

The background is a dark, textured collage of various social media posts and logos. At the top, there are several 'Scam Design' sponsored posts with a yellow smiley-face logo. In the center, a yellow banner reads 'THE ANATOMY OF'. Below this, the main title 'ONLINE PRODUCTS & SERVICES SCAMS' is written in large, bold, yellow capital letters. Underneath the title, the author's name 'BY ROSANINA ESTRELLA' is written in smaller, white capital letters. At the bottom, there are more social media posts, including one with a large orange and red circular logo and another with a yellow smiley-face logo. The overall aesthetic is digital and chaotic, reflecting the theme of online scams.

THE ANATOMY OF

ONLINE PRODUCTS & SERVICES SCAMS

BY ROSANINA ESTRELLA

Scam design: the anatomy of online products & services

The deconstruction and exploration of online product and services scams on social media and websites from a user experience, visual design and service design perspective.

ROSANINA ESTRELLA

A 90-point thesis submitted to Victoria University of Wellington, in partial fulfilment of the requirements for the degree of Master of Design Innovation.

Victoria University of Wellington
2020

Figure 1. Cover: Photomanipulation visual piece on scam social media posts

ACKNOWLEDGEMENT

To my supervisors Walter Langelaar and Dr Catherine Caudwell. Thank you for teaching me to take risks, to push boundaries and limits. Thank you for reminding me the importance of putting myself in my designs than just to follow the same old cookie cutter design structure. For challenging and helping me take my design to the next level

To Gillian and Dana - it's been fantastic knocking good user experience minds with you!

To the fellow Masters' students but especially Hazel, Stacey, Senai and Rick. It's been fun sharing this Masters journey with you.

To Micheal - thank you for coming back with me this last year. You looked after me at my worst and helped me overcome the hardest walls to climb. Thank you for always believing in me.

To my friends who kept me sane, reminded me to take breaks, played games and fed me - Izzy, Viv, Rissa, Emma, Brian, Derek and Eden.

To my awesome coworkers past and present in the Web Services family for being constantly supportive and inspiring (especially inhabitants of design island for always having my back)
- Michelle, Mike B, Corina, Brendon, Mallika, Jonathon, Catherine, Mel, Fiona, Christine, Phillip, Jai, Mike L, Dan, Alex, Craig, Zaid, Graham, Tim, Flo, Ian, Lance, Chris, Harshmin and Arapaoa.

To family, especially my parents Virigina and Renato, for your love, patience, support and good food throughout.

FORWARD

This thesis is written by a digital explorer, adventuring the depths of long term curiosity. I have always been fascinated by the craft of scams in the digital realm: how they are created, how they are mechanically put together and designed, and how they are implemented. I became just as excited when understanding who the people scams impacted - both victims and scammers alike. When I later entered the industry and became a user experience designer, my gained knowledge and expertise in designing digital products and interfaces further fueled my interest in understanding the deeper issues and technicalities within this subject area. I grew the temptation of using my practical skills and knowledge of user

interface design to combine them with my subject interest and further recreating digital scam design. “I can do it. So why not for fun?” By looking at existing scam websites and scams on social media including the relationship and process between the two, I knew how easy it was to design, recreate and implement believable and functional scams that would fool everyday internet users. Yet I am not a true scammer with malicious intent - just a curious designer.

The intention of designing to help internet users and to build knowledge on a largely unexplored area of scam design encouraged the development of this thesis and design output.

ABSTRACT

Netsafe New Zealand's (2018) quarterly reports indicate that millions of dollars are lost through online products and services scams in New Zealand through social media and online platforms every year. In 2018 alone, there were over 10,740 total scams, with the highest reported fraud type being products and services. However, despite regular media attention and community conversation on the problem, why is the number of everyday users who fall for the same online traps continuously increasing? From fake competitions to counterfeit online goods retailers, it is shown that many users are quick to believe these impersonated companies are real, only to publicly vocalise their distress once they have succumbed to a scam.

This study provides insights into the overarching processes of how online products and services

scams are constructed and implemented within social media and websites. Specifically, this study explores the mechanics, tools, techniques and frameworks that make up the basis of how online products and services scams work. Through these investigations, this study will develop a unique framework that captures the overarching process of how online products and services scams function from start to end.

Through 2 small experiments, this new framework is further demonstrated within the context of coronavirus (COVID-19) pandemic online scams by deconstructing then reconstructing both commonly encountered and potential COVID-19 New Zealand specific scams that have appeared between March-June 2020.

PART 1

1.0

INTRODUCTION 13

1.1 Research question 15

1.2 Defining boundaries 17

1.3 Research overview 18

1.4 Keywords 19

1.5 Aims & objectives 20

1.6 Methodologies 21

2.0

BACKGROUND RESEARCH 23

2.1 Scams through the ages 27

2.2 “Common sense” assumptions 29

2.3 Frameworks, Mechanics & Strategies 34

 Framework 1: Scam classification strategy 35

 Framework 2: Multilevel model of cybercrime 41

 Framework 3: Toolkit of scam strategies 44

 Framework 4: Dark patterns within scams 49

 Framework 5: The seven deadly sins of social engineering - 50

 Framework 6: Stages of a products & services scam 69

 Framework 7: 5-step model marketing process 80

 Framework 8: Social media marketing process 83

2.4 New framework output 86

PART 2

3.0

PRELUDE & CONTEXT 97

3.1 New Zealand scams 98

3.2 Event based scams 100

3.3 Introduction to COVID-19 102

3.4 COVID-19 in New Zealand 103

 3.4a Timeline of COVID-19 in New Zealand 104

 3.4b Impact of NZ leaders 107

 3.4c Unite against COVID-19 campaign 108

 3.4d COVID-19 scams 109

4.0

EXPERIMENTATION 117

4.1 Experiment 1 120

4.2 Experiment 2 160

4.3 Collection of Scams 178

5.0

DISCUSSION 180

5.1 Discussion 181

5.2 Limitations & opportunities 187

6.0

CONCLUSION 189

6.1 Conclusion 190

6.2 References 192

6.3 List of figures 196

6.4 Appendix 198

An introduction to the project's subject topics, outlining the research's aims and objectives, identifying the methodologies used and clarifying technical terminology and keywords will be used throughout the study.

1.1 Research question

1.2 Defining boundaries

1.3 Research overview

1.4 Terminology

1.5 Aims & objectives

1.6 Methodology

10

INTRODUCTION

13

RESEARCH QUESTION

**WHAT ARE THE MECHANICS, TECHNIQUES
AND OVERARCHING PROCESSES WITHIN
ONLINE PRODUCTS & SERVICES SCAMS ON
SOCIAL MEDIA & WEBSITES?**



Figure 1.1. Fake Noel Leeming Facebook page scam, promoting a competition to “Win a Nintendo Switch”.

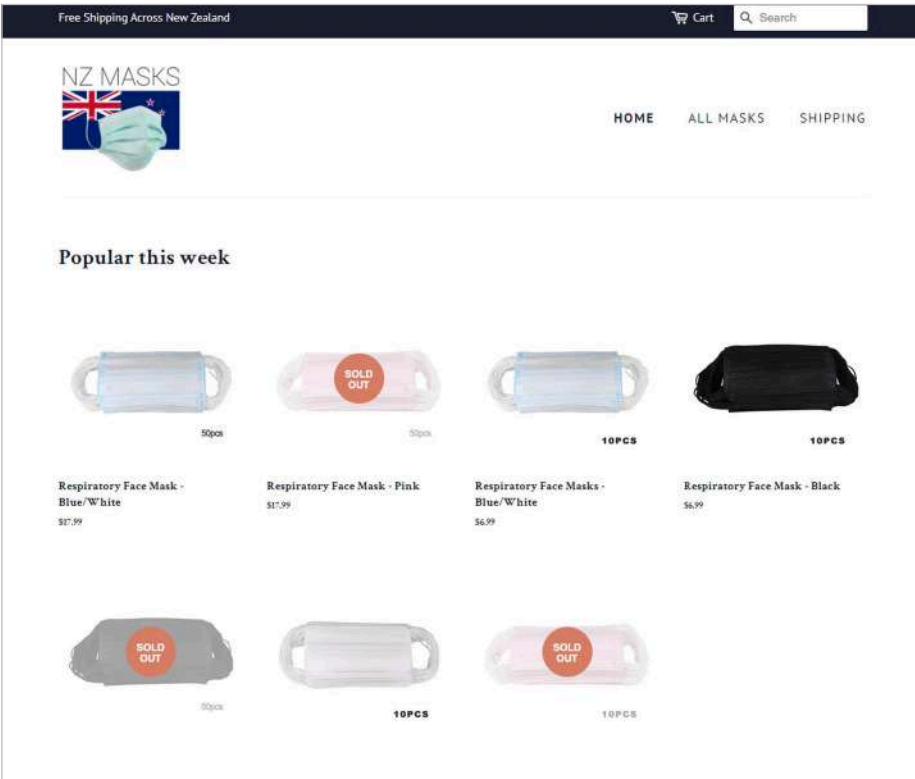


Figure 1.2. Fake scam store ‘masks-nz.myshopify.com’ originally advertising the selling of face masks when there was high demand, low stock in New Zealand.

DEFINING THE BOUNDARIES OF RESEARCH WITHIN ONLINE PRODUCTS AND SERVICES SCAMS ON WEBSITES AND SOCIAL MEDIA

Before diving into the depths of research, I find it important to clarify the scams which this research will be investigating specifically. Scams is a broad topic and even more specifically digital scams, thus understanding the scope of where this research area lies is crucial to acknowledging where the boundaries of the research starts and stops.

This research focuses on products and services that are advertised and sold on social media and websites.

Specifically the following:

- For social media products and services scams, I will focus primarily on scam posts, fake social media ads and fake social media pages (as seen on Figure 1.1) which advertises these product and services scams.
- For websites, I will focus primarily on scam ecommerce stores (such as Figure 1.2) that advertise and sell fake or non existent products.

The reason is that I have chosen to investigate scams on both platforms is that part of this research includes understanding the scam design process and mechanics between them.

1.1 RESEARCH OVERVIEW

PART 1
CHAPTER 1 - INTRODUCTION

An introduction to the project's subject topics, outlining the research's aims and objectives, identifying the methodologies used and clarifying technical terminology and keywords used throughout the study.

CHAPTER 2 - BACKGROUND RESEARCH

The second chapter helps build a better understanding of products and services scams including the origin of products and services scams, common assumptions often stated from everyday people, and scam diversity. To better interpret how products and services scams work, common techniques, mechanics and existing relevant frameworks are identified and further analysed to provide clarity when deconstructing them.

PART 2
CHAPTER 3 - PRELUDE & CONTEXT

This chapter creates the groundwork for the second part of the project and provides an introduction to the 2019-2020 coronavirus (COVID-19) pandemic within both a worldwide and New Zealand context. To- understand how products and services scams could take advantage of their victims using the COVID-19 pandemic, this chapter also discusses

New Zealand's approach, visualises the impact of the pandemic on the country and the role COVID-19 scams will play.

CHAPTER 4 - EXPERIMENTATION

The mechanical deconstruction, design-based recreation and visualisation of frequently encountered and potential New Zealand COVID-19 products and services scams through two speculative experiments. A focus of these speculative experiments is to illustrate and communicate the larger, overarching picture of these scams.

CHAPTER 5 - DISCUSSION

Theis chapter discusses the project's research process, ideation, iterative design process and relation to the context of the COVID-19 pandemic. Further discussion on limitations that caused restrictions within the project and opportunities that the research could take in the future.

CHAPTER 6 - CONCLUSION

This closing chapter concludes the research and reflects on the overall study and implications for the future.

1.2 KEYWORDS

The subject area of scams contains a variety of complex and unfamiliar words and terms. The terminology will be explained in further depth throughout the research and within the context they are placed in.

SCAMS

The fraudulent use of electronic communications to deceive and take advantage of users. Phishing attacks attempt to gain sensitive, confidential information by posing as a legitimate individual or institution via phone or email (Munton & Jelita McLeod, 2011).

PRODUCTS AND SERVICES

Products can be defined as anything (most commonly an item) that we can offer to a market for attention, acquisition, use or consumption that could satisfy a need or want (Merriam Webster, n.d.).
Services are a special form of product that consists of activities, benefits or satisfactions offered for sale that is intangible and do not result in the ownership of anything (Merriam Webster, n.d.).

USER EXPERIENCE (UX) DESIGN

User experience is the emotional experience a person has when they use a product or service. User experience design is the process design teams use to create products that provide meaningful and relevant experiences to users. It is defined as describing “all aspects of the person's experience when interacting with the product” (Stewart, 2015).

SERVICE DESIGN

Service Design is defined as the process used to understand the behaviour and journey of customers when they interact with a service, primarily focusing on the customer's experience and the service's quality that is provided (Saco and Goncalves, 2010).

1.3 AIMS & OBJECTIVES

	RESEARCH AIMS	RESEARCH OBJECTIVES	METHODOLOGY
PHASE 1	To investigate the current state and impact of products and services scams within websites and social media and it's relationship with its users.	1a. Investigate the research within the current bodies of literature to understand the commonalities, connections and gaps within the area of products and services scams	RESEARCH ABOUT DESIGN Literature Review
		1b. Analyse, deconstruct and describe the anatomy, framework and techniques of products and services scams	RESEARCH ABOUT DESIGN Precedent Review
PHASE 2	To explore and visualise both the overarching perspective and dissected view of products and services scams within the context of COVID-19.	2a. Analyse the New Zealand ecosystem of products and services scams within the context COVID-19	DOCUMENT & MEDIA ANALYSIS
		2b. Generate ideas and concepts of potential speculative New Zealand COVID-19 products and services scams based on the anatomy and findings from 1b and 2a	SPECULATIVE DESIGN
		2c. Design and create simple graphic design and interactive prototypes experiments demonstrating speculative New Zealand COVID-19 products and services services scams	RESEARCH THROUGH DESIGN Iterative Design Prototyping

1.4 METHODOLOGY

Methodologies that will be conducted within the research

RESEARCH ABOUT DESIGN
(LITERATURE REVIEW)

The initial stage of the research explores existing products and services scams to understand the broad research area and it's historical to modern evolution. This acknowledges the transition from analogue scams to digital scams and the impact and perception they have on its targets.

RESEARCH ABOUT DESIGN
(PRECEDENTS)

This research investigates existing products and services scam frameworks, processes and mechanics that have been acknowledged within other disciplines (such as marketing, security, technical etc.) (Findeli, 1995). This will explores the commonalities between frameworks, highlight potential gaps, investigate unique discipline viewpoints, translate and visualise these processes within a design angle.

By studying existing frameworks, it will allow the creation of a unique framework process for products and service scams.

SPECULATIVE DESIGN

Speculative design creates potential hypothetical future projections of events, situations, items, products and services while questioning, analysing and critiquing current states and opportunities (DiSalvo, 2012). I believe that speculative design is an appropriate method for this project as the analysis of existing scams and their mechanics can assist in identifying, speculating on future scam mechanics that do not currently exist, but could potentially surface in the near or far future and providing logical explanations to these speculative scams.

**QUALITATIVE DOCUMENT &
MEDIA ANALYSIS**

Altheide & Schneider (2003) indicate that undertaking analysis into contemporary mass media for products and services scams will shape the research by providing scope and clarification around the specific areas that this research will target. The analysis that this research will capture will include:

- The latest, current and relevant online products and services scams (especially those within the last 1-4 years) worldwide and specifically in New Zealand. Understanding the latest scam trends will help identify the most common types, mechanics, and strategies and how they function in a real-life context.
- How have products and services scams impacted people and legitimate organisations both internationally and in New Zealand? What examples are out there that tell the stories of the people who these scams have affected? What can we learn from these examples?

What is the current understanding and perception of online scams by everyday people? At what level of understanding do potential victims have? How has both international and New Zealand mass media shaped the idea of what online products and scams are - and what impact they could have on a person?

It is essential to acknowledge that non-academic material will potentially have bias to the author and/or misinformation/inaccurate information, therefore using official information (such as those released from official organisations and government agencies will be used to back these claims).

**RESEARCH THROUGH
DESIGN**

The research is human orientated and focuses on people's experiences and their relationship with "products, services, events and environments" (User Experience, 2009). Research through design will allow further visualisation, exploration and demonstration of speculative online products and services scam design.

The second chapter helps build a better understanding of products and services scams including the origin of products and services scams, common assumptions often stated from everyday people, and scams' diversity. To better interpret how products and services scams work, common techniques, mechanics and existing relevant frameworks are identified and further analysed to provide clarity when deconstructing them.

- 2.1 Scams through the ages**
- 2.2 “Common sense” assumptions**
- 2.3 Analysis of existing frameworks**
- 2.4 New Interwoven Scam Process**

20

BACKGROUND RESEARCH

The internet has become an integrated part of our everyday lives (Young & Nabuco de Abreu, 2010). Most individuals rely on the web for personal or work use such as entertainment, online retail, communication or business (Jeonga, Kim, Yuma & Hwang, 2016). From the attraction of convenience, variety of choice and impactful marketing, the area of e-commerce and online shopping has grown exponentially (Ward & Lee, 2000).

While new technology is rapidly introduced to optimise, connect and entertain its users, malicious individuals are taking this opportunity to find ways to misuse and take advantage of them (Wilson, 2017; Button, Nicholls, Kerr & Owen, 2014). While subjects within cybercrime are continuously being researched, the areas of scam study primarily focus on telecommunication and email platforms (Chih-Yuan, Sun, Jerry, Cian, Huei-Tse, and Lin, 2017). There is also a lack of research that focuses on the “misuse of social media by cybercriminals” who implement scams (Vishwanath, 2014). Furthermore, the constant evolution of online platforms, accessibility to personal data (Yin, Karimi, Lampert, Cameron, Robinson, & Power, 2018) and integration of current trends has allowed scams to develop more intelligently, realistically, genuinely, relative and personalised to the specific

user (Aleroud & Zhou, 2017; Button, Nicholls, Kerr & Owen, 2014). Scams keep up with the evolution of the internet, but the tools and methods to educate and prevent users from becoming targets ~~to~~ are falling behind (Hofman and Keates, 2013).

This literature review will discuss online consumer products and services scams on social media and web platforms. This includes the current state, evolution and diversity of products and services scams, analysing the construction of technical, social engineering, marketing and design mechanics that make up an online product or service scam. The study aims to uncover existing frameworks, understand repetitive commonalities and discover gaps that previous studies have not yet explored.

2.1 SCAMS THROUGH THE AGES: THE ORIGIN AND CURRENT STATE OF ONLINE PRODUCTS AND SERVICES SCAMS

A look into the origins of online products and scams.

Academic research into digital scams originates as far as the early 1980s (Arkin, 1986), with products, services and financial-based scams as one of the first introduced scams in academic studies (Smythe, 1999). The late 1970s brought a strong wave of product and services sales through telemarketing due to its convenience, efficiency and low cost in comparison to original door-to-door sales and direct mail. This prominent rise of this approach to retailing resulted in an increase of products and services scams. It provided opportunities for con artists to take advantage of the anonymity and lack of face-to-face contact that came with the telephone method. The 1990s brought email-based scams which frequently presented the emergence of prize, merchandise, travel and investment scams (Smythe, 1999). As the internet has grown more embedded into our everyday lives, it has coevolved alongside scams (Kolari, Java & Joshi, 2007).

The early 2000s popularised social media networking websites such as Friendster, MySpace and LinkedIn introducing new platforms and methods for scamming targets. As this new territory of networking was exciting for people to use, it was also a new avenue for scammers to benefit from. Fraudsters took advantage of openly available information that users were putting

out (Datar & Misland, 2010). As social media websites were in it's early phases of user adoption, I assume that privacy features would also be much more simple than the complexity of privacy features today. It could be assumed that users may not have possibly had a point of reference and were unfamiliar with the potential malicious uses the platforms.

The first notable recorded scam event was on Yahoo!'s social blogging community, MyBlogLog. Kolari, Java & Josh (2007) indicates one of the earliest examples of scammers who created fabricated online personas through fake crafted profiles with stolen profile pictures, fictitious friend lists, and fake comment interactivity. Morris (2014) labels this act of an "identity used for purposes of deception within an online community" as sockpuppetry. The later addition of business pages on social media sites such as on Facebook in 2007 (Boyd, 2019) gave scammers the ability to evolve their scams from simple sockpuppets to fake businesses.

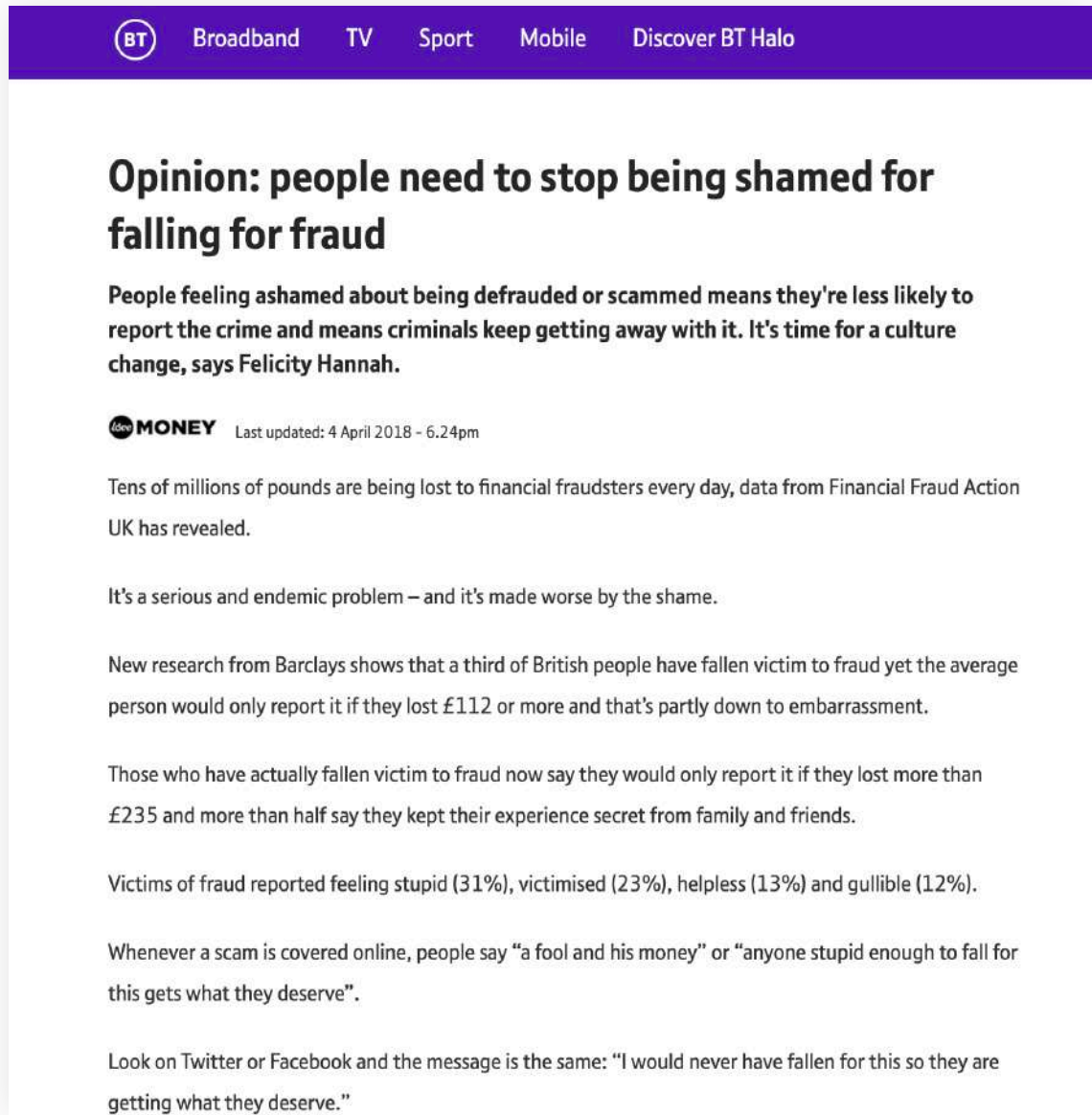
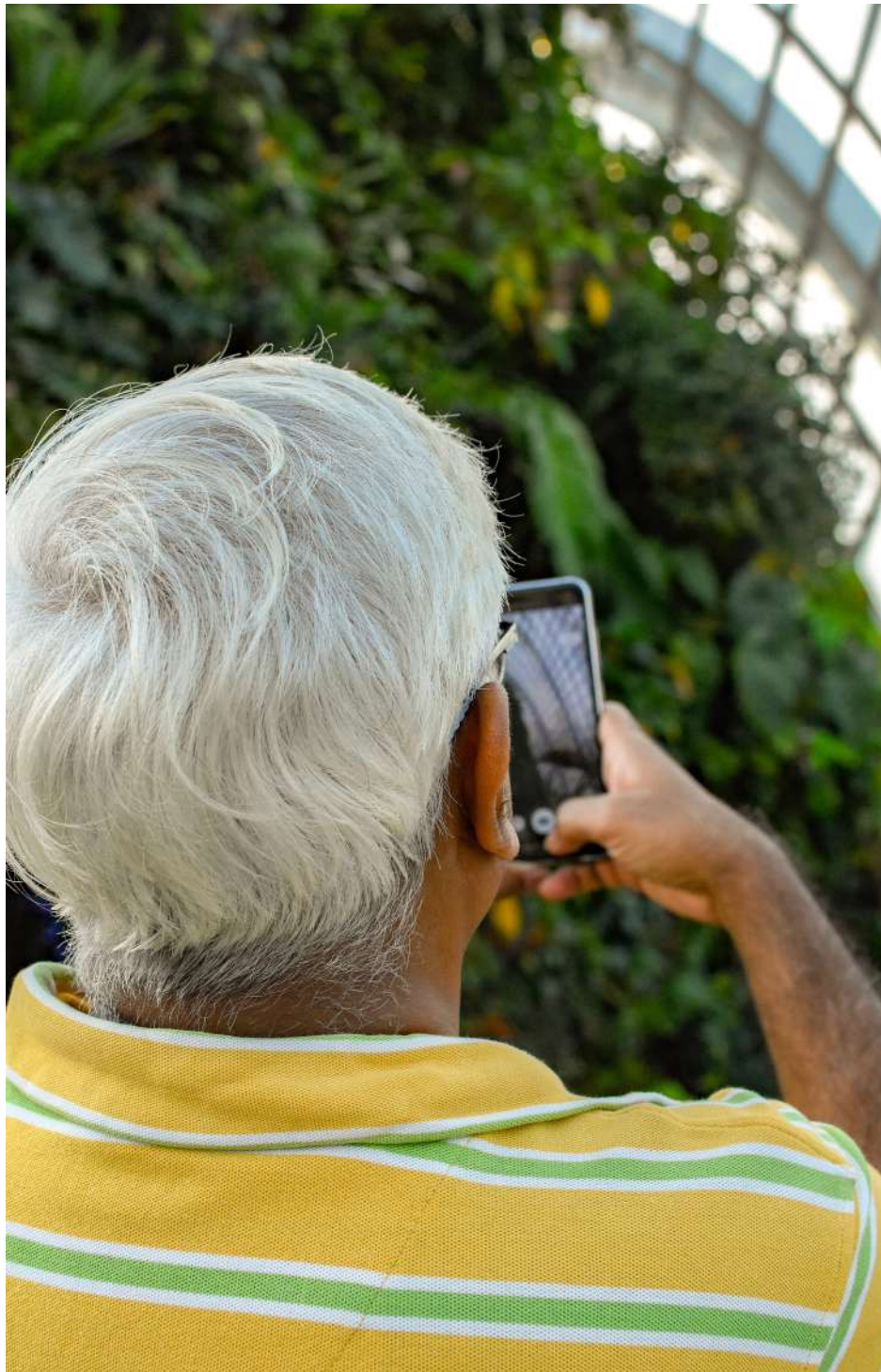


Figure 2. Media opinion piece on scam victim shaming

2.2 “COMMON SENSE” ASSUMPTION ABOUT ONLINE PRODUCTS AND SERVICES PHISHING

There are many assumptions about general online scams and specifically within online products and services scams. Having a lack of knowledge of what is publicly perceived as “common sense” can often result in shaming or humiliating a person. The shaming and blaming is even more prominent if they become a target or fall victim to a scam (Hooi Koon, 2014).



ASSUMPTION 1

THE PERCEPTION THAT OLDER ADULTS ARE THE MOST COMMON VICTIMS

One of the most common assumptions made by people is that the most likely victims of fraud and scams are older adults and elderly users (Deevy, Lucich and Beals, 2012). Much of academic research papers conducted from the early 1980s to the late 2010s focuses on older adults and elderly users who are targeted. Ross, Grossmann and Schryer (2014) also agreed that the notion that older users are “especially susceptible to consumer fraud” is both a psychological and widespread assumption. They push the point that there is “no compelling evidence” that elderly and older adult users are “disproportionately victimised” by these scams despite popular opinion. Martin (2013) states specifically that as people get older, failing memories, advancements in technology, and a lack of exposure and knowledge around new technologies make the internet a dangerous place for older adults, however, The Australian Competition and Commisions’s scam organisation Scam Watch (2020) emphasises that there isn't a specific group that is more vulnerable to scams than others. Deevy, Lucich and Beals (2012) also reiterate that everyone is susceptible to scams, however, each victim's exposure or susceptibility will vary between different types of scams.

Figure 3. Old man using a phone to take a photo

ASSUMPTION 2

BIASED PERCEPTION THROUGH EXPERIENCE

Williams, Beardmore and Joinson (2017) discuss the biased perception and preconceived knowledge that many users have about scams of how they work, function and successfully fool victims. For instance, the authors explain that people who have previously fallen for them establish their knowledge on their experience gained through being the victim. They also explain that exposure to scam knowledge and awareness can be biased through outcomes seen through the media. For example, a victim could watch a documentary or news broadcasting about another victim's scam experience, adding to their exposure and scam knowledge. Their knowledge could only be limited to what they've seen creating tunnel vision when learning and acknowledging alternative methods of the same scam.

ASSUMPTION 3

SCAMMERS PRIMARILY ARE FROM ASIAN COUNTRIES, IN PARTICULAR, INDIA AND CHINA

Attempted scams received by victims are often perceived to be predominantly from Asian regions. This assumption is commonly the result of victims picking up phone calls from strongly accented callers from commonly associated nationalities or emails with broken English and largely incorrect spelling and grammar errors (Arthur, 2010). The mindset of “if the phone call or email gives specific hints or red flags that the sender is either from India, China or other Asian countries, it can create tunnel vision for the victim. As their mind has decided what the scammer looks and acts like, it can make victims forget that scammers can be anyone (Australian Competition and Consumer Commission, 2018).

ASSUMPTION 4

PEOPLE AREN'T BOTHERED TO REPORT

Netsafe (2019) stated within two of their quarterly 2019 reports that products and services fraud were the most reported type of scams from April to September out of all the scams reported to the agency. The number of these products and services scam reports increased it's report rate from 41% to 51% from June to September. Netsafe comments that "fortunately, the reported financial losses to this scam have been low", implying the positive outcome on victims not losing much from this scam.

Some of the reasons that people are not bothered to report these scams may include the following.

Is not easily as noticed within a victim's bank balance history

(Button, Nicholls, Kerr, & Owen, 2014)

Seeing large amounts of money deducted without a victim's knowledge to an unknown receiver is an obvious red flag to victims, indicating that their account has been tampered with. By only taking small amounts of money at a time, the scammer can blend in with other smaller and more regular purchases.

Multiple successful scam attempts

(Button, Nicholls, Kerr, & Owen, 2014)

Instead of taking a single large amount of money in one go, scammers who deduct small amounts of money at a time can add up to a large amount over time if left unnoticed.

A lack of urgency due to only losing a small amount of money

(Button, Nicholls, Kerr, & Owen, 2014)

The victim's mindset of "it's only \$5, it's not that much" is often the case, especially when comparing the loss to scams where a more significant amount of money is lost. Victims of scams with more minor financial losses treat the misfortune as not a big deal and assume that it will be unlikely to happen again.

2.3 AN ANALYSIS OF EXISTING

FRAMEWORKS, MECHANICS & STRATEGIES

To better interpret how products and services scams work and the mechanics used within them, I will be analysing eight different existing frameworks created by other practitioners which I believe has significant relevance to the scam design process.

The frameworks that I will be analysing includes:

- Framework 1: Scam classification strategy (Stabek, Watters, & Layton, 2010)
- Framework 2: Multilevel model of cybercrime (Naidoo, 2020)
- Framework 3: The toolkit of products and services scam strategies (Australian Competition & Consumer Commission, 2016)
- Framework 4: Dark patterns within products and services scams (Brignull, 2010)
- Framework 5: The seven deadly sins of social engineering (Nodder, 2013)
- Framework 6: The stages of a product and services scam (Smith, 1922)
- Framework 7: 5-step model marketing process (Armstrong, Adam, Denize, Volkov & Kotler, 2018)
- Framework 8: Social media marketing process (Andzulis, Panagopoulos & Rapp, 2012)

FRAMEWORK ONE

SCAM CLASSIFICATION STRATEGY

The ‘Scam classification strategy’ (Stabek, Watters, & Layton, 2010) categorises scams into seven different types by grouping scams with similar processes, mechanics, information and intentions. With each scam classification, a goal of the scammer’s intended outcome is also stated. I find that this framework is relevant to the research because many products and services scams fall into these provided categories while giving clarity to their process, mechanics and scam goals.

DIVERSITY OF SCAMS

Within their research, Button, Nicholls, Kerr & Owen (2014) describes the diversity of scams as “not just old wine in new bottles” explaining that scams are more than just the same mechanics reused on different platforms and technology. The authors mention that the internet has given fraudsters and scams a “boost and new dimension”. Even commonly known scams can use various new strategies, platforms and approaches that can catch targets off guard unexpectedly (Australian Competition and Consumer Commission, 2018). The regular person can’t know of every variation and type as scams are constantly evolving (Australian Competition and Consumer Commission, 2018).

Diversity in scams comes from the natural evolution of scams over time. For example, products and services scams originated from in-person and telemarketing before jumping from analogue into the digital space of email, online stores and most recently social media (Kunwar & Sharma, 2016). While some forms of strategies can retire (often due to the retirement of the technology it’s built upon - e.g fax), new strategies add to the complexity and diversity to improve existing methods rather than to replace them.

(Button et al., 2014)

Stabek, Watters, & Layton (2010) acknowledge that different people have their own classification strategies to identify different types of online scams. The authors’ aim is to determine an overarching scam classification framework that can be used within various other industries and situations while identifying the scam’s core goal.

The seven scam types that were identified in the following first framework included:

- Low Level Trickery
- Developed story based applications
- Employment based scams
- Implied Necessary Obligation
- Apparently Authentic Appeal
- Merchant and Customer Based Exploitation
- Marketing Opportunities



LOW LEVEL TRICKERY

The most basic form of scams in which, while not spontaneous, planning and details of conducting the scam are not as thorough as other complex scams. These scams are commonly one-off transactions that use minimal basic techniques to fool victims into giving their money. However, some may have the potential to grow into more than just one-offs.

This scam type’s goal is financial gain.



DEVELOPED STORY BASED APPLICATIONS

These scams incorporate the building of trust and relationship with the victim, often taking advantage of their wants and needs. The basis of these scams relies on “assumption based public knowledge” or a “global tragedy”. These scams are complex, created with in-depth planning and detail.

The scam type’s goal is financial gain and information gathering.



EMPLOYMENT BASED SCAMS

Scams under the guise of employment opportunities for victims, but ultimately, a method of obtaining their personal information. Being an applicant for the ‘potential job’ can result in personal information stolen from these scams. These scams are complex, created with in-depth planning and detail.

This scam type’s goal is identity and information gathering.



IMPLIED NECESSARY OBLIGATION

While this scam type is explained in vague terms and can be confused with Low level trickery, the victim is tricked into responding by financial means where it seems necessary. Where Low level trickery’s financial tricks are made to be unnoticeable, this technique forces the user to use money. These scams are complex, created with in-depth planning and detail. This scam type’s goal is financial gain.



APPARENTLY AUTHENTIC APPEALS

Technical scams that aim to capture personal and financial information through digital tools such as spyware and keylogging software. These scams are complex and the scammer must be technologically knowledgeable to work successfully. These scams are complex, created with in-depth planning and detail.

This scam type's goal is nformation gathering.



MERCHANT AND CUSTOMER BASED EXPLOITATION

Transactional scams which involve both sellers and buyers through a collection of multiple similar styled scams. Examples of these scams include shill bidding, bid shielding, undelivered merchandise, undelivered payment, and product authenticity. While interaction with the victim is short, these scams and their details are heavily researched and planned prior.

This scam type's goal is fnacial gain and information gathering.



MARKETING OPPORTUNITIES

These scams are a mixture of multiple scam types that advertises money-making opportunities (such as gambling, shares, investment and business opportunities) to the victim. These scams are heavily researched and planned before further development.

This scam type's goal is fnacial gain and information gathering.

WHAT WOULD ONLINE PRODUCTS AND SERVICES SCAMS BE CATEGORISED AS?

From Stabek, Watters and Layton's (2010) framework, products and services scams seem to fall obviously within the merchant and customer based exploitation scam type. It involves sellers, buyers, aspects of developed story-based applications, apparently authentic appeals, marketing opportunities scam types could also be relevant.

Figure 4. Visualises each scam catagory and identifies where their goal's fit as a whole. I believe that products and services scams would primarily fit within fnacial gain and information gathering, however can also fit within identity gathering.

FINANCIAL GAIN

IDENTITY GATHERING

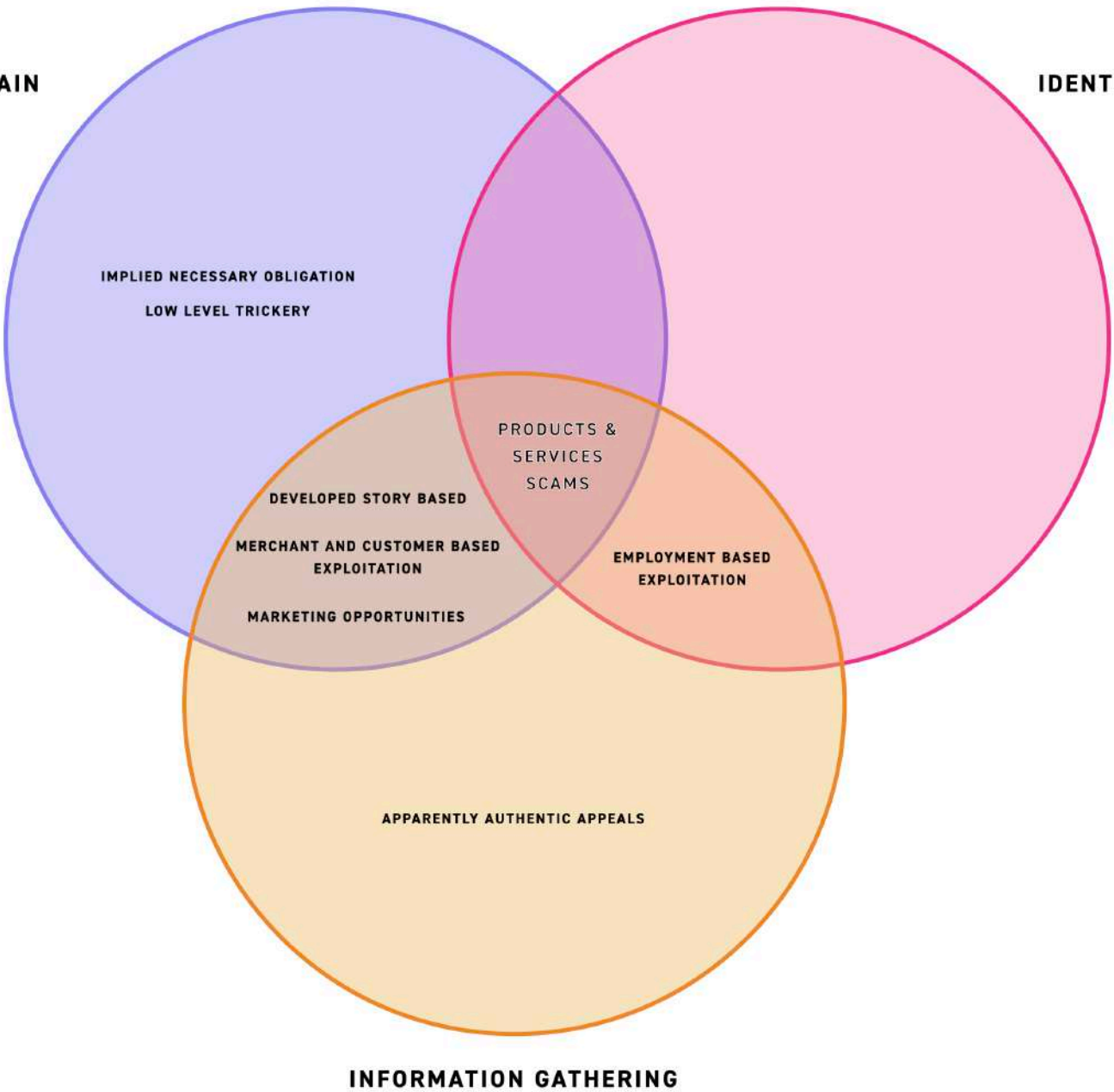


Figure 4. Visualisation of Stabek, Watters, & Layton (2020) created by research portfolio's author.

PRODUCTS AND SERVICES SCAMS – MECHANICS AND STRATEGIES

To better understand how products and services scams work, scams and frameworks must be further deconstructed to explore the mechanics, strategies and processes that they are built up of.

FRAMEWORK TWO

MULTILEVEL MODEL OF
CYBERCRIME

The 'Multilevel model of cybercrime' (Naidoo, 2020) captures the crucial areas, makeup and layers of what makes a digital scam. I find that this framework is highly relevant to the research as it gives an overarching view of what is encompassed in a digital scam. This will allow me to provide scope and boundaries when creating a unique framework for online products and services scams while capturing all fundamental parts of a scam.

THE DECONSTRUCTION OF THE MULTI-LEVEL COMPOSITION OF ONLINE SCAMS

Naidoo (2020) creates an overarching “exploratory sensitising model for cybercrimes” which encompasses all areas of general online scams as seen in Figure 5. The components of this scam are organised into 4 layers:

- **Situational factors:** unique external factors often relating to environments, events, personal situations, trends and patterns
- **Evolving targets:** people and platforms.
- **Evolving attack methods:** methods of how an attack is implemented within a scam.
- **Social engineering techniques:** emotional elements or influential techniques on a target.

While demonstrated by capturing the multilevel influence within the context of pandemic scams, the model fits well within the context of online products and services scams. Naidoo (2020) presents this framework by analysing archived documents of cybercrimes about COVID-19 between March and April 2020, giving relevant examples that would be found within online products and services scams. These examples include cybercrimes within online shopping, banking and airlines:

Naidoo’s (2020) model will be further adapted with the context of online products and services scams. This will be one of the existing frameworks used within the later parts of the research that will demonstrate the process and mechanics of products and services scam design.

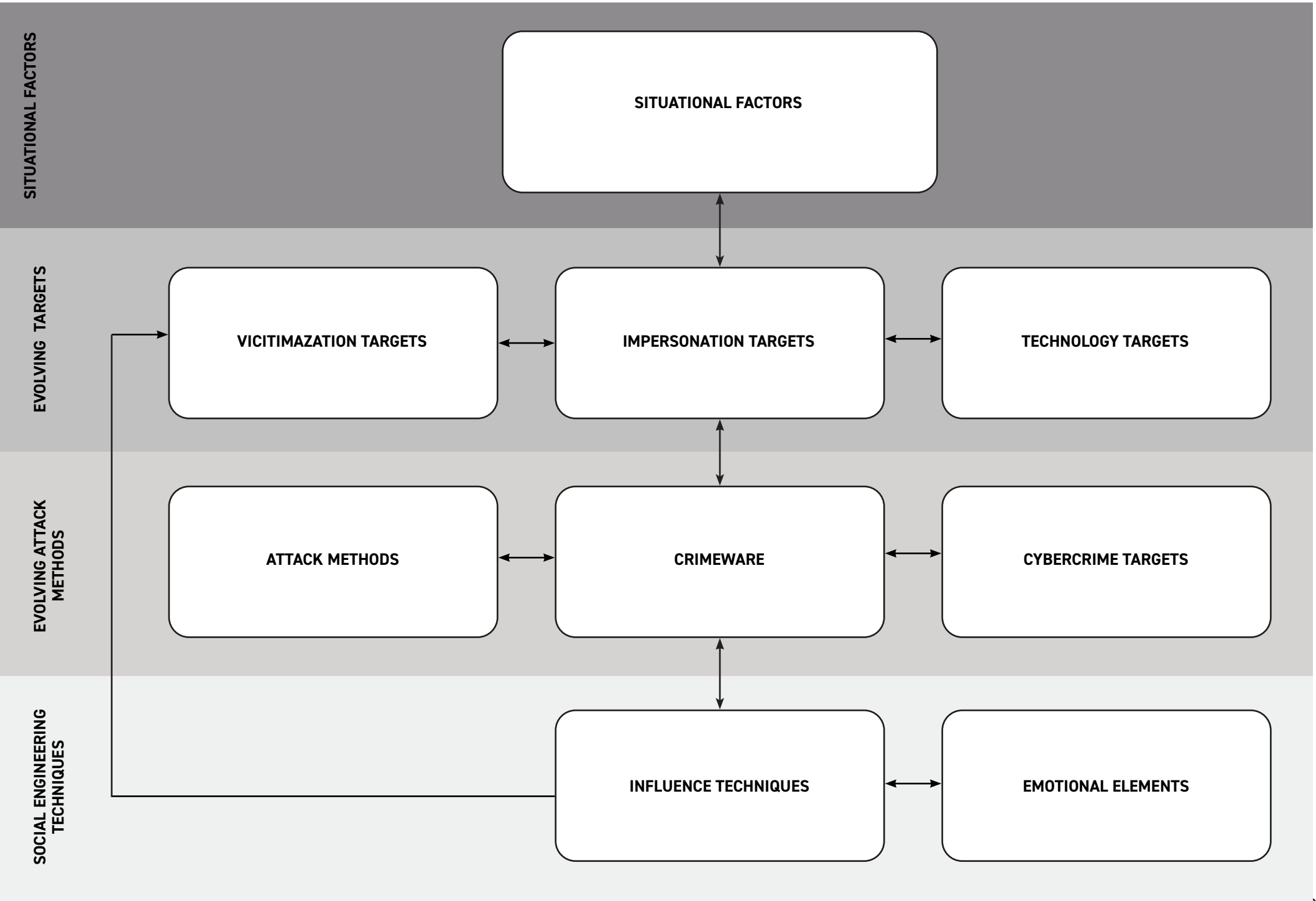


Figure 5. Naidoo's multilevel model of cybercrime (2020)

FRAMEWORK THREE

THE TOOLKIT OF PRODUCTS AND SERVICES SCAM STRATEGIES

The toolkit of products and services scam strategies (Australian Competition & Consumer Commission, 2016) highlights the most common and popular scams that “regularly targets consumers and small businesses” in Australia and New Zealand. This framework gives a brief description of how these scams work and what to look out for. I find that this framework is relevant to the research as this is actual information provided to local New Zealanders, from an official government organisation, about scams relevant to their local environment and how to face them.

In December of 2016, the Australian Competition & Consumer Commission (2016) released a guide that highlighted the most common and popular scams that “regularly target Australian consumers and small businesses”. New Zealand followed this lead, producing their own guide in 2018. These guides were highly relevant to the research as they were directly related to consumers, buyers, products and services scams. More specifically, the information directly targeted New Zealanders and Australians. The authors suggest that scammers keep a toolbox of scam strategies to combine and increase the chances of successfully catching many victims simultaneously.

The following is a list of key scam strategies and examples that heavily impacts New Zealand consumers and businesses as communicated through these guides:

SOCK PUPPETEERING AND IMPERSONATION

Like the term “sock puppet” suggests, scammers play the role of a fake persona much like an actor who creates characters with socks in a puppet show. As previously mentioned, Morris (2014) describes sock puppetry as the act of an identity used for purposes of deception online. In more specific terms of products and services, Zheng, Ming Lai, Chow, Hui & Yiu (2011) depicts the term of sockpuppetry as the act of pretending to be different people by using multiple different fake identities to “to praise or create the illusion of support for the product”.

BUSINESS FRONTS

In which a scammer or scam team carries the appearance of a legitimate business or organisation including professional business models, offices, call centres and procedures.

IDENTITY THEFT

The New Zealand Department of Internal Affairs (2019) defines identity theft as “Using another person’s personal information without their permission to impersonate or pretend to be them”. Similar to the nature of romance and online dating scams, Whitty (2013; 2015) discusses how scammers can steal personal information and photos from legitimate profiles to portray a real person Identity theft is not as in-depth in products and service scams as that in romance scams. A sockpuppet account that impersonates a real person only needs to look authentic on the surface. The scammer needs just enough information and visual interest on the profile to pass off as being legitimate, in comparison to an online romance scam where as much information is necessary.

NOT-SO-TALL TALES

In which the scammer crafts an elaborate tale or backstory to lure their target victims in on an emotional level (Freiermuth, 2011). The scam seller attempts to create a scenario that they can relate to, to convince the potential victim that they too can have their life improved simply by obtaining the product.

INFORMATION HARVESTING

In which the scammers invest time, money, research and effort into obtaining and collecting information about potential victims from social media, public listings, Google searches, victim lists harvested and stolen from hacked organisations and websites which store that data and black-market sales.

WHIZ-BANG GADGETS AND OFFERS

Offers and sale tactics such as discounts, deals, bonus deals including extra free items or deals to entice the victim into buying an appealing looking product. This can be commonly used alongside with ‘high pressure sales tactics’ and enhanced with ‘counterfeit and official-looking documents’ and is regularly used within products and services scams.

HIGH PRESSURE SALES TACTICS

Sales tactics that highly pressure their targets positively (getting excitement through sales and discounts), or negatively (time pressure, guilt tripping sales people) to pressure the victim into pursuing a particular outcome. This is commonly used alongside with ‘whiz-bang gadgets’ and offers and is regularly used in products and services scams.

COUNTERFEIT AND OFFICIAL-LOOKING DOCUMENTS

While described as a document with official authority looking stamps that gives a scam the ‘air or authenticity’, in the context of products and services scam, this can also relate to official-looking sales and marketing assets such as posters, pamphlets, email and advertisements.

MIRROR AND FAKE WEBSITES

Fake websites which are fabricated with intentions different from what the website sells itself as.

Mirror websites identically copies the visuals and content of a legitimate website, and pretends to be them. The scammer can also change elements of the site (such as the items or purchasing mechanics) for their benefit.

The technique is regularly used in products and services scams.

INTERNATIONAL MONEY WIRES OR TRANSFERS

In the context of products and services scams, a variation of this method includes presenting imitated trusted payment sites such as paypal within the payment system of their fraudulent site.

SCAM PACKAGING

While there is little to no research on this scam strategy, social media marketing practices for products and services e-commerce reiterate the process of attracting customers and the bridged relationship between social media pages and their primary e-commerce website (Andzulis, Panagopoulos & Rapp, 2012). For this research, this strategy will be defined as Scam Packaging - the combination of multiple platforms to increase the scam business' online presence to produce the image of perceived credibility and trustworthiness. This can include a combination of a website, social media pages and legitimate looking contact information. This study will have a large focus on scam packaging within the research.

PHISHING

The act of sending emails, text messages and private messages to collect personal information from victims under the guise of being a trusted organisation, company or individual. This scam method is commonly used within products and services scams where victims voluntarily give their information to online forums that seem to be from trusted organisations.

FRAMEWORK FOUR

DARK PATTERNS
WITHIN PRODUCTS AND SERVICE SCAMS

Dark patterns are user experience, user interface (UI) and social engineering tricks created to deceive the user into performing actions they didn't intend to perform (Brignull, 2010). I find that Brignull's dark patterns are an essential aspect of the research as the combination of UI and social engineering tricks are the foundation of digital scams. I believe that through combinations of different dark patterns, it provides scammers with the ability to create variations of complex digital scams. As dark patterns within digital products and services scams have only been lightly touched, I have decided to explore this area further within my research.

There has been minimal academic research conducted on the integration of dark patterns through existing online platforms where dark pattern practitioners do not own or have control over - such as social media, blogs or website building websites. These specific uses of dark patterns are established through content and visual design alone rather than functionality and user interface techniques. The limited research was partaken by Trice & Potts (2018), who investigated the integration of dark patterns into the existing platform, Twitter, through the Gamergate controversy. The authors state that three specific dark patterns were highly relevant within existing media platforms such as Twitter, Github and Reddit. These patterns were:

- **Bait and Switch:** The promise of one experience, but provides another.
- **Captive Audience:** The user enters a system expecting one type of platform activity (Twitter community) and becomes subjugated to another (GamerGate).
- **Misdirection:** The participant is encouraged to focus on one action to hide the existence of another less preferable activity.

There has also been an absence of academic research of dark patterns that have been conducted between multiple platforms that connect with each other as research primarily focuses on dark patterns within a single location or platform. Thus it is crucial to identify the relevance and applicability of dark patterns within both social media platforms and products and services e-commerce websites. For this research, it is important to explore this bridge and relationship in the context of products and services scams.

DARK PATTERN	DESCRIPTION	SOCIAL MEDIA	PRODUCTS & SERVICES WEBSITE	RELATIONSHIP BETWEEN PLATFORMS
Trick Questions	While filling in a form you respond to a question that tricks you into giving an answer you didn't intend. When glanced upon quickly the question appears to ask one thing, but when read carefully, it asks another thing entirely.	Not applicable. Cannot be implemented onto a platform where dark pattern practitioners have no control over the functionality.	Applicable within account sign up and purchasing forms. Using wording within account sign up and purchasing detail forms that asks for certain information, but phrased in a way that would trigger them to provide that information - even if they do not intend to. This could also include checkboxes that would permit the scam retailer to regularly keep contacting the user, send them emails, offers and updates until the user would try to unsubscribe.	No
Sneak in to the Basket	You attempt to purchase something, but somewhere in the purchasing journey, the site sneaks an additional item into your basket, often using an opt-out radio button or checkbox on a prior page.	Not applicable. Cannot be implemented onto a website where dark pattern practitioners have no control over the platform's e-commerce capabilities.	Applicable within products and services online retailers. Sneaking in additional scam products within the user's shopping cart as they are purchasing a scam product	No
Roach Motel	You get into a situation very easily, but then you find it is hard to get out of it.	Not applicable. Cannot be implemented onto a platform of which dark pattern practitioners have no control over the functionality.	Applicable within subscription based products and services. Promote and offer a scam subscription of a product or service. When the victim realises the product or service isn't what was advertised, make it difficult for them to end the subscription, close their account or get in contact with the scamming business. The longer it takes for them to end their subscription, the scammer should continue to charge until they are cut off (e.g by the bank).	No

DARK PATTERN	DESCRIPTION	SOCIAL MEDIA	PRODUCTS & SERVICES WEBSITE	RELATIONSHIP BETWEEN PLATFORMS
Privacy Zuckering	You are tricked into publicly sharing more information about yourself than you really intended to.	<p>Applicable through social media permissions.</p> <p>Through the guise of the user needing an account or for the platform to have the ability for the user to access more content, websites have the functionality to ask the user permission to access their social media accounts.</p>	<p>Applicable within products and services e-commerce storefront, pop up ads and offers.</p> <p>In which the product or service provides a deal or offer, such as a “free 2 month deal” or “50% off”, but the user must provide certain information upfront (e.g name and email to receive a deal).</p> <p>The user must offer information to receive a deal, offer or product that they want to obtain.</p>	<p>Yes</p> <p>Works as a bridge, but also includes website only opportunities.</p>
Price Comparison Prevention	The retailer makes it hard for you to compare the price of an item with another item, so you cannot make an informed decision.	Could be applicable by making it difficult to compare prices between ads and the ecommerce store, but also be unlikely to be used as it could clash with more effective marketing dark patterns.	<p>Applicable within the products and services ecommerce storefront.</p> <p>The scam seller has the option to put variations of the same scam product e.g a scam product and a bundle of the same scam product, but using different pricing between items to make it unclear which is the better deal.</p>	<p>Yes</p> <p>Works as a bridge, but also includes website only opportunities.</p>
Misdirection	The design purposefully focuses your attention on one thing in order to distract you from another.	<p>Applicable within products and services marketing ads and business social media pages.</p> <p>Using visually appealing graphic design, realistic product imagery and strategic marketing content to pull attention away from any indicators that show that the product or service is a scam.</p>	<p>Applicable within the product and service imagery and website visual design/UI.</p> <p>Using well-designed marketing graphics within the website, well crafted and realistic looking product or services imagery to distract the user that the products or services offered are not legitimate.</p>	<p>Yes</p> <p>Works as a bridge, but also includes website only opportunities</p>

DARK PATTERN	DESCRIPTION	SOCIAL MEDIA	PRODUCTS & SERVICES WEBSITE	RELATIONSHIP BETWEEN PLATFORMS
Hidden Costs	You get to the last step of the checkout process, only to discover some unexpected charges have appeared, e.g. delivery charges, tax, etc.	<p>Applicable within products and services marketing ads.</p> <p>The product or service advertises a price within the social media ad, but has extra costs hidden when the customer proceeds to buy the product or service within the connecting retail website.</p>	<p>Applicable within products and services e-commerce storefront.</p> <p>The price advertised for the item is listed within the scam product search listings and on the scam product’s page, but extra costs such as tax, shipping and handling, customisation etc. are not viewable until you are about to purchase the item within the store’s shopping cart.</p> <p>Scams could also include hidden costs within the site or page terms and conditions / small print that is barely noticeable unless the user notices the deduction within their bank account.</p>	<p>Yes</p> <p>Works as a bridge, but also includes website only opportunities.</p>
Bait and Switch	You set out to do one thing, but a different, undesirable thing happens instead.	<p>Applicable within products and services marketing ads and organisation social media page.</p> <p>What the business page and advertisements promote, is different to the content that is accessible within the product or service's website.</p> <p>Within social media platforms, this is often known as clickbaiting - the use of over exaggerated language and taking advantage of trends regardless of what the actual content, product or service is.</p>	<p>Applicable within pop up deals and offers.</p> <p>The user enters the product or service site intending to purchase or browse, often through the motivation of clicking on a social media advertisement, but is distracted by a popup offer or deal.</p>	<p>Yes</p> <p>Works as a bridge, but also includes website only opportunities.</p>

DARK PATTERN	DESCRIPTION	SOCIAL MEDIA	PRODUCTS & SERVICES WEBSITE	RELATIONSHIP BETWEEN PLATFORMS
Confirmshaming	The act of guiltling the user into opting into something. The option to decline is worded in such a way as to shame the user into compliance.	Somewhat applicable within products and services marketing ads. Rhetorical questions that nudge users to question, think and jog curiosity before engaging with the product or service.	Applicable within the product or service e-commerce website's cart and pop up deals. Confirmshaming can appear in multiple areas of a products and services scam website. The user is about to opt into a scam and submit their personal information before backing out. The scammers use guilt-inducing wording and imagery to make the user doubt their decision to potentially cancel their action. Situations can include: almost cancelling a purchase of a scam item or about to close out of a popup deal.	No Works as a bridge, but also includes website only opportunities.
Disguised Ads	Adverts that are disguised as other kinds of content or navigation, in order to get you to click on them.	Somewhat applicable. Promoted content within social media platforms that is similarly identical visually to authentic posts (with minor indicators that visualise what posts are promoted). Scammers take advantage of provided functionality offered by Facebook, Twitter or instagram.	Applicable within popup deals. Ads in the form of popup deals and offers which disguise as familiar UI elements such as exit buttons or download buttons. Instead of proceeding with the intended action, the user unintentional pursues the ad further.	Yes Works as a bridge, but also includes website only opportunities.
Forced Continuity	When your free trial with a service comes to an end and your credit card silently starts getting charged without any warning. In some cases this is made even worse by making it difficult to cancel the membership.	Not applicable. Cannot be implemented onto a platform that dark pattern practitioners have no control over the functionality.	Applicable within subscription based products and services. In which a free trial of a product or service is taken, but the user is continuously charged after the trial is over. Scammers can take advantage of writing hidden terms and conditions as reasons for the extra charges.	No

DARK PATTERN	DESCRIPTION	SOCIAL MEDIA	PRODUCTS & SERVICES WEBSITE	RELATIONSHIP BETWEEN PLATFORMS
Friend Spam	The product asks for your email or social media permissions under the pretence it will be used for a desirable outcome (e.g. finding friends), but then spams all your contacts in a message that claims to be from you.	Applicable through social media permissions. Requiring the platform to have permission to access the user's account, including their contacts and friends list. While the platform mentions they will need access to their accounts, but not use them maliciously - scammers could lie about this.	Applicable within website registration and mailing list forms which asks for the user's email. The scam site asks for the user's email, either registering on the website, filling in a form to receive offers or be added to the email mailing list but uses this to find and spam their contact list.	Yes Works separately and not as a bridge.

USERS AND THEIR INTERACTIONS WITH PRODUCTS AND SERVICES SCAMS

Scams are successful, not solely on the technological side of platforms, but also through human actions and influence (Muscanell, Guadagno & Murphy, 2014). Hadnagy (2010) emphasises that emotions and beliefs are key ingredients within persuasion and influence, describing the “art of persuasion” as the process of controlling how a person acts, thinks and believes “in the way you want them to”.

SOCIAL ENGINEERING: PLAYING WITH EMOTION AND VULNERABILITY FACTORS

Krombholz, Hobel, Huber and Weippl (2015) define social engineering as “the act of getting users to divulge information or perform actions through influence, emotional manipulation and persuasion techniques”. Hadnagy (2010), states that while social engineering is often painted negatively (emphasizing on antagonising words such as ‘manipulative’), it is a tool with “many uses” used “everyday by everyday people” for both good and bad intentions. Both Krombholz, Hobel, Huber and Weippl (2015) and Hadnagy (2010) mention the grey area of social engineering: both legitimate businesses and scammers use the same social engineering techniques to persuade their victims into interacting with them, however, the intent could be good or bad for their customers.

Williams, Beardmore and Joinson (2017) specify key emotions and triggers that are most common within online scams, encouraging people to make errors in their decision making and judgement. This includes positive emotions (excitement, hope, curiosity,

empathy) and negative emotions (fear, sadness, anger, anxiety, depression). These emotions are only discussed at surface level and were not explored in depth. The authors mention there is limited understanding of what, why and how techniques using the specified emotion are effective.

However, Nodder (2013) explores this topic area explicitly, further explaining how and why they work, what emotion-based techniques are used and demonstrate examples in which both businesses with good intentions and con artists alike use these techniques. The author uses the Seven Deadly Sins (pride, sloth, gluttony, anger, envy, lust and greed) to categorise and better illustrate these techniques. In the context of products and services, marketing and digital commerce, the author emphasises why designers must be aware and be educated in designing for supposed ‘evil human traits’. These techniques are later demonstrated within the later practical areas of the research within the context of online scams.

FRAMEWORK FIVE

THE SEVEN DEADLY SINS OF SOCIAL ENGINEERING

The 'Seven deadly sins of social engineering' (Nodder, 2013) investigates how human emotions (specifically pride, greed, lust, envy, gluttony, wrath, and sloth) play a role in digital scams. I find this framework relevant to the research as human emotion is one of the large factors which decides if an internet user successfully falls victim or escapes the traps of a digital scam. When creating an overarching framework for digital scams, human emotions must always be acknowledged.

PRIDE

Pride is often defined as a feeling of deep pleasure or satisfaction obtained from one's actions or achievements (Merriam Webster, n.d.). In the context of products and services, the action of pridefully choosing and following through with a decision to purchase. Nodder (2013) describes the negative connotations of pride as "hubris", emphasising one's excessive arrogance, cockiness and overconfidence. The author suggests pride as a way to pressure a person into dedicating themselves to a decision. He further adds that "misplaced pride creates "cognitive dissonance", meaning inconsistent thoughts, beliefs, or attitudes for prideful people.

Pride based techniques in online products and services scams include:

- Giving consumers good reasons that encourages them to obtain the scam product while keeping their "pride intact" - even if the reasons are exaggerated or not legitimate.
- Creating social proof through fake validation by fabricated reviews and social interaction (comments, likes on social media pages) to give the impression that others have had a positive experience with the product.
- Making the product and business-to-consumer (B2C) interactions personal by referring to them by their name or allowing product customisation for consumers.
- Persuading consumers to publicly commit (share that they are purchasing or have purchased a product on social media) as they are more likely to go through with the purchase and become too prideful to admit if they change their mind.
- Including images of certification and endorsement to persuade the customer that the product is legitimate, trustworthy and backed by trustworthy organisations - even if they are fake or stolen.
- Encouraging consumers to complete a collection. Offering pieces of a more extensive collection complimentary with a purchase or for free to persuade them into purchasing the remaining parts.

SLOTH

Sloth takes advantage of a person's lazy motivations - avoiding putting extra effort into taking action and the feeling of “not caring” in an online environment (Nodder, 2013). The author describes how people are naturally trained to go through the path of minimum effort to get to their desired destination, often giving up when a website makes them work too hard.

Sloth based techniques in online products and services scams include:

- Providing consumers with a path of least resistance to the scam product purchase through an easy to use e-commerce website user experience with clear labelling, imagery, navigation and taxonomies.
- Providing a limited number of store scam items to choose from so that the consumers spend less time comparing items and deciding what to purchase.
- Pre-picking the preferred scam product by highlighting and emphasising features or reasons as to why it is the best option to buy.
- Making it difficult or impossible for the consumer to opt-out by hiding the feature deeper within the website or removing the feature completely.
- Turning familiar website features, layouts, visuals design and browsing habits (such as skim reading) against the user by reversing or changing feature functionality resulting in consumers committing to actions they may not intend to take.

GLUTTONY

The author illustrates gluttony as motivating a person to “over consume and indulge to the point of extravagance or waste”. In digital commerce terms, Nodder (2013) highlights gluttony through a business' push to make people feel like they deserve a reward or a form of compensation by committing to more than what the person had initially intended.

Gluttony based techniques in online products and services scams

include:

- Offering a reward with a purchase to persuade the consumer that the purchase is worth it. Rewards can be products (e.g a collectable toy within a box of cereal), but can also be psychological (fulfilling a consumer's nutritional goals by buying food seemingly labelled as healthier) - in scams, these rewards could also be cheap variations or non-existent.
- Hiding any maths to reduce time when decision making and simplify making justifications by: making the maths look too complicated, using unique website currency and not displaying extra costs. In scams, the advertised maths and prices may differ significantly from what the scammers charge the consumer.
- Using the foot-in-the-door technique which asks a consumer for a small favour initially before later convincing them of a larger task. Within the context of scams, this could be used to obtain information (e.g ask for their email first, then later a survey to steal information).
- Providing the content that consumers are looking for, but only after they have given “valuable information”. This can mean only allowing consumers who have a registered account on the provided scam website to supposedly gain access to information or products they need.

- Adding a time constraint on purchasing a scam product forces consumers to act and make decisions fast without doing research. Rushing a consumer means they are more likely to make “errors in judgement and decision making” (Nodder, 2013) due to pressure.
- *The Tom Sawyer effect* takes advantage of scarcity to push a person to take action and “to appeal to people's natural gluttonous tendencies”. This can include:
 - Infrequency* – products and services that only appear for a limited time.
 - Exclusivity* – products and services that are exclusive to a specific seller.
 - Competition* – products and services that have a limited quantity.
- Instilling doubt, consumers will think twice about cancelling their order and may change their mind by reminding them of the benefits or limited sales they will be losing out on.

ANGER

Nodder (2013) explains that anger must be used with caution. By considering anger as a technique does not necessarily mean to use it as a tool, but also to keep in mind that avoiding anger may be the better course of action. While anger can be “a highly motivating force” it is not entirely suited for products and services scams as consumers will unlikely buy a product or service out of anger.

The only anger based technique that is relevant to online products and services scams is:

- Using fear-mongering to scare consumers to intentionally incite fear or panic and offering a scam product as a solution for it. Using fear as a sales tactic is most commonly demonstrated through product categories including fear of ill-health (health based products) and home and digital security (home alert systems and anti-virus software). This strategy can often be seen through event based issues such as natural disasters, pandemic, local issues etc.

ENVY

Envy can be both a powerfully motivating and destructive force when maliciously taken advantage of (Nodder, 2013). Envy can be seen as desiring or aspiring to “have or to be”. This is commonly in the form of a person, possession, status and achievement - in most cases, people envy what they don’t have.

Envy based techniques in online products and services scams include:

- Creating desirable products that produce envy to those who do not own them. They will be persuaded to obtain the products out of envy. Nodder (2013) describes some ways to create desirability:

- **Secrecy:** Being in a select group of people that knows about the item
- **Scarcity:** A limited number of a the item, available to a small number of people
- **Identity:** The item is associated with a desirable lifestyle, person, or activity.
- **Aesthetics:** It is delightful to look at, hold, and use the item
- **Functionality:** The item either solves a problem nobody else is solving, improves an aspect of a person's life or is an improvement to an item the person already owns.

- Using aspiration to heighten appeal by advertising the scam product with idols or individuals who scam targets look up to and aspire to be like implying they endorse the product.
- Allowing consumers to be involved in a scam product or service before it's released which may allow them to form an emotional attachment to the item before it's even owned. This could involve pre-release updates and encouraging consumers to pledge money in exchange for bonus items.

- Highlighting status and hierarchy between people by acknowledging a group as being more favourable than other groups, providing them with exclusive services and opportunities. Consumers who are not in the favoured group may become envious by missing out.

LUST

While the emotion of lust is often linked to romance and sexuality, and in the area of scams, romance and dating scams, Nodder (2013) explores lust in the form of desire. Like any other emotions, the author explains that both liking and desire can be manipulated, creating feelings of obligation and want and cravings that a person must work to satisfy.

Lust based techniques in online products and services scams include:

- Use flattery to persuade people to view the product and service scam business in a positive and legitimate light. Those who receive flattery often subconsciously act positively towards the initiator because of the “warm, fuzzy feelings”.
- Frame the message as a rhetorical question. By using a rhetorical question, influences viewers into asking and answering the same question in their mind and raises questions about competitors without naming them directly.
- Offer a product for free. Ariely (2008) describes that when an item is displayed as free, the rationality of deciding the positives and negatives disappears because the person cannot lose anything by taking what costs nothing.

GREED

Greed is depicted as the selfish and spiteful feeling of obtaining and keeping more possessions at the expense of another person (Nodder, 2013). By greedily obtaining more than enough to fulfil one’s needs prevents others from being able to equally access.

Greed based techniques in online products and services scams include:

- Rephrasing a lottery into a competition amplifies a consumer’s fear that they will miss out if they don’t give it a try. While buying gives the consumer full control, a lottery indicates casual chance, using the phrase “win” implies a high achievement of success.
- Creating a ‘walled garden’ in which a customer cannot obtain a product unless they create an account. When the user has an account, the scammer can easily take advantage of any information or data the person has given.
- Anchoring the retail environment to control how consumers see the products can influence how they search and make decisions. This can include the order of how the products are displayed, their visual appearance and search tagging.
- Purposefully make products more expensive by price and/or visual image. This can manipulate the perception of the product’s worth. If a product looks more expensive, it may imply that the product has more value than it actually has. Scammers can use this to their advantage to increase profit for scam products they sell.

STAGES OF A PRODUCT OR SERVICE SCAM

Existing frameworks which capture processes similar to those potentially for products and services scams

There is currently minimal research on online scams' underlying frameworks and no findable existing models or overarching processes explicitly created for online products and services scams. Most common current research focuses on creating strategic models for online dating romance scams (Kopp, Sillitoe, Gondal and Layton, 2016; Whitty, 2015; 2013). While there are several similarities and strategic techniques used between dating romance scams and other digital scams, the frameworks created for romance scams is tailored to fit the specific scam type alone. For instance, dating romance scams are designed to target specific individuals who focus on interacting with the victim on a personal and emotional level. In comparison, products and services scams aim for a broader scope, targeting many people at once for a better chance to deceive multiple people at once.

To determine the anatomy of online products and services scams and to create an overarching process and framework for it, it is beneficial to analyse frameworks and methods of correlated and similar activities.

1 The first framework looks at the overarching process within what is included within a basic scam strategy. While Smith's (1922) 'Confidence (Con) Trick' strategy is a historical scam process conducted for analogue scams and could be considered outdated, it is meaningful to understand the underlying process stages of a scam at its most basic form. The second reason to use this framework is the difficulties locating an overarching process for generic scams that demonstrate the key stages that are most prominent and consistent in all scams while still being flexible to fit various scam types. Existing frameworks are most commonly connected to a specific scam type, and either miss key stages and/or adapt stages to accommodate the scam type. The steps mentioned inside the framework are similar to other frameworks that were examined for this research - even if they were created more than a century later.

Smith (1922) introduces the concept of the 'Confidence (Con) Trick', a strategy that has become a core method in successful scams. The confidence trick is described as a deception strategy in which the initiator works to gain the victim's trust before deceiving and taking advantage of them.

The author breaks down the anatomy of scams by describing the six key stages of a con or scam, stating that some steps may be left out or added depending on the con's situation. While this framework is only described at a high level by Smith (1922), this research will explain each step in the context of online products and services scams. To assist with visualising this historical framework, I have visually recreated this process in Figure 6.

2 The second model used is mentioned earlier in this chapter - the “exploratory sensitising model for cybercrimes” by Naidoo (2020) (p40), which encompasses all areas of general online scams. While this model is crucial to visualise and describe the underlying aspects that make up the scam strategy, it does not demonstrate the process and stages within a scam. However, I believe this model works hand-in-hand alongside a scam process framework, and both would be essential when planning a scam strategy.

These frameworks will help understand the anatomy of online products and services scams, assisting in creating a baseline foundation for them. While Smith (1922) discusses these stages at a very high level,

it is essential to deconstruct these stages in further detail and ask questions to gain a more robust understanding of what makes up these stages, setting them into the context of an online environment.

Whether selling products and services legitimately or as a scam, the overarching processes between the two would not be too different - despite different aims and end goals. To create a successful products and services scam, the scam should appear and act as similar to a legitimate products and services sale. Thus, this upcoming analysis of the online products and services scam process is compared to the more modern and moral marketing strategy and social media marketing strategy frameworks.

This is visualised in Figure. 7 (page 81) and Figure 8 (page 84)

FRAMEWORK SIX

THE STAGES OF A PRODUCT AND SERVICES SCAM

While Smith's (1922) 'Confidence (Con) trick' strategy can be considered a historical scam process, I find that it provides a starting point in understanding the basic start-to-end process and stages of a scam. As this is an older resource, I will not only be analysing the contents of the framework but also adapting to fit the more modern scams of today while comparing it to the remaining two frameworks.



Figure 6. Visualisation of Edward H. Smith's original Confidence Trick strategy (Smith, 1922)

STEP 1: FOUNDATION WORK

Foundation work is the preparation steps that are undertaken before the scam is initiated. Within a products and services scam, this includes (but not limited to):

Background research

- *About the subject topic that will be the main focus of the scam*
Is it a scam that involves an already existing product or service?
Is it a unique product? Does it exist already? Is it fake? What is the product, what does it offer? Why should customers use it?
- *The intended target victims*
Who will the scammers approach or who are customers that will be attracted to the scam? Are they a specific age, gender, stereotype?
Is the content of the scam relevant to the intended users?
- *Location / country / regional and cultural research to where the scam will be targeted?*
Do they speak English or another language? Both? What is classified as relatable or originating from the location? What is classified as being local versus international?
- *Local ‘competitors’, identities of individuals, organisations, brands etc. that target users would know and are familiar with*
Are we impersonating an organisation or brand that doesn't exist in the country?

Doing background research can determine how genuine and realistic the scammers look to outsiders. A single mistake or incorrect fact may cause the facade to fall apart.

Plan of approach

- Just like a good intentioned project, even a scam needs some form of plan. A plan of approach gives the scam a clear vision, goals, a direction, resources priorities and reduces chances of failing.
- Which scam strategies will be involved in making this scam a success?
 - Which scams shouldn't be used?
 - Which scams will produce the best results?
 - What are the risks involved?
 - Is there a timeline of how this scam will run?
 - What will happen if we get caught?

Scammers who do not plan their approach to implementing scams run the risk of a failed outcome and increase the possibility of being caught. As previously mentioned, 'Low level trickery' is the only type of scam that is not planned in depth and would not consider these steps Watters and Layton (2010).

Obtaining required related information and data

This includes gathering personal information directly about the target users that identifies who they are, such as people's names, contact details, financial health, bank account details, etc (Deevy, Lucich, & Beals, 2012). With social media and online profiles, it has become significantly easier to find information, including email addresses, phone numbers, location, interests, based on their social media profiles alone (Kunwar & Sharma, 2016).

While no academic research details this, I want to assume that for businesses and organisations, this could involve a mix of both personal information (about their employees, consumers, and third parties they work with) and confidential business-like trade secrets, security, sales and marketing plans, blueprints and financial data.

The hiring of assistants and accomplices

While it's possible for an individual to achieve a successful scam, scams often may have a team of connivers to pull it off with ease, efficiency and authenticity (Yan, 2019). Like an organisation with good intentions, having a balanced team with specialists in particular areas such as marketing, development, and design gives them the advantage to highly succeeding in delivering within that area (Yan, 2019). Bringing on board specialised staff who can produce high-quality services can increase the level of believability and deceive more victims.

Design and creation of online identity

Constructing an authentic online presence is key to a successful online products and services scam. Users of the internet are getting smarter when identifying false identities, so it is essential for scammers to avoid creating the obvious red flags that victims are used to (Australian Competition and Consumer Commission, 2018).

The creation of an online identity will often entitle creating:

- ***A website with a custom web address***
A web address ending with a known domain such as .com, .co.nz and .nz etc. gives an indicator that the site is most likely a trusted and a safe domain to be going into (Choi & Stvilia, 2015).

Kalia, Kaur and Singh (2014) emphasises on the importance of a business' website within the context of online shopping and how it plays a pivotal role in attracting and retaining customers, influencing intentions to purchase from them and the perceived quality of their merchandise.

- ***Contact information***
Choi and Stvilia (2015) presents that listing contact information such as email, contact phone and address has a large impact on perceived credibility and trustworthiness of the site as customers feel that because of this information, there are actual people behind the site and organisation.

- ***Social Media pages***

This includes social media pages such as Facebook, Instagram, Twitter etc., that are relevant to the scammer's business. The scam business should only create a presence on the most necessary and appropriate platforms. This is so that they can consistently maintain their pages to the highest quality and are able to pull pages down if there is an instance they are called out for being a scam (Choi and Stvilia, 2015).

- ***A brand identity - new created identity or a stolen one?***

There is a lack of existing research for products and services scams that creates entirely new brands to manipulate customers to buy fake products and services. The majority of scam based brand identities comes in the form of brandjacking. Mancusi-Ungaro (2014), Ramsey (2010), Milam (2008), Wunder (2009) and Hofman and Keates (2013) all explore the significance of 'brandjacking' within social media. Pang and Sterling (2013) and Lin (2011) discuss the in-depth details of physical counterfeit goods within China. This includes the rise and popularity of purchasing imitated physical products such as handbags, shoes and clothing to pursue the perceived image and esteem that comes with carrying brand name items such as Louis Vuitton, Chanel and Nike. Chang (2006) further investigates the complex nature of fake logograms and their impact, particularly within the fashion and entertainment industries.

Wunder (2009) describes brandjacking as the “unauthorised use of a business or organisation’s trademarked brand name and image” - in other words, to hijack an existing brand for a malicious purpose to

falsely present as an existing brand. While Wunder (2009) states that brandjacking has been an ongoing problem since as early as 2002, this method of misusing a company's brand continues to evolve.

Mancusi-Ungaro (2014), Milam (2008) Hofman and Keates (2013) all agree that users who have any negative interaction with a brand impersonator could lose a customer's trust completely. Brand impersonators who take advantage of an organisation's customers trust and naivety (Milam, 2008) by misleading them under the brand's guise will ultimately leave their customers feeling betrayed, disappointed and no longer feel safe to interact with the legitimate brand (Hofman and Keates, 2013).

- ***Creation of content and assets***

While not mentioned within Smith's (1922) framework, one of the final steps within the foundation stages of a scam that should be included should be the creation of content and assets on the site. This step is mentioned within Andzulis, Panagopoulos & Rapp's (2012) social media marketing framework and would be well integrated within the foundation stage of a scam. This step includes:
Website design and social media brand assets (graphic banners, logos and photography)
Assets for marketing such as digital advertisement banners for email, social media posts and physical mailbox spam
Design of a the counterfeit product - digital and/or physical

ORIGINAL STEP 2 REMOVED: APPROACH

The step captures the con artist’s strategy in approaching or contacting the victim (Smith, 1922). However, this particular step indicates that the con artist needs to initiate a one-on-one interaction with them and does not fit the context of products and services scams. This also does not fit the digital medium of online scams as online, it is more common to prey on a pool of people within a set target audience to increase the chances of successfully hooking multiple victims at once. They do not go out of their way to approach a chosen victim but use techniques to entice and lure victims into approaching them.

As this step isn’t truly entwined with products and services scams at the current state, a suggested more suited step that should replace this step is to “lure” the victim.

REPLACING STEP 2: LURE

To lure victims would entail capturing the target audience's attention through social engineering means by amplifying positive emotions such as curiosity, excitement or lust towards the product or service. Studies have shown that impulse buying within an online environment is hugely significant for advertisers and online retailers (Dodoo & Woo, 2019) in which 60% of customer purchases were implied to be the result of impulse buying (Amos et al., 2014).

As Dodoo & Woo's (2019) studies investigates “the impact of social media advertising on online impulse buying tendency”, they highlight

that the act of impulse buying and impulsive action can be stimulated from a variety of factors. This includes attractive product stimuli, ease of access, virtual cues (LaRose, 2001), product images, visual marketing and limited offers (such as limited time, low prices and special prices) (de Kervenoael et al., 2009).

ORIGINAL STEP 3 REMOVED: BUILD-UP

The build-up stage gives the victim the chance to profit by participating in the scam, encouraging impulsive need and greed with a clouding of their rational judgement (Smith, 1922). While this method may not be relevant to online products and services scams, it implies the use of greed, gluttony, and lust-based social engineering mechanics used to build trust and attachment to the product that may be used in the scam.

ORIGINAL STEP 4 REMOVED: PAY-OFF

This stage entitles a victim to receive compensation or a gift that demonstrates the scheme's legitimacy (Smith, 1922). What the victim receives also may or may not be legitimate. While this method may not be relevant to online products and services scams, it also implies using greed, gluttony and lust-based social engineering mechanics that can be used within the scam.

The similarities mentioned within Smith's (1922) 'build-up' and 'pay-off' steps indicate that these stages have evolved to become a small part of a larger social engineering stage.

REPLACING STEP 3: ENTICE & RETAIN

This works in conjunction with the “lure” stage and can be used both within social media and websites. While the “lure” stage focuses on creating “impulsive appeal” and “impulsive action” to get the user to act quickly without thinking, this step focuses on further retaining the victim to pursue the end of the goal and to assure that they do not change their mind before they take the final step.

While the “lure” stage only showcases a small preview of the product to get them initially interested, the “entice & retention” step works on further convincing the victim to buy. While this uses the same toolbox of techniques, the scammer must understand that the user will decide at their own pace. This means the scammer must consider the right combination of social engineering and dark pattern techniques to sell the product's appeal and provide the easiest process for the user to buy the product.

STEP 4: THE “HURRAH”

The stage in which a change of events occurs causes the victim to promptly decide whether or not to choose between pursuing the scheme or not. Working alongside the “build up” stage of sale based mechanics, giving victims a special deal for a limited time or indicators that there are a limited number of the advertised item, the target victim may feel time-pressured and compel them into impulsively giving in (Nodder, 2013).

RENAMED STEP 5: VALIDATION

~~PREVIOUSLY: THE IN-AND-IN AND CORROBORATING~~

Within the in-and-in phase, an accomplice (an individual involved in the con, but makes the appearance of being a bystander or fellow customer) participates in the scheme “to add an appearance of legitimacy”. The appearance of another individual who indicates that they also are or have participated in the scheme can reassure the victim of the ploy's legitimacy (Smith, 1922).

Smith (1922) discloses that some schemes may require corroboration. Corroborating evidence is evidence that supports or confirms a statement or idea to ensure bias and provide assurance (Vocabulary.com, n.d.). This can include witnesses or third parties testifying something they have seen or experienced. Corroboration used by con artists for scams may not necessarily be legitimate and can be falsely created to give the impression that the scam is legitimate.

In the context of products and services scams, this could be in the form of fake validation or reviews (comments, ratings) on their social media pages, external rating sites and video reviews communicating their positive experience about the product or service.

Scammers have taken notice of this customer reliance of validation, implementing it into their strategy. While victims look at the product or service details and are aware that it could be fake, they may not realise that reviews that praise the product could also be fake. Kokate

and Tidke (2015) mention that it can be hard to identify between real and fake reviews, describing that due to the openness that review sites have and that scammers can portray themselves as multiple different identities, it isn't easy to get rid of fake reviews completely.

As this stage has been redefined to better fit the area of products and services scams (having a similar aim, but a more expansive approach) this step is more suited to be renamed as “validation”. This step is better situated before the “hurrah” stage instead of after.

STEP 6 (PREV. STEP 7): THE DISAPPEARING ACT-

Smith (1922) does not discuss many details about the ending stages of a con. However, Smyth (1994) explains this in connection with telemarketing scams. He illustrates how these scams are difficult to identify as they are quite broad and sophisticated and, therefore, difficult to catch.

He analyses how telecommunications fraud is comparable to online scams. In both scenarios, target victims never interact with their scammers face-to-face, so they don't know what the offender truly looks and acts like. They do not know where the offender really is, therefore it is easy for the culprit to hide their tracks and make an escape. The author clarifies that even the most complex and elaborate schemes can be stripped apart and hidden away faster than the preparation it takes to create the scheme.

In romance dating scams, con artists take a similar approach that when they decide to put an end to a scam of a particular victim by ghosting them - the act of suddenly cutting off all communication with the victim and disappearing without an explanation (Rege, 2009).

When victims and officials become suspicious, scams that impersonate or give the image of being a fake individual, company or organisation can quickly shut down any social media pages, websites and traces of them existing on the internet in just a few minutes. In many cases, they can make changes to them and recreate their online identity without any proof that they were the initial entity that had scammed victims in the first place. New Zealand television host Hayley Holt comments that these scams are like “whack-a-mole .. you take one down and another pops up at a different web address” (Higgins, 2019).

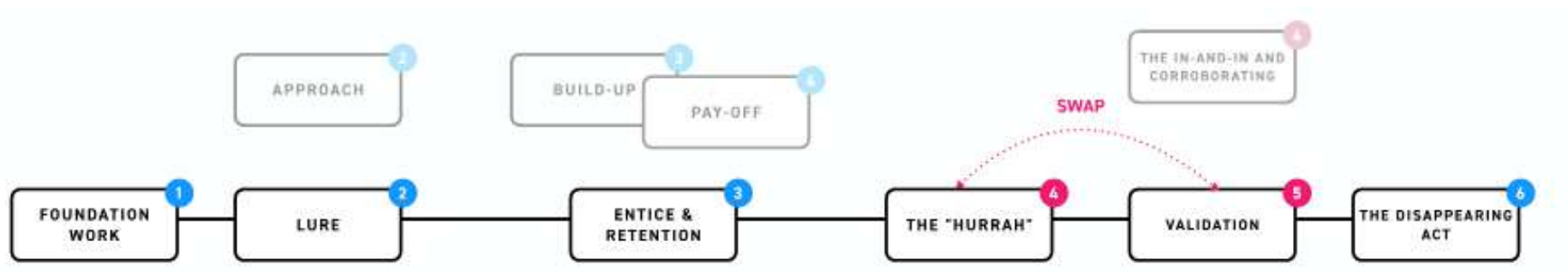


Figure 6.1 Adaption of Edward H. Smith's Confidence Trick strategy to better fit today's scam environment

**UNDERSTANDING PRODUCT MARKETING AND SOCIAL MEDIA
MARKETING PROCESSES**

Moral and malicious are two sides to the same coin. To develop a framework for malicious product and services scams, we must first observe it's moral counterpart

Armstrong, Adam, Denize, Volkov & Kotler (2018) and Andzulis, Panagopoulos & Rapp (2012) highlight the evolution of marketing and social media marketing (SMM), emphasising businesses are moving into social media as a marketing sales platform and creating relationships with their customers. Surprisingly, the frameworks developed by these two sets of marketing authors also share a similar process to Smith's (1922) con artist's strategy, despite Smith's (1922) framework serving a malicious purpose and its existence from over a century prior. This verifies that despite its age and lack of digital platform, the mechanics that were used in the original framework are still highly relevant in today's digital marketing and social media marketing processes.

FRAMEWORK SEVEN

PRINCIPLES OF MARKETING
5-STEP MODEL MARKETING PROCESS

‘Principles of marketing’ (Armstrong, Adam, Denize, Volkov & Kotler, 2018) visualises and describes the 5-step marketing process highlighting the critical steps to marketing a product. I believe that this model is essential to the research as understanding the legitimate process of marketing products and services will impact how realistic the scam is and how to enhance the scam to make it more appealing.

Armstrong et al. (2018) demonstrate the overarching process of marketing through a simple 5-step model (shown in Figure 7). The authors specifically place the model in the context of Australia and New Zealand. Despite developing the model in 1996, it has continued to have relevance in today's marketing landscape. This model outlines the marketing process's steps and demonstrates how a relationship is built with the customer.

1. Understand the marketplace and customer needs and wants

Similarly to Smith's (1922) step of 'background research', this stage investigates the current state of the intended product's marketplace and the customers who exist within it - specifically their relevant wants, needs, and target audience demands. In comparison, this stage has a higher focus on the customer.

2. Design a customer-driven marketing strategy

Another comparable aspect of Smith's (1922) framework, the step 'plan of approach' that creates a strategy around the selected target audience. This includes their needs, wants, demands and identifying a unique value proposition, how the business positioned within the market against their competitors and what is the plan to execute this specific strategy.

3. Construct an integrated marketing program that delivers superior value

A stage which focuses on the product and it's delivery. While aspects of this stage are mentioned within Smith's (1922) framework between the 'background research' and 'plan of

approach' stages, there is not a strong focus on the product, how its strategy is designed and developed in the best way to deliver it to the marketplace. This stage involved building a strong brand, considering product and service design, creating valued pricing, distributing the product, and promoting through platforms.

4. Build profitable relationships and create customer delight

Smith's (1922) framework includes a 'build up' stage giving the customer a chance to be part of the scam. However, the mechanics that were explained did not fit within the area of products and services scams. However, the build up of creating relationships with customers is both highly relevant and applicable when maximising on profitable trust - with the opportunity for long term commitment.

5. Capture value from customers to create profits and customer equity

An add-on from the previous stage emphasising creating ongoing loyalty and satisfied customers. While not mentioned in Smith (1922), the context of this stage within products and services scams also involves keeping the disguise and appearance of being a legitimate business. By increasing trust, delight and loyalty while increasing the customer base, decreases the chances of being found to be illegitimate. The authors also emphasise the importance of ensuring ethical and social responsibility, but this may be disregarded within the context of scams as their aims tend to be with malicious intent.

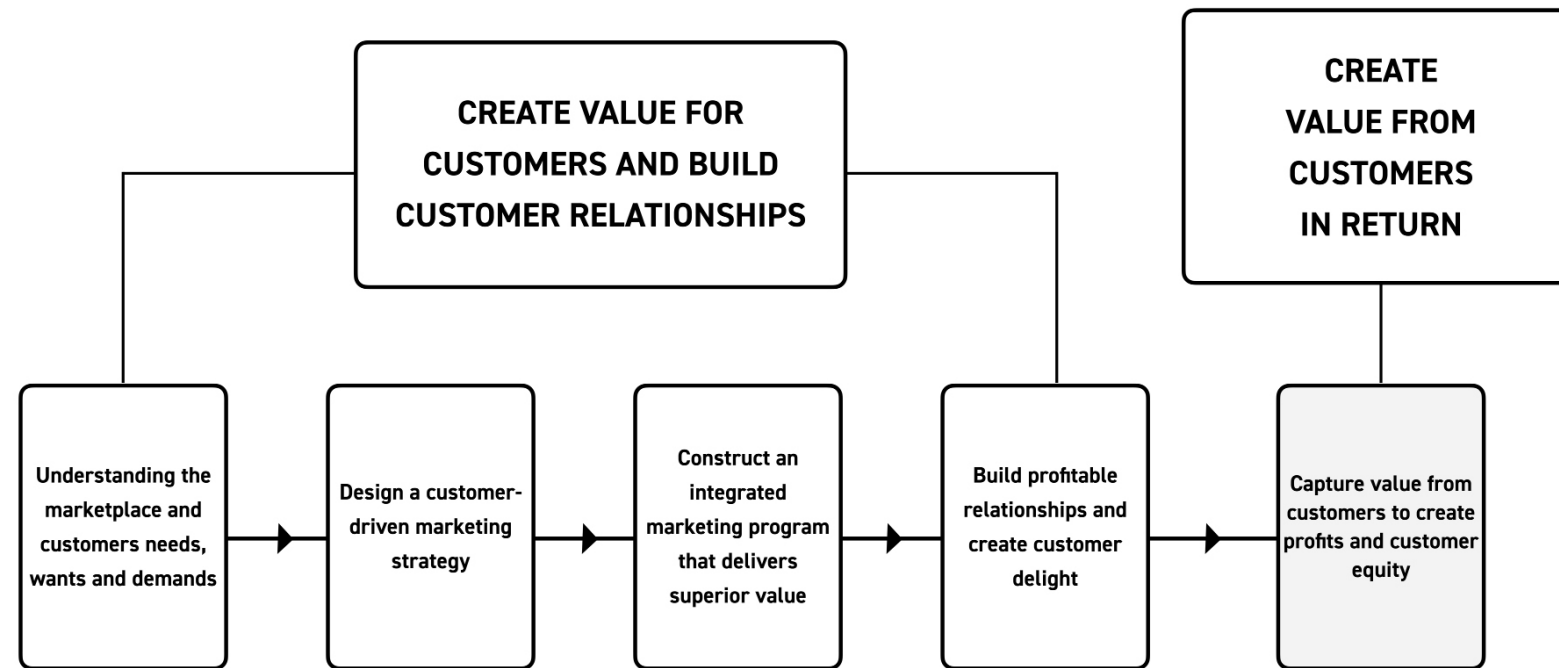


Figure 7 Armstrong et al.'s (2018) 5-step marketing model

FRAMEWORK EIGHT

SOCIAL MEDIA MARKETING PROCESS

Similarly to the previous marketing process, the 'Social media marketing process' (Andzulis, Panagopoulos & Rapp, 2012) captures the critical steps for marketing products on social media. I believe that this scam is essential to the research as understanding the process of marketing and advertising a product or service through social media will impact how realistic the scam is. This also includes how to further enhance its reach to social media users and how to convince a user to engage with the scam on a platform where the scammer has minimal control of the platform.

Similarly, Andzulis et al. (2012) analyse the process of SMM through how it impacts sales online and how customers are influenced to purchase within this process.

Andzulis et al. (2012) also describe the selling process in the context of online and social media through a process framework of 6 core steps from approaching the customer, concluding interaction and following up. Andzulis et al. (2012) visualise this evolution through Figure 8. Steps within this process include:

1. Understanding the customer

Identical to the previous two frameworks, this framework also starts with background research focusing on its customers. This stage is explained to include knowledge gathering through joining the customers' marketplace, observing conversation and comments, monitoring questions and feedback, determining communication style, analysing risks and buying situations.

2. Approach

While the same-named stage is mentioned within Smith's (1922) framework, it was highlighted that the exact implementation of the method did not fit within the area of product or services scams. Andzulis et al. (2012) confirm the notion of "luring" the victim through mechanics such as establishing credibility to gain trust, gain attention from trends and involvement in community interactivity.

3. Needs discovery

A similar stage to Armstrong et al. (2018)'s 'understanding the customer' stage. However, this implements more interactive and engaging tasks with the target audience to discover their needs, wants, and demands. This can include interactive polls, initiating customer feedback areas, and generating content (like blogs) to start conversations.

4. Presentation

An identical stage to that of Armstrong et al. (2018), in which the product communicates value proposition through using visual aids (product images and branding), demonstrations and success stories through social media platforms. Andzulis et al. (2012) also further explains the use of social media, fulfilling the needs of users wanting to learn more and be educated about the product at this stage.

5. Close

A stage that isn't mentioned by Armstrong et al. (2018), but included within Smith's (1922) 'Hurrah' stage in which the customer is persuaded into purchasing the product. Additionally, the authors also include the opportunity for the business to negotiate and address issues raised about the product.

6. Follow up

Providing opportunities for the business to keep interacting with the customer even after the initial purchase. This can include using tactics such as referrals, providing offers and newsletters. Despite not specifying Business to Customer (B2C) relationships, this stage is essential in keeping long-term relationships and loyalty with customers. However, this stage may not be relevant within a products and services scam as it may raise suspicion of legitimacy.

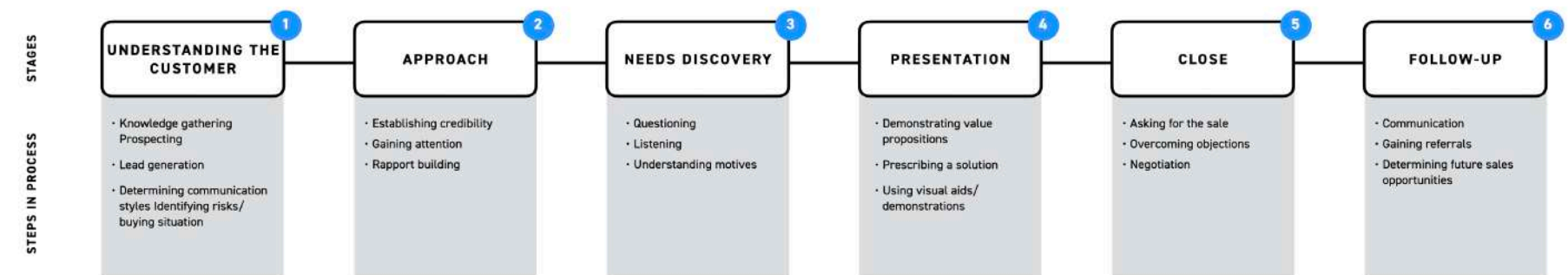


Figure 8 Visualisation of Andzulis et al.'s (2012) Social Media Marketing process

2.5 NEW FRAMEWORK OUTPUT

INTERWOVEN PRODUCTS & SERVICES SCAM PROCESS

Through exploring these virtuous and malicious frameworks, the similarities, differences and gaps within this analysis, this can be used to create a unique interwoven framework suited specifically for online products and services scam.

This new framework created by the researcher can be seen in Figure 9 and further explained in Figure 10.

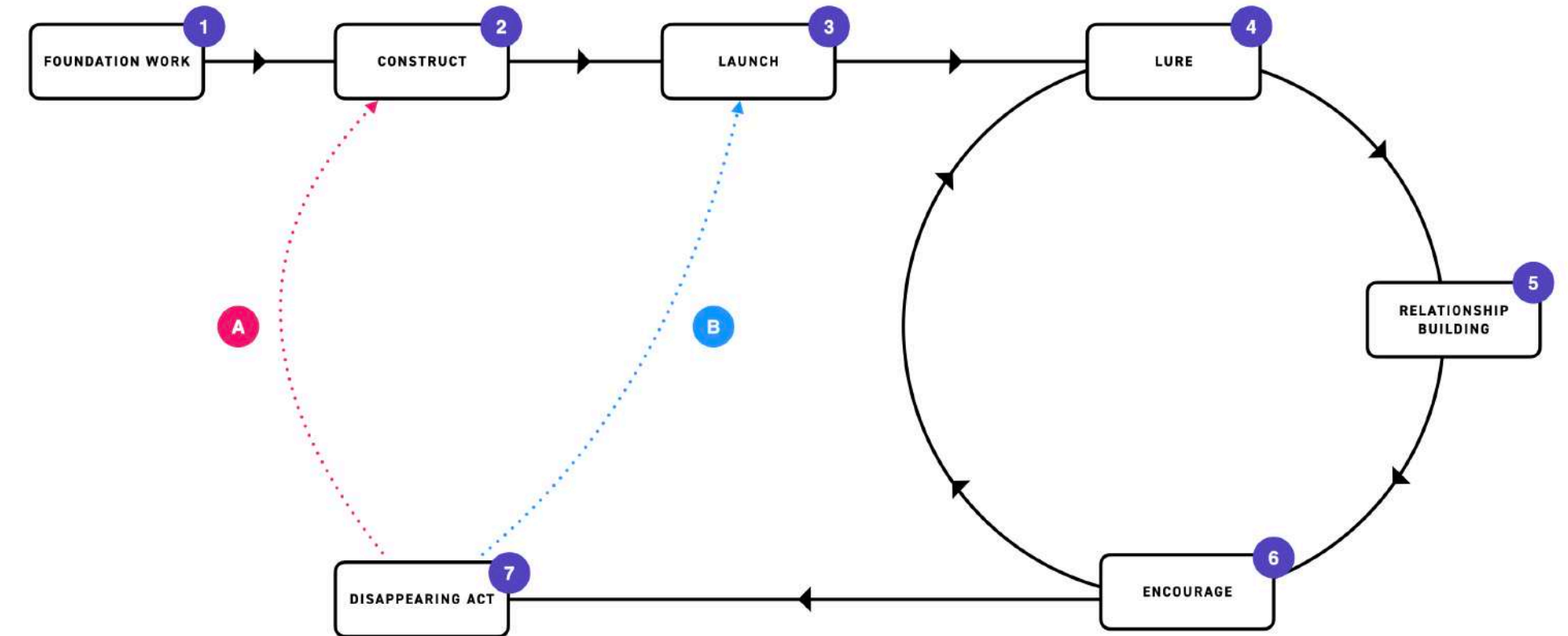


Figure 9. Visualisation of new 'Interwoven products & services scam process'

PREPARATION & ESCAPE

NO INTERACTION WITH SCAM TARGETS & VICTIMS

FOUNDATION WORK

Creates the groundwork and infrastructure of the online consumer Products and Services' scam. This assures that all aspects of the scam operation are considered, prepares the scam to act and feel as genuine as possible, increases chances of success and longevity. This stage is split into multiple areas.

Research

To gain a better understanding of the product and service's environment, background research is conducted for, but not limited to:

- Victim (User) Research
- Environment Research

- Product Research
- Competitor Research

Strategy

An overarching plan of approach to assure that the operation is executed consistently, and believably. This also decreases the chances that the operation will fail.

Obtain

Obtaining necessary material and resources needed to better pursue the operation. This includes obtaining information and data in relation to specified fields within the Research area.

CONSTRUCT

Creating or stealing visual material and platforms that establishes the scam organisation's digital presence, attracts victims and concretises it's look of legitimacy. This can include, but not limited to:

- Creation or stealing of assets
- Design or stealing of brand identity, colours and logo
- Design or stealing of product design or photographs
- Creating and development of platforms (website and social media)

LAUNCH

Any visual material and platforms that create the scam organisation's online digital presence are launched into the public.

This is an intermission step between preparation and action stages where victim customers are finally able to interact with the scam organisation and scam operation.

IMPLEMENTATION & ACTION

INTERACTING WITH SCAM TARGETS & VICTIMS

LURE

Attracting a victim and persuading them into interacting with the product or service's organisation. This is initiated through a combination of multiple social engineering techniques, specific dark patterns and scam strategies that intend to draw the victim towards the scammer (and not normally the other way). Luring intends to bait multiple victims primarily of the same target audience at once.

The aim of this stage is for initial interaction between both parties to have been initiated.

RELATIONSHIP BUILDING

The act of building a deeper connection, bridging the connection between the user and the product or service while assures they are kept within the site. This is initiated through social engineering, scam strategies, marketing strategies and visual design with the intention of building trust, establishing organisational presence and providing positive validation.

ENCOURAGE

Using a combination of techniques that will push the victim customer is to proceed with the purchase of the scam product or service.

This often involves making the process of purchase easier, or incite negative or positive forms of pressure. The stage is accomplished when the victim customer has successfully purchased the product or service with minimal to no suspicion.

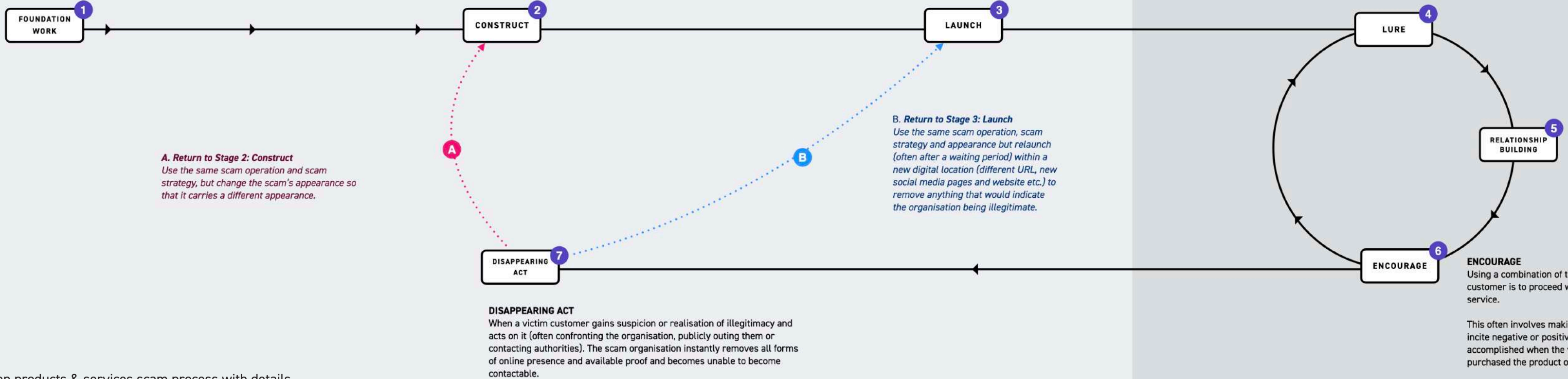


Figure 10. Interwoven products & services scam process with details

WHAT DOES THIS NEW INTERWOVEN
PRODUCTS & SERVICES SCAM PROCESS LOOK
LIKE WITHIN SCAM WEBSITES AND SCAM
SOCIAL MEDIA?

STAGE

PRODUCTS & SERVICES SCAM SOCIAL MEDIA PAGE

PRODUCTS & SERVICES SCAM WEBSITE

	<div>ENTRY POINT Google → Scam social media page Scam website → Scam social media page Email → Scam social media page Text → Scam social media page Physical marketing materials → Scam social media page Third party website → Scam social media page Third party social media → Scam social media page Third party website → Scam social media page Third party social media → Scam social media page</div>	<div>ENTRY POINT Google → Scam website Social media → Scam website Scam website → Scam website Email → Scam website Text → Scam website Physical marketing materials → Scam website Third party website → Scam Website Third party social media → Scam website Internet advertisement → Scam website</div>
Foundation work	<div>Research Victim (User) research within social media Environment research within social media Product research Competitor research within social media</div> <div>Strategy Creation of a social media marketing strategy</div> <div>Obtain Obtaining user data and information through social media profiles or purchasing data through third party means. Hiring of accomplices to assist running scam social media pages.</div>	<div>Research Victim (User) research both online and offline Environment research both online and offline Product research Competitor Rresearch both online and offline</div> <div>Strategy Creation of an overarching plan of approach and product marketing strategy</div> <div>Obtain Obtaining or purchasing user data and information through third party means. Hiring of accomplices to assist running website</div>
Construct	<div><ul style="list-style-type: none">Design and creation of social media assets (banners, icons, marketing material)Design and creation of product or service imagesCreation of necessary social media pages (Facebook, Twitter, Instagram etc.)</div>	<div><ul style="list-style-type: none">Design and development of scam websiteDevelopment and implementation of data and information capture mechanics within the scam websiteDesign and implementation of dark pattern mechanics within the scam websiteDesign of visual assets</div>
Launch	<div><ul style="list-style-type: none">Launching of scam social media pagesLaunching of scam advertisementsPurchase and obtaining of a fake platform following (followers, friends, likes, subscribers)</div>	<div><ul style="list-style-type: none">Launch of scam websiteEstablish scam website search engine analyticsEstablish scam website search engine optimisation</div>

STAGE	PRODUCTS & SERVICES SCAM SOCIAL MEDIA PAGE	PRODUCTS & SERVICES SCAM WEBSITE
Lure	Luring through paid internal social media advertisements within the established platform. Other luring methods can include advertising through messages (text, email), mentioned or advertised through third party social media pages and websites, advertised through physical marketing material, redirected from its connected scam website or found through search.	Luring through external advertisements outside of the site. Primarily through social media, but can be lured through high google search listing, emails, text, physical marketing materials or mentioned and/or advertised on a third party website or social media page and advertisements on the internet.
Relationship Building	<p>Relationship building for scam organisations within social media comes in the form of creating a trusting presence on the platform they are occupying.</p> <p>A trusting online business presence can be implemented through:</p> <ul style="list-style-type: none">• Well designed, professional and legitimate-looking branding, advertisements and visuals• Has a decent-to-large following and customer base• Has positive, genuine-looking reviews• Part of a scam package: Has a website for the business connected to the social media page	<p>Building a customer relationship with the scam website should feel like the organisation understands the customer and looks after them while they are in their territory. This can be implemented through:</p> <ul style="list-style-type: none">• Welcoming and caring language• Well designed, professional and legitimate looking branding, advertisements and visuals• Images of endorsement and certification• Offer of free items• Positive reviews within the site• Offer for customer to be involved within the product (personalization)• Part of a scam package: Has a website for the business connected to the social media page
Launch	<p>As scammers have limited power within social media, building a relationship through social media is quite limiting and primarily relies on mechanics within advertisement of visuals, text and social engineering. For success, the victim customer must leave the scam social media page and move onto the bridging scam website.</p> <p>Triggers to push this behaviour can include:</p> <ul style="list-style-type: none">• Negative pressuring mechanics - limited time and quantity through advertisement text and visuals• Positive, encouraging mechanics - need to satisfy curiosity, excitement over sales and details through advertisement text and visuals.	<p>Encouraging customers and pushing them to purchase an item uses a combination of visuals, text and social engineering mechanics implemented from the moment they enter the site and as they are buying the product. For success, the victim customer must have successfully purchased the scam item and leaves the website with little to no suspicion.</p> <p>Triggers to push this behaviour can include:</p> <ul style="list-style-type: none">• Negative pressuring mechanics - limited time countdown clocks, display limited remaining quantity numbers• Positive, encouraging mechanics - Path of least resistance, the pre-picked preferred option, giving something free with a purchase, item endorsement, positive reviews from other customers
Disappearing act	<ul style="list-style-type: none">• After gaining suspicion or realisation of illegitimacy, the victim customer either confronts the scam organisation on their social media page comments, publicly outing on their personal social media pages, reporting the pages to staff on the platform that they are on, before contacting local authorities about the page. The scam organisation deletes all social media pages.	<ul style="list-style-type: none">• After gaining suspicion or realisation of illegitimacy, the victim customer either confronts the scam organisation on their social media page comments, publicly outing the scam on their personal social media pages before contacting local authorities about the page. The scam organisation deletes all website pages..

Figure 11. Photomanipulation of hacker pretending to be a young girl



This chapter creates the groundwork for the second part of the project and provides an introduction to the 2019-2020 coronavirus (COVID-19) pandemic within both a worldwide and New Zealand context. To understand how products and services scams could take advantage of their victims using the COVID-19 pandemic, this chapter also discusses New Zealand's approach, visualises the impact of the pandemic on the country and the role COVID-19 scams will play.

3.1 New Zealand scams

3.2 Event based scams

3.3 Introduction to COVID-19

3.4 COVID-19 in New Zealand

3.0

PRELUDE & CONTEXT

3.1 NEW ZEALAND SCAMS: AT A GLIMPSE

Between January and December 2019, Netsafe New Zealand reported a total loss of \$18.44M to scams and fraud. This resulted from 16,416 scam and fraud specific reports, covering 69% of the 23,621 total number of reports to Netsafe in 2019.

While the first quarter of 2019 saw 'relationship and trust' fraud top the list for most reported scam categories at 58%, April onwards saw 'Products and Services' scams skyrocket from 23% to 60.3% by the end of the year. 3,200 of these cases reported that there was some loss financially. Other fraud categories that NetSafe acknowledged in their quarterly reports included consumer investment, prize & grant, blackmail, phantom debt collection fraud and employment fraud.

Reports do not cover the emotional and personal impact these scams have on their victims. Experts must be aware of and communicate the potential damage that products & services scams could create. While the report highlights the high-level numbers of products & services scams, they cover the finer details of what these scams aim to do.

HOW DOES NEW ZEALAND CURRENTLY WARN ITS PEOPLE ABOUT SCAMS?

The two most common methods seen to educate people are writing blog posts / creating a list of tips (Figure 12 and Figure 13) or businesses warning their follower-base on their social media platforms (Figure 14) to watch out for scams. These methods, while could work momentarily, would potentially be forgotten the moment the person has moved onto something else. Blogs / tip lists only cover scams at a surface level and consumers may interpret the complexity level of that as the actual complexity level of the scam.

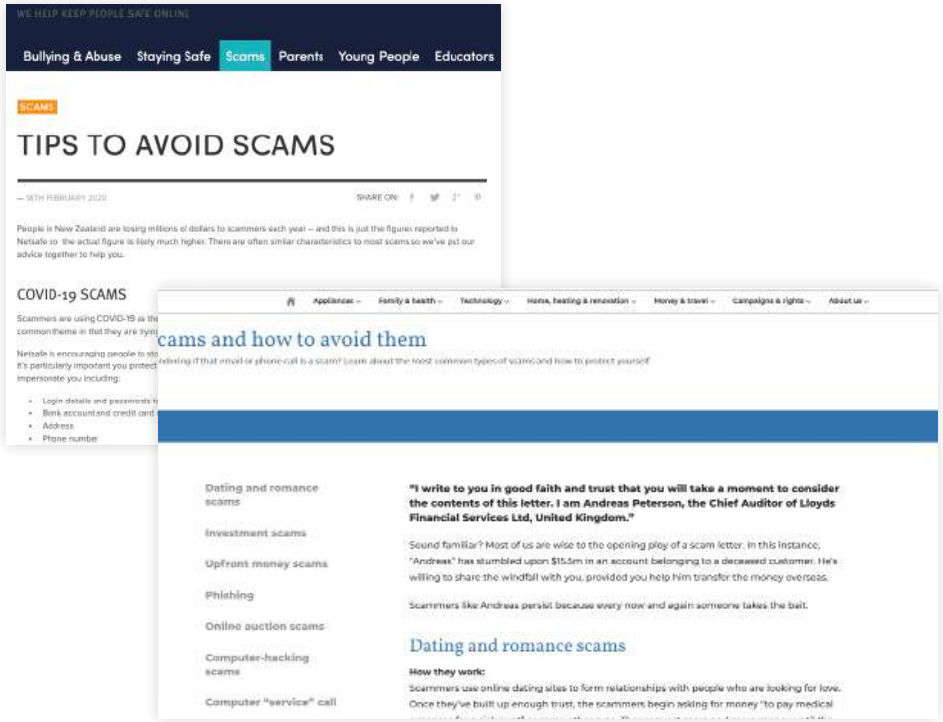


Figure 12. Screenshots of NetSafe New Zealand's scam tips page

Figure 13. Screenshots of Consumer. New Zealand's scam tips page



Figure 14. Noel Leeming repeatedly posting on their Facebook page that they are not performing actions that scammers are advertising.

3.2 EVENT BASED SCAMS

Many products and services take advantage of occasions, public holidays and date based events that take place around the year as that is when retailers often hold store sales (Hache & Ryder, 2011). Customers often gravitate towards a retailer upon seeing sales advertise, while other customers wait and save for these sales to happen before they buy. These events include calendar year events (Christmas, Valentines Day, Boxing Day, Black Friday, Easter), Seasonal (Summer, Winter, Autumn, Spring) and country/ region/ culture-specific events (4th of July, Waitangi Day, Queens Birthday, Wellington Anniversary, Matariki) (Hache & Ryder, 2011). Event-based scams can also be planned events - often unique and have a specific audience such as concerts, sports events, conferences, and meet & greets (Ferrick, 2019). As these events are triggers for products and services sales, there is a high chance that scammers will take advantage of this to carry out retail scams to take advantage of the large group of potential victims.

However, a unique variation of event-based scams that I believe has not been mentioned at a generalised level is “impact and cause” -based scams. These scams do not take advantage of product sales, customers who buy and retailers who sell products or services. Scammers take advantage of a large group of people who come together through a specific cause, often through unity and compassion to fight, rather than money related means. Examples of this can be seen through protests (Black Lives Matter and Climate Change) and impactful, emotionally affecting and devastating events (9/11, 2019 Christchurch mosque shootings and the Coronavirus (COVID-19) pandemic). These scams take advantage of their emotions, empathy and compassion, before exploiting them financially.

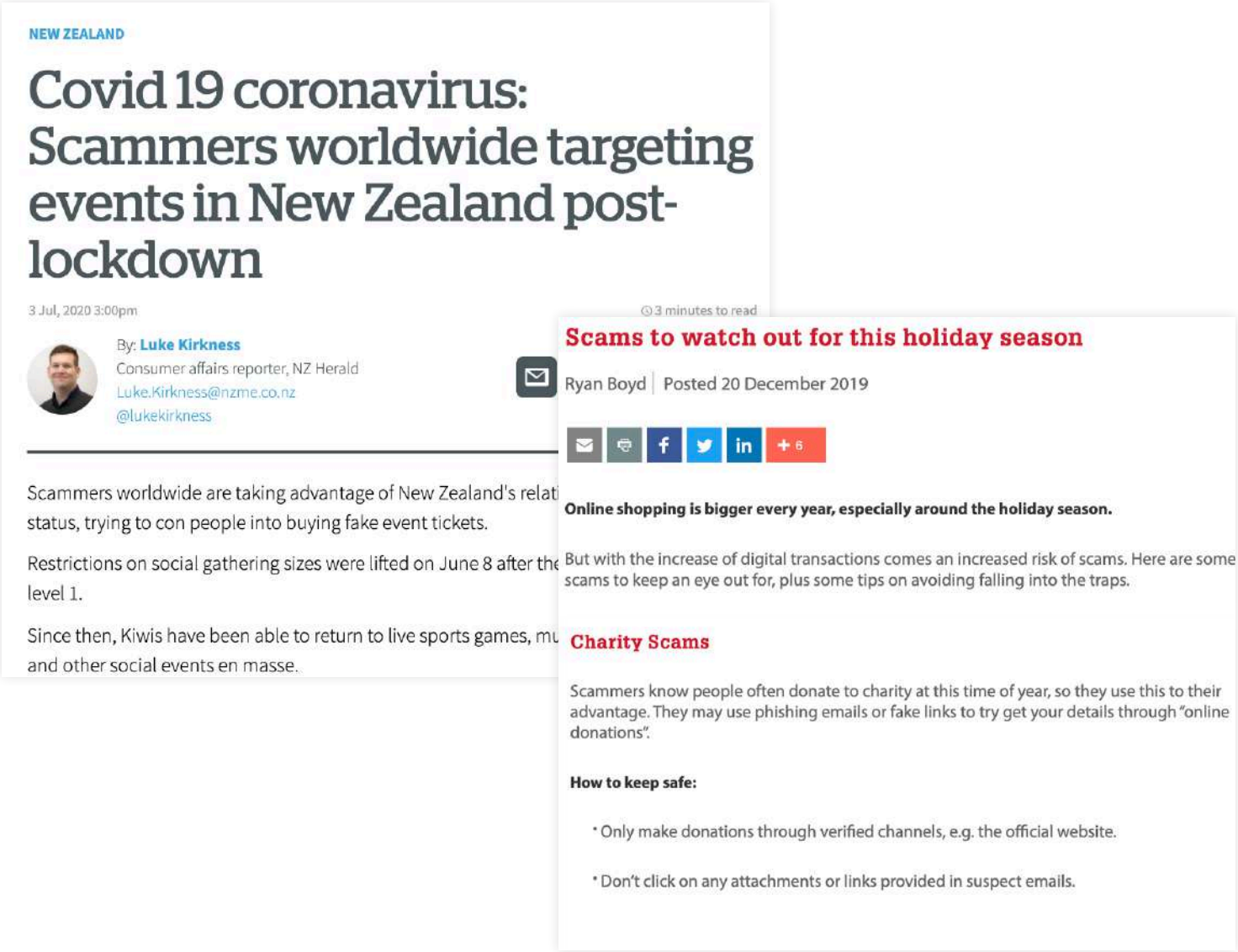


Figure 16. Media piece on COVID-19 scams (Kirkness, 2019)

Figure 17. Media piece on Holiday season scams (Boyd, 2019)

3.3 INTRODUCTION TO COVID-19

In December 2019, a cluster of pneumonia cases was identified by health officials in Wuhan, China. Initial investigations determined that the infectious disease caused by severe acute respiratory syndrome (SARS) was potentially fatal and a threat to global health (Fauci, Lane & Redfield, 2020). The World Health Organisation (WHO) defined the disease, Coronavirus as a ‘family of viruses’ causing sickness to both animals and humans, with the recent novel coronavirus discovery labelled COVID-19 (WHO, 2020).

WHO (2020) states that symptoms of the virus that were commonly found included a fever, dry cough, and tiredness, but other symptoms could range from aches and pains, headaches, conjunctivitis, sore throat, diarrhoea, among others. However, some who had caught the virus were symptomless and were still able to carry the disease to other people. People who had underlying health issues such as high blood pressure and, most particularly, heart and lung problems were highly at risk. The

elderly were particularly the most vulnerable, but people of all ages could be affected by the disease.

Within less than a month of its identification, COVID-19 has had outbreaks in many countries around the world, as of July 27, 2020 more than 16.1 million cases have been confirmed worldwide and killing almost 645,000 people (WHO, 2020).

The pandemic has caused large-scale disruption to people's everyday lives, shaken the economy, and caused mass panic. Countries worldwide are taking strict measures, implementing lockdowns and introducing new restrictions and regulations to people's lives (Coibion, Gorodnichenko and Weber, 2020). There is still a lack of knowledge, and research around the pandemic is still being undertaken (Heymann and Shindo, 2020).

On January 31st, WHO declared COVID-19 as a global health emergency.

3.4 COVID-19 IN NEW ZEALAND

Despite being an isolated country, New Zealand was not spared from being hit by the rapidly growing COVID-19 pandemic. New Zealand media first reported that the Ministry of Health would be monitoring the situation overseas on January 22nd, 2020, and had already warned health professionals about the virus. Fears of the virus spreading resulted in the projection of racism against Asians.

As overseas New Zealanders started to head home, unwell returnees were reported to be tested when arriving at Auckland Airport beginning January 27th. Requirements for travellers to self isolate for 14 days after arriving in New Zealand was established on February 3rd. Around this time, many large crowded events such as the Auckland Arts Festival were cancelled. New Zealand's first case was confirmed on February 29th, 2020, causing panic within the country. As days passed, the total number of cases grew before reaching its peak on April 2nd, with the highest daily rate of new cases at 89.

The New Zealand government implemented a 4 level alert system that specified a risk assessment and measures to be taken against

COVID-19 at each level that can be applied regionally or nationally. New Zealand was placed under a strict nationwide lockdown with the implementation of Alert Level 4 (the highest level of lockdown) for 4 weeks, lifting some lockdown restrictions upon moving down to Alert Level 3 on April 27th and fully lifting the lockdown with distancing requirements 2 ½ weeks later on May 13th. All remaining restrictions were lifted on June 8th, when the country moved down to Alert Level 1.

However, 24 days after 0 cases, new cases in small numbers had started to emerge. Director-General of Health Dr Ashley Bloomfield had outlined this stating that this was to be expected as new arrivals from overseas arrive within New Zealand. These new arrivals would be isolated for the required 14 days.

New Zealand recorded 1,506 cases (1,159 confirmed and 350 probable) and 22 deaths - all of which were older adults.

A timeline of all major key events in New Zealand has been visualised by the researcher in Figure 18. from Radio New Zealand COVID-19 headlines (Radio New Zealand, 2020).

Figure 18. Visualisation of COVID-19 New Zealand timeline from Radio New Zealand headlines created by the author

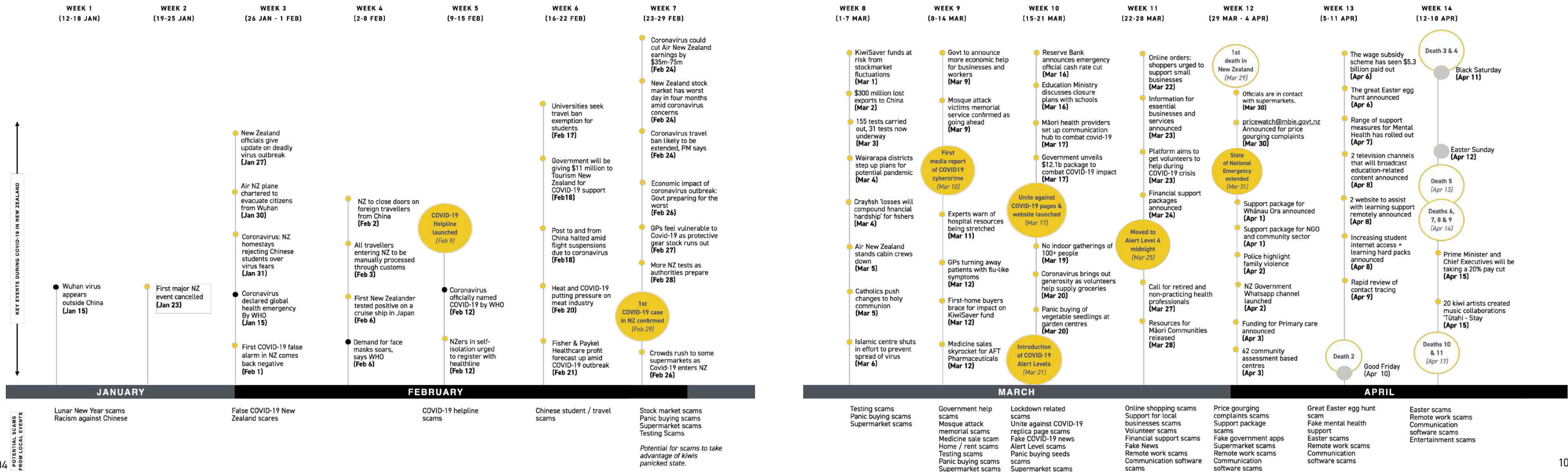
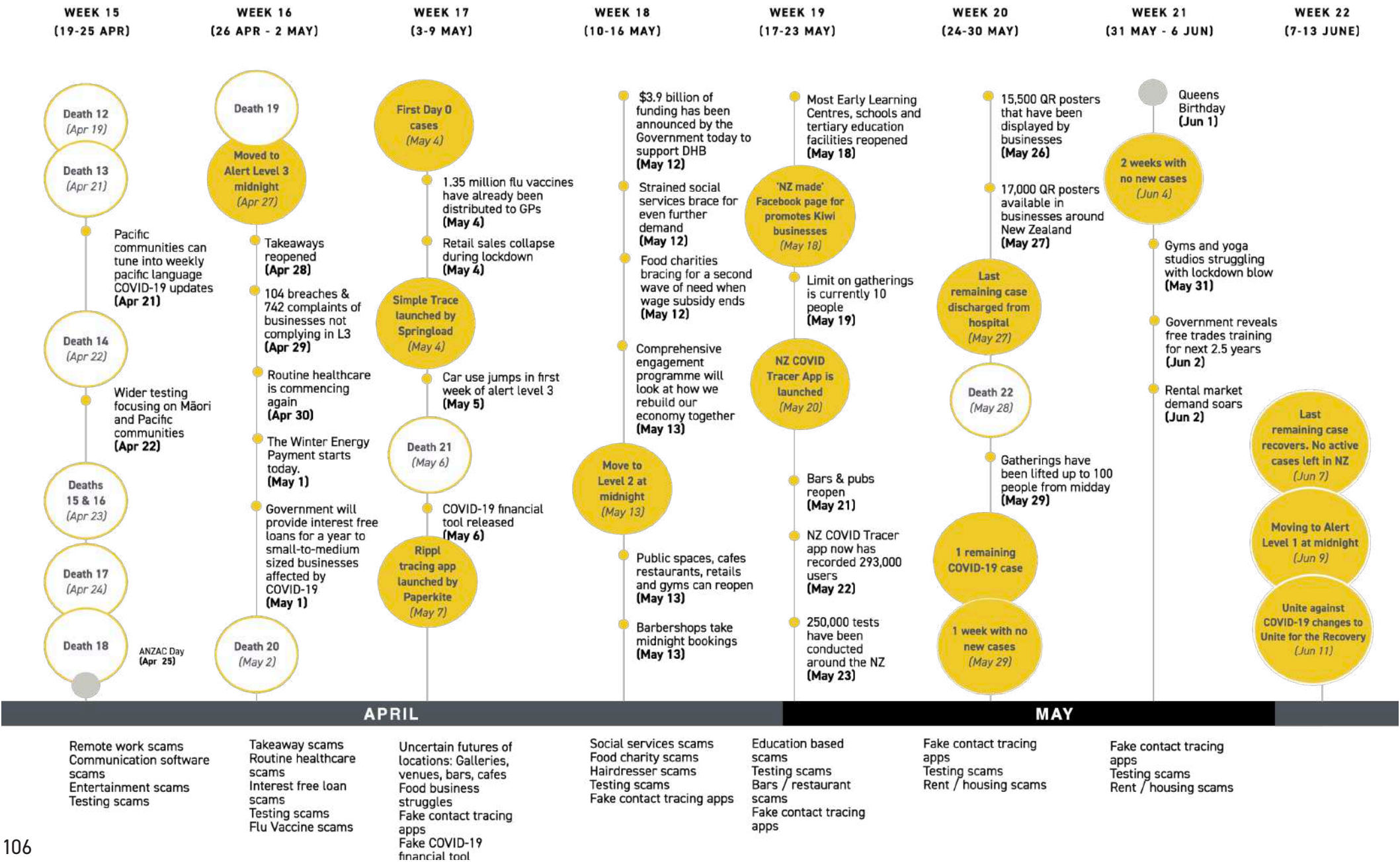


Figure 18. Visualisation of COVID-19 New Zealand timeline from Radio New Zealand headlines created by the author cont.



3.4B THE IMPACT OF NEW ZEALAND LEADERS: JACINDA ARDEN & ASHLEY BLOOMFIELD

New Zealand has been praised and admired internationally within the media for it's "aggressive approach" in tackling and defeating COVID-19 (Gunia, 2020). Among this, Prime Minister Jacinda Arden, taking the spotlight for her showcase of masterclass leadership skills with empathy, humility and collaboration (Zalis, 2020). While quickly enforcing strict rules and lockdowns to minimise the pandemic's spread, Arden communicated messages daily through compassion and emphasised the country's importance to unite as one, a "team of 5 million", to beat COVID-19.

An unsuspecting local celebrity to arise from the pandemic is the Ministry of Health's Director-General of Health, Dr. Ashley Bloomfield. Standing alongside Prime Minister Jacinda Arden during daily COVID-19 updates, Bloomfield calmly delivered the pandemic's current status in the country, providing the country with a sense of comfort, security, and reliability.

It is a combination of these two individuals that brought a sense of positivity and hope for the country. Arden's compassionate and collaborative leadership and Bloomfield's medical expertise providing knowledgeable understanding and clarity to the situation.

While Bloomfield was "just doing his job" as a public servant, many New Zealanders started to hero-worship him, creating a range of tributes in his name, including Facebook fan pages, earrings, music videos, etc. soundtracks, hand towels and cakes. Arden, who has been admired previously for her compassionate leadership tackling other national problems, has been subject to similar tributes.

3.4C STRONG BRAND AND ONLINE PRESENCE TO FIGHT AGAINST COVID-19

On March 17th, the New Zealand Government launched ‘Unite against COVID-19’, a government program and national marketing campaign established to provide clear messaging, information and communication clear about COVID-19. This was established 2 weeks after the announcement of the first case. The campaign had an online presence included:

- **A website (www.covid19.govt.nz)**
A hub of information to educate New Zealanders about COVID-19 , how to protect themselves, advice and support for businesses, community, wellbeing, jobs & training, regular updates and resources.
- **Social Media platforms**
The campaign's social presence consisted of Facebook, Twitter and Instagram platforms used to announce daily updates, major and alert level announcements, and connect with New Zealanders and answer their COVID-19 related questions.

- **Print and digital advertisements**
The campaign had a simple yet recognisable and impactful visual identity used on all COVID-19 government-related content. This consisted primarily of egg yolk yellow and white stripes, thin, black, san-serif typeface that is clean and easy to read and minimalistic line based iconography that clearly communicates and emphasises announcements. This visual branding was not only used on their digital platforms, but could be seen physically through posters, billboards, wayfinding and flyers.

Written copy and content was portrayed with empathic and caring based attitudes and words with a repetitive emphasis on Prime Minister Jacinda Arden’s key messages:

- “Stay Home, Stay Safe, Be Kind”
- “Stay Home, Stay Safe, Save lives.”

After over 2 weeks with no new cases, on June 11th, the branding was modified from ‘Unite against Covid-19’ to ‘Unite for the Recovery’ to match the government's decision to move down to Alert Level 1. While the visual design stayed the same, the brand’s new message pivoted to aim for the recovery of New Zealand after the impact of the pandemic. This further emphasised the message of uniting together and getting the country back on its feet.

In a global survey initiated by Provoke Media(2020), New Zealand topped the survey at just over 20% of votes for having the best response against the pandemic. This specifically targeted the communication efforts of the government.



Figure 19. Unite against COVID-19 logo and brand colours (New Zealand Government, 2020)

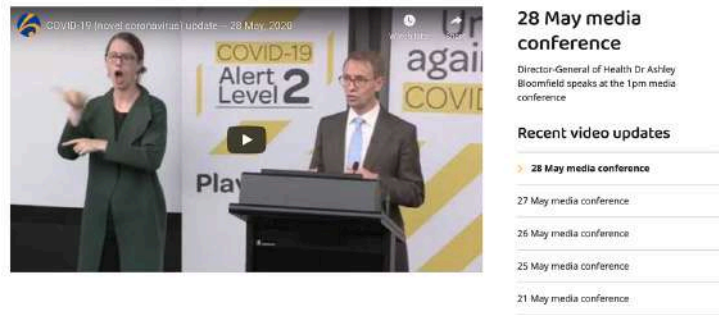
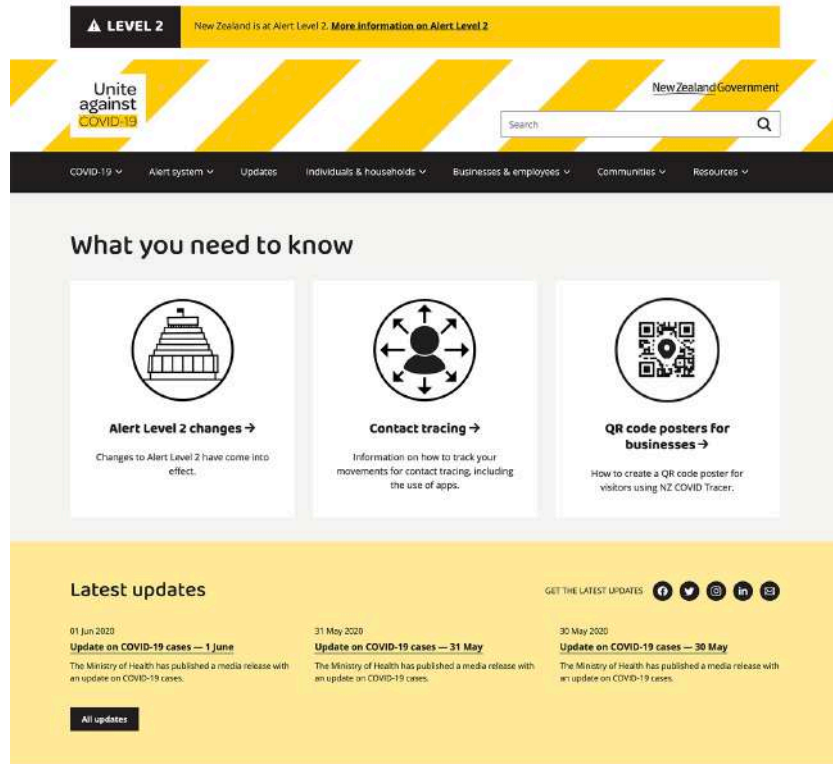


Figure 20. Unite against COVID-19 Campaign website (New Zealand Government, 2020)

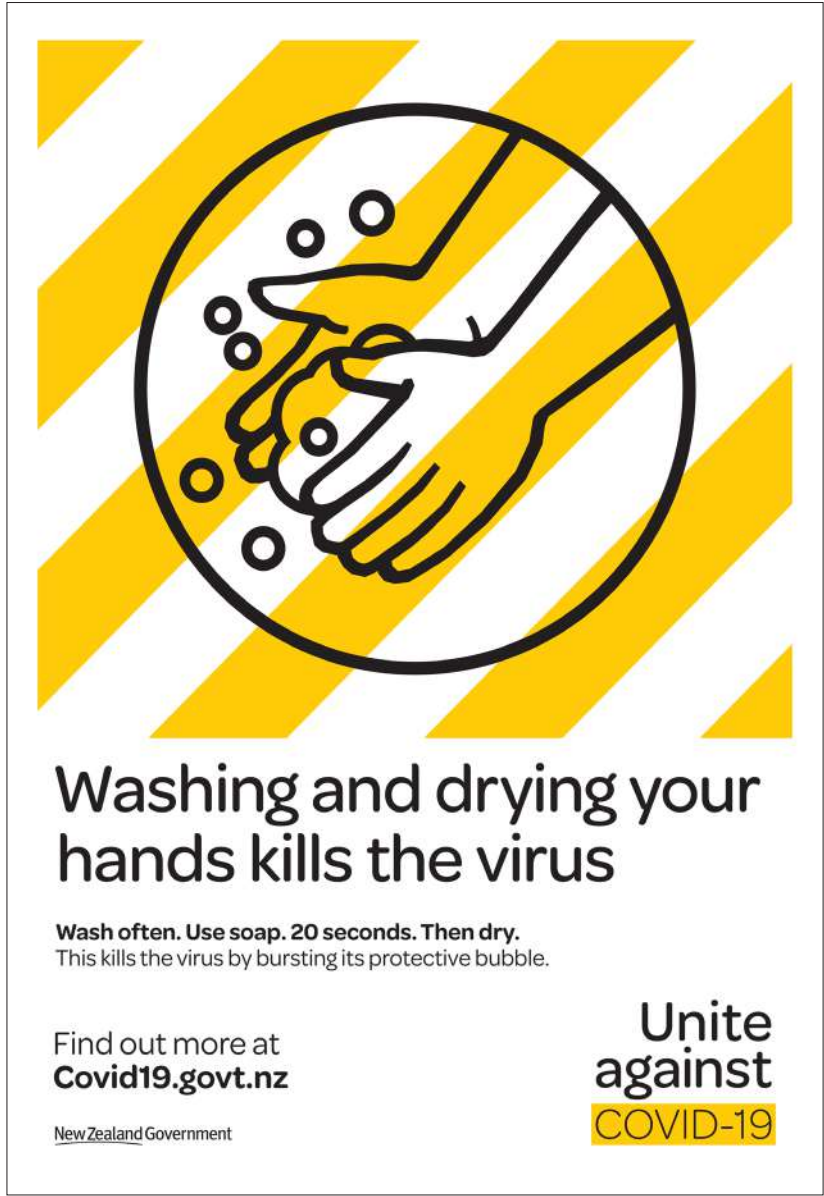


Figure 21 Unite against COVID-19 Campaign (New Zealand Government, 2020)



3.4D COVID-19 SCAMS

Both government agencies, organisations and media highlight the appearance of scams that take advantage of COVID-19. Similarly, they all give a few examples of some of the scams and advice on avoiding them. There is currently no place that captures the complete list of COVID-19 scams, and products and services scams are only mentioned at surface level as “shopping scams”. New Zealand media also only discuss products and service COVID-19 scams with general details and has only covered a few within the context of New Zealand.

Across the ditch, Australia has recorded 3400 scam COVID-19 related reports with a loss of over \$1,790,000. Scamwatch (Australian Competition and Consumer Commission, 2018) has listed the most relevant scam types during COVID-19 as classified scams, health & medical products, online shopping scams, investment scams, identity theft, phishing and hacking. Through exploring different media and government sources, COVID-19 scams listed have been categorised as a product, services, or other scam.

PRODUCT SCAMS	SERVICES SCAMS	OTHER
<ul style="list-style-type: none">• Testing kits• Coronavirus map• Shopping scams• Vaccine / Cure scams• Air filter scams• Supply scams• Contact-tracing mobile apps• Supermarket vouchers• Software and fake anti-virus scams	<ul style="list-style-type: none">• Offers of investments• Testing services• Virus treatment• Payment for non-existent pandemic services• Fake job websites• Contact tracing hotline• Charity scams• Donation scams• Treatment payment• Travel agent / holiday cancellation scams• Wi-Fi provider phishing calls• Online service and subscription providers• Tech support• Economic support / government subsidy• Education support	<ul style="list-style-type: none">• Impersonation health officials• Fake news• COVID-19 fraudulent websites• Bank scams• Tax scam

COVID-19 SCAMS IN DETAIL

A surface overview of what each of these COVID-19 scams entitle

PRODUCT SCAMS

TESTING KITS (VERY COMMON)

Scams that offer unauthorised or fake COVID-19 at-home testing kits. This scam is for information and financial gain.

CORONAVIRUS MAP TRACKER APP (VERY COMMON)

Scams that provide the user with a worldwide tracking map that shows COVID-19 cases and death worldwide, but installs malware that can steal information, spyware or lock the user out of their phone. This scam is primarily for information and financial gain.

ONLINE SHOPPING SCAMS/SUPPLY SCAMS (VERY COMMON)

Broad scam type where customers purchase counterfeit or non-existing products online during COVID-19. This takes advantage of people's reliance on online shopping during lockdowns and panic buying. Most commonly, this takes the form of scammers posing as fake or clone online shopping websites for both information and financial gain.

TREATMENT / VACCINE / CURE SCAMS (VERY COMMON)

Scams that offer vaccines and cure products like creams, edibles or injections said to cure COVID-19. This scam is for information and financial gain.

AIR FILTER / AIR PURIFIER SCAMS
(UNCOMMON IN NEW ZEALAND)

Scams that sell air filters or purifiers under the guise that the device will filter out the COVID-19 virus from the surrounding air. This scam is for information and financial gain.

CONTACT-TRACING APPS (SOMEWHAT COMMON)

Scammers develop and launch malicious contact tracing web and mobile applications to steal it's users data while pretending to keep track of users who may have COVID-19 legitimately. This scam is for information gain

SUPERMARKET VOUCHERS (COMMON)

Scams that advertise competitions or offers to obtain vouchers to well-known supermarkets and retailers by submitting the provided form. This scam is for information gain.

SOFTWARE AND FAKE ANTI-VIRUS SCAMS (COMMON)

Scams that provide high demand software or discounted software during COVID-19 with incorporated malware to steal user information. This scam is for information gain.

SERVICES SCAMS

INVESTMENTS SCAMS (COMMON)

Scams that lure people into investing in research initiatives, businesses or organisations researching or developing reports or products for COVID-19. This scam is for information and financial gain.

TESTING SERVICES (COMMON)

Scams that offer services to test a person for COVID-19. This scam is for information and financial gain.

PAYMENT FOR TREATMENT/NON-EXISTENT PANDEMIC SERVICES (SOMEWHAT COMMON)

Scams which contacts people asking them for payment for a service they have been told that they used. In most cases, they did not use the service, or the service is fake. This scam is for financial gain with the potential for information gain.

COVID-19 HOTLINE (SOMEWHAT COMMON)

Scams which provides a phone number for people to call and get information about COVID-19 but misinforms them instead. This scam is for information gain, but has the potential for financial gain.

CHARITY/DONATION SCAMS (SOMEWHAT COMMON)

Scams which prey on the generosity and goodwill of people persuading them to donate for a COVID-19 cause. This scam is primarily for financial gain, with the potential for information gain.

TRAVEL AGENT/HOLIDAY CANCELLATION SCAMS (SOMEWHAT COMMON)

Scams that contact a person about holiday related purchases that have been impacted due to COVID-19 - whether they had booked a holiday or not. This can include cancelled airfares, accommodations, postponement of travel etc. This scam can also include offers and discounts due to COVID-19 for after the pandemic. This scam is for information and financial gain.

WIFI PROVIDER SCAMS (SOMEWHAT COMMON)

Scams where the scammer is posing as a person's internet provider. Scams often involve the scammer informing the victim of issues surrounding their current wi-fi with offers to repair or threatening to cut their service off. This scam is for information gain.

FAKE JOB WEBSITES (SOMEWHAT COMMON)

Scams that advertise fake or real jobs to lure people into giving their personal information by submitting job applications. The scam can also lure organisations into posting job and company information within the scam platform. This scam is for information gain but the potential for financial gain if application fees are introduced.

TECH SUPPORT (COMMON)

Scams where scammers posing as tech support contacts people that there is an issue with either hardware or software they own. By following their instructions, the scammers will hack into their accounts when it seemed the initial intention was to help them. This scam is for information and financial gain.

ECONOMIC SUPPORT / GOVERNMENT SUBSIDY (SOMEWHAT COMMON)

Scams which offer struggling individuals or businesses financial support. This scam is for information gain with the potential for financial gain.

ONLINE SERVICE AND SUBSCRIPTION PROVIDERS (COMMON)

Scams that contact people about online services and subscriptions they currently use or are offered to use (video streaming services, software subscriptions etc.). This can include letting them know their account has been hacked or offers to obtain the service at a discounted price. This scam is for information and financial gain.

The mechanical deconstruction, design-based recreation and visualisation of frequently encountered and potential New Zealand COVID-19 products and services scams through 2 speculative experiments. A focus of these speculative experiments is to illustrate and communicate the larger, overarching picture of these scams.

4.1 Experiment 1

4.2 Experiment 2

4.3 Collection of scams

4.0 EXPERIMENTATION

EXPERIMENTATION INTRODUCTION

This chapter puts theory into practice by implementing the new interwoven framework into a current situation. While Part 1 of this research focused on understanding the past and present state, previous precedent frameworks and creating a unique framework that aligns with the research area, Part 2 draws this research into the new framework’s practical application. Putting this interwoven framework into the context of the coronavirus (COVID-19) pandemic will provide insight into how the framework is put into action.

The following two experiments will investigate two online product and services scam issues within COVID-19 and how implementing a unique framework can provide clarity on how they function. For both experiments, a case study is included to frame and put into context the investigation.

EXPERIMENT 1

SELLING COUNTERFEIT COVID-19 GOODS:
TAKING ADVANTAGE OF NEW ZEALAND COVID-19 AWARENESS BRANDING

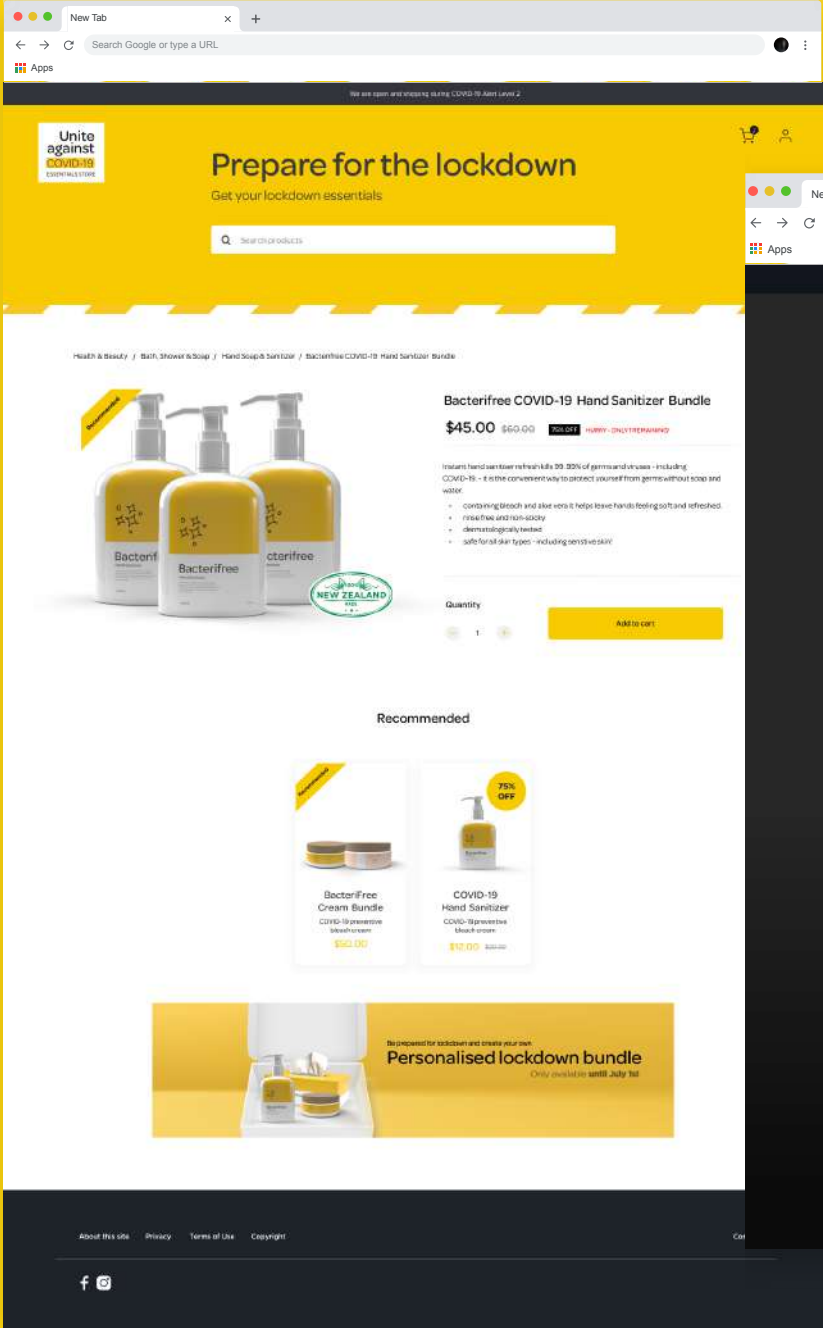


Figure 22. Design of fake COVID-19 ecommerce store

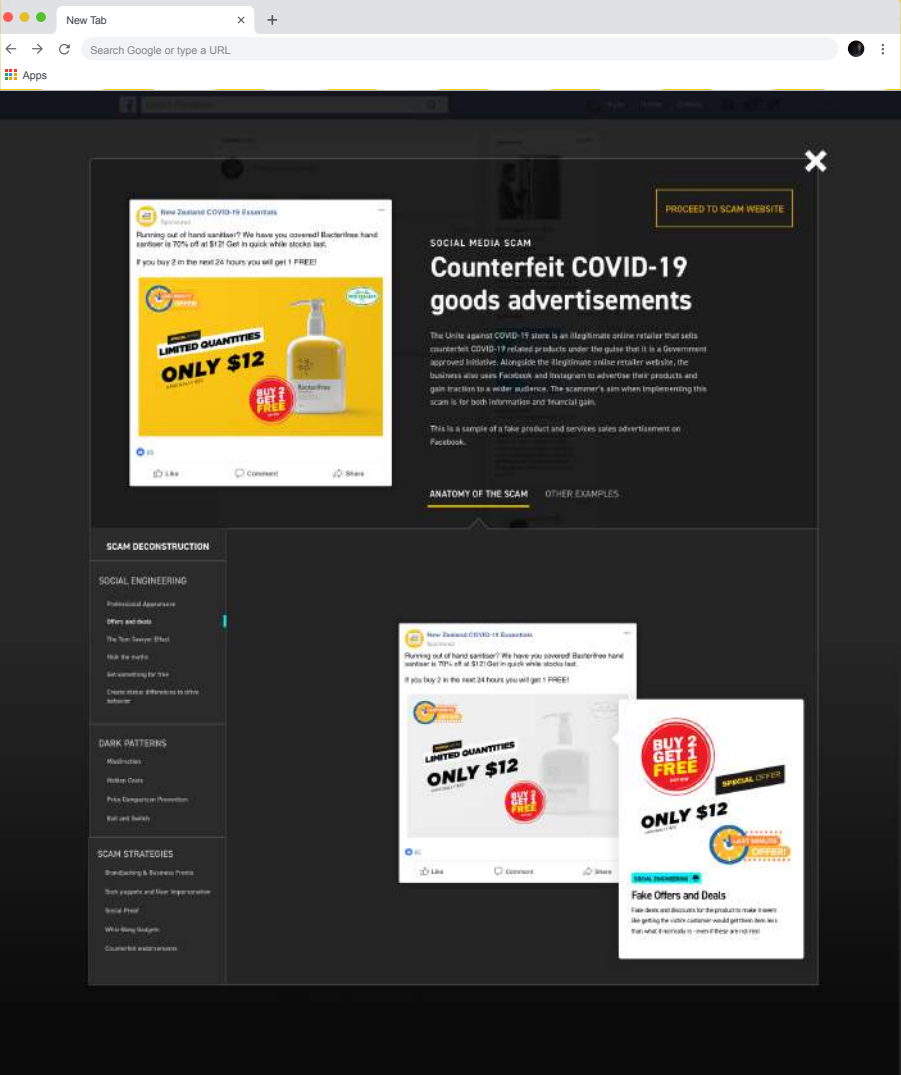


Figure 23. Design of scam analysis tool

The 'Unite against COVID-19' brand has been the core visual impacting image since the pandemic started to enter New Zealand's grounds. From the pull-up banners seen within Jacinda Arden and Dr. Ashley Bloomfield's daily live streamed announcements, posters around major cities, social media platforms and an overarching campaign.

Many government agencies followed and used all or parts of the 'Unite against COVID-19' branding within their own websites. For example, the New Zealand Ministry of Education launched 'Learning from Home' (Figure. 24), a website that provided distance learning support for parents, teachers and students between Early Learning to Year 13, used the Unite against COVID-19 brand colours as their primary homepage header banner (Figure 24)

With a call for businesses to follow, the 'Unite against COVID-19' website provided free to use graphic resources for organisations to use within their social media platforms, websites and physical shop fronts. Retailers started to implement the familiar yellow and white striped branding on their websites to alert and highlight any COVID-19 related information when their customers would visit their platforms.

However, with the simplicity of the brand including the readily available graphic resources that could be obtained, how could scammers use these to manipulate customers into interacting and buying from them? How can the use of brand, layout and colour influence customer assumptions for local products and services?

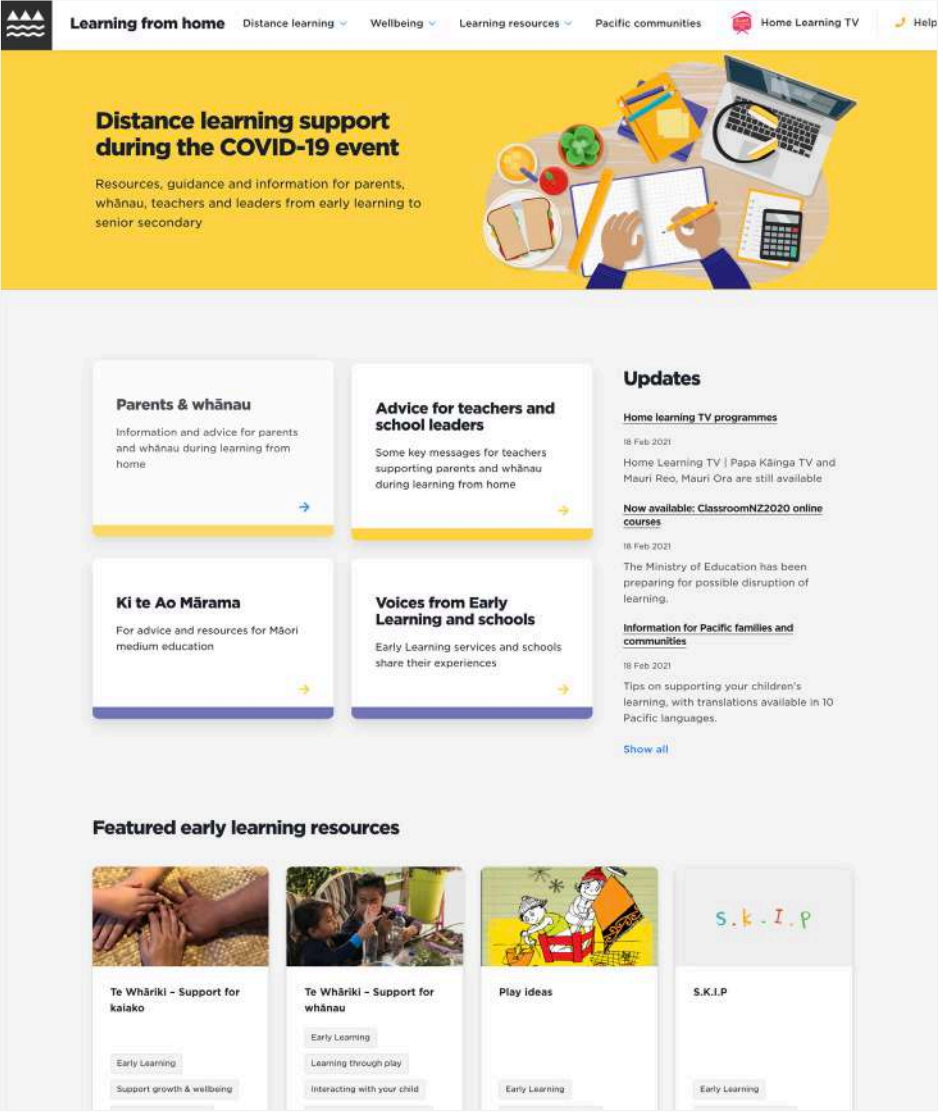


Figure 24. learningfromhome.govt.nz using Unite against COVID-19 branding

Many local companies have followed suit and have used COVID-19 branding to help users navigate COVID-19 information easier. The use of yellow and stripes are used as visual indicators that users automatically associate with and gravitate towards.

This can be seen in (Figure 25) where the NZ Association of registered hairdressers - N.Z.A.R.H. promoted their discounted membership with the aim of promoting their pandemic assistance package helping New Zealand hairdressers during COVID-19.



Figure 25. Screenshot of NZ Association of Registered Hairdressers using Unite against COVID-19 branding for pandemic assistance opportunities

However, some companies are using this technique for organisational gain (financial or increasing their customer base etc.). They will be able to more findable when searching on search engines as they are advertising with keywords such as COVID-19, lockdown and pandemic.



Figure 26. Screenshot of New Zealand Golf Warehouse using COVID-19 as a means to push their sale to more people



Figure 27. Screenshot of Beds4u using sponsored ads and COVID-19 to push their bed sale.

CASE STUDY 1: MIRACLE MINERAL SUPPLEMENT NEW ZEALAND CURING COVID-19

On May 28, 2020, articles on Radio New Zealand and New Zealand Herald reported the online sales of a bleach product, Miracle Mineral Supplement/Solution (MMS) in New Zealand (2020, Strongman). The supplement had been so-called “proven” to cure diseases such as “HIV, hepatitis, acne, cancer, autism and now COVID-19”. Despite Miracle Mineral Solution existing since 2006 (Humble, 2011), the discovery of this New Zealand site advertising the product as a cure for COVID-19 occurred a month after the backlash against United States President Donald Trump’s public advice to inject disinfectant as a cure for COVID-19 (BBC, 24 April 2020).

The seller, a New Zealand “bishop” of the “cult-like American organisation” Genesis II Church of Health and Healing, sells MMS through his online company, NZ Water Purifier Limited, stating on his company website that through dozens of studies, the supplement is safe and “scientifically proven safe for human consumption”.

However, worldwide experts, scientists, health professionals and Medsafe, the New Zealand Ministry of Health medical safety

authority, has broadcasted to potential customers, warning about the dangerous, life-threatening side effects and indicating that these should be avoided.

Despite these messages, the New Zealand Miracle Mineral Supplement website fought back with a dedicated COVID-19 page within their site which discussed “The truth about COVID-19 and chlorine dioxide”. This was an attempt to prove their statement “Fact: Chlorine Dioxide kills COVID-19” explaining that official organisations, such as the American Food and Drug Administration (FDA), were incorrect in their statements.

Many of the sources that the specified page links to only referred to scientific studies of the successful use of chlorine dioxide for COVID-19. However, many of these did not relate to any studies discussing people who had digested the product. 1 of the 4 studies (out of 32) that were showcased for success with digesting the harmful chemical also included a “seemingly well documented and scientifically fact based” video by a biophysicist and known anti-vaccination advocate who “provided” that Chlorine Dioxide cures many diseases, including COVID-19 and autism. On May

29th, 2020, NBC News reported Amazon’s removal of books that promoted “dangerous cures” involving the use of bleach for “autism and other conditions” including COVID-19.

The FDA is stated to be “responsible for protecting the public health by ensuring safety, efficacy, and security”. They are the national standard in the United States of America that evaluate and approve of “drug products on the basis of safety and effectiveness” which is also trusted by international medical agencies around the world. As they are the lead organisation which handles the approval of drug products that go out to the public within the United States of America, they have a wide knowledge and understanding of all approved drugs that exist - not just specific ones or specific categories. While the FDA have stated that they “are not aware of any scientific evidence supporting the safety or effectiveness of MMS products”, they have detailed lethal adverse effects that people have experienced and reported such as life-threatening low blood pressure, acute liver failure, severe vomiting and diarrhea etc.

Why should non-qualified professionals who share no relations to the medicine and pharmaceutical industries can market, sell, and provide these products while claiming to be legitimate? If the FDA

have been actively warning against the use of chlorine dioxide and bleach for “cures” against illnesses such as COVID-19 and have not approved of the product, there are reasons why the product has fallen short when meeting the standards of other approved drug products.

Another question this poses is if there is any reasoning as to why the website cannot be forced to cease? Yes, there is nothing forcing the creators to shut the site down, then stand another one back up in its place, but if this product has been recognised as dangerous to consumers by official government agencies, then why can’t it be shut down instead of keeping it still standing for years?

The organisation owns two separate sites:

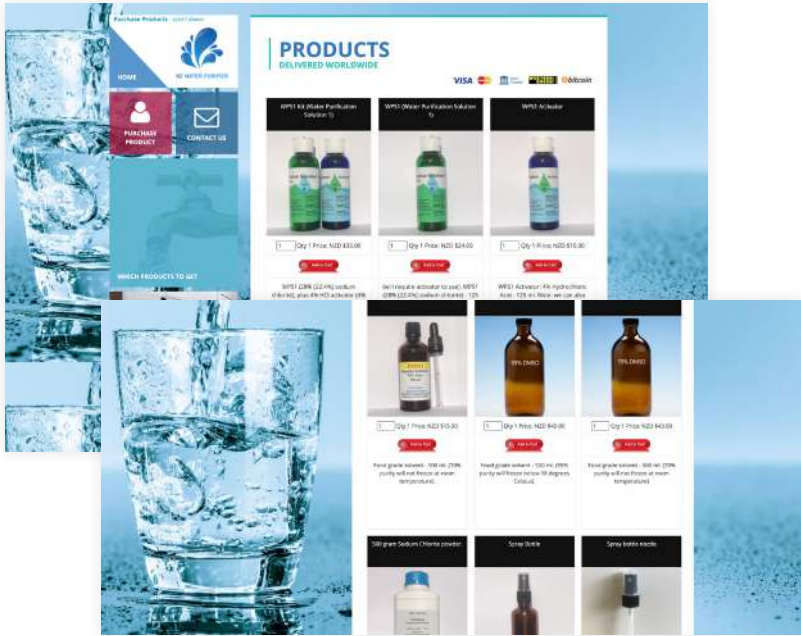


Figure 28. Screenshot of NZ Water Purifier Limited's website (2020)

NZ Water Purifier Limited (nzwaterpurifier.com)

Their first website focuses on selling the bleach supplement product and additional accessories offer 5 different products (originally 19 at the start of the research). These products range from Water Purification Solutions, Alternative WPS1 Activators, Chlorine Dioxide Solutions, Dimethyl sulfoxide solutions, Sodium Chlorites and gelatin capsules.



Figure 29. Screenshot of Miracle Mineral New Zealand website (2020)

Miracle Mineral New Zealand (miraclemineral.co.nz)

Their second website focuses on providing information about Miracle Mineral Supplement, why the product is proven to work and what it 'cures', it's success including stories, information on how to obtain the product and buy the online video course on how to make the cures at home.

FROM A DESIGN PERSPECTIVE THESE SITES:

- Lack a strong visual brand
- Are messy and visually unprofessional looking websites

NZ Water Purifier Limited

Uses a picture of water as the site's background which feels random and unprofessional. The way the products are advertised lack information on the product, text used to sell the product and the title of the product are just the ingredient names (without prior knowledge about this 'cure' it would be difficult to know that the product is a 'cure' based on just the ingredients listed).

Miracle Mineral New Zealand

A large information dump that is hard to navigate. The homepage is a mix of trying to sell their products, prove the product's success, and prove that official organisations are wrong while throwing screenshots of proof. Success stories list positive experiences about using MMS as a product, but as these are listed within the site there is no proof that shows that this feedback is legitimate.

- Products being sold have weak marketing imagery (lousy quality and bland sales photography to market the product), packaging design and sales strategy.
- Lack of marketing and sales-like written content.
- Lack of trustworthy organisations or figures who promote the product.

QUESTION RAISED

But what if these had been designed better with proper design thinking, visual design and marketing strategy behind them? Would they look more legitimate to fool consumers even with a lack of knowledge about the controversies surrounding bleach as a cure for COVID-19. How could design be used to emphasise product positives while hiding it's negatives and red flags?

CASE STUDY 2: HAYLEY HOLT SKIN CARE AND ESSENCE OF ARGAN SCAM

January 2019 saw New Zealand presenter Hayley Holt advertised on social media to be leaving the popular morning news show, Breakfast to focus on starting her own beauty skincare company (Higgins, 2019). Many fans of the presenter were sad to see her leave Breakfast, but were excited to learn about the free samples of her new face cream she was giving to her fans through Facebook and online store. Just pay for shipping and everything else is free – but was it too good to be true?

It wasn't until customers of the alleged beauty company discovered the unexpected deduction of hundreds of dollars from their bank accounts (Higgins, 2019). How could Hayley Holt do this to them: a local celebrity figure they grew to trust after watching her every morning on TV media? Holt addressed the situation both on Breakfast and on its social media platforms stating, "I am not leaving Breakfast and I absolutely do not have a skincare cream". This left fans and customers feeling manipulated and humiliated, fooled to fall victim to such a scam. While the Breakfast team have been investigating and handling the situation legally, Holt (2019) has voiced the struggle of impersonation scams as being like "whack-a-mole... you take one down, and another pops up at a

different web address".

TVNZ later exposed the company behind the Hayley Holt skin care scam was found to be Essence of Argan - a beauty products company originating "apparently from Malta" that catches unsuspecting victims who admire Hayley Holt, by advertising free samples on social media (Higgins, 2019). What many victims miss while interacting with the company is a small hidden disclaimer in the fine print that if the samples are not returned within a short timeframe, they would be charged for every month they are not returned.

While a scam, Essence of Argan visually looks and acts like any other online beauty products company holding an established brand used throughout their visual content and platforms, visually appealing products, legitimate-looking website and social media platforms and well written marketing copy that sell the product. Despite how convincing Essence of Argan looks and feels, the disappointing reviews tell another story.

Company behind Hayley Holt face cream scam exposed

GILL HIGGINS, FAIR GO REPORTER
MAY 7, 2019 • SOURCE: FAIR GO



It boasts offices in several countries, with a headquarters in Malta. Its call centre staff are polite and well-spoken, claiming the company's operations are totally legitimate. But it's leaving a trail of furious customers, and has celebrities the world over crying foul play.



Welcome to the world of Idratherapy and Essence of Argan. Warnings about signing up to free trials of these beauty products have been circling for years.

Yet when Hayley Holt became one of the latest celebrities whose image was falsely used to advertise the beauty products, dozens – maybe hundreds, or even thousands – of Kiwis fell for the line about a free trial.

Figure 30. Media article on Hayley Holt's face cream scam exposed (2019)

DESIGN EXPERIMENT

The Unite against COVID-19 store is an illegitimate online retailer (designed by the researcher as part of this design experiment) that sells counterfeit COVID-19 related products under the guise that it is a Government approved initiative.

Products that are sold on the store include:

- COVID-19 preventative health products (skincare, vitamins disinfectant, face masks etc.)
- COVID-19 cleaning products (disinfectants)

This store states that it has been approved as a retailer that sells essential goods during Alert Level 3. Purchases that are bought online in this store are labelled to take 3-7 business days (but warns of longer wait times because of COVID-19). However, these purchases are never intended to be followed through by the scammer, and in the end, customers never receive them.

The scam takes advantage of the lack of supply and high demand of these products due to the panic buying of New Zealand customers.

Alongside the illegitimate online retailer website, the business also uses Facebook and Instagram to advertise their products and gain traction to a broader audience. The scammer's aim when implementing this scam is for both information and financial gain.

This design experiment will visualise and demonstrate the process and use of visually enhancing scam products, particularly COVID-19 miracle cures, with better product designs and implementing trusted figures and organisations to sell these products falsely. This design experiment will not use the names of MMS and NZ Water Purifier Limited within the experiment to minimise the usage of these designs to benefit these organisations.

EXPERIMENT 1: COUNTERFEIT COVID-19 PRODUCT SCAMS CYBERCRIME MODEL

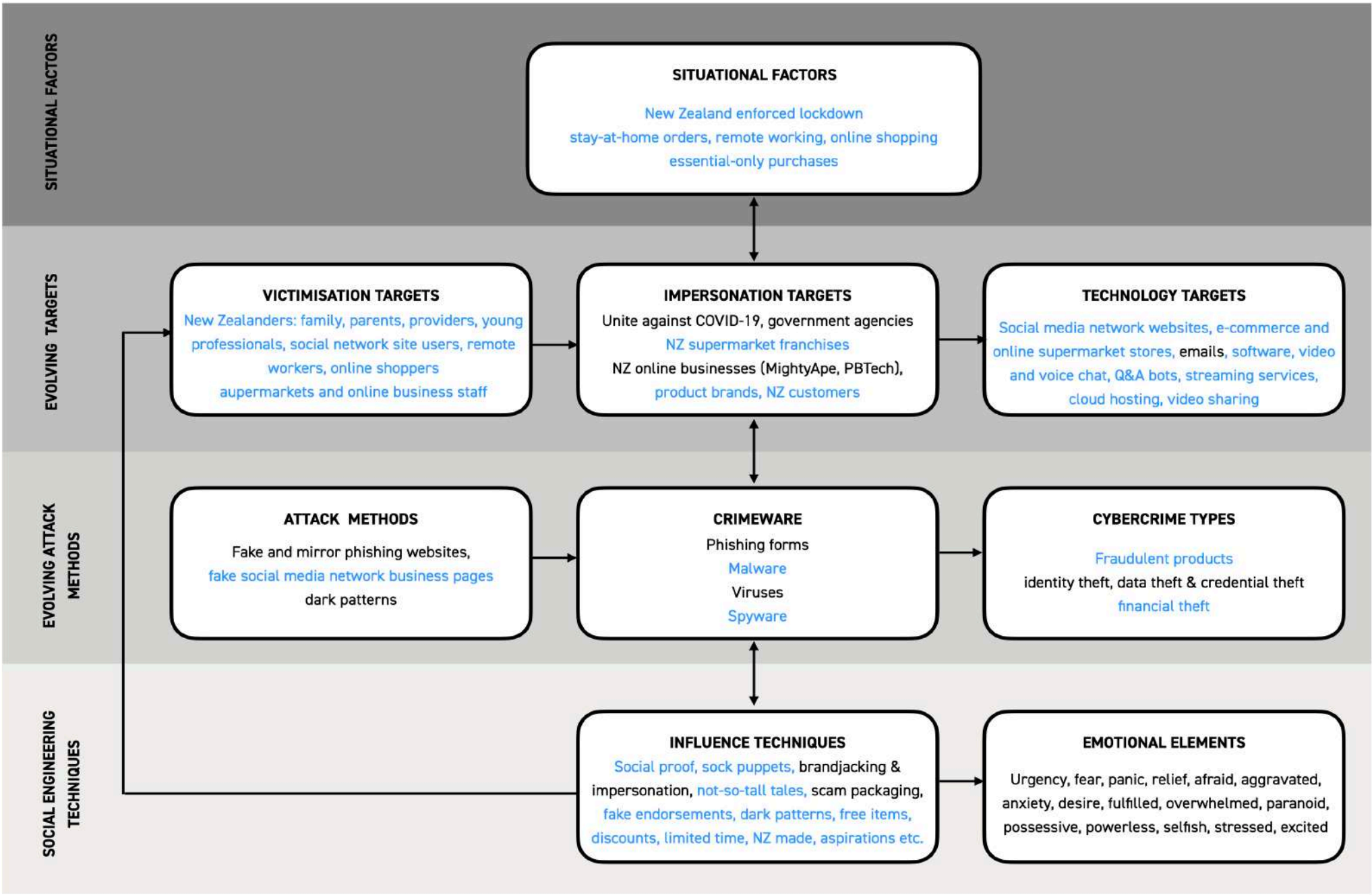
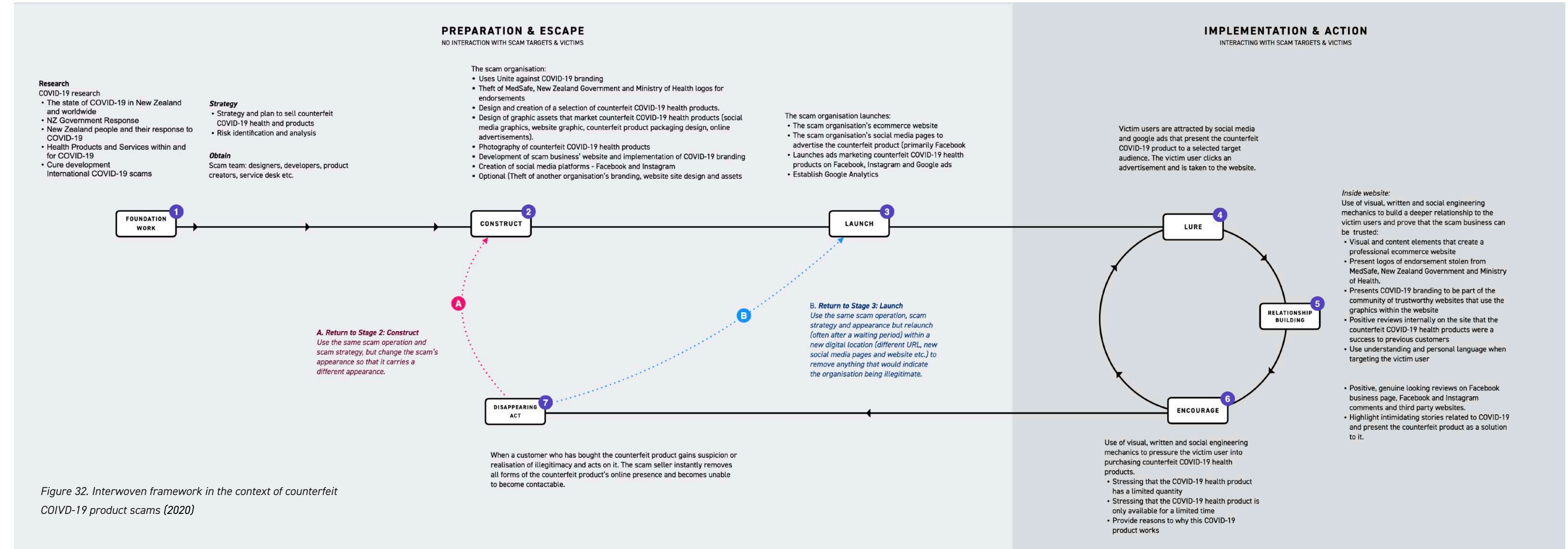


Figure 31. Naidoo's Multilevel model of cybercrime in the context of counterfeit COVID-19 product scams (2020)

EXPERIMENT 1: COUNTERFEIT COVID-19 PRODUCT SCAMS PROCESS (INTERWOVEN FRAMEWORK)



EXPERIMENT 1: SCAMMER-VICTIM EXPERIENCE MAP - COUNTERFEIT COIVD-19 PRODUCT SCAMS

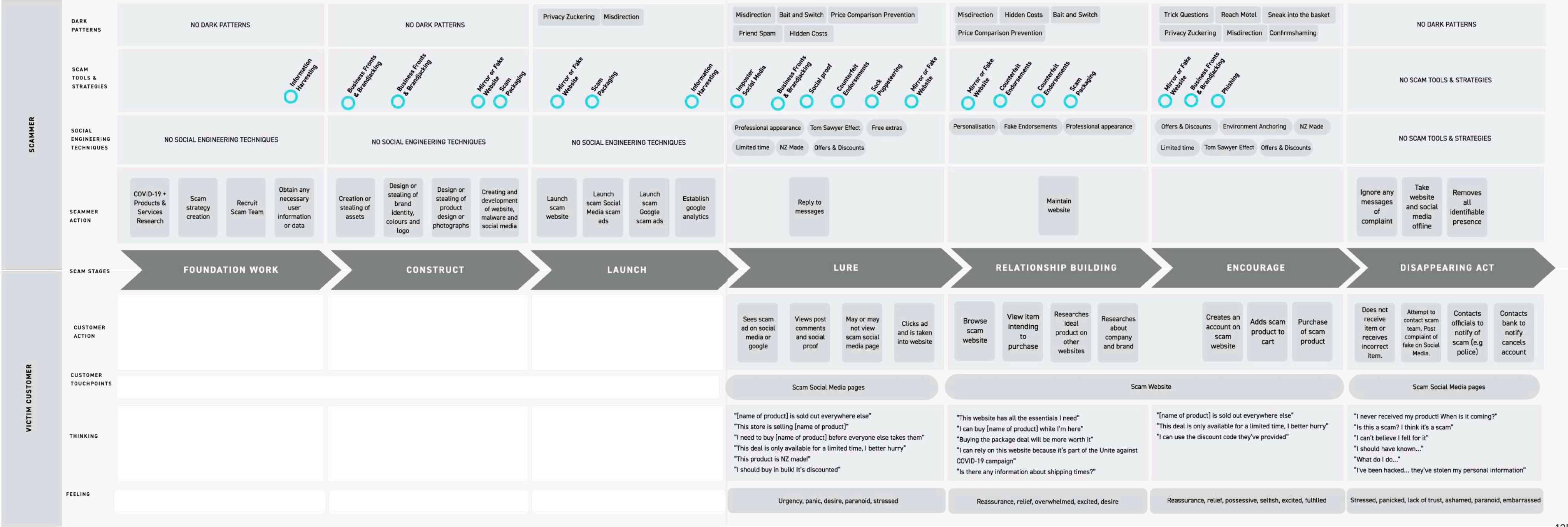


Figure 33. Unique Scammer-Victim experience map created to capture the context of counterfeit COVID-19 product scams (2020)

SCAM STRATEGIES
What scam strategies
are within the counterfeit
product sales scam?

DARK PATTERN	APPLICABILITY		HOW CAN THE SCAM TOOL BE USED?
	SCAM SOCIAL MEDIA	SCAM WEBSITE	
Sock Puppeteering and User Impersonation	✓	✓	<i>Location: Social media comments (highly common)</i> The scam retailer generates several sock puppet accounts, which leaves positive reviews, visualising the external perspective that the seller of the counterfeit COVID-19 product, social media platforms and website are positively trustworthy.
Business Fronts & Brandjacking	✓	✓	<i>Location: Scam brand identity and visuals (highly common)</i> The scam seller takes advantage and makes use of the already existing Unite against COVID-19 branding and implements within the counterfeit product, it's website and social media platforms.
Information Harvesting	✗	✗	The scammer doesn't need to go out of the way to find the information as the scammer is actively giving it to them.
Not-So-Tall Tales	✓	✓	<i>Location: Scam advertisement post texts on social media (highly common)</i> The counterfeit COVID-19 product is advertised with marketing text that details a problem of which the victim user can relate to or tells a tale of a previous customer who has benefited from using the counterfeit product.
Whiz-Bang Gadgets And Offers	✓	✓	<i>Location: The product (highly common)</i> The counterfeit COVID-19 product is advertised with marketing text that details a problem that the victim user can relate to or tells a tale of a previous customer who has benefited from using the counterfeit product.

DARK PATTERN	APPLICABILITY		HOW CAN THE SCAM TOOL BE USED?
	SCAM SOCIAL MEDIA	SCAM WEBSITE	
Mirror And Fake Websites	✗	✓	<i>Location: Scam website (highly common)</i> The scam website houses counterfeit COVID-19 items that will be sold on it. While the website looks like it's aim is to sell legitimate-looking products, it provides a number of opportunities to steal from the victim.
Counterfeit, official-looking documents and endorsements	✓	✓	<i>Location: On product packaging and product imagery (highly common)</i> The COVID-19 counterfeit product includes official-looking endorsements, badging or stolen logos of official organisations used for endorsement without the original logo owner's permission to emphasise official-ness and trustworthiness.
Scam Packaging	✓	✓	<i>Location: Scam website and scam social media platforms (highly common)</i> <i>The scam package contains two steps:</i> Scam social media platforms where the scam seller advertises the counterfeit product or service <ul style="list-style-type: none">Scam website where the victim user can purchase the scam product or service
Phishing	✗	✓	<i>Location: Sign up forms, login forms, purchase forms, mailing list forms (Highly common)</i> The scam website is disguised as a legitimate COVID-19 store website where the victim user must fill in a form (sign up for an account, newsletter, contact seller, deals and offers etc.) to receive content or access the site further - yet the scam seller is stealing the information they provide.

DARK PATTERNS

Which dark patterns are within the counterfeit product sales scam?

DARK PATTERN	APPLICABILITY		HOW CAN THE SCAM TOOL BE USED?
	SCAM SOCIAL MEDIA	SCAM WEBSITE	
Trick Questions	✗	✓	<i>Location: Scam website forms and data input</i> Trick questions are used within the scam website where the victim user must fill in a form (sign up for an account, newsletter, contact seller, deals and offers etc.)
Sneak in to the Basket	✗	✓	<i>Location: Scam website ecommerce store basket</i> When purchasing a scam product or service, the website tries to sneak additional scam products or services into the victim user' basket.
Roach Motel	✗	✓	Location: Scam website sign up The scam website requires a login to access or purchase items. It may be difficult for the victim user to get their account deleted off the website after they have created it.
Privacy Zuckering	✗	✓	<i>Location: Website terms and conditions</i> The scammer hides small print information within the form or site terms and conditions that allow them to use and sell any information and data that the victim user has been persuaded to give e.g. through forms.
Price Comparison Prevention	✓	✓	<i>Location: Scam website ecommerce store, social media advertisement posts</i> Creates multiple variations of a counterfeit COVID-19 product within the scam website's store (e.g. bundles) to make customers feel they are getting a better deal when it is the scam seller who is.
Misdirection	✓	✓	<i>Location: Scam product service visuals and graphics</i> Uses visually appealing images to distract the user from any hints or details that would identify the seller or COVID-19 product being sold to be illegitimate.
Hidden Costs	✓	✓	<i>Location: Scam website ecommerce store, terms and conditions</i> The scammer could include extra one-off or ongoing hidden costs within the scam website's terms and conditions, product small print or within the ecommerce store shopping basket.

DARK PATTERN	APPLICABILITY		HOW CAN THE SCAM TOOL BE USED?
	SCAM SOCIAL MEDIA	SCAM WEBSITE	
Bait and Switch	✓	✓	<i>Location: Scam social media product advertisement post, scam website product page</i> The COVID-19 product is advertised as one thing on social media advertisements, but when the user proceeds on to the product's website, it is on sale as a different product. Alternatively, the product can also be advertised as one thing on social media advertisements and the product's site, but it is entirely different when the customer receives the product.
Confirmshaming	✗	✓	<i>Location: Scam deals, offers, mailing list, ecommerce basket</i> When the scam COVID-19 website store provides deals, sales, offers to keep in touch, if the user decides not to take it, the site uses guilt-inducing text to doubt exiting out of the offer. This also includes if the user decides not to proceed with the purchase
Disguised Ads	✗	✗	While it is possible for the seller to use this dark pattern within their scam COVID-19 website store, chances of it being used are more unlikely as this may conflict with the scam products on the website that is intended to be purchased. The victim seller may be confused and the possibility of finding details that highlight the site's illigitmacy may be uncovered.
Forced Continuity	✗	✓	<i>Location: Billing, account settings</i> The scam COVID-19 website store can also provide scam subscriptions with their product. The scam seller will make it difficult for the victim to cancel (or be unable to at all) the seller could continue to charge for the subscription even if they altogether remove their existence online.
Friend Spam	✓	✓	<i>Location: Account login / sign up, social media permissions.</i> The scam website asks permission to log in / sign up or access certain information through their social media accounts or email. While the site may say that it won't use private information, the scam site and seller may lie about this.

DESIGNING A FAKE BRANDS

Creating two fake brands to use for the scam campaign, fake products and fake websites.



Figure 34. Fake brand design iterations: Bacterifree

Bacterifree (Bacteria + free) is a scam brand that initially drew inspiration from “cleaning product” impact styled logos that are flexible on a family of products, but settled on a more simplistic brand. Minimalistic brands are a trend that many health care products use, giving the “natural ingredient” vibe.

ELIXIR OF HEALING



SERUM THAT HEALS ALL

Figure 35. Fake brand design of Elixir of Healing

Elixir of Healing draws inspiration from malcious bleach “can cure all” products. However, the addition of visually expensive and classy branding could change the perception of potential customers.

PACKAGING DESIGN OF FAKE COVID-19 HEALTH PRODUCTS

Iterating on a series of packaging designs that could be used on several types of health products on Sketch app, Adobe Illustrator and Photoshop. I can use COVID-19 branding because on covid19.govt.nz it clearly states all content on covid19.govt.nz is licensed for re-use under a Creative Commons 4.0 Attribution Non-Commercial International Public Licence. However, outside of this research a scammer would take content with no regard to licenses.

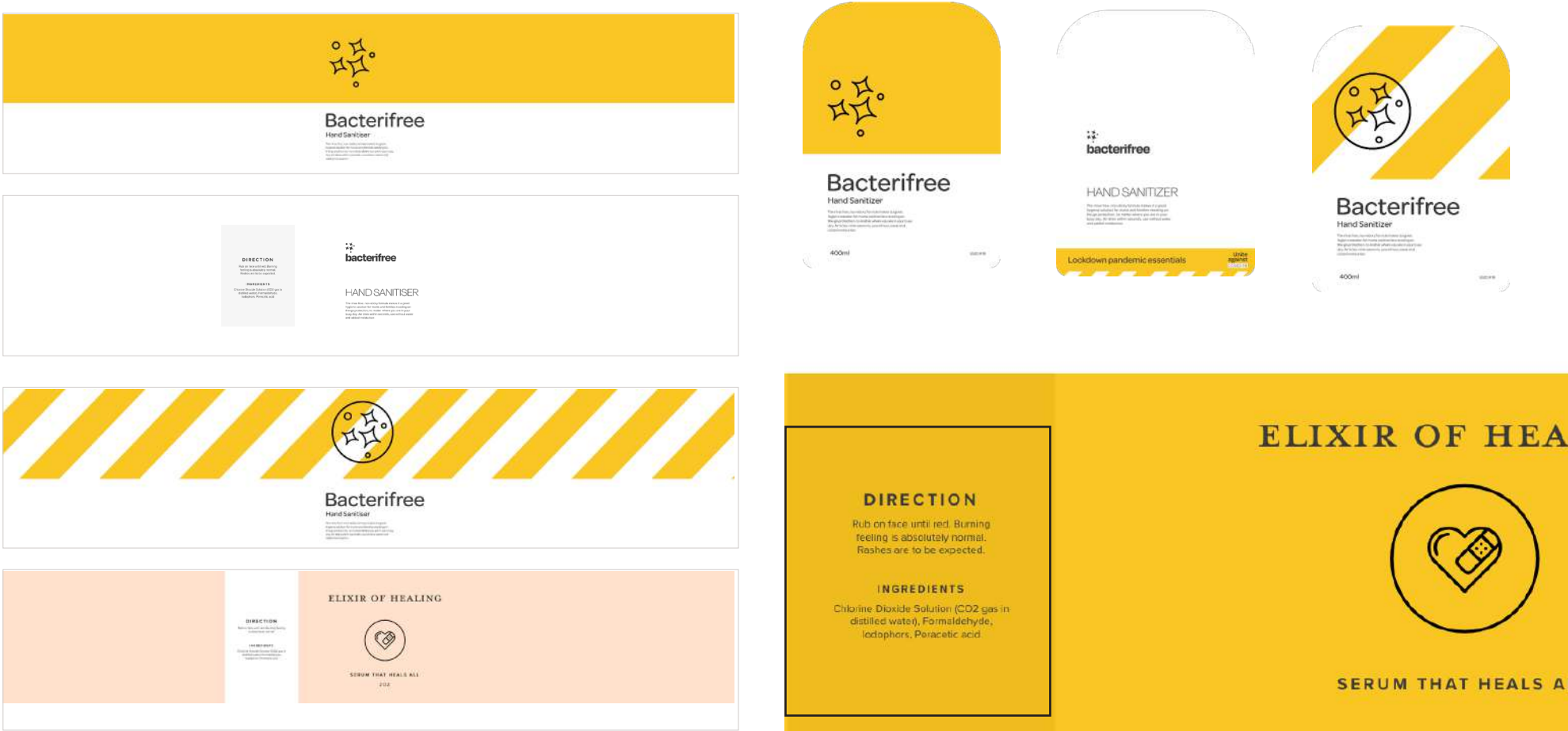


Figure 36. Fake brand design iterations

Use visual design to misdirect attention away from the deadly details.

RECREATION OF COMMONLY ASSUMED APPEARANCES OF ‘SCAM HEALTH PRODUCTS’

Exploring Adobe Dimension by creating product visualisations of the types of packaging that common customers would potentially judge as being scams. I first experimented creating “obviously fake” scam products with weak brands before I started working on more believable scam products. These weak branded scam products were based off Miracle Mineral Supplement’s real products.



Figure 37. Render of “Scam cream” iteration
Figure 38. Render of “Scam drink” iteration
Figure 39. Render of “Scam medicine pills” iteration

CREATING THE FAKE PRODUCTS

I then did further iterations on a number of fake products using the created fake brands on Adobe Dimension. Using design and branding elevated these scam products to look more legitimate. I took inspiration from existing brands found in pharmacy stores and supermarkets, such as QV and Aveeno. I used soft, clean and natural colours such as light greens and pinks, before taking the yellow, commonly associated with COVID-19 and adding it to the design to create an official and professional look.



Figure 40. Render of initial Elixir of Healing Cream
Figure 41. Render of final Elixir of Healing Cream - pink
Figure 42. Render of final Elixir of Healing Cream - COVID-19 yellow
Figure 43. Render of Bacterifree, COVID-19 themed Tissue Paper
Figure 44. Render of Bacterifree COVID-19 themed hand sanitizer
Figure 45. Render of regular Bacterifree hand sanitizer

Once I had completed creating the fake scam products, I started creating advertisement graphics that would showcase the products in an attractive light that would capture the attention of potential scam victims.

This included staging them further onto mockups, writing catchy marketing content with guidance of the scam techniques referenced from the initial research investigation.



Figure 46. Mockup iteration of fake scam website's custom pack

Finally, I iterated on creating a series of social media posts combining scam advertisement graphics with catchy marketing text within the post. Writing content for these posts was also written with guidance from the scam techniques referenced from the initial research investigation.

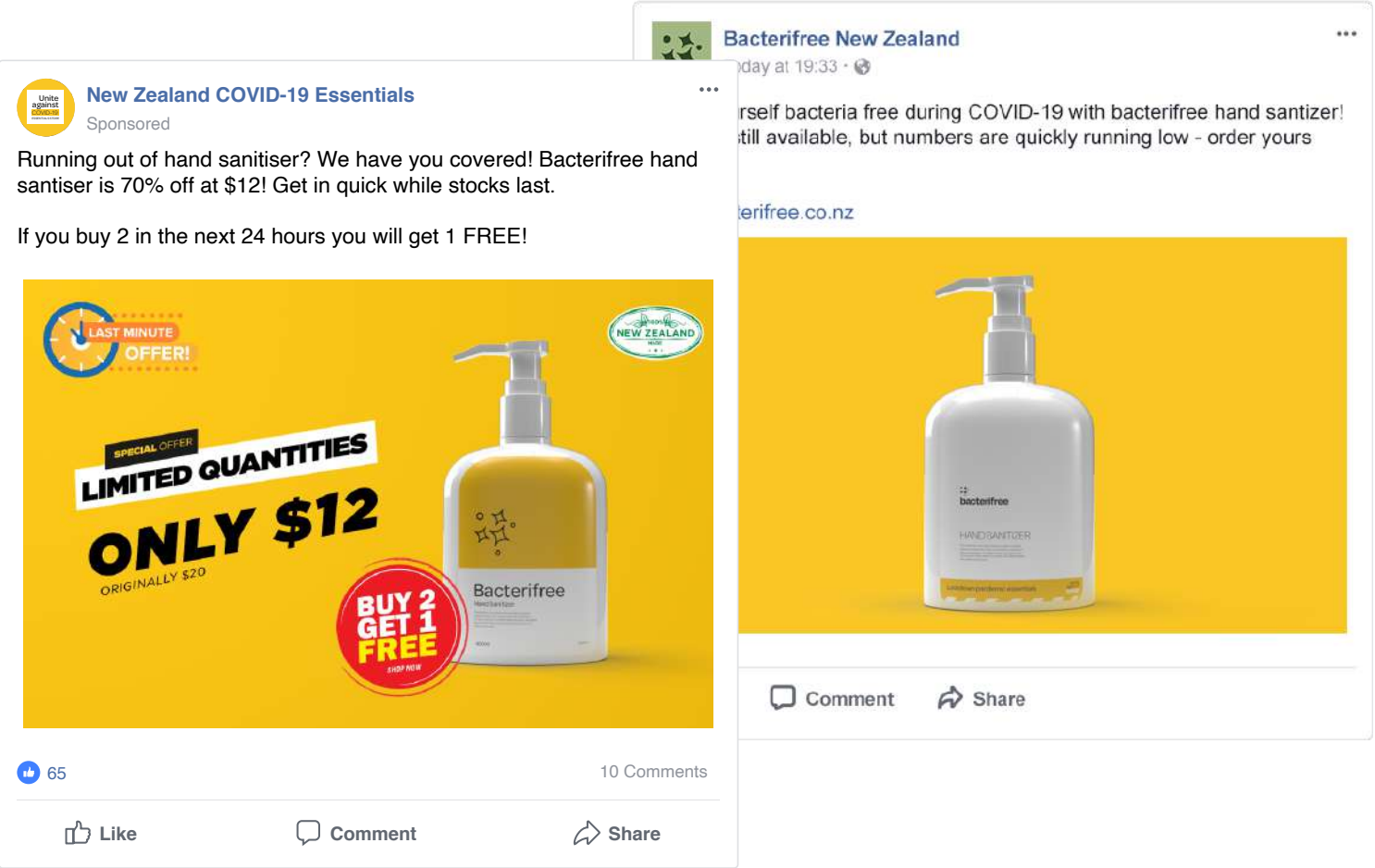


Figure 47. Design iterations of social media posts

A



Which hand sanitiser looks trustworthy?

B



A



Which hand sanitizer would a New Zealander most likely notice during COVID-19?

B



Figure 48. Product design comparisons

ENHANCING A WEAK ONLINE PRODUCTS & SERVICES SCAM



Figure 49. Obvious bad design scam product

A badly slapped together product scam that carries similar traits to other product scams that have very little design or marketing considerations.

Many scams are visually unattractive, use default go-to fonts such as Times New Roman - particularly physical cosmetic and medical product scams.



Figure 50. Improved design scam product

In which simple design elements have been applied to enhance the visual appeal of the product. Copywritten marketing text has been added to the social media post to provide a more realistic reproduction of a marketing post.



Figure 51. COVID-19 themed scam product

In which 'Unite against COVID-19 branding' has been applied to the product, including the predominant yellow and white stripes, iconography style and font.

However, the use of the yellow and white stripes with the aim of making a profit has been called out and frowned upon within New Zealand media, therefore using the stripes added onto the post. As there have been no official announcements of products by the brand, this would have a higher chance of being caught out.



Figure 52. Subtle COVID-19 scam product

Simplifying the previous iteration of the design that uses 'Unite against COVID-19" branding, removing the stripes but leaving the yellow and white split, the same font and use iconography.

The approach is kept similar to 'Unite against COVID-19" branding, but a minimalistic style quite similar to other cleaning and cosmetic items is used, thus cannot be accused as a direct copy.

EXPERIMENT SITE MAP

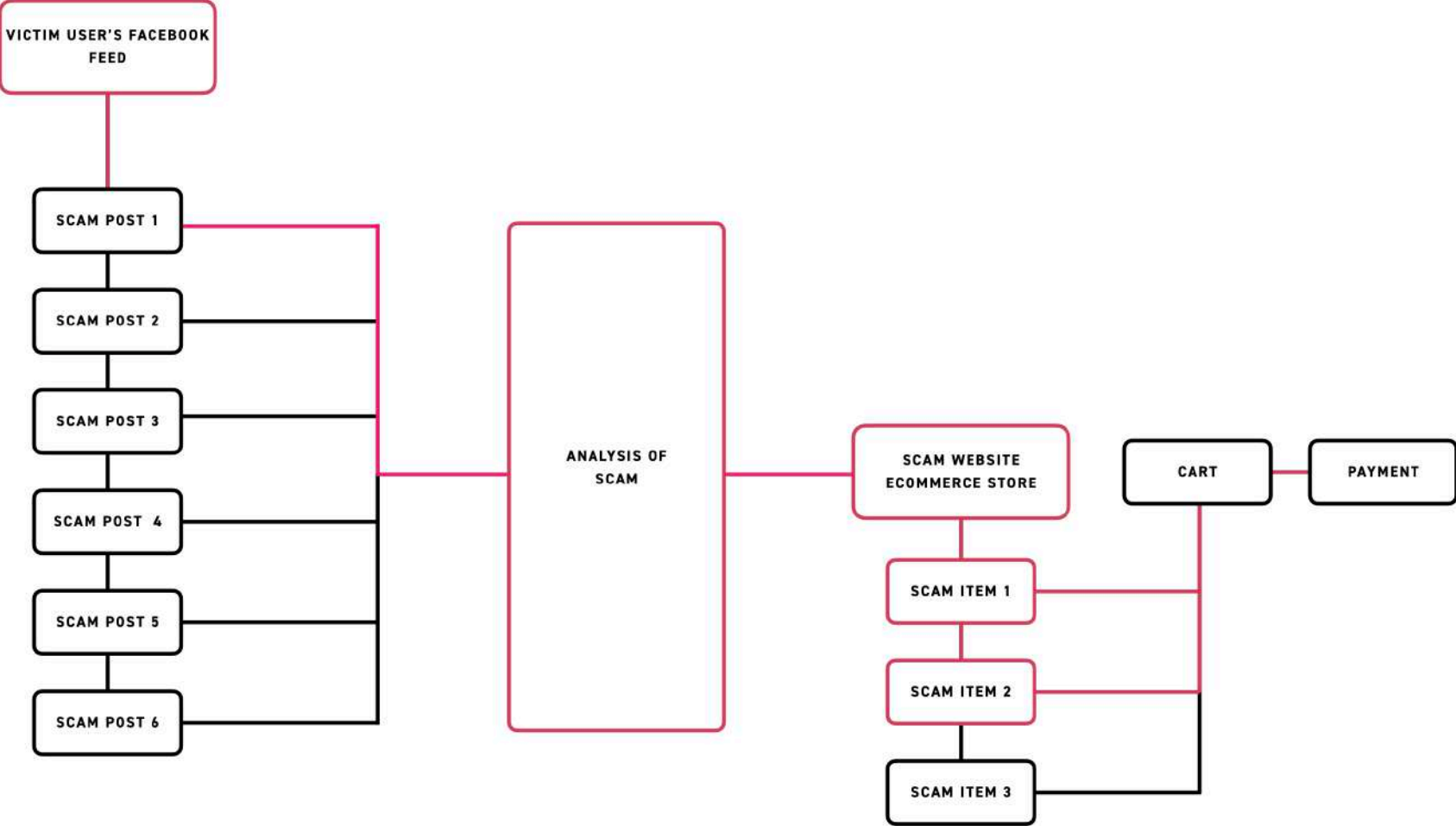


Figure 53. Sitemap and user interaction for Experiment

WIREFRAMES OF SCAM WEBSITE DESIGN

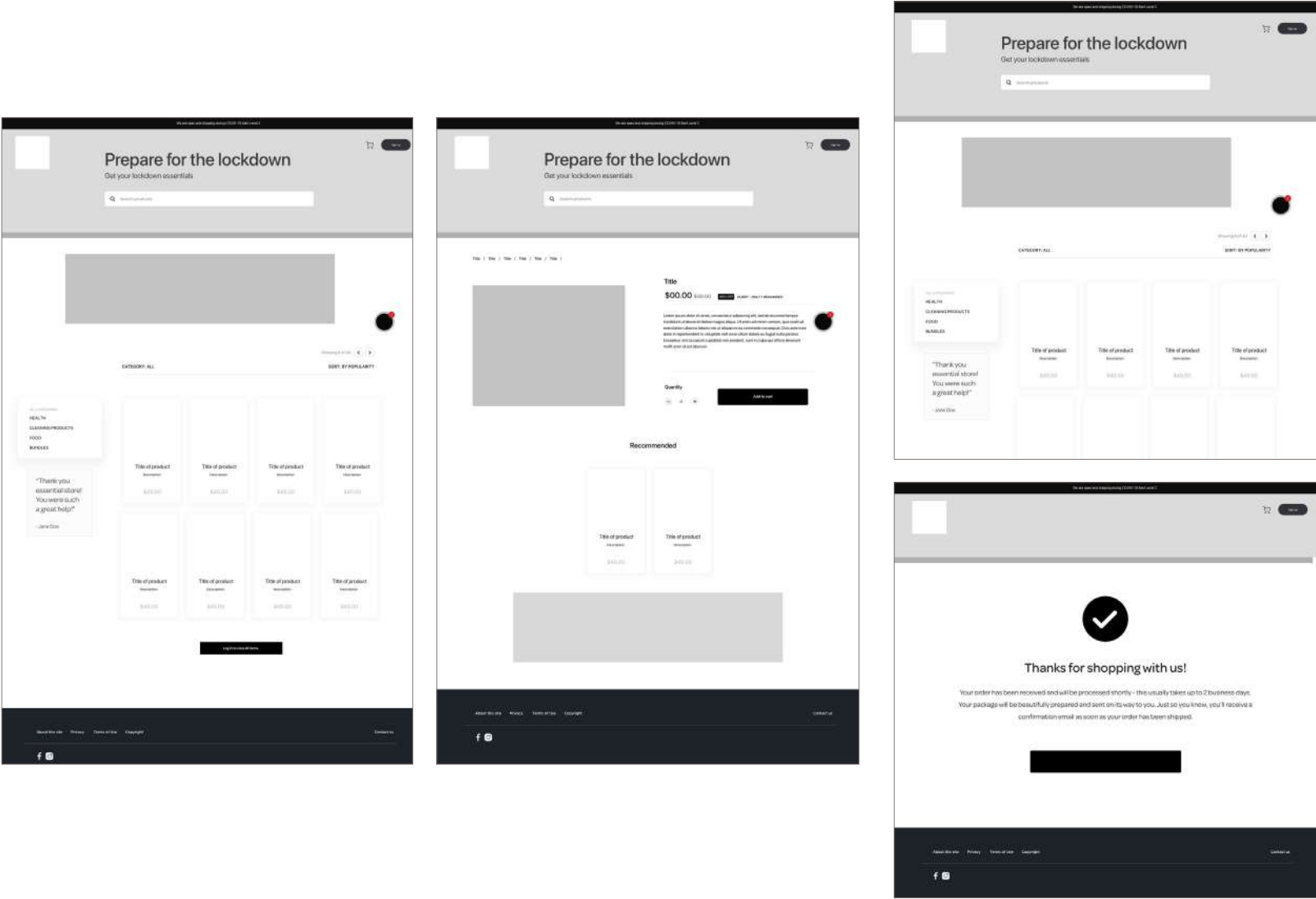


Figure 54. Hi-fi wireframes for scam website

RECREATION OF FACEBOOK WITH SCAM ENVIRONMENT IMPLEMENTED

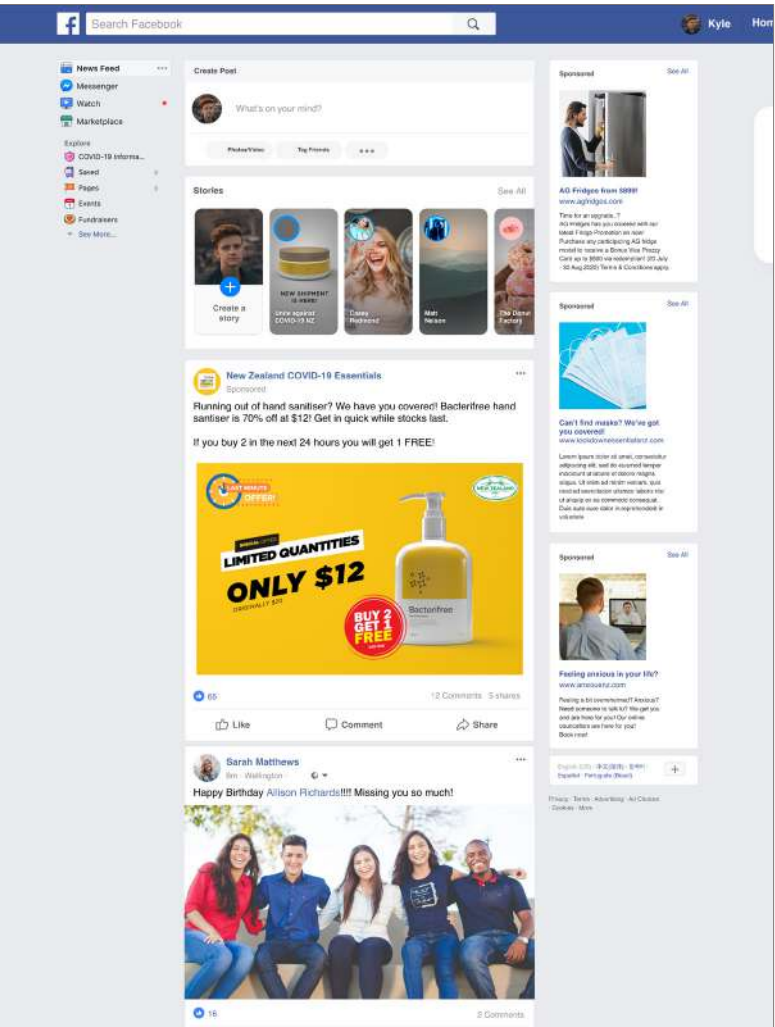


Figure 55. Design experiment starting prompt

Upon entering the interactive experience, the user is prompted to find all the scams

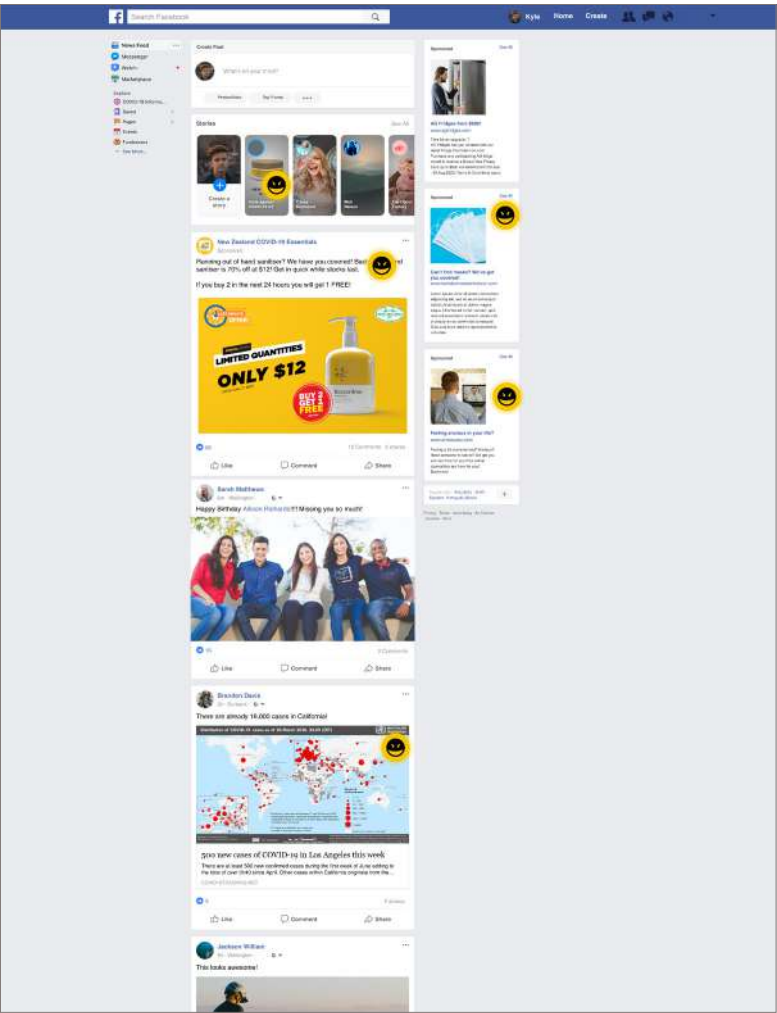


Figure 56. Design experiment Facebook scam environment

The user must try and find the scams that are hidden on the website.

SCAM ANALYSIS TOOL

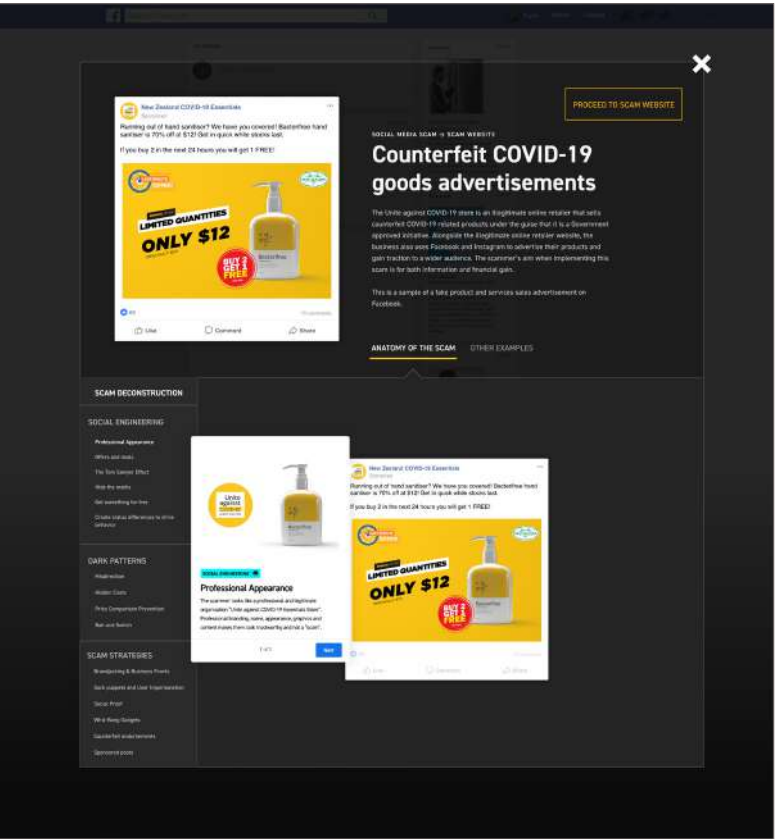


Figure 57. Scam analysis of counterfeit product ad

Upon selecting the scam, an overlay and analysis tool appears on the screen allowing the user to interact and deconstruct each element of the scam.

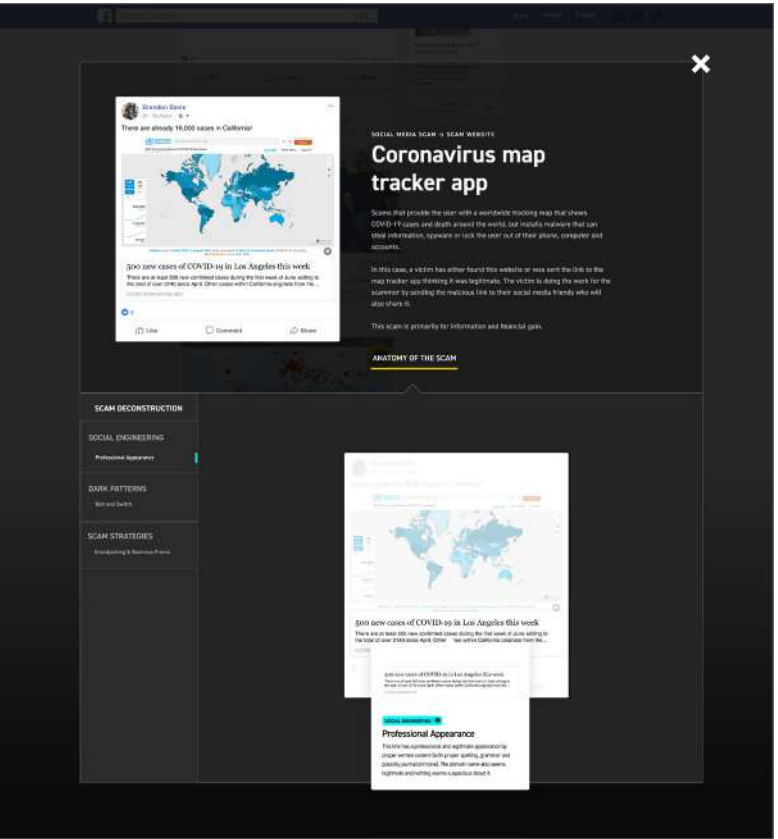


Figure 58. Scam analysis of fake COVID-19 tracker

On the Facebook scam environment there are a select number of scams with a variety in scam complexity. This is to help users to experience that not all scams are the same and that some are more complex than others.

DECONSTRUCTING A SCAM STORE

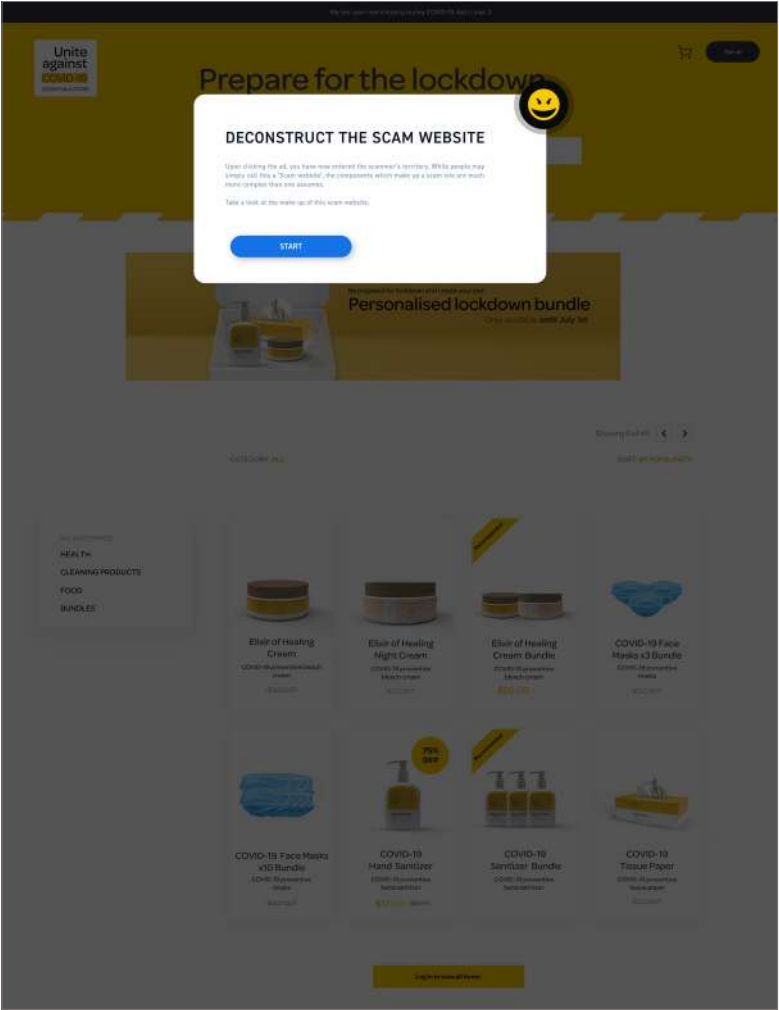


Figure 59. Scam store starting prompt

For one of the scam ads, one will lead to a scam products store which will let users to do the same.

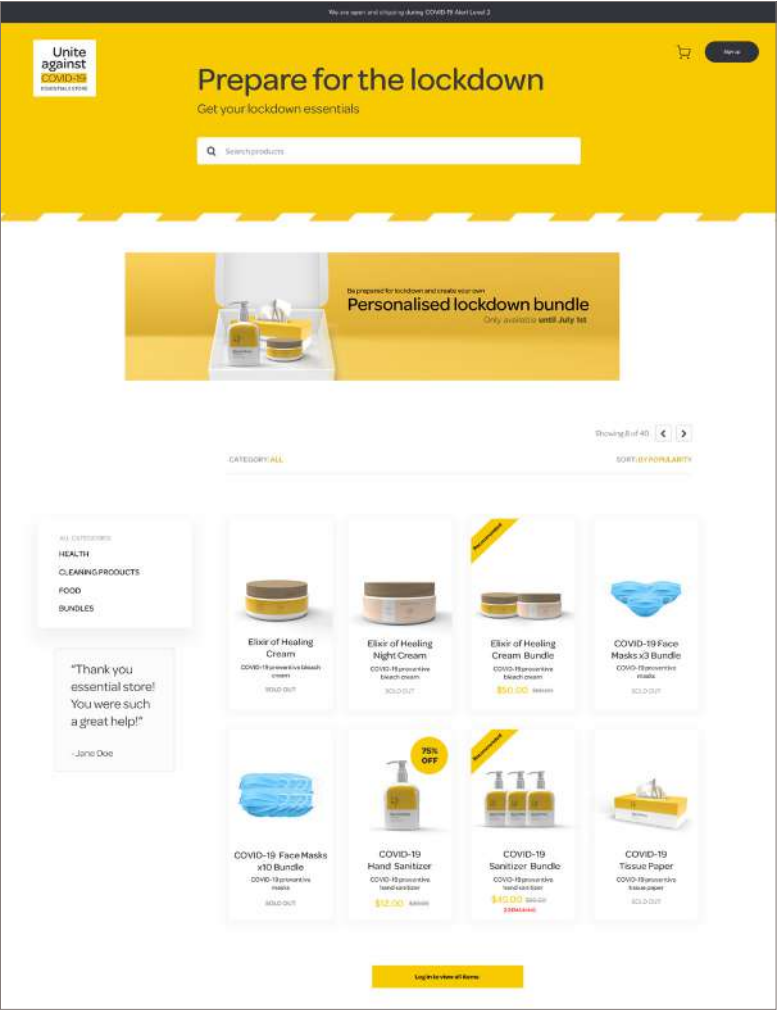


Figure 60. Scam store design

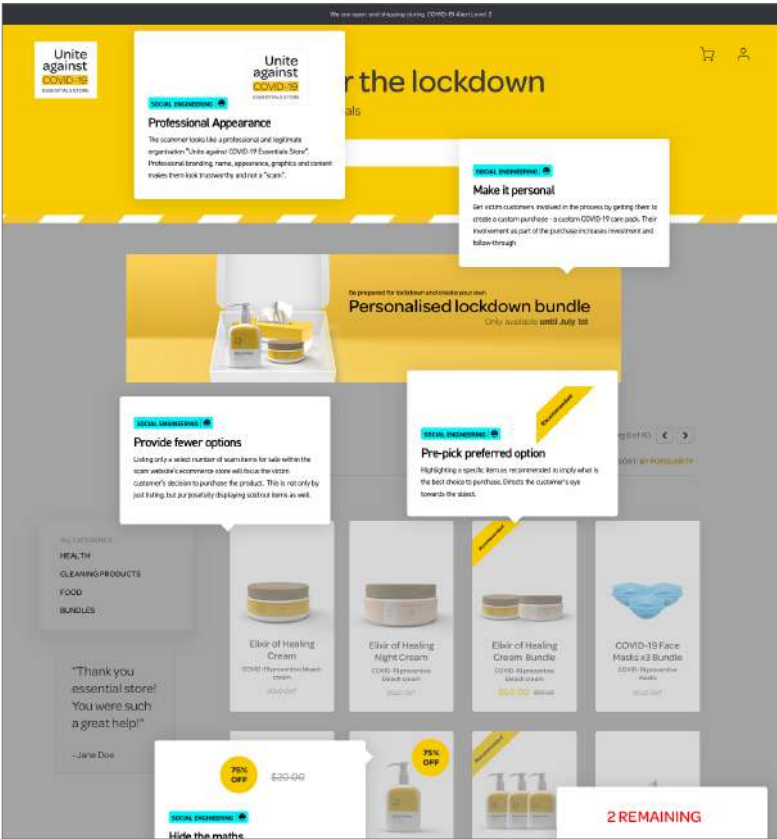


Figure 61. Scam website deconstructed

Disguised as a chatbot helper, will give the user the ability to deconstruct the entire website by types of scam mechanics.

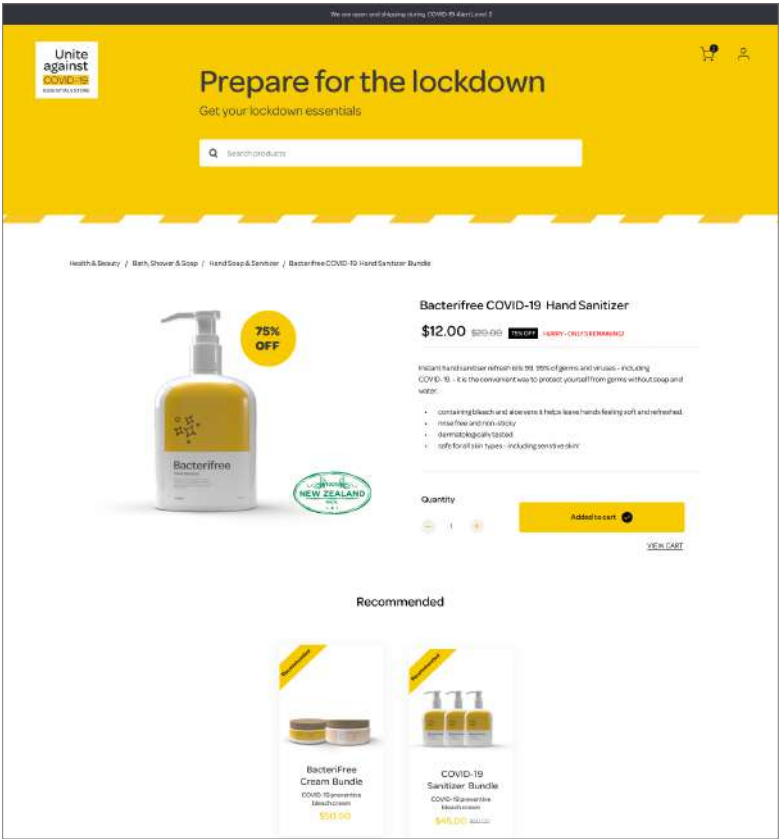


Figure 62. Scam website item page

The user will be able to navigate through the website from home page all the way to buying the scam product and will be able to see how the scam is built on every page.

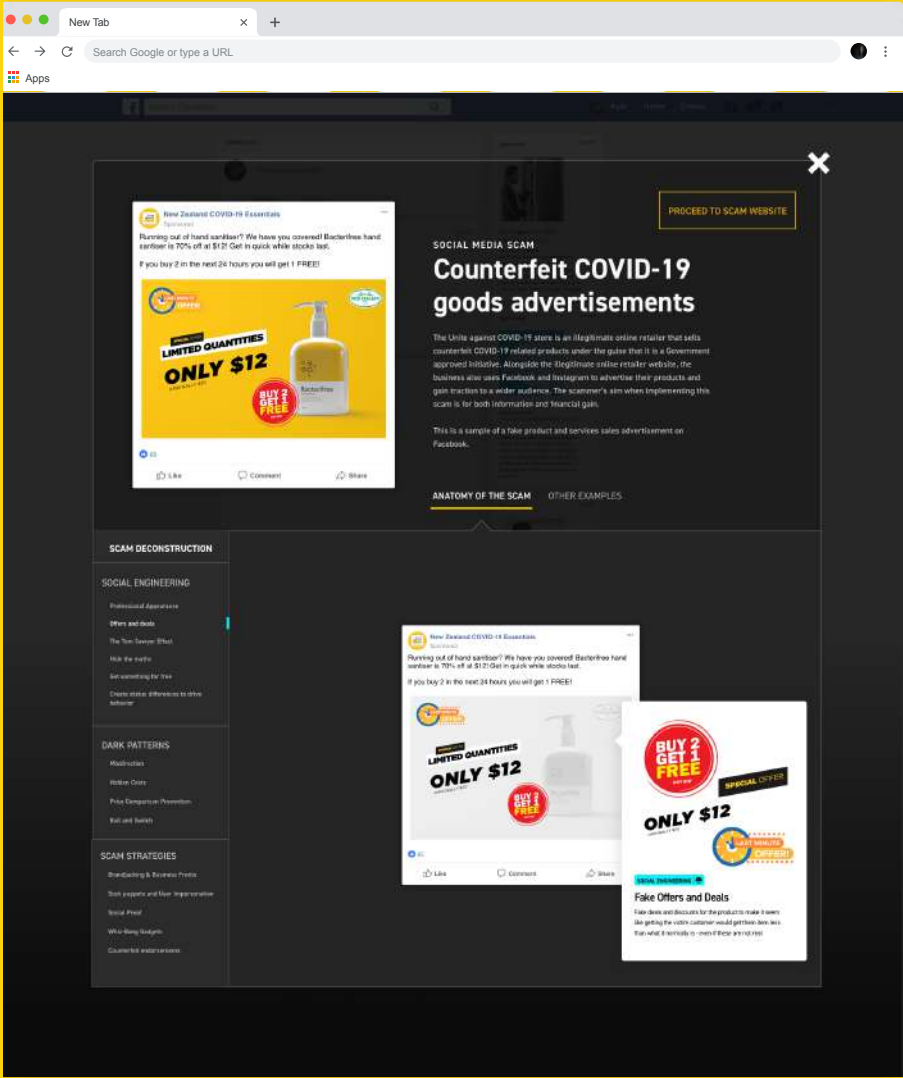


Figure 63. Design of scam analysis tool

TRY EXPERIMENT
OUT

<https://invis.io/AHYAZBUR4VD>

EXPERIMENT 2

CONTACT TRACING APPLICATIONS & QR CODE SCANNERS

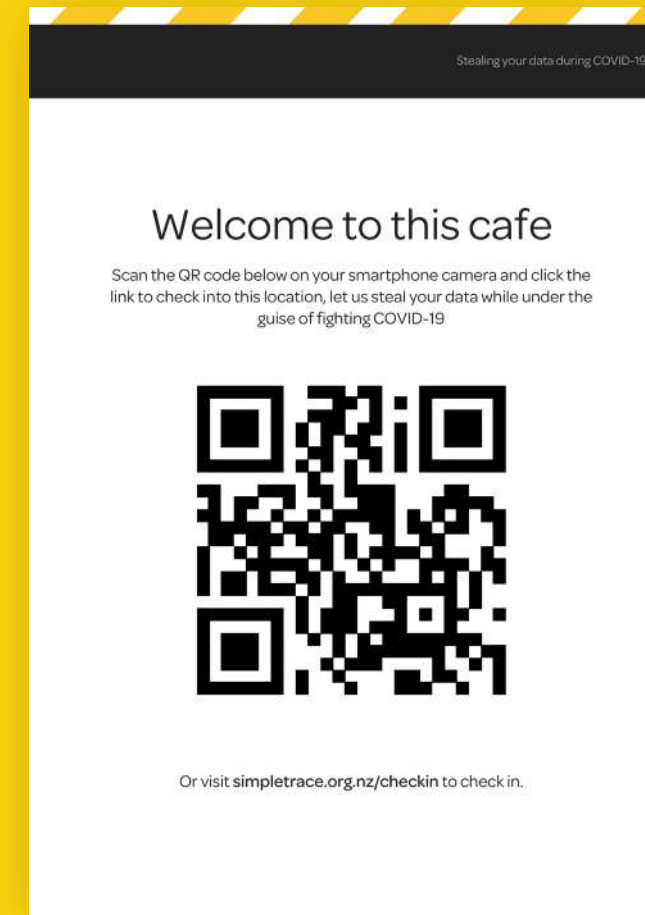
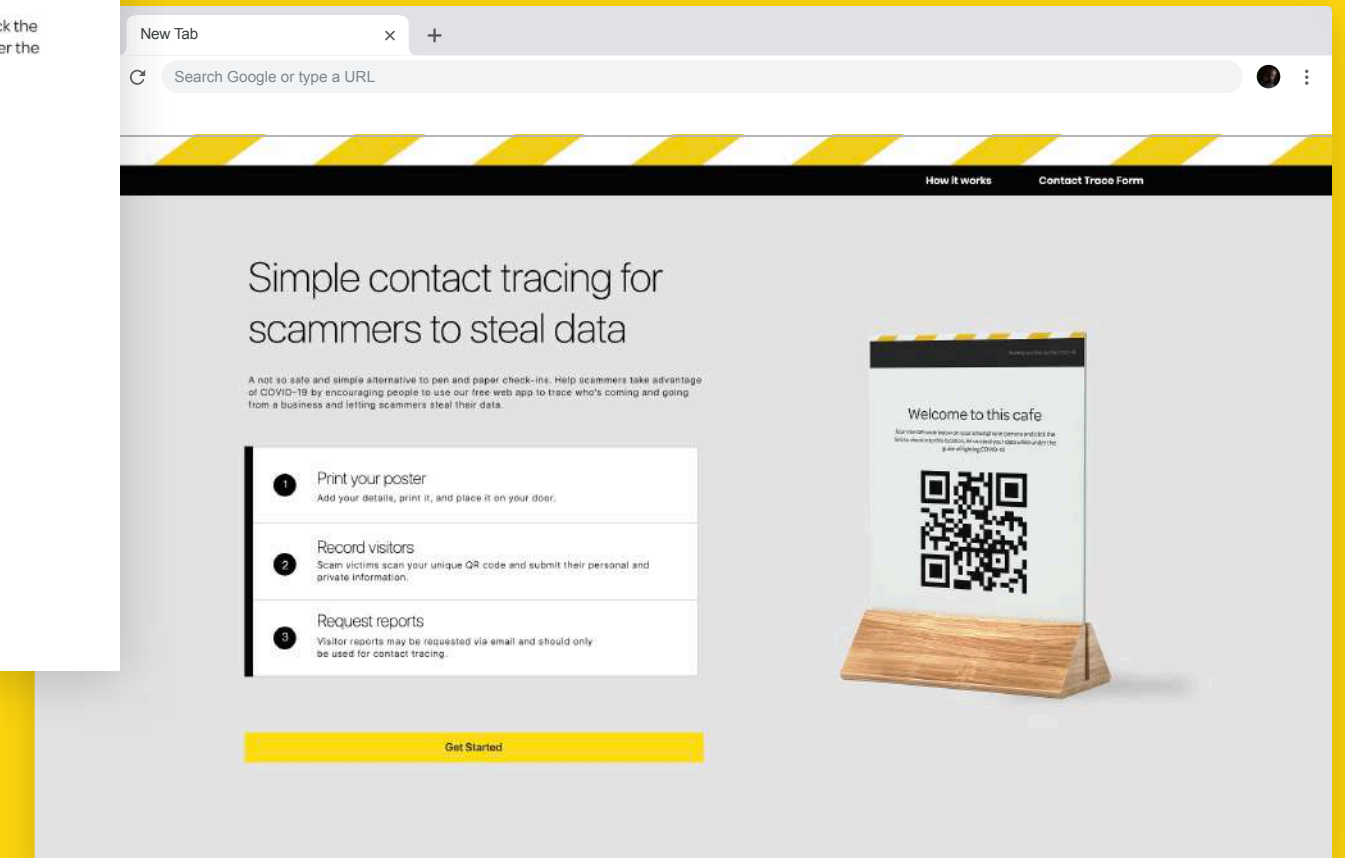


Figure 64. Fake contact tracing poster
Figure 65. Mirrored brandjacked malicious contact tracing website



April 9, 2020 was one of the first days New Zealand media had mentioned contact tracing technology options that could be used in the country (Pennington, 2020). The article suggested the lack of government voice on implementing contact tracing applications within New Zealand, mentioning the launch of Singapore’s contact tracing application TraceTogether that was downloaded by more than 1 million people which identified people that have been up to 2 metres near a COVID-19 patient for up to 30 minutes (Chong, 2020).

Juliet Gerrard, the prime minister’s chief science advisor, voiced that they had been looking into tracing technology for weeks prior, however, there was no off the shelf package that could just be implemented specifically in New Zealand (Radio New Zealand, 2020, April 8).

One of the biggest concerns that users have about contact tracing involving using applications surrounds privacy. In an interview on Nine To Noon (Radio New Zealand, 2020, April 8), privacy commissioner John Edwards mentions the avoidance of centralised aggregation of all users location, contact information

until it’s necessary. Many Facebook users who followed the New Zealand contact tracing application’s updates still voiced that they would still not be downloading any application due to fear of invading their privacy. Other issues that were brought up also highlight that Māori people (indigenous New Zealanders) could “suffer further discrimination” (Radio New Zealand, 2020, April 8).

The New Zealand contact tracing “digital diary” application was later rolled out a month later on May 18th, 2020. The New Zealand Ministry of Health released an accompanying video to explain further the application and how it works. The key messaging emphasises how vital privacy was: “We take your privacy seriously. Your information is kept private and secure”.

Radio New Zealand (2020) later reported that on the first day of release, 92,000 people had already downloaded the tracer app and 1000 businesses registered for a QR code. Almost a week later, this had increased to 380,000 users and 13,600 businesses, but the numbers were only a small percentage of how many businesses there were in total in the whole country.

The official government contact tracing application was not the only application to be designed and used in the New Zealand community.

On May 4th, digital agency Springload released Simple Trace, a simple contact tracing web application that did not require any application download. Businesses could print a Simple Trace poster with a unique QR code and place them within or outside their physical locations. Through scanning the QR code through the user's built in camera application, the user would be taken to an online web form where they could fill in their details.

Each day, customers would receive a list of locations they had visited on that day. If a user may have been potentially exposed to COVID-19 from one of those locations, they could share this list with the Ministry of Health upon being contacted. Businesses would also be contacted if someone who had received COVID-19 had been within their premises while they had the virus.

On May 9th, digital agency Paperkite released Rippl, a Privacy-first check-in and alerting mobile application designed to support New

Zealanders and Kiwi businesses within Wellington and Dunedin. Similarly to Simple trace, Rippl allowed businesses to register and receive a unique QR code that could be displayed within their business. However, Rippl had more functionality - customers would scan the application and keep the information on the app before being deleted after 21 days.

Both Springload and Paperkite engaged with the Ministry of Health, with Paperkite also engaging both the Wellington City Council and Dunedin City Council as their app explicitly targeted Wellington and Dunedin.

QUESTIONS RAISED

Contact tracing for businesses in New Zealand was designed and created in a way that was simple (both to use for customers and to install for businesses), easy to follow (both in instructions and the processes of how the contact tracing works) and visually looks professional with its minimalist design. However scammers could take advantage of how contact tracing is designed to use for malicious purposes.

This is an issue raised that is only relevant to digital contact tracing that redirects users to sign an online form. Fortunately, those who have downloaded a contact tracing application would avoid this issue. However, this means that it particularly targets users who do not download a mobile app out of security concerns or are too lazy, thus, using a redirect QR code scan instead.

- Contact tracing posters are quite easy to recreate, and QR codes the redirect to any website can easily be generated through QR code generators on the internet. It is quite easy to recreate these contact tracing QR code posters with the same visual design, but with a QR code that links to a malicious site.
- The website with the contact tracing form that the QR code redirects to is also straightforward and can easily be recreated, replacing the intended safe form with one that could steal the data of the customers.
- Contact tracing posters can be found stuck to the front entrance of a business. Scammers could easily take these posters down and replace them with their own.

If a customer falls victim to this scam, they could lose trust in the business that displayed the contact tracing poster, the organisation that created the contact tracing scheme and the government agencies behind it. A single complaint about this through social media and TV media could see a backlash on the

DESIGN EXPERIMENT

There are several contact tracing solutions that different government organisations and digital agencies have launched for New Zealand. For this experiment, the researcher plays the role of a scammer who has taken advantage of a newly established contact tracing method. This method assists local retail businesses to provide contact tracing without the need to download an app.

Retailers can print custom QR code posters for their store to record visitors who sign in through the form linked from scanning the QR code with their smartphone camera. Custom posters can be displayed by the retailers anywhere in their store or office space such as on the front door, by the counter or just lying down on a table.

The scammer has physically gone around Wellington and has replaced the legitimate contact tracing QR code posters with counterfeit ones. Scanning the QR code poster will redirect the user to a visually identical form, however, the information will be saved with the intention of future malicious use. The scammer's aim when implementing this scam is primarily for information gain.

This design experiment will visualise and demonstrate the processes and impact of misleading QR code scanning. This design experiment recreates QR code posters with incorrect QR codes that redirects users to website forms that can steal a victim's data.

EXPERIMENT 2: COVID-19 CONTACT TRACING SCAMS CYBERCRIME MODEL

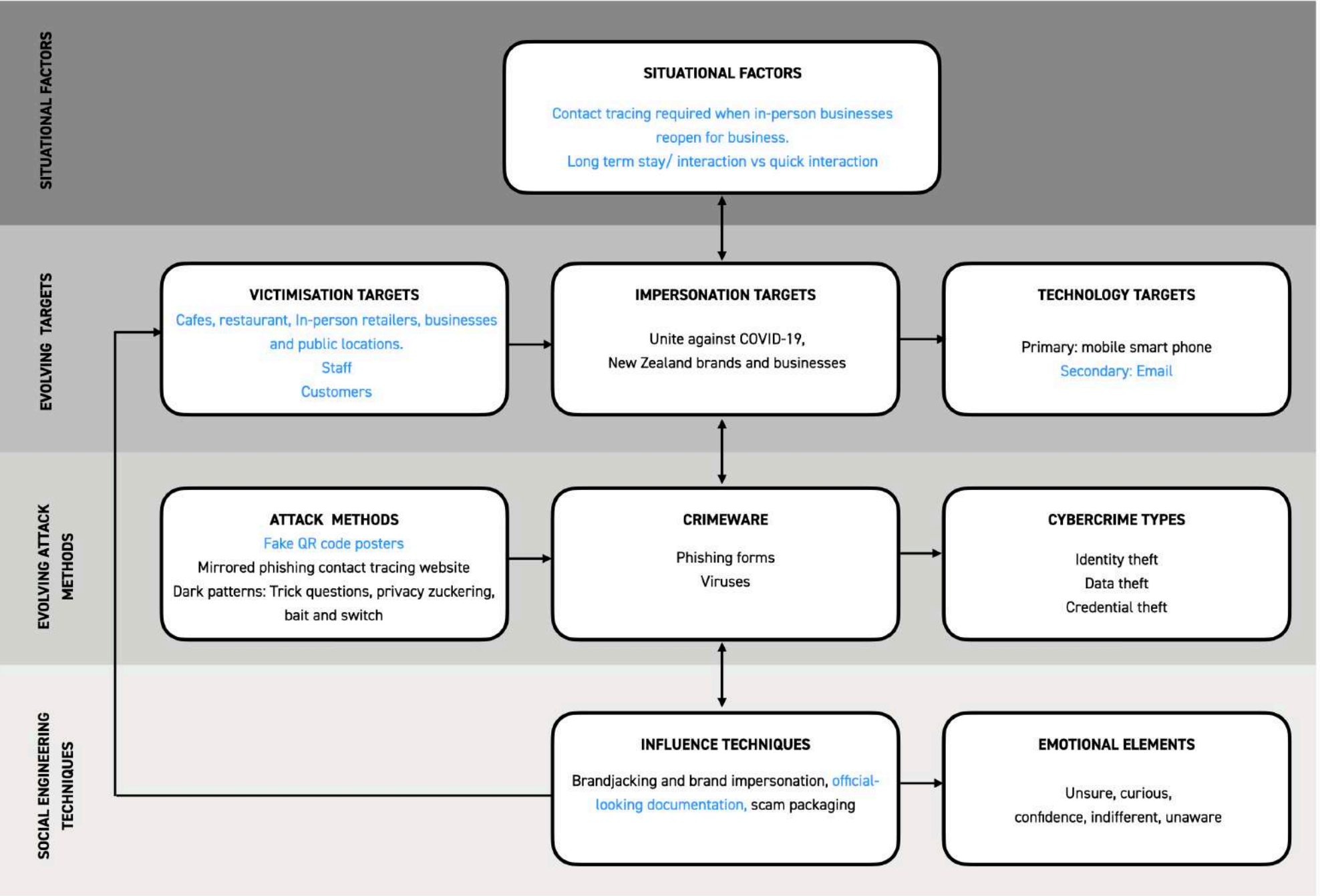


Figure 66. Naidoo's Multilevel model of cybercrime in the context of counterfeit COVID-19 contact tracing scams (2020)

EXPERIMENT 2: COVID-19 CONTACT TRACING SCAMS - PROCESS (INTERWOVEN FRAMEWORK)

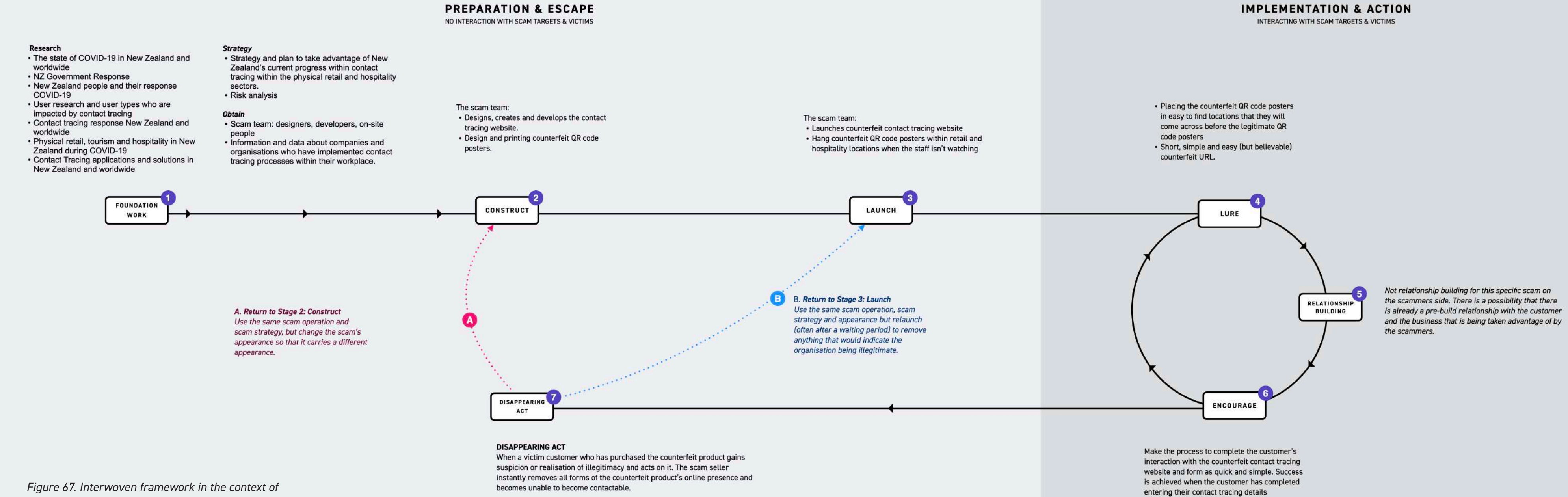


Figure 67. Interwoven framework in the context of COVID-19 contact tracing scams 2020)

EXPERIMENT 2: SCAMMER-VICTIM EXPERIENCE MAP - COVID-19 CONTACT TRACING SCAMS

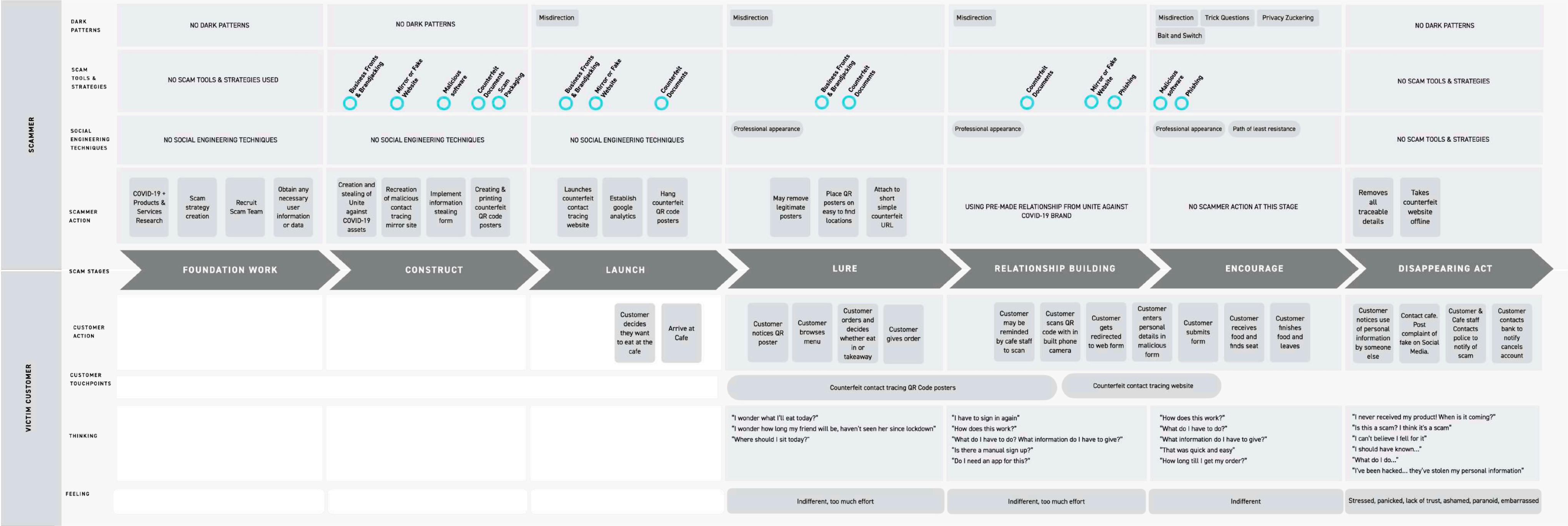


Figure 68. Unique Scammer-Victim experience map created to capture the context of COVID-19 contact tracing scams (2020)

SCAM STRATEGIES

What scam strategies are within contact tracing QR scams?

DARK PATTERN	APPLICABILITY		HOW CAN THE SCAM TOOL BE USED?
	SCAM SOCIAL MEDIA	SCAM WEBSITE	
Sock puppeteering and user impersonation		✗	This is a simple scam that relies solely on impersonating a brand and businesses. As the scam process is performed individually by the user, there is no need to impersonate users.
Business fronts & brandjacking		✓	This scam takes advantage of an existing brand and business and pretends to be them.
Information harvesting		✗	The scammer doesn't need to go out of the way to find the information as the scammer is actively giving it to them.
Not-so-tall tales		✗	The scammer does not need to create an elaborate tale or backstory to lure their target victims.
Whiz-bang gadgets and offers		✗	The scam does not provide any offers or gadgets.
Mirror and fake websites		✓	This scam mirrors and creates fake copies of the already existing tracing form website.
Counterfeit, official-looking documents and endorsements		✓	Recreation of contact tracing posters, both visual style, almost identical written content
Scam packaging		✓	The scam package contains two steps: <ul style="list-style-type: none">Physical contact tracing posterFake contact tracing form website that captures and steals a customer's information.
Phishing		✓	The user is actively giving the scammer their information to assume that they are giving that information to a trusted seller.

DARK PATTERNS

Which dark patterns are within contact tracing QR scams?

DARK PATTERN	APPLICABILITY		HOW CAN THE SCAM TOOL BE USED?
	SCAM SOCIAL MEDIA	SCAM WEBSITE	
Trick questions		✓	Trick questions could be used within a fake contact tracing website to capture unnecessary information that may be useful to the scammer.
Sneak in to the basket		✗	The user isn't actively buying a product within the fake website. Chances for the scammer to include any financial details is quite low as all contact tracing forms do not ask for this.
Roach motel		✗	The user is already actively giving the information and it is more important to get them out as quick as possible so that they do not notice that anything is wrong.
Privacy Zuckering		✓	The scammer could hide small print information within the form or site terms and conditions that allows them to “legally” sell or use any private data that the user submits.
Price comparison prevention		✗	The user isn't actively buying a product within the fake website and there are no products being advertised on the site.
Misdirection		✓	The scammer could use particular UI design features to misdirect the user's attention to giving more information.
Hidden costs		✗	The user isn't actively buying a product within the fake website. Chances for the scammer to include any financial details is quite low as all contact tracing forms do not ask for this.
Bait and switch		✓	The user expects to redirect to a website form to fill in their contact tracing details, but instead gets redirected to one that steals this private information. However, the user may not notice this as it is under the guise of a legitimate-looking contact tracing form website.
Confirmshaming		✗	There is a lack of reason to guilt the user into pressing the confirm button and shaming them for it.

SCAN TO TRY OUT

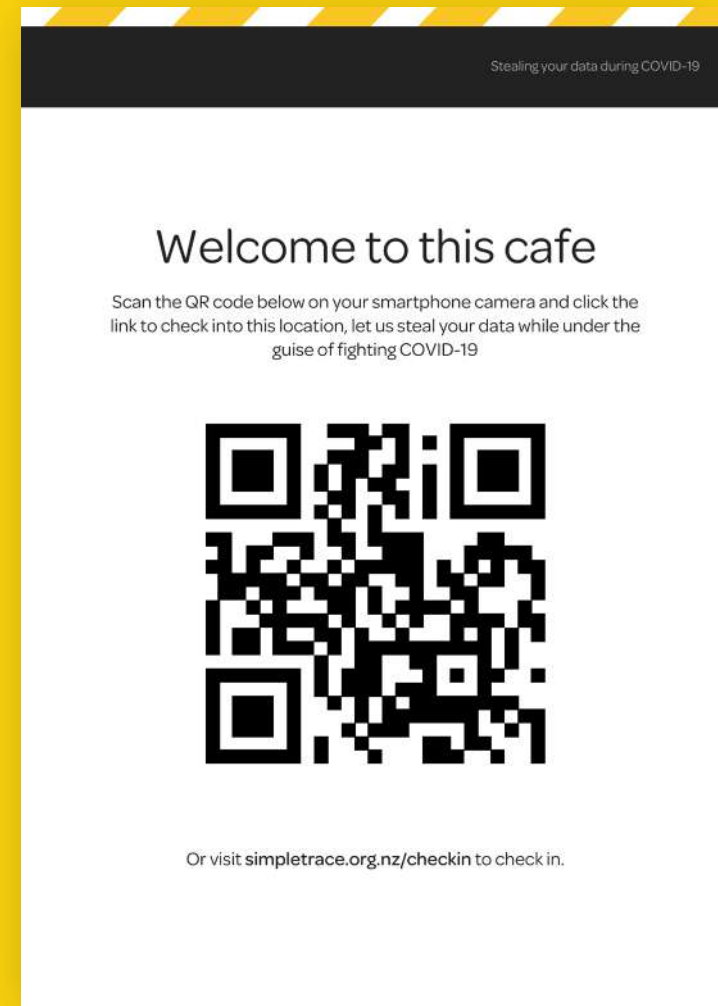


Figure 69. Fake contact tracing poster

Take a look at the website:
SimpleTrace.org.nz

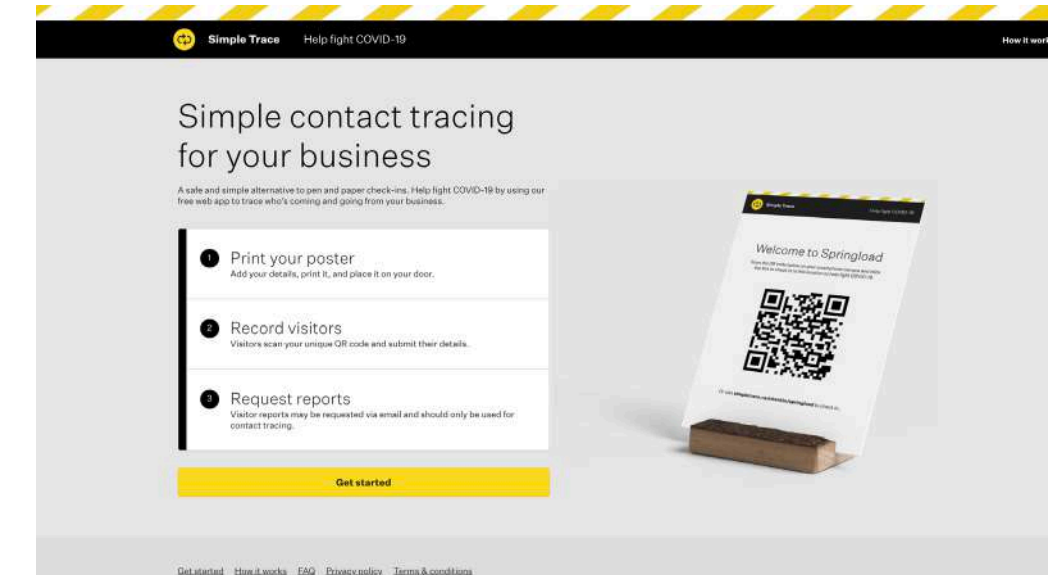


Figure 70. Legitimate contact tracing website

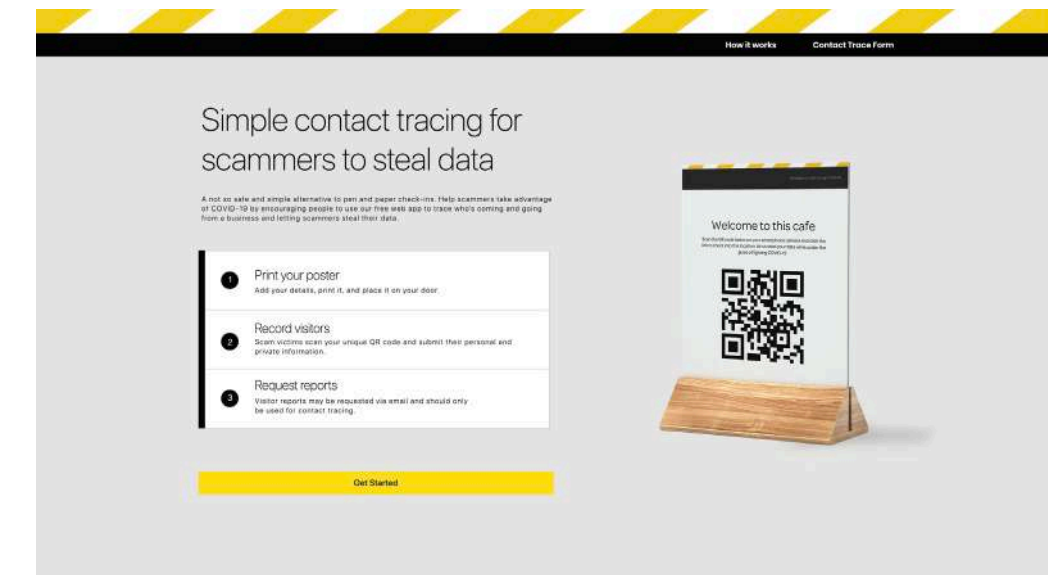


Figure 71. Fake mirrored & brandjacked website created on wix

Upon scanning the QR code, the victim user will land on the fake contact tracing website form, a parody of the original website which has implemented brandjacking and mirror website techniques.

The screenshot shows the 'Simple Trace' website. The header is black with a yellow and black striped border on the left. It contains the 'Simple Trace' logo, the text 'Help fight COVID-19', and a 'How it works' link. The main content area is white and titled 'Welcome to Springload' with the subtitle 'Help fight Covid-19'. It features a form with fields for 'Your name:', 'Phone number:', 'Email:', and 'Organisation (optional):'. Below the form are two buttons: a green 'Check in' button and a red 'Check out' button. At the bottom, there is a small disclaimer: 'By using Simple Trace you accept our Terms and conditions'.

Figure 72. Legitimate contact tracing form

The contact tracing form will be identical to that of the legitimate form, however, it can add extra fields as an opportunity to steal additional information. Scammers must do this subtly and only include fields that match the situation.

The screenshot shows a 'Welcome!' page with the subtitle 'Help fight Covid-19'. It features a form with fields for 'Your Name *', 'Phone number *', 'Email *', and 'Organisation (Optional)'. Below the form are two buttons: a green 'Check in' button and a red 'Check out' button. At the bottom, there is a small disclaimer: 'By using COVID-19 Trace you accept our Terms and conditions'.

Figure 73. Fake mirrored & brandjacked contact tracing form made on wix

This fake form is not connected to any database. The buttons only navigated to another page and are not connected to the form.

The screenshot shows a page with a grey background and a black header with a yellow and black striped border on the left. The header contains the text 'How it works' and 'Contact Trace Form'. The main content area features a large red octagonal 'STOP' sign. Below the sign, the text reads 'Wait a second... stop right there!'. This is followed by a paragraph: 'Did you notice this isn't a real New Zealand contact tracing website? Scammers are getting smarter when creating online scams and often will make websites that look identical to legitimate ones. Keep aware constantly and make sure you are on the legitimate website.' Below this is a 'DISCLAIMER' section: 'This website does not store, keep or use any information submitted through the previous page's form. This is only for demonstration purposes - the buttons only links to this page.' This is followed by another paragraph: 'This identical website is part of a larger research study on New Zealand online products and services scams- a 90-point thesis submitted to Victoria University of Wellington, in partial fulfillment of the requirements for the degree of Master of Design Innovation.' Below this is a link: 'For more any questions, please contact below:'. At the bottom, there is a link: 'For information on this project, please check out: scam-design.com'.

Figure 74. Alert page and end of design experiment

Upon clicking the button, the user is taken to this page. It informs the user that this is not in fact, the legitimate website, but could have been a scam. This page also takes time to explain the experiment and lets them know that no information was stored in the process. I believe that having mirrored websites with purposefully placed red flags are great ways to train people to be aware of them. To teach them on websites they regularly use. There are opportunities to test this within other websites as well.



4.3 COLLECTION OF SCAMS

With the original plan of having 5 experiments with a future to expand, this website was created to house the collection of website. This website's secondary aim is an information portal to link to the experiments if the user wants to find out more about them.

VIEW: www.scam-design.com

5.0

DISCUSSION

This chapter discusses the project's research process, ideation, iterative design process and relation to context of the COVID-19 pandemic. Further discussion on limitations that caused restrictions within the project and opportunities that the research could take in the future.

5.1 Discussion

5.2 Limitations & opportunities

5.1 DISCUSSION

This research focuses on understanding the process framework and mechanics that make up online products and services scams between social media and websites. While everyday users have created their own assumptions about how scams work based on personal experience and media consumption, it is these assumptions that cause people to heavily underestimate the complex nature and variety of scams that exist (Williams, Beardmore and Joinson, 2017).

Online products and services scams are an evolving aspect of today's internet. However, existing research on scams is concentrated on isolated areas and remains fragmented. There is little to no research on the processes and mechanics of how online products and services scams work.

Analysis of similar, related and comparable frameworks, combined with academic, media-based research and government resources has identified that:

- Despite it's malicious nature, products and services scams share similarities to marketing and social media marketing processes. I believe that these are two different sides of the same coin.
- The goal is primarily for information gain and/or

financial gain, stating that some scams are spontaneous while others are planned and calculated in more depth (Watters and Layton, 2010). However, there is nothing that discusses the differences in process and implementation for scams that focus where the weight focuses on the information gain or financial gain (or both equally).

- The role of emotions is heavily downplayed (Williams, Beardmore and Joinson, 2017) (Naidoo, 2020), focusing on more of the technical and security aspects (such as malware). However, emotions play an integral role in a scam's success (Muscanell, Guadagno & Murphy, 2014).
- I believe that the process of scams does not truly have an "endpoint", but an ongoing cycle that adapts based on situational factors and victim reaction. As visualised within the new interwoven framework in Figure 10., when a scam is discovered, it can be reused or repurposed in the future.

Based on the analysis of these existing related frameworks, this study develops a new interwoven framework from a user experience, visual design and service design perspective. This interwoven framework captures and integrates the following:

- The underlying foundation of a scam communicating the steps that are used during execution (Smith, 1922). When creating this proposed interwoven framework, I used this as a starting point basis to create its initial foundations.
- The moral counterpart of marketing (Armstrong, Adam, Denize, Volkov & Kotler, 2018) and social media marketing (Andzulis, Panagopoulos & Rapp, 2012) processes. The interwoven framework carries extreme similarities to these moral processes so that scams are executed and visibly appear legitimate.
- Button, Nicholls, Kerr & Owen's (2014) diversity classifications of scam types focused on information and/or financial gain. This was used to identify the goals and aims, providing clarity and direction between different kinds of products and services scams.
- Brignull's (2010) list of dark patterns.
- Australian Competition and Consumer Commission's (2016) scammer's toolkit and scam strategies.
- Nodder's (2013) social engineering seven deadly sins.
- Naidoo' (2020) multi-level influence model of cybercrime which captures the necessary components adapted to suit the context of products and services scams on a deeper level. These three levels of components this model

identifies include evolving targets, evolving attack methods and social engineering techniques.

This framework is further developed within the context of online COVID-19 scams. This is demonstrated through a designed clickable prototype that demonstrates the process of online products and services scams between platforms (scam social media and scam website) while also deconstructing and highlighting the social engineering, dark pattern, and scam strategy components within the scam.

Through this prototype, breaking down individual components has shown the difference in complexity between different scam types, demonstrating that not all scams are the same. For example, a products and services scam portraying a fake organisation selling fake products on Facebook could contain at least 7 social engineering techniques, 4 dark patterns and 6 scam strategies or tools. However, a malicious link to a fake COVID-19 statistics dashboard could contain one of each.

By creating and experimenting with this prototype, I find that New Zealand's attempts to educate the public on scams come off as half-hearted, easily forgettable, and easily

become outdated quickly. Currently, New Zealand media and safety information announcements and demonstrations only cover scams at a surface level which hides the complexity of scams and variety within each communicated category. As they are captured only on surface level, these scams do not appear to change despite the mechanics and methods evolving rapidly. Without a change in the way and frequency that scams are communicated into the community, I do not believe that people being affected by scams and falling for them will change and that victims and financial loss will continue to increase until drastic changes are made.

THE GREY AREA BETWEEN MARKETING SCAMS AND MORAL MARKETING

This study dives into the research that is the grey area between marketing scams and moral marketing. There are similarities between scam processes and marketing processes and I believe that they could be two sides of the same coin in which the intent of approach is moral or malicious. This asks the question of where is the line between ethical and malicious within this grey area.

From my analysis and explorations within my research

observations can be made that:

- **Scammers are risk takers.**
They are not afraid to put the brand or business' image at risk knowing that they can pull the website down if they are caught and stand it up again. Legitimate marketing practices keep in mind that actions are reflective of their business' brand image. If they are called out for bad practices or mistakes, they will make an effort to make up for their mistakes. On the other hand, scammers either actively ignore, make excuses, or run away from the problem, only to return as if the problem had never existed.
- **Scammers often promise and offer more but often never follow through.**
Legitimate marketing looks after their customers and continues to grow a trusting relationship. Scammers build this relationship for the purpose of malicious gain only to destroy this when they do not follow through with what was promised. They do not see their victims as people, nor do they care about how their actions will impact them.

- **Scammers partake in a lack of ethical practice.**
They will go out of their way to obtain information and financial gain often through malicious processes harming those who interact with them on a mental and psychological level. This can be seen through trust violating actions such as tricking victims into installing malicious crimeware (violation of personal space) or using/selling personal information and data without the victim's knowledge (violation of trust and lack of consent). Legitimate marketing practices may take advantage of their consumers, but are unlikely to cause them harm so as not to damage their trust (which again may impact brand image).
- **Scammers have completely different intentions to what they portray themselves to be.**
Legitimate marketing may use social engineering techniques and dark patterns to exaggerate the truth to sustain and increase their customer base, performing as how they have visually portrayed themselves to be. However, scammers cannot do this as they cannot obtain what they need through legitimate means. Similarly to the dark pattern 'bait and switch', scammers portray

themselves as a legitimate business under the guise they are offering legitimate products and services, however actually use this image for malicious information and financial gain.

Dark patterns within scams

Previous academic research on dark patterns primarily focused on its use by legitimate businesses and products, questioning the ethics and implications when implemented. There was a lack of dark patterns used within online scams, in particular, of online products and services scams.

From my research and exploration, I have deduced that dark patterns used within online products and services scams context focuses on a) hiding that they are not legitimate and b) hiding to gain more. The most common dark pattern implemented within scams is 'misdirection', often used to direct users to look at specific areas of a platform. In this case, the dark pattern is to portray the image of a real business through authentic visual and content means.

I believe that scammers take dark patterns to the next level by implementing incomplete dark patterns within their scams.

While dark patterns are implemented within a scam's strategy, scammers can purposely leave out aspects of the dark pattern completely during implementation. This is only able to happen within a scam context due to the unimportance of victim trust and relationship. This can be seen through the following dark patterns:

- Hidden cost - in which there are hidden costs and unexpected charges that are visible, most commonly, in small fine print or just before the end of a purchase. However, they are completely non-existent on the platform - the victim only discovers this after the purchase.
- Roach motel and Forced continuity - in which normally the functionality of being able to cancel subscriptions or delete accounts is often very hidden deep within the platform. However, scammers can completely take this function out and ignore any victim attempts of contact to solve this issue.

Dark patterns hugely focuses on implementation within digital mediums, however this research has identified the possibility of digital to analogue dark pattern implementation. This is demonstrated through the 'bait and switch' dark pattern of which a customer can purchase a physical product online, but when

they receive the product in person, it is not the same product, a fake version of the product or a completely different product to what it was expected to be.

Dark pattern research on existing platforms

Dark pattern research has focused on it's implementation on a functional and technical level; therefore, it is primarily researched on mediums that the dark pattern practitioners have control over. Throughout this research, I have focused on exploring dark pattern implementation on platforms, mainly social media, in which practitioners have some control over content (making profiles, business pages, uploading pictures), but little to no control of the functionality of the platform. While I have only used Facebook as an example within this research, future research would incorporate other popular social media platforms, like Instagram and Twitter due to the differences in the way they are used by it's broad range of different user groups. An expansion of this could be the inclusion of social platforms which aren't network-focused, but have (or could create) either a viewer or community base, such as YouTube and blogs.

Despite the lack of functional control, scammers can still implement these dark patterns by content means (such as

graphics and written content) to bridge victims into the scam environment that the scammers have control over.

While this research portfolio's overall results are speculative and have yet to undergo user testing, it provides insight into the more profound research area and complexity of online products and services scams. This proposed framework, after more development, further implementation and demonstration on different scam types inside of products and services scams could further enhance understanding of the development of future scams. The framework could provide suitable advancements to improve scam prevention solutions and scam education in New Zealand.

5.2 LIMITATIONS & OPPORTUNITIES

LIMITATIONS

The broad spectrum of existing research

While this research covers an extensive range of existing research, there is still a broader field of academic research that this study cannot review. As many studies within general scams are relevant to this subject, it is out of scope to consider more than what is currently within this study. Thus, there are potentially relevant pieces of research, frameworks and experimentation that may have been unintentionally excluded from the research or left unstudied.

The limitations of ethics

There is a high level of consideration that must be taken when undertaking experimentation around scamming with people, especially as deception is a central action behind scams. By telling people the true intentions of scam based experiments could sway authentic results. Scammers most often do not consider any human ethics when carrying out scams, however, academic research has to cross this bridge in order to learn and improve this research area.

This study was based on secondary research

Inability to conduct primary research with people to measure their

actual behaviour. For the scope of the project, the main aim was to gain a strong understanding of the current existing academic material within products and services. Due to the COVID-19 pandemic, interaction with people was also minimal.

The quick progression of the COVID-19 pandemic

With the pandemic quickly picking up in March, there was a limited timeframe to supervise the pandemic and application of the research within the context of COVID-19. As COVID-19 will not be concluded by the end of this research, the study will not be able to consider anything beyond July 2020.

Scope of experimentation

Due to the extensive technical background needed to explain and give context to each small experiment, the experiments implemented were decreased from 5 to 2 with a more significant focus on each remaining experiment.

Obtaining permissions

There was difficulty in receiving permissions to use specific imagery and branding images of local organisations to use within the research. Many emails of requests sent were left unanswered, thus, a pivot in process was made to accommodate this loss.

OPPORTUNITIES

Further research

Opportunity for further investigation of gaps and unstudied research that is relevant to further building this research study.

Further proceeding with ethical experimentation

This research produces a clearer understanding of the area of online products and services scams. The substantial research and pre-designed experiments provide clarity and direction in further developing these experiments to incorporate user interaction safely.

Taking the research, frameworks and experiments to later test with people and measure their behaviour

To validate and improve this research, it is essential to incorporate primary research and involve interactions and voices of real people. Future research outside of the scope should take the opportunity to include this.

Scope of experimentation

Due to the large technical background needed to explain and give context to each small experiment, the experiments implemented were decreased with a larger focus on each remaining experiment.

Further in depth experimentation within other products and services scam variations

As the scope of the research could only incorporate a small sample of online products and services examples, future research has the opportunity to discover, deconstruct and reconstruct a broader scope of scam varieties.

Further long-term research for COVID-19 pandemic scams and also applying research, output frameworks and experimentation within other specified situations and areas of studies

Expansion of this research could observe the impact of COVID-19 over more extended periods of time (over a year or even the length of COVID-19's existence). Future research has the opportunity to take the research and findings and apply them within other contexts outside of COVID-19 within the area of Products and Services scams.

Collaboration with relevant organisations and government agencies

As the study looks at online products and services scams from a New Zealand perspective, there is an opportunity to work with relevant local organisations to collaborate on improving the state of these scams in the country. Potential organisations could include NetSafe NZ, InternetNZ, Consumer NZ, Consumer Protection and Ministry of Business and Innovation etc.

The closing chapter which concludes the research and reflects on the overall study and implications for the future.

6.1 Conclusion

6.2 References

6.3 List of Figures

6.4 Appendix

6.0 CONCLUSION

6.1 CONCLUSION

This research explores the overarching process of online products and services scams within social media and websites. As these scams continue to rapidly increase in frequency and evolve in complexity with the reliance on the internet and technology, everyday people will continue to be at risk.

The focus of this research was to delve into the complex nature of online products and services scams exploring areas that have only been touched broadly at surface level and provide clarity on how they function together. By creating transparency, it will ultimately assist in the collective awareness of subject complexity for everyday people. Transparent understanding will provide more in-depth guidance when developing solutions against online products and services scams and create better-informed material to educate regular people.

Approaching this research area with a user experience perspective has allowed for exploration and understanding of the human aspect in which previous academic research has largely neglected and ignored. Observing online products and services scams through a service design lens brings clarity to the broader situation: providing context on how people fit into the process, a more cohesive understanding of how people are affected and when and how scammers take advantage of that.

By developing a unique, interwoven, amalgamated framework specifically for this research of online products and services scams, this research aims to support future research, providing a foundation to assist future understanding

of new scams that have yet to emerge.

The design output showcases this framework to visually and interactively communicate the research problem and its complexity. This is demonstrated by deconstructing specific online products and services scams down to it's individual components and illustrating it's influences as a part of the scam.

As this research has yet to undergo user testing, further exploration of this topic should incorporate involving people to validate and improve proposed research, frameworks and design outputs. Additional research development could include a more comprehensive selection of online products and services scams to deconstruct and analyse. Further opportunities for this research could involve collaborating with relevant organisations and government agencies to add to New Zealand specific scam research, potentially impacting how scam-related initiatives are conducted.

It is essential for research within this area to progress continuously. Scams within the digital realm will continue to exist and evolve. Without people to keep understanding the past, present and future state of online products and services scams, maintain the knowledge hub and continuously explore innovative solutions, it will become increasingly more challenging to look after our community and protect them. Scammers have always been ahead of the game, but it's time for us as a community and as practitioners to catch up.

6.2 REFERENCES

REFERENCES

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security, 68*, 160-196. doi:10.1016/j.cose.2017.04.006

Amos, C., Holmes, G. R., & Keneson, W. C. (2014). A meta-analysis of consumer impulse buying. *Journal of Retailing and Consumer Services, 21*(2), 86-97. doi:10.1016/j.jretconser.2013.11.004

Andzulis, J. ", Panagopoulos, N. G., & Rapp, A. (2012). A Review of Social Media and Implications for the Sales Process. *Journal of Personal Selling & Sales Management, 32*(3), 305-316. doi:10.2753/pss0885-3134320302

Arkin, J. (1986). Guarding against purchase scams. *Battery Man; (United States)*. Retrieved from <https://www.osti.gov/biblio/5035001>

Armstrong, G., Adam, S., Denize, S., Volkov, M., & Kotler, P. (2018). *Principles of Marketing* (7th ed.). Melbourne, VIC: Pearson Education Australia.

Arthur, C. (2010, July 18). Virus phone scam being run from call centres in India. *Guardian*. Retrieved from <https://www.theguardian.com/world/2010/jul/18/phone-scam-india-call-centres>

Australian Competition and Consumer Commission. (2018, January 04). Types of scams. Retrieved August 01, 2020, from <https://www.scamwatch.gov.au/types-of-scams>

Australian Competition & Consumer Commission. (2016). *The Little Black Book of Scams*. Canberra, NSW: Commonwealth of Australia 2016. Retrieved from <https://www.accc.gov.au/publications/the-little-black-book-of-scams>

BBC (2020, April 24) Coronavirus: Outcry after Trump suggests injecting disinfectant as treatment. *BBC*. Retrieved from <https://www.bbc.com/news/world-us-canada-52407177>

Brignall, H. (2010). Dark Patterns. Retrieved July 31, 2020, from <https://darkpatterns.org/>

Boyd, J. (2019, January 25). The History of Facebook: From BASIC to global giant. Retrieved August 04, 2020, from <https://www.brandwatch.com/blog/history-of-facebook/>

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391-408. doi:10.1177/0004865814521224

Chang, P., & Chieng, M. (2006). Building consumer–brand relationship: A cross-cultural experiential view. *Psychology and Marketing, 23*(11), 927-959. doi:10.1002/mar.20140

Chih-Yuan Sun, J., Kuo, C., Hou, H., & Lin, Y. (2016). Exploring Learners' Sequential Behavioral Patterns, Flow Experience, and Learning Performance in an Anti-Phishing Educational Game. *Educational Technology & Society, 20*(1), 45-60. Retrieved from https://www.researchgate.net/publication/313375613_Exploring_learners'_sequential_behavioral_patterns_flow_experience_and_learning_performance_in_an_anti-phishing_educational_game

Choi, W., & Stvilia, B. (2015). Web credibility assessment: Conceptualization, operationalization, variability, and models. *Journal of the Association for Information Science and Technology, 66*(12), 2399-2414. doi:10.1002/asi.23543

Chong, C. (2020, April 1). About 1 million people have downloaded the TraceTogether app, but more need to do so for it to be effective: Lawrence Wong. *The Straits Times*. Retrieved from <https://www.straitstimes.com/singapore/about-one-million-people-have-downloaded-the-tracetogogether-app-but-more-need-to-do-so-for>

Coibion, O., Gorodnichenko, Y., & Weber, M. (2020). The Cost of the Covid-19 Crisis: Lockdowns, Macroeconomic Expectations, and Consumer Spending. doi:10.3386/w27141\

Commission for Financial Capability. (2018). *Little Black Book of Scams*. Auckland: Commission for Financial Capability. Retrieved from <https://cfc.govt.nz/about/national-strategy/articles/the-little-black-book-of-scams/>

Deevy, M., Lucich, S., & Beals, M. (2012). Scams, Schemes and Swindles: A review of consumer financial fraud. Financial Fraud Research Centre, Stanford. Retrieved from <http://archive.ncpc.org/resources/files/pdf/fraud/Scams-Schemes-Swindles.pdf>

DiSalvo, C. (2012). FCJ-142 Spectacles and Tropes: Speculative Design and Contemporary Food Cultures. *The Fibreculture Journal, 1*(20), 109-122. doi:<http://twenty.fibreculturejournal.org/2012/06/19/fcj-142-spectacles-and-tropes-speculative-design-and-contemporary-food-cultures/>

Dodoo, N. A., & Wu, L. (2019). Exploring the anteceding impact of personalised social media advertising on online impulse buying tendency. *International Journal of Internet Marketing and Advertising, 13*(1), 73. doi:10.1504/ijima.2019.097905

Ferrick, B. (2019). The Times They Are A-Changin': Incorporating Blockchain Networks into the Event Ticket Industry. *Texas Review of Entertainment & Sports Law, 20*(1), 113-132.

Findeli, A. (1995). Design History and Design Studies: Methodological, Epistemological and Pedagogical Inquiry. *Design Issues, 11*(1), 43. doi:10.2307/1511615

Frankel, Lois and Racine, Martin (2010). The complex field of research: for design, through design, and about design. Available at www.designresearchsociety.org/docs-procs/DRS2010/PDF/0436pdf.

Freiermuth, M. R. (2011). Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting. *Discourse & Communication, 5*(2), 123-145. doi:10.1177/1750481310395448

Gunia, A. (2020, April 28). Why New Zealand's Coronavirus Elimination Strategy Is Unlikely to Work in Most Other Places. *TIME*. Retrieved from <https://time.com/5824042/new-zealand-coronavirus-elimination/>

Hache, A. C., & Ryder, N. (2011). 'Tis the season to (be jolly?) wise-up to online fraudsters. Criminals on the Web lurking to scam shoppers this Christmas:1a critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud. *Information & Communications Technology Law, 20*(1), 35-56. doi:10.1080/13600834.2011.557537

Hadnagy, C. (2011). *Social engineering: The art of human hacking*. Hoboken, N.J: Wiley.

Heymann, D. L., & Shindo, N. (2020). COVID-19: What is next for public health? *The Lancet, 395*(10224), 542-545. doi:10.1016/s0140-6736(20)30374-3

Higgins, G. (2019, May 7). Company behind Hayley Holt face cream scam exposed. *TVNZ*. Retrieved from <https://www.tvnz.co.nz/one-news/new-zealand/company-behind-hayley-holt-face-cream-scam-exposed>

Hofman, C., & Keates, S. (2013). An Introduction to Brand Risk. *Countering Brandjacking in the Digital Age SpringerBriefs in Computer Science, 1*-7. doi:10.1007/978-1-4471-5580-5_1

Hofman, C., & Keates, S. (2013). An Overview of Branding and its Associated Risks. *Countering Brandjacking in the Digital Age SpringerBriefs in Computer Science, 9*-35. doi:10.1007/978-1-4471-5580-5_2

Hofman, C., & Keates, S. (2013). Brand Risk Management Theory. *Countering Brandjacking in the Digital Age SpringerBriefs in Computer Science, 37*-61. doi:10.1007/978-1-4471-5580-5_3

Hofman, C., & Keates, S. (2013). Brand Risks in Cyberspace. *Countering Brandjacking in the Digital Age SpringerBriefs in Computer Science, 79*-84. doi:10.1007/978-1-4471-5580-5_5

Hooi Koon, T. (2015). Persuasive techniques in internet romance scams. 1-152.

Humble, J. V. (2011). *The miracle mineral solution of the 21st century: Part 2*. Montreal, (Quebec): Osmora.

Jeong, S., Kim, H., Yum, J., & Hwang, Y. (2016). What type of content are smartphone users addicted to?: SNS vs. games. *Computers in Human Behavior, 54*, 10-17. doi:10.1016/j.chb.2015.07.035

Kervenoael, R. D., Aykac, D. S., & Palmer, M. (2009). Online social capital: Understanding e-impulse buying in practice. *Journal of Retailing and Consumer Services, 16*(4), 320-328. doi:10.1016/j.jretconser.2009.02.007

Kokate, S., & Tidke, B. (2018). Fake Review and Brand Spam Detection using J48 Classifier. *International Research Journal of Engineering and Technology (IRJET) E, 5*(4), 58-63. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/summary?sessionid=F91416805E7A72C9BA18A553C93CC00B?-doi=10.1.1.695.2101>

Kolari, P., Java, A., & Joshi, A. (2007). *Spam in Blogs and Social Media, Tutorial*. Retrieved from <https://ebiquity.umbc.edu/paper/html/id/362/Spam-in-Blogs-and-Social-Media-Tutorial>

Kopp, C., Sillitoe, J., Gondal, I., & Layton, R. (2016). *Online Romance Scam: Expensive e-Living for romantic happiness*. Bled eConference 2016.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113-122. doi:10.1016/j.jisa.2014.09.005

Kunwar, R. S., & Sharma, P. (2016). Social media: A new vector for cyber attack. *2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring)*. doi:10.1109/icacca.2016.7578896

Larose, R. (2006). On the Negative Effects of E-Commerce: A Sociocognitive Exploration of Unregulated On-line Buying. *Journal of Computer-Mediated Communication, 6*(3), 0-0. doi:10.1111/j.1083-6101.2001.tb00120.x

Lin, Y. J. (2011). *Fake stuff: China and the rise of counterfeit goods*. New York: Routledge.

Mancusi-Ungaro, G. (2014). Brandjacking on Social Media and Beyond. *Risk Management, 61*(10), 14-16. Retrieved from <https://www.questia.com/magazine/1G1-393209865/brandjacking-on-social-media-and-beyond>

Martin, N., & Rice, J. (2013). Spearing High Net Wealth Individuals. *International Journal of Information Security and Privacy, 7*(1), 1-15. doi:10.4018/jisp.2013010101

Mazar, N., Amir, O., & Ariely, D. (2008). The Dishonesty of Honest People: A Theory of Self-Concept Maintenance. *Journal of Marketing Research, 45*(6), 633-644. doi:10.1509/jmkr.45.6.633

Merriam-Webster. (n.d.). Pride. Retrieved August 01, 2020, from <https://www.merriam-webster.com/dictionary/pride>

Merriam-Webster. (n.d.). Product. Retrieved August 01, 2020, from <https://www.merriam-webster.com/dictionary/product>

Merriam-Webster. (n.d.). Service. Retrieved August 01, 2020, from <https://www.merriam-webster.com/dictionary/service>

Milam, M. (2008). The rise of brandjacking against major brands. *Computer Fraud & Security*, 2008(10), 10-13. doi:10.1016/s1361-3723(08)70149-0

Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. *Wiley*.

Morris, M. N. (2014). The utilization and management of sockpuppets within online communities. *Engineering*. Retrieved from <https://www.semanticscholar.org/paper/The-utilization-and-management-of-sockpuppets-Morris/35c4dfe3141014ae2b14cda7bf7e8bde503438ae#paper-header>

Munton, J., & McLeod, J. (2011, July 22). The Con: How Scams Work, Why You're Vulnerable, and How to Protect Yourself. Retrieved from <https://books.google.co.nz/books?id=kAUcySEUpTEC>

Muscanell, N. L., Guadagno, R. E., & Murphy, S. (2014). Weapons of Influence Misused: A Social Influence Analysis of Why People Fall Prey to Internet Scams. *Social and Personality Psychology Compass*, 8(7), 388-396. doi:10.1111/spc3.12115

Wilson, B. (2017). Using social media to fight fraud. *Risk Management*, 64(2), 10+.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, 29(3), 306-321. doi:10.1080/0960085x.2020.1771222

Netsafe New Zealand. (2018). *Netsafe Quarterly Report October – December 2018*. <https://www.netsafe.org.nz/the-kit/fy19-q2/>

Netsafe New Zealand. (2019). *Netsafe Quarterly Report January – March 2019*. <https://www.netsafe.org.nz/the-kit/fy19-q3/>

Netsafe New Zealand. (2019). *Netsafe Quarterly Report April – June 2019*. <https://www.netsafe.org.nz/the-kit/fy19-q4/>

Netsafe New Zealand. (2019). *Netsafe Quarterly Report July – September 2019*. <https://www.netsafe.org.nz/the-kit/fy20q1/>

Netsafe New Zealand. (2019). *Netsafe Quarterly Report October – December 2019*. <https://www.netsafe.org.nz/the-kit/fy20q2/>

Nodder, C. (2013). *Evil by design: Interaction design to lead us into temptation*. Indianapolis, IN: Wiley.

Pang, C. L., & Sterling, S. (2013). From Fake Market to a Strong Brand? The Silk Street Market in Beijing. *Built Environment*, 39(2), 224-235. doi:10.2148/benv.39.2.224

Pector, E. A., & Hsiung, R. C. (2011). Clinical Work with Support Groups Online: Practical Aspects. *On-line Counseling*, 203-224. doi:10.1016/b978-0-12-378596-1.00011-3

PRovoke Media. (2020, June 04). Covid-19 Comms: US Government Worst, New Zealand & Germany Best Say PR Pros. Retrieved August 01, 2020, from <https://www.provokemedia.com/latest/article/covid-19-comms-us-government-worst-new-zealand-germany-best-say-pr-pros>

Radio New Zealand (2020, April 8) Chief Science advisor: How and when we exit alert level four. *Radio New Zealand*. Retrieved from <https://www.rnz.co.nz/national/programmes/ninetonoon/audio/2018741963/chief-science-advisor-how-and-when-we-exit-alert-level-four>

Radio New Zealand (2020, April 9) Pennington, P. Covid-19: Government quiet on contact tracing tech options. *Radio New Zealand*. Retrieved from [rnz.co.nz/news/national/413847/covid-19-government-quiet-on-contact-tracing-tech-options](https://www.rnz.co.nz/news/national/413847/covid-19-government-quiet-on-contact-tracing-tech-options)

Radio New Zealand. (2020, May 20). More than 92,000 people already registered on NZ tracing app - Bloomfield. *Radio New Zealand*. Retrieved from <https://www.rnz.co.nz/news/national/417084/more-than-92-000-people-already-registered-on-nz-tracing-app-bloomfield>

Radio New Zealand. (2020). Covid-19: RNZ News. Retrieved August 06, 2020, from <https://www.rnz.co.nz/news/covid-19>

Ramsey, L. P. (2010). Brandjacking on Social Networks: Trademark Infringement by Impersonation of Markholders. *Buffalo Law Review*, 58, 851-929. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1498557

Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to Psychological and Popular Opinion, There Is No Compelling Evidence That Older Adults Are Disproportionately Victimized by Consumer Fraud. *Perspectives on Psychological Science*, 9(4), 427-442. doi:10.1177/1745691614535935

Saco, R. M., & Goncalves, A. P. (2010). Service Design: An Appraisal. *Design Management Review*, 19(1), 10-19. doi:10.1111/j.1948-7169.2008.tb00101.x

Smith, E. H. (1922). *Confessions of a Confidence Man: A Handbook for Suckers*. Independently Published.

Smythe, H. R. (1994). Fighting Telemarketing Scams. *Hastings Communications and Entertainment Law Journal*, 17(1), 346-381. Retrieved from <https://docplayer.net/99782902-Fighting-telemarketing-scams.html>

Stewart, T. (2015). User experience. *Behaviour & Information Technology*, 34(10), 949-951. doi:10.1080/0144929x.2015.1077578

Stabek, A., Watters, P., & Layton, R. (2010). The Seven Scam Types: Mapping the Terrain of Cybercrime. *2010 Second Cybercrime and Trustworthy Computing Workshop*. doi:10.1109/ctc.2010.14

Te Tari Taiwhenua Department of Internal Affairs (2019). *Identity: Are you a victim of identity theft?*. Retrieved from <https://www.dia.govt.nz/Identity---Are-you-a-victim-of-identity-theft>.

Trice, M., & Potts, L. (2018). Building Dark Patterns into Platforms: How GamerGate Perturbed Twitter's User Experience. *Present Tense*, 6(3), 1-10.

Tsoutsanis, A. (n.d.). Tackling Twitter and Facebook Fakes: ID Theft in Social Media. *World Data Protection Report 2012*, 12(4), 1-3. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2047190

Vishwanath, A. (2014). Habitual Facebook Use and its Impact on Getting Deceived on Social Media. *Journal of Computer-Mediated Communication*, 20(1), 83-98. doi:10.1111/jcc4.12100

Vocabulary.com. (n.d.). Corroborating Evidence. Retrieved August 05, 2020, from https://www.vocabulary.com/dictionary/corroborating_evidence

Ward, M. R., & Lee, M. J. (2000). Internet shopping, consumer search and product branding. *Journal of Product & Brand Management*, 9(1), 6-20. doi:10.1108/10610420010316302

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412-421. doi:10.1016/j.chb.2017.03.002

Wunder, G. C. (2009). Brandjacking Big Pharma on the Web. *Journal of Internet Commerce*, 8(1-2), 58-69. doi:10.1080/15332860903341323

Whitty, M. T. (2013). Anatomy of the online dating romance scam. *Security Journal*, 28(4), 443-455. doi:10.1057/sj.2012.57

Whitty, M. T. (2013). The Scammers Persuasive Techniques Model: Development of a Stage Model to

Explain the Online Dating Romance Scam. *British Journal of Criminology*, 53(4), 665-684. doi:10.1093/bjc/azt009

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), 662-674. doi:10.1002/asi.20779

World Health Organization. (n.d.). Coronavirus disease (COVID-19). Retrieved August 01, 2020, from <https://www.who.int/emergencies/diseases/novel-coronavirus-2019>

Yan, J. (2019). From Sicilian mafia to Chinese "scam villages". Retrieved from <https://arxiv.org/abs/1905.03108>

Yin, J., Karimi, S., Lampert, A., Cameron, M., Robinson, B., & Power, R. (2015). *Using Social Media to Enhance Emergency Situation Awareness: Extended Abstract*. Retrieved from https://www.researchgate.net/publication/280829031_Using_Social_Media_to_Enhance_Emergency_Situation_Awareness_Extended_Abstract

Young, K. S., & Nabuco de Abreu, C. (2010). *Internet Addiction: A Handbook and Guide to Evaluation and Treatment*. Hoboken, NJ: John Wiley & Sons. Retrieved from <https://assets.thalia.media/images-adb/c0/e1/c0e1ab5b-7c82-4603-86f8-45bb860d298b.pdf>

Zalis, S. (2020, June 10). In the COVID-19 era, female leaders are shining — Here's why. *NBC News*. Retrieved from <https://www.nbcnews.com/known-your-value/feature/covid-19-era-female-leaders-are-shining-here-s-why-ncna1227931>

Zheng, X., Lai, Y. M., Chow, K., Hui, L. C., & Yiu, S. (2011). Sockpuppet Detection in Online Discussion Forums. *2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. doi:10.1109/iihmsp.2011.69

6.3 LIST OF FIGURES

All figures that are not mention in the following list were either designed or created by the author, Rosanina Estrella

Figure 1.1 Noel-Leeming New Zeland. (2020, April 3). Noel Leeming Nintendo Switch competition. Retrieved August 07, 2020, from <https://www.facebook.com/Noel-Leeming-New-Zealand-102031001462435/>

Figure 1.2 NZ Masks. (2020). NZ Masks sale. Retrieved May 01, 2020, from masks-nz.myshopify.com

Figure 2. BT.com. (2018). Opinion: People need to stop being shamed for falling for fraud. Retrieved August 07, 2020, from <https://home.bt.com/lifestyle/money/mortgages-bills/opinion-people-need-to-stop-being-shamed-for-falling-for-fraud-11364232954184>

Figure 3: Louis, G. (2018). Man holding camera. Retrieved from <https://unsplash.com/photos/mtxZQ4vz3-w> (Originally photographed 2018)

Figure 4. Visualisation of framework created by research author Rosanina Estrella based on the information found in: Stabek, A., Watters, P., & Layton, R. (2010). The Seven Scam Types: Mapping the Terrain of Cybercrime. *2010 Second Cybercrime and Trustworthy Computing Workshop*. doi:10.1109/ctc.2010.14

Figure 5: Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, 29(3), 306-321. doi:10.1080/0960085x.2020.1771222

Figure 6. Smith, E. H. (1922). *Confessions of a Confidence Man: A Handbook for Suckers*. Independently Published.

Figure 7. Armstrong, G., Adam, S., Denize, S., Volkov, M., & Kotler, P. (2018). *Principles of Marketing* (7th ed.). Melbourne, VIC: Pearson Education Australia.

Figure 8. Visualisation of framework created by research author Rosanina Estrella based on the information found in: Andzulis, J. ", Panagopoulos, N. G., & Rapp, A. (2012). A Review of Social Media and Implications for the Sales Process. *Journal of Personal Selling & Sales Management*, 32(3), 305-316. doi:10.2753/pss0885-3134320302

Figure 12. Boundy, A., Sean, Elizabeth, & Kimberly. (2020). Tips to avoid scams - Netsafe – Providing free online safety advice in New Zealand. Retrieved August 07, 2020, from <https://www.netsafe.org.nz/scam-tips/>

Figure 13. Boyd, J. (2019, January 25). The History of Facebook: From BASIC to global giant. Retrieved August 04, 2020, from <https://www.brandwatch.com/blog/history-of-facebook/>

Figure 14. Noel Leeming. (2020, July 1). Noel Leeming Scam Alert. Retrieved August 07, 2020, from <https://www.facebook.com/NoelLeemingOnline/posts/10158499803573276>
Figure 17. Consumer. (2020). Scams and how to avoid them. Retrieved August 07, 2020, from <https://www.consumer.org.nz/articles/scams>

Figure 18. Visualisation created by research author Rosanina Estrella based on the information found in Radio New Zealand. (2020). Covid-19: RNZ News. Retrieved August 06, 2020, from

<https://www.rnz.co.nz/news/covid-19>

Figure 19. New Zealand Government. (2020). Unite against COVID-19. Retrieved August 06, 2020, from <https://covid19.govt.nz/>

Figure 20. New Zealand Government. (2020). Unite against COVID-19. Retrieved August 06, 2020, from <https://covid19.govt.nz/>

Figure 21. New Zealand Government. (2020). Unite against COVID-19. Retrieved August 06, 2020, from <https://covid19.govt.nz/>

Figure 24. Ministry of Education. (2020, April). Distance learning support during the COVID-19 event. Retrieved August 07, 2020, from <https://learningfromhome.govt.nz/>

Figure 25. NZ Association of Registered Hairdressers. (2020). 3 months free membership. Retrieved August 07, 2020, from <https://www.facebook.com/NzarhNzAssociationOfRegisteredHairdressers/photos/a.274288449321970/2863328950417894/?type=3>

Figure 26. Golf Warehouse. (2020, May 31). SALE ends tomorrow 5:00pm In-store & 11:59pm online 📍 Don't Miss out - <https://t.co/2b3odGVQV5> pic.twitter.com/GKhQtHAaNz. Retrieved August 07, 2020, from <https://twitter.com/golfwarehousenz/status/1267003458940538881>

Figure 27. Beds4u. (2020). LOCKDOWN BED SALE. Retrieved August 07, 2020, from https://www.instagram.com/beds4u_nz/

Figure 28. Pure Water. (2020). Pure Water. Retrieved August 07, 2020, from <http://nzwaterpurifier.com/>

Figure 29. Genesis II Church. (2008). Miracle Mineral. Retrieved from <https://miraclemineral.co.nz/>

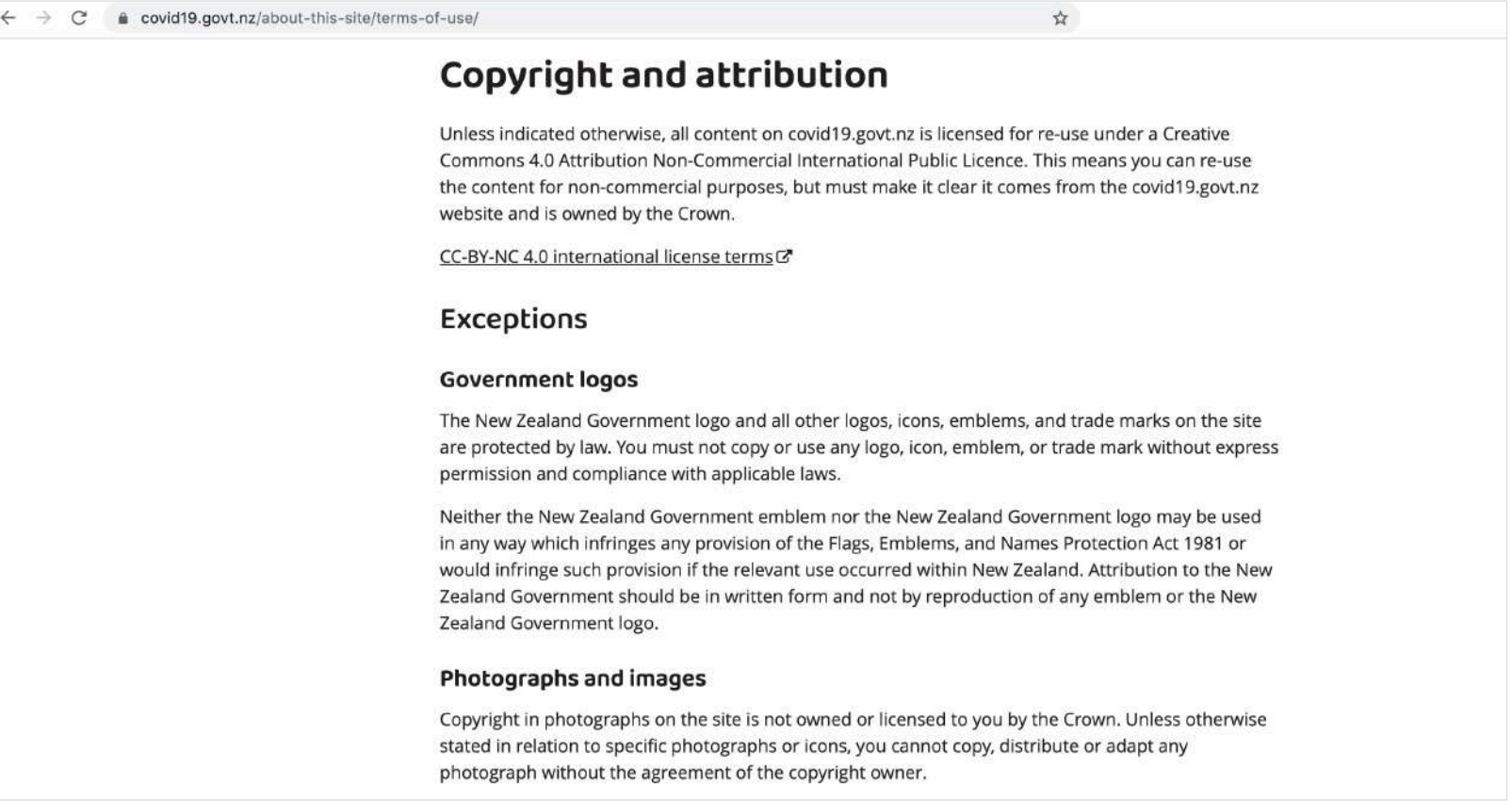
Figure 30. Gill Higgins, F. (2019, May 07). Company behind Hayley Holt face cream scam exposed. Retrieved August 07, 2020, from <https://www.tvnz.co.nz/one-news/new-zealand/company-behind-hayley-holt-face-cream-scam-exposed>

Figure 70. Springload. (2020). Simple Trace - Help fight COVID-19. Retrieved August 07, 2020, from <https://simpletrace.nz/>

Figure 72. Springload. (2020). Simple Trace - Help fight COVID-19. Retrieved August 07, 2020, from <https://simpletrace.nz/>












6.4 APPENDIX

APPENDIX A: Unite against COVID-19 branding usage





According to covid19.govt.nz's Terms of use I am able to use all content on the website (includeing Unite against COVID-19 branding for non-commercial purposes, but must make it clear it comes from the covid19.govt.nz

New Zealand Government. (2020). Unite against COVID-19. Retrieved August 06, 2020, from <https://covid19.govt.nz/>

Date	Thumbnail	Author	ID	Media Type	License	
7/15/20, 11:19 PM		© CGTrader	430836431	3D Model	Enhanced	License Again Download
8/11/20, 8:16 AM		© HQ3DWOOD	4308972076	3D Model	Enhanced	License Again Download
8/21/20, 8:16 AM		© Marcus	4295002960	3D Model	Enhanced	License Again Download
8/21/20, 8:09 AM		© HQ3DWOOD	4294398823	3D Model	Enhanced	License Again Download
8/21/20, 8:09 AM		© HQ3DWOOD	4293812490	3D Model	Enhanced	License Again Download
8/21/20, 8:09 AM		© HQ3DWOOD	4293812490	3D Model	Enhanced	License Again Download
8/21/20, 8:09 AM		© HQ3DWOOD	4293812490	3D Model	Enhanced	License Again Download
8/21/20, 8:09 AM		© HQ3DWOOD	4293812490	3D Model	Enhanced	License Again Download
8/21/20, 8:09 AM		© HQ3DWOOD	4293812490	3D Model	Enhanced	License Again Download
8/21/20, 8:09 AM		© HQ3DWOOD	4293812490	3D Model	Enhanced	License Again Download
8/21/20, 8:09 AM		© HQ3DWOOD	4293812490	3D Model	Enhanced	License Again Download

I am using the Enhanced Licence for 3D models used for Adobe Dimension. Any 3D model that is not listed was a provided asset by Adobe Dimension.

Adobe. (2020). Adobe Stock: License information and Terms of Use. Retrieved August 07, 2020, from <https://stock.adobe.com/license-terms>

License Certificate	freepik																												
																													
<table><tr><td>License type:</td><td>Premium license (Unlimited use without attribution) *</td></tr><tr><td>Licensor's Author:</td><td>11freestock - Freepik.com</td></tr><tr><td>Licensor:</td><td>nina estrella</td></tr><tr><td>For the item:</td><td>Portrait beautiful young asian woman wear mask for protect coronavirus or covid19</td></tr><tr><td>Download date:</td><td>07 Aug 2020</td></tr><tr><td>Subscription ID:</td><td>ag_b0be53ee-215f-4e7b-9094-f5969dc47242 **</td></tr><tr><td>Item url:</td><td>https://www.freepik.com/free-vector/portrait-beautiful-young-asian-woman-wear-mask-for-protect-coronavirus-or-covid19_8258588.htm</td></tr></table>	License type:	Premium license (Unlimited use without attribution) *	Licensor's Author:	11freestock - Freepik.com	Licensor:	nina estrella	For the item:	Portrait beautiful young asian woman wear mask for protect coronavirus or covid19	Download date:	07 Aug 2020	Subscription ID:	ag_b0be53ee-215f-4e7b-9094-f5969dc47242 **	Item url:	https://www.freepik.com/free-vector/portrait-beautiful-young-asian-woman-wear-mask-for-protect-coronavirus-or-covid19_8258588.htm	<table><tr><td>License type:</td><td>Premium license (Unlimited use without attribution) *</td></tr><tr><td>Licensor's Author:</td><td>Alexvolat - Freepik.com</td></tr><tr><td>Licensor:</td><td>nina estrella</td></tr><tr><td>For the item:</td><td>Anonymous man hiding his face behind neon mask in a colored smoke</td></tr><tr><td>Download date:</td><td>07 Aug 2020</td></tr><tr><td>Subscription ID:</td><td>ag_b0be53ee-215f-4e7b-9094-f5969dc47242 **</td></tr><tr><td>Item url:</td><td>https://www.freepik.com/free-vector/anonymous-man-hiding-his-face-behind-neon-mask-in-colored-smoke_7454353.htm</td></tr></table>	License type:	Premium license (Unlimited use without attribution) *	Licensor's Author:	Alexvolat - Freepik.com	Licensor:	nina estrella	For the item:	Anonymous man hiding his face behind neon mask in a colored smoke	Download date:	07 Aug 2020	Subscription ID:	ag_b0be53ee-215f-4e7b-9094-f5969dc47242 **	Item url:	https://www.freepik.com/free-vector/anonymous-man-hiding-his-face-behind-neon-mask-in-colored-smoke_7454353.htm
License type:	Premium license (Unlimited use without attribution) *																												
Licensor's Author:	11freestock - Freepik.com																												
Licensor:	nina estrella																												
For the item:	Portrait beautiful young asian woman wear mask for protect coronavirus or covid19																												
Download date:	07 Aug 2020																												
Subscription ID:	ag_b0be53ee-215f-4e7b-9094-f5969dc47242 **																												
Item url:	https://www.freepik.com/free-vector/portrait-beautiful-young-asian-woman-wear-mask-for-protect-coronavirus-or-covid19_8258588.htm																												
License type:	Premium license (Unlimited use without attribution) *																												
Licensor's Author:	Alexvolat - Freepik.com																												
Licensor:	nina estrella																												
For the item:	Anonymous man hiding his face behind neon mask in a colored smoke																												
Download date:	07 Aug 2020																												
Subscription ID:	ag_b0be53ee-215f-4e7b-9094-f5969dc47242 **																												
Item url:	https://www.freepik.com/free-vector/anonymous-man-hiding-his-face-behind-neon-mask-in-colored-smoke_7454353.htm																												
<p><small>* as defined in the standard terms and conditions on Freepik.com</small></p> <p><small>** Agreement valid only upon payment of a subscription</small></p> <p>For any queries related to this document or license please contact Freepik Support via www.freepik.com/profile/support</p>	<p><small>* as defined in the standard terms and conditions on Freepik.com</small></p> <p><small>** Agreement valid only upon payment of a subscription</small></p> <p>For any queries related to this document or license please contact Freepik Support via www.freepik.com/profile/support</p>																												
<table><tr><td>License type:</td><td>Premium license (Unlimited use without attribution) *</td></tr><tr><td>Licensor's Author:</td><td>Alexvolat - Freepik.com</td></tr><tr><td>Licensor:</td><td>nina estrella</td></tr><tr><td>For the item:</td><td>Anonymous man in black hoodie hiding his face behind a neon mask</td></tr><tr><td>Download date:</td><td>07 Aug 2020</td></tr><tr><td>Subscription ID:</td><td>ag_b0be53ee-215f-4e7b-9094-f5969dc47242 **</td></tr><tr><td>Item url:</td><td>https://www.freepik.com/free-vector/anonymous-man-in-black-hoodie-hiding-his-face-behind-neon-mask_6670823.htm</td></tr></table>	License type:	Premium license (Unlimited use without attribution) *	Licensor's Author:	Alexvolat - Freepik.com	Licensor:	nina estrella	For the item:	Anonymous man in black hoodie hiding his face behind a neon mask	Download date:	07 Aug 2020	Subscription ID:	ag_b0be53ee-215f-4e7b-9094-f5969dc47242 **	Item url:	https://www.freepik.com/free-vector/anonymous-man-in-black-hoodie-hiding-his-face-behind-neon-mask_6670823.htm	<p><small>* as defined in the standard terms and conditions on Freepik.com</small></p> <p><small>** Agreement valid only upon payment of a subscription</small></p>														
License type:	Premium license (Unlimited use without attribution) *																												
Licensor's Author:	Alexvolat - Freepik.com																												
Licensor:	nina estrella																												
For the item:	Anonymous man in black hoodie hiding his face behind a neon mask																												
Download date:	07 Aug 2020																												
Subscription ID:	ag_b0be53ee-215f-4e7b-9094-f5969dc47242 **																												
Item url:	https://www.freepik.com/free-vector/anonymous-man-in-black-hoodie-hiding-his-face-behind-neon-mask_6670823.htm																												



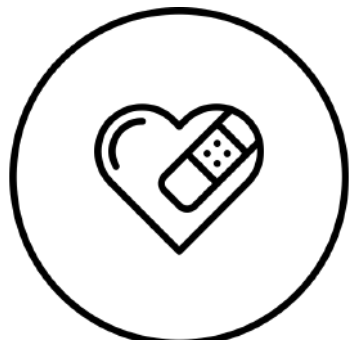
Created by luketaibai
from Noun Project



Created by Flatart
from Noun Project



Created by Giselle Pereira
from Noun Project



Created by Chameleon Design
from Noun Project

All iconography that was used was from thenounproject.
com and is licensed as Creative Commons CCBY

When using it for any project, you are required to give
credit to the icon’s creator or purchase a royalty-free
license.



This icon was taken from Flaticon using the Flaticon
License (Free for personal and commercial purpose with
attribution). Created by iconixariconixar.

[flaticon.com/free-icon/stop-sign_3225531?term=stop&pa
ge=1&position=25](https://www.flaticon.com/free-icon/stop-sign_3225531?term=stop&page=1&position=25)



Azevedo, N. (2018). Group of people sitting on bench. Retrieved from
https://unsplash.com/photos/Q_SeI-TqSlc (Originally photographed
2018)

