlíková, and L. Kaaria, "Can You Spot a Scam? Measuring and Improving Scam Identification Ability," *SSRN Electronic Journal*, 2023, doi: 10.2139/SSRN.4344411.

[95] M. DeLiema, Y. Li, and G. R. Mottola, "Correlates of Compliance: Examining Consumer Fraud Risk Factors by Scam Type," *SSRN Electronic Journal*, Feb. 2021, doi: 10.2139/SSRN.3793757.

[96] M. T. Whitty, "Predicting susceptibility to cyber-fraud victimhood," *J Financ Crime*, vol. 26, no. 1, pp. 277–292, Jan. 2019, doi: 10.1108/JFC-10-2017-0095.

[97] M.-Y. Fan and O. Nunyuie, “Investigating the Effects of Cyber Fraud on Customer Trust for Online Shopping: The Ghanaian Setting,” *European Journal of Business and Management www.iiste.org ISSN*, vol. 11, no. 36, 2019, doi: 10.7176/EJBM/11-36-10.

[98] N. Sugunaraj, A. R. Ramchandra, and P. Ranganathan, “Cyber Fraud Economics, Scam Types, and Potential Measures to Protect U.S. Seniors: A Short Review,” *IEEE International Conference on Electro Information Technology*, vol. 2022-May, pp. 623–627, 2022, doi: 10.1109/EIT53891.2022.9813960.

[99] F. Sudzina and A. Pavlicek, “Virtual Offenses: Role of Demographic Factors and Personality Traits,” *Information 2020, Vol. 11, Page 188*, vol. 11, no. 4, p. 188, Mar. 2020, doi: 10.3390/INFO11040188.

[100] W. Nurazim, E. Wan, A. Rahim, and A. Kamaluddin, “Online Consumer’s Behavior on Product Review and The Likelihood of Them Being Fraud Victims,” *International Journal of Business and Technopreneurship*, vol. 11, no. 3, 2021.

[101] C. Fonseca, S. Moreira, and I. Guedes, “Online Consumer Fraud Victimization and Reporting: A Quantitative Study of the Predictors and Motives,” *Victims & Offenders* , vol. 17, no. 5, pp. 756–780, 2022, doi: 10.1080/15564886.2021.2015031.

[102] Ipsos, “SURVEY ON ‘SCAMS AND FRAUD EXPERIENCED BY CONSUMERS’ Final Report,” Jan. 2020, Accessed: May 01, 2023. [Online]. Available: https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

[103] K. Prasain, “Wage gap between men and women persists, report says,” Jun. 17, 2021. https://kathmandupost.com/money/2021/06/16/wage-gap-between-men-and-women-persists-report-says (accessed Jun. 04, 2023).

Appendices

Here the document that should not be included in the main part of the thesis are included.

Survey Questionnaire

Key Objectives of Survey

- To **map the most frequent types of fraud/scams** and understand which types of fraud/scams are most common;
- To map the **channels** most frequently used by fraudsters to deceive consumers;
- To identify **financial and nonfinancial impact** of fraud/scams;
- To identify to which extent consumers **report scams and fraud** and if they are aware of any **awareness raising in relation to scams** and if they have acted to **protect themselves from scams**;
- To identify to which extent online scams and fraud **impact online behavior**.

Name: Signature:

1. Age:

2.Gender:

1. Male
2. Female

3.Education

1. School
2. High School
3. College
4. Master or Higher

4.Internet Use

1. At least once a week
2. Once a month or less
3. Hardly ever or never

5.Current Address Urbanity

1. Rural area or village
2. Small or mid-size
3. Large town

6.Subjective income (How hard is it to earn money you need?)

1. Very difficult
2. Fairly difficult
3. Fairly easy

4. Very easy

7.Province No.

1. Province 1
2. Province 2
3. Province 3
4. Province 4
5. Province 5
6. Province 6
7. Province 7

8.Which type of scam did you become a victim of? (type of fraud or scam)

Buying scam

1. You ordered free or relatively cheap products or services, but it turned out you had been tricked into a costly monthly subscription.*
2. You bought what you thought was a good deal, but you never received the goods/service or the goods /services turned out to be fake or non-existent.*
3. You received a fake invoice for products that you had not ordered and you were asked to pay the cost.

Identity theft

4. You were contacted - by phone, face to face, by email or by another mean - by someone pretending to be from a legitimate organization such a bank, telephone or internet service provider, or government department, and asked to provide (or confirm) personal information.
5. You were approached - by phone, face to face, by email, by another mean - or you accessed a website and were informed that you had a computer or internet problem. Then you were asked for your personal details and your bank or credit card details to have the problem solved.

Monetary fraud

6. You were promised you would receive a good, a service, a rebate or an important investment gain if you transferred or invested money.
7. You bought tickets for an event, concert or travel but it turned out the tickets were not genuine and/or you never received them.*
8. You were contacted by someone pretending to be from a legitimate organization, such as a bank, internet provider or government, who claimed there were problems with your account or other documentation and threatened you with harm if you did not pay to resolve the problem.
9. You received notification of a lottery win or a competition win but were informed you would need to pay a fee or buy a productin order to collect your prize.

Please Explain

_____

_____

_____

_____

_____

9.Did you suffer from the scam and/or fraud experienced? (Impact)

1. Suffered emotionally
2. Suffered financially
3. Suffered physically
4. Did not suffer

Please Explain

_____

_____

_____

_____

10.What was the level of financial loss experienced as a result of a fraud/scam? (Impact)

1. Nothing (Rs 0)
2. Less than Rs 500
3. More than Rs 500 but less than Rs 5,000
4. More than Rs 5,000 but less than Rs 20,000
5. More than Rs 20,000

11.Online and offline behavior and experience with fraud in the last two years

1. You are suspicious of letters or emails containing spelling and grammar mistakes
2. You avoid clicking links in emails or text messages unless you know the sender
3. You are suspicious of people you don't know when they approach you in person, via
4. You install anti-spam software or anti-virus
5. You perform checks on the credibility of the vendor
6. You only provide your identity card or information from your ID in person or on a secured…
7. You only make online purchases with a credit card (in order to get your money back if…
8. You carefully read terms and conditions
9. You subscribe to a specific service to avoid commercial calls
10. You transfer money to someone you don't know (e.g. via Western Union)

12.Online buying behavior before or after fraud experience.

Before	After
1. Frequent 2. Occasional 3. Never	1. Frequent 2. Occasional 3. Never

13. Reason for buying or not buying (impact on online behavior)

1. I am not interested in general
2. Victim of Scam or Fraud
3. Too Expensive
4. Too Cheap
5. Other

14.When did you experience fraud?

1. No, I have not
2. Yes, I have - in the past 2 years ago
3. Yes, I have - more than 2 years ago

15.Which channel did you experience fraud through? (Channel)

1. Via an email
2. Via fax
3. Via an advertisement in a magazine or newspaper
4. In person through someone approaching you at another location
5. In person through someone approaching you at home
6. Via WhatsApp, Facebook messenger or other mobile messaging channels
7. Via a postal letter
8. Via an online advertisement on a social media website, blog or forum, like Facebook
9. Via SMS/text message
10. Via an online advertisement on a non-social media website
11. Via a phone call on your landline phone
12. Via a phone call on your mobile
13. In some other way

16.Channels used for reporting (reporting)

1. No, I have not
2. Yes, to family/friends
3. Yes, to officials such as police
4. Yes, to the vendor

17.Which official authority did you report to? (reporting)

1. The bank or credit card company

2. The police
3. An industry regulator (e.g. telecom authority, bank supervision authority)
4. A consumer association
5. A consumer protection authority
6. Another channel

18. Please state your reason for reporting

_____

_____

_____

_____

19.Please state your reason for not reporting

1. I didn't know how to report
2. I was Embarrassed
3. I Couldn't work on device anymore
4. I didn't have Time
5. I didn't want to give out ID Details
6. I was unclear about reporting authority
7. I felt it would not make a difference
8. There was no Financial Harm

20.Please state where would you prefer to report fraud

1. A dedicated free phone number operated by the government
2. A dedicated governmental website
3. A dedicated helpdesk via email
4. A booth in a central location in my country
5. A dedicated free phone number operated by a non-governmental organization
6. A dedicated non-governmental website

21.Have you seen a commercial, advertisement or other campaign to warn about fraud in the past two years (awareness raising)

1. Yes, tell us more about it:_____
2. No
3. Don't know / Can't remember

What should be done to avoid scams/fraud?

_____

_____

_____