information

MDPI

Article

Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model

David Airehrour [1,*], Nisha Vasudevan Nair [1] and Samaneh Madanian [2]

[1] Nelson Marlborough Institute of Technology, Nelson 7010, New Zealand; nishavnair88@gmail.com
[2] School of Engineering, Computer and Mathematical Sciences, Auckland University of Technology, Auckland 1010, New Zealand; sam.madanian@aut.ac.nz
* Correspondence: david.airehrour@nmit.ac.nz

Received: 21 March 2018; Accepted: 1 May 2018; Published: 3 May 2018

Abstract: Social engineering attacks are possibly one of the most dangerous forms of security and privacy attacks since they are technically oriented to psychological manipulation and have been growing in frequency with no end in sight. This research study assessed the major aspects and underlying concepts of social engineering attacks and their influence in the New Zealand banking sector. The study further identified attack stages and provided a user-reflective model for the mitigation of attacks at every stage of the social engineering attack cycle. The outcome of this research was a model that provides users with a process of having a reflective stance while engaging in online activities. Our model is proposed to aid users and, of course, financial institutions to re-think their anti-social engineering strategies while constantly maintaining a self-reflective assessment of whether they are being subjected to social engineering attacks while transacting online.

Keywords: social engineering attack; cyber-attacks; phishing; malware; New Zealand; banking

1. Introduction

Over the last 10 years, digitalization has revolutionized commercial and social collaborations. It has changed the way business, training, communication and data sharing are conducted. Advancements in information technology, especially the internet, has opened an era of opportunities for organizations, especially for the banking sector, to serve their customers through new channels. From small-scale transactions to corporate operations, transactions are now made in an instant due to advancements in technology. This has led people all over the world to depend on the banking system for various financial transactions since it provides a secure, safe and convenient way to create a good financial future. However, with the ease of banking operations comes several threats and vulnerabilities, which have affected this industry. The banking industry has been exposed to numerous security and privacy vulnerabilities.

Cybercriminals are mindful of this upheaval and are taking full advantage of vulnerabilities in the banking system. A survey by Price Waterhouse Cooper (PWC), a multinational professional services network, reported that 93% of financial institutions suffered security breaches in 2016, with a trend indicative of an exponential growth in cyber-attacks [1]. The key challenge in cyber security is providing protection and countering cyber-attacks whilst keeping up-to-date with growing challenges. The significance of cyber security varies according to business needs, market pressures, investment into emerging markets, business modernization prerequisites, and budget. However, billions of dollars have been invested into the financial sector of the global market to counter cyber-attacks [2]. Cybercriminals have made and are continuously making profound efforts to find advanced methods

for hacking the banking system in dynamic ways. Of several kinds of cyber-attacks, one is the social engineering attack. Social engineering attacks have become a real source of worry to the management of banking institutions, since many of their customers have been the victims of this kind of attack [3]. Social engineering attacks are one of the cyber-attacks that use human behavior to collect information to circumvent the security policies of a bank instead of using technical means of attack on systems [4]. The authors in [5] investigated and found that 64% of New Zealanders did not know of existing New Zealand cyber security issues, while 40% of those who understood the cyber security issues expressed that New Zealand lacks good secure cyber policies.

This research study assessed the major aspects and underlying concepts related to social engineering attacks, and its influence in the New Zealand banking sector. In addition, a user-reflective mitigation model was proposed. The remainder of this paper is organized as follows. Section 2 provides an in-depth literature review, which is carried out to analyze social engineering types and approaches. The significance of understanding social engineering attacks is established based on a statistical study conducted in New Zealand over the past five years. In Section 3, we utilize the results of this study to offer measures to address social engineering attacks, proposing a simple model for the mitigation of attacks. In Section 4, a model is proposed that provides users with a reflective stance that while they are online conducting their activities, they could be subjects of an ongoing online social engineering attack. Our model, therefore, provides the means to verify and reflect at every stage that online users are not victims, and, if they are, they can identify what stage of the attack they are in and take precautionary steps to avert or mitigate the attack. Finally, in Section 5, we conclude and provide some final thoughts on online banking threats and the need to maintain a continuous reflective consciousness of the possibility of social engineering attacks while online.

2. Background

2.1. Banking and Cyber-Attacks

The financial service sector is extremely diverse. According to the US Department of Treasury [2], financial services include thousands of banking institutions; providers of venture products, insurance concerns, credit and financing firms; and critical financial utility providers and their supporting service functions. Financial sectors vary extensively in size, ranging from some of the largest global banking companies with thousands of employees and billions of dollars in assets, to small credit unions and local community banks that have only a few number of employees but serve individual communities [2,6]. The financial sector forms the backbone of the global economy, with broad networks and systems across the world. Due to advancements in information and communication technology (ICT), the volume and value of transactions among financial institutions have grown enormously in recent years. This has resulted in transaction complexities and security concerns. Financial transaction service entities are connected through telecommunication systems in multiple ways. Further, third-party services such as SWIFT and Real Time Gross Settlement (RTGS) have external relationships with the banking sector, which has added to the complexity, as well as the susceptibility, of the system [6]. This has led banking operational methods and risk management strategies to be more reliant on main service providers. For instance, instant messaging services are used to transmit information regarding banking transactions, which include details about the payer, the payee and the transferred amount. SWIFT is an example of a third-party provider which connects financial systems across the world. It provides a messaging platform to the financial sector, connecting more than 200 countries together [6]. Even though interconnectedness and closer public connections have helped the banking sector to build a strong infrastructure and global payment facilities, several risks and susceptibilities can trigger cyber-attacks. In addition, the financial industry is coming to the understanding that these threats have become significantly complicated [7]. The complex nature of banking systems and practices makes it hard to respond to or detect threats in the event of an organized cyber-attack, as in the case of Coincheck–a Japanese-based cryptocurrency platform that

was hacked to the tune of US$530 million [8]. To compound the issue, security specialists believe that the trend and frequency of threats will continue to grow [7].

2.2. The New Zealand Banking System

According to the Reserve Bank of New Zealand, there are 24 registered banks in New Zealand [9]. The concept of internet banking in New Zealand developed during the significant upgrade of modern telecommunication infrastructure and internetworking. This provided a favorable environment for the establishment of online financial services over the public network. In 1996, ASB (Auckland Savings Bank) first introduced internet banking, offering several services through their branches across New Zealand [10]. This was followed by Bank Direct, which commenced internet banking in mid-1997. Bank of New Zealand (BNZ) and National Bank of New Zealand (NBNZ) later followed suite. In early 2001, Australia and New Zealand (ANZ) and Westpac both enabled online banking. The last bank to offer internet banking facilities was Kiwi Bank in 2002. During that period, more than 90 percent of the online internet banking market was controlled by ANZ, ASB, BNZ and Westpac [11]. According to Statistics New Zealand [12], approximately 2.25 million Kiwis use online banking facilities through their mobile phones or desktop/laptops to check daily transactions, while the population of New Zealand stands at 4.6 million [12]. In New Zealand, typical online banking services include daily transactions, payments, product applications, mortgage/loan calculators, location services and contacts.

2.3. Social Engineering Attacks

According to Christopher Hadnagy, the term social engineering is defined as "the act of manipulating a person to take an action that may or may not be in the target's best interest" [13]. In contrast to this definition, SANS Institute describes social engineering as "a euphemism for non-technical or low-technology means—such as lies, impersonation, tricks, bribes, blackmail and threats used to attack information systems" [14]. The descriptions above provide an insight into how social engineering attacks rely purely on the human factor. An attacker may use human behavior as a tool to attack information systems by manipulating an unsuspecting target. Social engineering attacks are multifaceted and include physical, social and technical aspects, which are used at different stages of the actual attack. This section presents an organized account of common maneuvers, strategies and tactics used in social engineering attacks.

2.3.1. The Attack Cycle

The social engineering attack process was first described by Kevin Mitnick. He described it as an attack cycle of four phases [15,16]:

1. Research: This involves gathering information about the target. The final result is dependent on the quality of the information collected at this stage. The data collected is utilized in succeeding phases and is of crucial importance in making the attack successful.
2. Developing Rapport and Trust: Various types of social engineering techniques are deployed in this phase to ensure the victim trusts the attacker. The data collected in the first phase, such as public name, employer's details, and company details, are used to make the victim believe they are truly dealing with the organization.
3. Exploiting Trust: Attackers manipulate human behavior and exploit trust and stealthily steal the desired information. This can be executed in multiple ways, for example email spoofs, scam phone calls, or malware installation.
4. Utilize Information: This final phase is also referred to as "cashing in", where the information gained from the previous phases is used to perpetrate the attack.

Various researchers have presented variants of Mitnick's social engineering attack cycle, providing description variants and extensions. Since social engineering attacks essentially exploit an information system by gathering details of individuals or organizations, the exploitation can be a single-stage or multi-stage attack.

- *Single-stage attack*: As the name indicates, the attack is performed just once. The information collected is utilized to exploit the users' financial transactions for fraudulent purposes. The single-stage attack ends after conducting the attack only once [3].
- *Multiple-stage attack*: A multiple-stage attack occurs when the information collected from a successful attack is used to deploy one or more similar social engineering attacks. The time duration of multiple-stage attack can be minutes, hours or even weeks or months. This depends on the nature of the threatened person and/or the organization involved [3].

2.3.2. Social Engineering Taxonomy

Several experts have given numerous approaches to categorizing the types of social engineering attacks, such as technology-based, human-based, online perception-based and intelligence-based. Some combination of types may occur during single-stage or multiple-stage attacks. A social engineering attack in the financial sector likely falls into the single-stage attack category since the attack is identifiable after one incident. When analyzing the social engineering taxonomy in relation to the financial sector, the approach may be interpersonal or non-interpersonal. Figure 1 shows two main categories of social engineering approaches and some examples based on each classification.

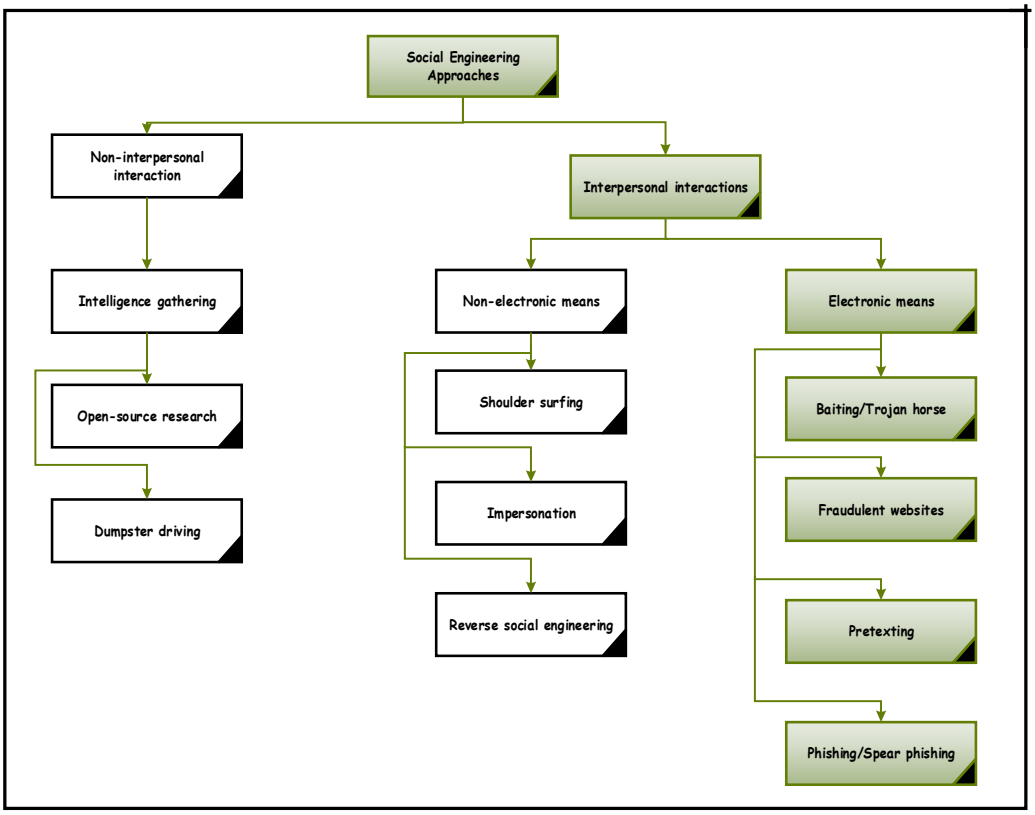

Figure 1. Social engineering attack taxonomy.

The approach described in Figure 1 is characterized according to the means of communication between the hacker and the victim. The non-electronic means of the interpersonal approach generally happens via direct face-to-face communication between the attacker and their victim. Impersonation,

shoulder surfing and reverse engineering are some of the threats that fall under this section. Using personal skills, a hacker may stealthily steal financial credentials through various techniques like friendliness, conformity and sympathy. The majority of social engineering attackers avoid face-to-face contact with their victims, but prefer to utilize electronic means like email, the internet or any other digital media to exploit human behavior, betray the victim and achieve their objective. Baiting, website spoofing, pretexting and phishing are among the most popular social engineering attacks through digital media. The authors in [17] outlined the different types of online social engineering attacks. Our interest is electronic means of perpetrating various kinds of social engineering attacks, hence, a description of some popularly used online attacks is presented below.

1. Vishing: Vishing is a form of social engineering attack in which an attacker uses a phone call to trick a victim to reveal sensitive information such as credit card number, pin code or detailed home address. The attack exploits voice over IP (VoIP) technology since it is cheap, and the attacker could be calling from anywhere around the world, with their identity concealed [18,19].
2. Baiting/Trojan Horse: Baiting uses digital devices such as USB drive or RAM to gain a victim's attention and perpetrate an attack. This technique relies on human curiosity to deploy the attack, which in turn spreads the malware installed on their device [3]. As a result, the organization's internal network will fall under the control of the hacker.
3. Fraudulent Websites: With this attack type, the hacker exploits a victim's trust, leading them to access their fake website, which automatically downloads malicious files onto the victim's computer [16]. As with the Trojan Horse attack, the downloaded file gives the attacker access to sensitive information from the local browser of the victim.
4. Pretexting: This is an exploit that uses a scripted scenario to trick the victim to reveal sensitive information or accomplish other malicious activities unknowingly. Reverse social engineering is the best example for pretexting, in which an attacker creates a scene or situation and an innocent victim believes that the hacker can provide a solution [3].
5. Phishing/Spear Phishing: Phishing is the most popular social engineering attack in the online banking system. Typically, a hacker sends an email using the legitimate organization's trademark to get the attention of their target. The fake email appears to be from a trusted bank requesting that the customer updates their account information using the provided link (which is a bogus link). The attached fraudulent website leads the victim to divulge sensitive financial credentials [3]. Phishing is considered one of the most effective attacks and the technique has become more sophisticated over the years. Spear Phishing uses the personal details of a potential victim to tailor the email content, with a higher probability of success [16].

2.3.3. Causative Factors

The US Software Engineering Institute [3], reported three contributing factors as the major causative factors for social engineering attacks: *organizational*, *demographic* and *human* [3]. The three categories, along with the sub-factors, are discussed below.

1. Demographic Factors: Gender, age, personality characters and cultural factors are the main demographic aspects which influence social engineering attacks. These susceptibilities, however, may vary between male and female, young and old, literate and illiterate and so on. A survey conducted by Carnegie Mellon University revealed that women were more susceptible than men. The reason advanced for this was that women feel more comfortable using digital media and are more likely to reply to junk advertisements or commercial offers [3]. Factors such as normative commitment, affective commitment, trust and fear are related to personality traits and contribute to susceptibility to attacks [20].

2. Organizational Factors: Insufficient management and security policies can make an organization vulnerable to cyber-attacks. Strong cyber security strategies and network protections must be ensured to reduce any kind of exploits. The lack of proper resource management and job pressure may poorly influence human performance [3]. Organizational components can create susceptibilities that attackers may abuse, directly or indirectly, for financial benefit. Failure of management systems can also negatively impact employee fulfilment, causing discontentment that could potentially result in the employee sabotaging the organization.
3. Human Factors: An individual may exhibit many emotions depending on their character, surroundings, habits, or physical impairments. These emotions and circumstances may well be utilized by an attacker to make an attack successful. Lack of attention, memory failure, faulty judgment, poor risk perception, casual values about compliance, stress, anxiety and physical impairments are some of the human behaviors that create vulnerabilities. Social engineering scams, particularly phishing attacks, exploit human emotional flaws to gain unauthorized access to information. Ignorance and lack of awareness towards cyber-attacks leads to the rapid growth of social engineering attacks. Studies [21] have shown that the majority of online users have difficulty distinguishing the difference between real and fake websites.

Table 1 summarizes the prominent features of social engineering attacks, the typical information gathered, and possible outcomes of the attack. Although the methods used to deploy the attacks are different, the data collected, and the intention of the attack remains same. Table 1 supports the premise of this report by characterizing the attacks based on the approaches and patterns used in the attacks.

Table 1. Summary of social engineering attack characteristics.

Salient Features	Information Captured	Potential Consequences
Appeal • Generally good news or bad news • Sense of urgency • Delicate or confidential matter • Impersonating known sender **Desired response** • Deliver detailed information • Update account information • Click on link in email message • Open an attachment **Suspicious indicators** • Generic greetings • Suspicious context • Poor grammar or spelling • Strange or unusual sender • Incorrect information • Legitimate embedded URLs	• Account information • User name • Password and PIN • Credit card number • Social security number • Bank account number • Bank routing number • Email address • Telephone number • Other personal information	• Financial loss • Identity theft • Personal, confidential or proprietary information stolen • Intellectual property stolen • Computer compromised, malware or virus implanted • Data, software or hardware assets manipulation • Political gain • Denial of service

2.3.4. New Zealand Banks and Cyber-Attacks: A Five-Year Review

In 2016, Symantec—an IT security organization—revealed that New Zealand's global rank rose for five out of six cyber threat types including: phishing, bots, spam, web and network attacks [22]. Internal security threats reported by Symantec revealed that New Zealand faced about 108 cyber-attacks per day and that it was becoming a growing hazard. The report noted that phishing traffic in New Zealand ranked among the highest in the world.

Figure 2 reveals that New Zealand, like other countries, is faced with cyber security issues at a rate of nearly 10% of global cybercrimes. Global economic crime research, as surveyed by Price Waterhouse Cooper [1], showed that 40% of New Zealand businesses had experienced security breaches in the past two years [1].

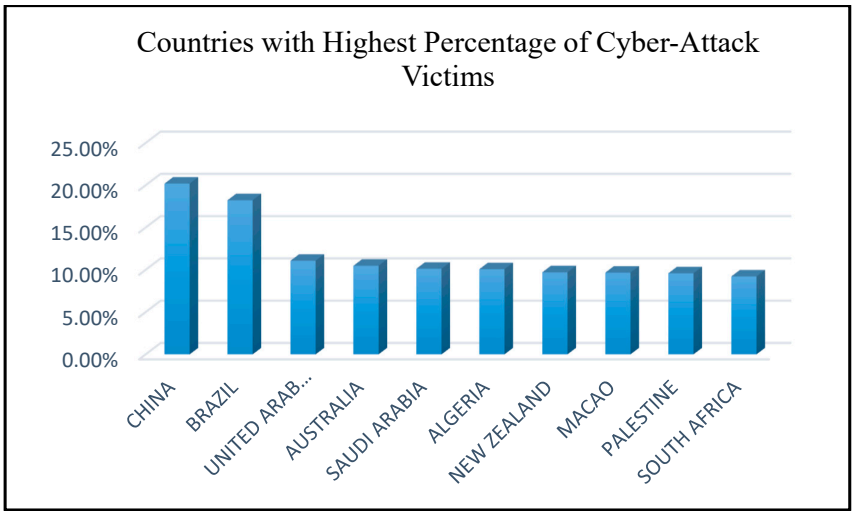

Figure 2. Countries with the highest percentage of cyber-attack victims [1].

These destructive attacks could be personal or corporate, and the impact was the loss of confidential data leading to financial crisis and reputational damage. Figure 3 shows a five-year statistical review of the different cyber-attacks faced by New Zealand during the period 2012–2016. From the figure, it can be seen that New Zealand faced more social engineering-based attacks than any other attacks during the period under review. From Figure 3, out of the various types of cyber-attacks in the New Zealand banking sector, social engineering attacks and phishing attacks were the most popular and widely perpetrated attacks. Social engineering and phishing are two sides of the same coin. Phishing uses social engineering techniques to trick end users and gather sensitive information [23].

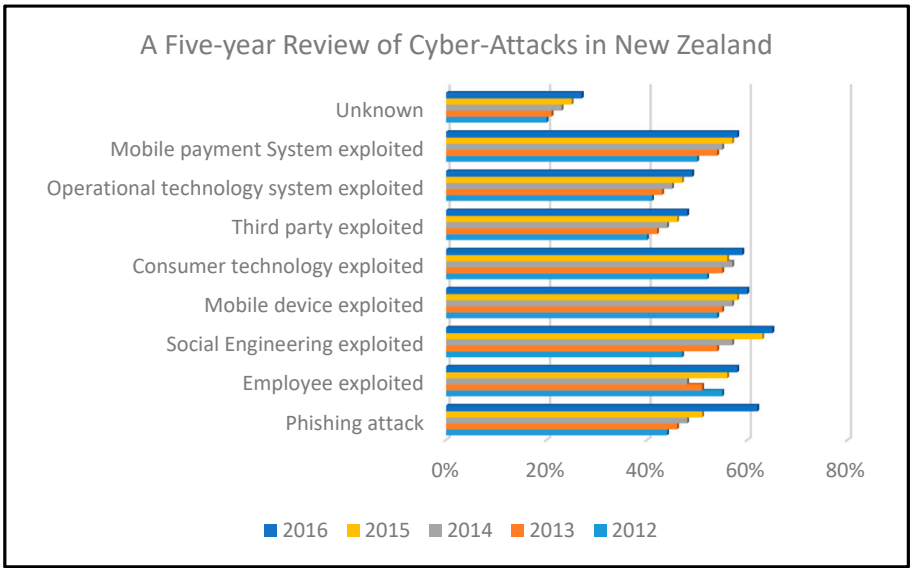

Figure 3. New Zealand cyber-attacks: a five-year review [23].

In 2016, the percentage of social engineering attacks and phishing attacks was more than 60% of the overall cyber-attacks in the New Zealand financial sector. Even though social engineering techniques targeted individuals, the real focus of this assault was the organizations the individuals where affiliated with. Phishing is as dangerous as social engineering attacks, particularly in the financial sector. Studies [24] show that more than 37% of phishing attacks utilize the trademarks of organizations and their traditional banking policies, while 21% of phishing attacks focus mainly on financial credentials. These kinds of attacks undermine customers' trust in banks, put banks at significant risk of identity theft, and cause financial losses. Cyber security, especially in the financial sector, is a complex and intricate challenge that is growing in significance. In PWC's Global Economic Crime Survey, the security team found that around 7111 financial firms across the world had cyber vulnerabilities [25]. As technology advances, cyber criminals find new, sophisticated tools for attacking and exploiting businesses. Legacy IT systems have become a risk factor to the cyber security departments of major banks and the majority of financial institutions across the world have spent billions on cyber security [25].

2.4. Analysis of Customer Behaviour to Social Engineering Attacks

The authors in [21] expressed that the tactics used by hackers reveal how vulnerable users can be when online. Their study showed that the impact of "human factors" in social engineering attacks. Cyber-attackers have historically relied on technical attacks to exploit their victims, but today, there has been a swift change to the use of ingenious social engineering techniques to perpetrate attacks. These techniques include: malware installation, the art of stealthily stealing user credentials, and making fraudulent transactions. Figure 4 shows that in the past five years, the majority of email-based financial fraud attacks were kick-started by human clicks. Figure 4 further reveals that cyber criminals exploit the emotional weakness of human behavior by providing malicious URLs that link to credential phishing. The attacks can be international; aimed at victims in specific geographical locations using attachments in their local languages [26]. The impact of every attack relies on how the victims responds to the online malware.

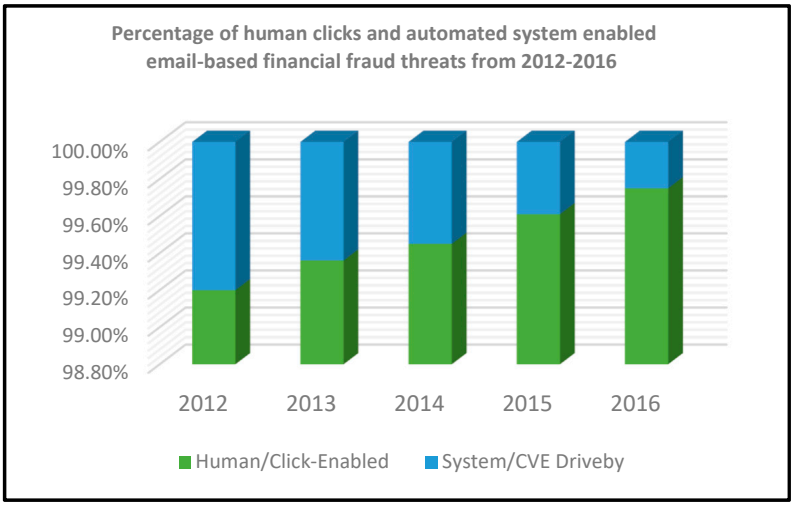

Figure 4. Percentage of human clicks and automated systems enabled by email-based financial fraud threats between 2012–2016 [26].

2.4.1. Online Customer Behavior

Online customer behavior towards online banking depends on various factors, such as demographic characteristics, internet experience, perceived security and available services [10]. According to New Zealand Statistics, in 2015, the adoption of online banking was becoming

increasingly popular among all age groups [12]. Table 2 shows the percentage of online banking users based on age group in New Zealand. It can be inferred from Table 2 that a high a percentage of users across all age groups use online banking facilities for various services. It is not an activity limited to youth, although they are more likely to interact with digital means of communication. In fact, more than 50% of senior citizens (65+ years) used online banking infrastructure.

Table 2. Age group distribution of the percentage of online banking users in New Zealand. Source: [12].

Age Group (Years)	Percentage of Online Banking Users
15–24	68%
25–34	87%
35–44	81%
45–54	73%
55–64	69%
65–74	55%
75+	35%

Convenience, time-saving and effort-saving are among some of the factors that attract customers to use internet banking. With this huge number of online users, cybercriminals have an even greater platform of attack. Most users (across all age groups) are likely to have been taught how to log on and use their online facilities, but they may not have been adequately sensitized to being cyber vigilant. The authors in [26] found that more than 90% of cyber-attacks in the financial sector were initiated by human-clicks on malicious attachments while using online services.

2.4.2. Customers' Perception of Online Threats

There is no doubt that online banking has become an established means of financial dealing. The adoption of digitalization in the banking sector has created a rise in email communication between service providers and their customers. Symantec estimated that the number of daily emails in circulation was 190 billion in 2016 [21]. The popularity of email communication has further accentuated its use by cybercriminals. Scammers use a victim's personal data gathered from social media profiles to create personalized phishing emails, which are highly convincing. This increases the likelihood of a positive response from the target victim to a phishing attack. Figure 5 shows the results from a New Zealand survey into the likelihood of online users opening email attachments or responding to online requests or links related to their banking activities. It shows how susceptible online users can be with regards to their online subscription services like online banking. This is further corroborated by the authors in [21], that the percentage of phishing email in the finance sector was about 52.1% in 2016.

Among the key metrics analyzed in Figure 5, was online user's perception of phishing attacks when engaging in online banking services. Other metrics were customers' level of technical knowledge in identifying the threats behind every pop-up, web browsing and online advertisements. The trend shows that men were more technically savvy than women, and hence, were less likely to respond to suspicious requests. Also, users in the age group of 28–38 were more cautious in providing their personal details online. According to Fu [5], a user's security awareness is an important influential factor for a social engineering attack to be successful. According to [5], New Zealanders are generally trusting of people which makes them susceptible to attacks. In addition, more than half of New Zealanders are unaware of the latest data breaches and security warnings.

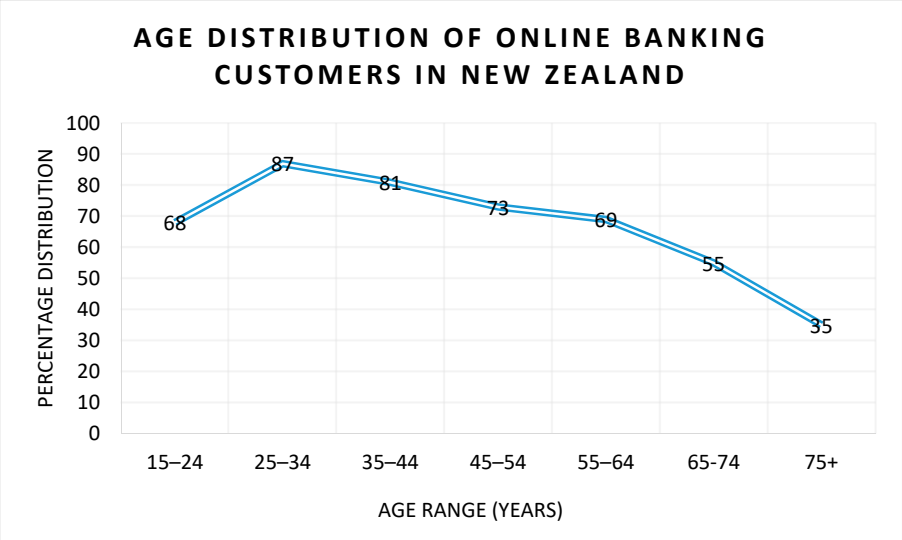

Figure 5. Age distribution of online banking customers in New Zealand (Data from [12]).

2.5. Impact of Social Engineering Attacks in the Banking Sector

Most cyber security study reports have shown that the increasing trend in social engineering attacks on the financial sector aims at a nation's economic interests, and not on specific customers [27]. Any cyber risk can affect a bank's financial infrastructure, in addition to reputational damage to customers' trust [28], while the collective impact of a security breach at few banks can cause significant consequences to a nation's financial markets due to their interconnectedness with a nation's economy. According to the authors in [18], one out of five call center staff at UK banks were engaged in fraudulent activities. Social engineering attacks on the banking industry basically involve a three-step hierarchy attack process of *legitimate access*, *device control* and *credentials theft*. Based on this hierarchy process, the attacker compromises a victim's security through social engineering tricks, and further takes control of the victim's computer system (mostly through malware). Finally, the malware mines the personal information of the victim and sends it to the attacker [18].

In 2008, a survey conducted by Microsoft showed that fraudulent, phishing website-related scams of banks accrued financial charges amounting to more than US$5 billion [29]. In another report, it was discovered that a single social engineering attack at Wells Fargo Bank amounted to US$2.1 million stolen in 2011 [30]. The Gartner Group revealed that, based on their estimations, US banks and credit card issuers lose about US$2.8 billion annually due to phishing activities [31].

Figure 6 illustrates the depth of consequences of social engineering attacks on the financial sector globally [32]. The three key factors investigated in the research of [32], after a breach in the banking system, were (i) reputational damage of the organization; (ii) customer trust and; (iii) financial losses. The significant impact of social engineering attacks on reputation in the wider market place accounted for 21.9%, which is significant for any bank globally. This translated to a 28.6% lower level of trust in the services provided by banks globally. The financial losses incurred as a result of social engineering attacks amounted to 23.1%, which is a significant value, showing that people are very susceptible to social engineering attacks.

In New Zealand, Price Waterhouse Cooper found that 29% of New Zealand organizations affected by economic crime also experienced cybercrime, while 40% of New Zealand organizations expected to experience cybercrime in the next two years [1]. The deceptive nature of cyber-attacks is such that more than half of the victims do not even know that they have been hacked.

Security and data breaches have the potential to destabilize the financial sector and customer confidence within a short period of time. Therefore, maintaining a secure banking system and

protecting customers' confidence is important for the survivability of any bank, and by extension, the performance of a nation's economy.

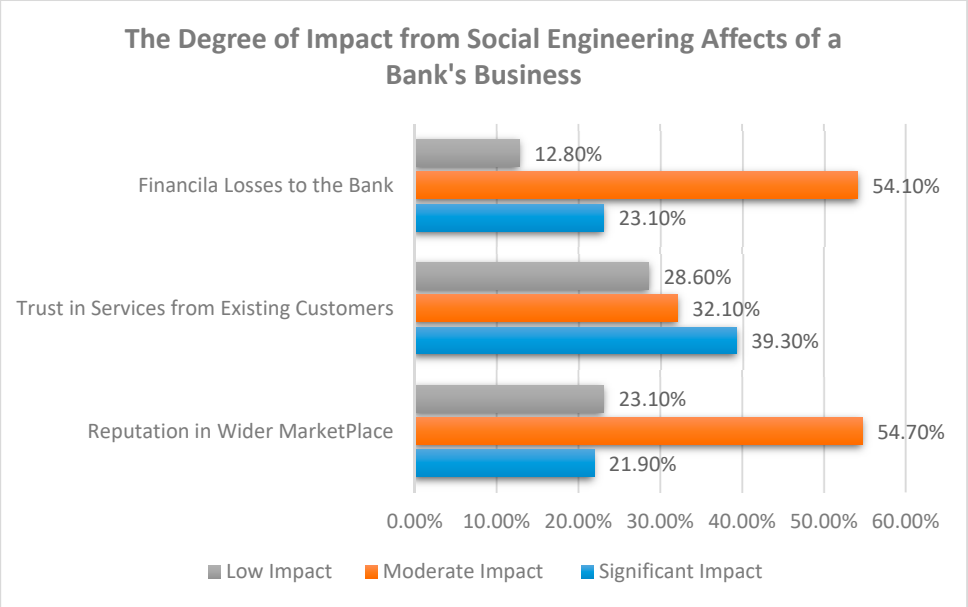

Figure 6. Global impact of social engineering attacks on key banking operations (Data from [32]).

3. Addressing Social Engineering Attacks in New Zealand Bank

Social engineering attacks can be diverse and complex since the attacks subsist on the ability to manipulate human behavior. Therefore, it is necessary to adopt security measures in multifaceted ways. Initially, proper security should be given to physical access to deny unauthenticated persons entry into a premise. Organizations must provide multiple control strategies based on the type of security [5]. Technical-oriented social engineering may be allowed up to a certain limit by implementing identity verification or multifactor authentication. This helps monitor any online, fraudulent financial transactions. Furthermore, implementing a general security policy for banks and their customers is an important element to defend against social engineering attacks. The relevance and content of security policies should be well distributed among the public via education and public enlightenment. Public enlightenment has the potency of reducing users' vulnerability to online threats while performing online financial transactions.

New Zealand Banks have adopted several offensive strategies to combat social engineering attacks. These include: fraud detection systems, exploit blockers, vulnerability shields, anti-phishing systems, signature type detection systems, authentication methods and customer alert systems. In New Zealand, fraud detection systems, authentication methods and customer practices are among the top three offensive security practices adopted by banks to mitigate the impact of cybercriminals. A discussion of the three popular offensive security practices is presented.

3.1. Fraud Detection System

New Zealand Banks like Westpac, ANZ and ASB have some secure fraud detection systems to ensure customer protection while banking online. The system monitors all banking transactions and identifies unusual activities. It also performs authentication methods when initiating international transfers. Verification codes and security questions attached to the account will authenticate the user's identity before completing any transaction. ANZ's "online code" and Westpac's "online guardian" are examples of mechanisms used to authenticate that a transaction was initiated by the real owner.

3.2. Authentication Methods

Banks use authentication methods to provide multi-level protection through the use of passwords. This includes textual password entry, and the receipt of a confirmation text through the user's registered mobile phone number or email address. This enhanced security makes it difficult for hackers to guess the password. In addition, security tokens are widely used to strengthen the authentication process. If the bank is providing authentication, then the authentication is mostly done via the user's mobile phone [33]. This multi-factor authentication strategy is implemented by most New Zealand banks.

3.3. Customer Practices

Every New Zealand bank has emphasized the role of appropriate customer behavior when conducting online banking. This includes the guidelines put forward by the banks on their official websites for customers. The guidelines include safeguard steps to follow to avoid getting trapped by spurious mail spams and bogus links. Banks advise their customers to manually type their bank login address into the internet browser when they wish to conduct online banking. In addition, customers are advised to look at the address browser to verify that the security certificate is genuine. Finally, updating account passwords or pin codes on a regular basis and storing them in a safe journal can protect a user from password attacks [34]. Banks regularly advise customers to use reliable anti-virus and firewall software on their computers and keep them updated. Regular review of one's bank transactions provides personal monitoring of one's banking activities.

3.4. Challenges of Secure Practices used by New Zealand Banks

Despite the security measures adopted by New Zealand banks, they still face many challenges in dealing with the number of perpetrated attacks, including social engineering attacks. Public awareness is considered a critical aspect for making customers aware of cybercriminals. While many banks are providing awareness through media, including social media, reports, however, show that only about 30% of banking customers are well-aware of cyber-security issues [32], Banks have good *professional* communication with their customers, but lack *social* communication with them. *Social* communication implies informal, sociable bonding between banks and their customers. This creates a communication gap and, hence, when there are poignant security breach issues, customers are largely unaware.

Apart from this communication gap and public awareness, technical policies can also be a challenge in mitigating cyber-attacks, and keeping digital identities safe and secure is also becoming a challenge. The authors in [33] expressed in their findings that the use of two factor-authentication is no longer sufficient to keep banking data safe. They further expressed that for password protected systems, an attacker can constantly monitor network traffic and, thus, find ways of intercepting passwords to gain access through the traditional authentication system [33].

3.5. Mitigating Social Engineering Attacks

Research conducted by Longitude Research [32] surveyed 250 participants knowledgeable on the cyber-security risks their organizations faced. The study was distributed across the retail (55%) and commercial banking (45%) sectors. The study revealed that social engineering attacks were commonly executed at multiple stages against target victims to break sequential layers of offensive measures. The assault generally proceeded iteratively, and occasionally deftly to exploit an individual until the last protective barrier point was broken [32]. The findings of [32] and the key challenges faced by banks while deploying cyber security strategies are summarized in Figure 7. Challenges include technical, physical, as well as individual, challenges. From the figure, the difficulty in keeping pace with rapidly changing cyber risks is one major issue banks struggle with. Of equal importance is technology limitations, like keeping up-to-date with the latest defense software and hardware. As highlighted earlier in Section 3.1, limited customer awareness is also a factor of concern, as most customers are

surreptitiously taken unware by attackers. In general, Figure 7 highlights the need for banks to take a more risk-based approach to dealing with changing cyber threats.

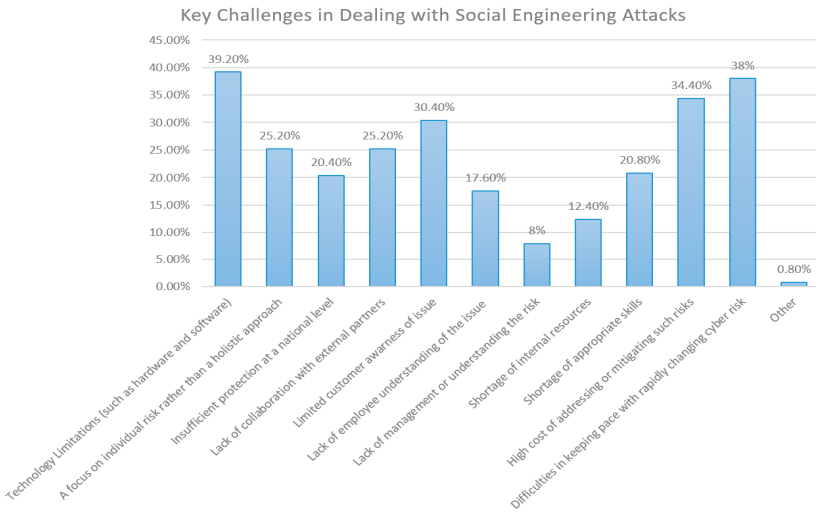

Figure 7. Key challenges in dealing with social engineering attacks (Data from [32]).

From the research presented so far, and to effectively address the social engineering attacks perpetrated by cybercriminals, a systematic analysis of possible attack patterns should be conducted to help identify the steps by which an attack commences and, thus, when counter measures can be initiated. We propose a simple mitigation model, as shown in Figure 8, to address attacks and the steps to be taken at every stage of a social engineering attack. Our model in Figure 8 is based on a single-stage social engineering attack, which consists of five stages of attack: researching the victim's personal information; planning and preparing the attack; executing the phishing attack; capturing sensitive data; and lastly, exploiting this information. For every stage, a possible cause of action is advised for an individual to take. Our proposed model could also be applied to a multi-stage attack, as every stage in the multi-stage attack is also captured in the single-stage attack scenario.

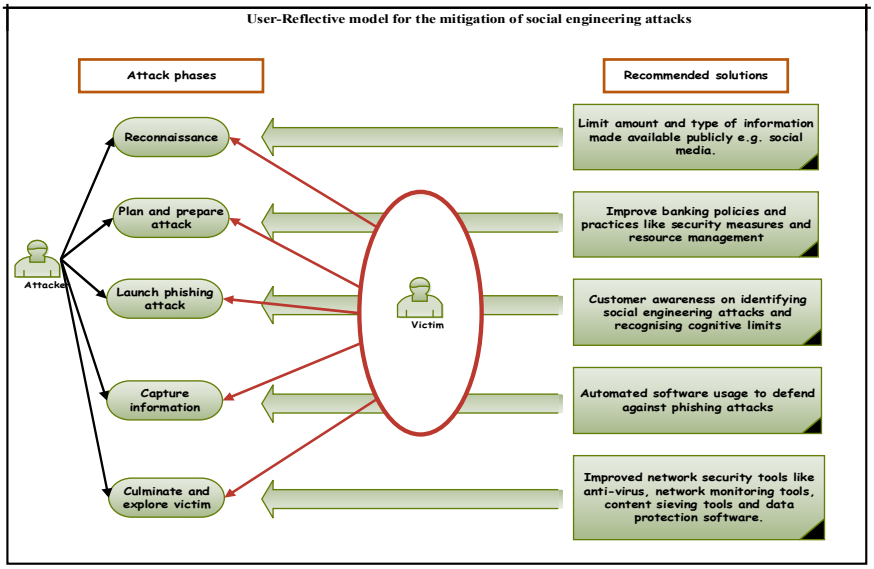

Figure 8. A user-reflective model for the mitigation of social engineering attacks.

4. The User-Reflective Mitigation Model

Most organizations are astonished with the relative ease with which their networks are penetrated via social engineering attacks. From studies [21,26] previously presented, it is quite obvious that social engineering attacks are largely due to human factors, which allows them to easily penetrate corporate networks and is, hence, a worrisome issue for organizations. The human factor has proven to be a potent means of circumventing well-hardened hardware and software security systems, yet it has often been ignored or considered extremely challenging to address.

This section proposes a user-reflective mitigation model to address single-stage social engineering attacks. The model requires users to reflect at every stage that they may have been compromised and, hence, a part of a social engineering attack. A user, therefore, maintains this reflective stance to avert attacks. The model presented in Figure 8 provides the stages of possible social engineering attacks against a victim, and the possible actions a victim may take at any stage to curb further attacks. Even if a victim has progressed through some stages with the attacker, a victim could still identify from our model what stage they are at and take appropriate steps to mitigate further attacks. The model shows the five stages of attacks and the recommended steps a user should follow to curb or mitigate the attack. The detailed stages and possible actions are given below.

i. Reconnaissance

At this stage, an attacker tries to gather as much information about a victim as possible. When a victim is unsure of the party involved, the victim should limit the amount of details divulged to the attacker. In fact, do a verification check on the attacker by confirming through reasonable channels the attacker's true identity. Also, users should limit the amount of personal information posted to public domains like the social media. Lastly, if it is a transaction involving a user's bank or organization, the user needs to report it through the provided information channels.

ii. Plan and Prepare Attack

Users should only interact via organizational verified websites and not through e-mail links received as these could be phishing mails. For email links received, users should always look at the address bar of the site to verify the authenticity of the certificate of the site. The certificate of a website can be verified by opening the certificate component of the website page and clicking on the certificate a user wishes to view. Information such as the certificate's issuing party, the validity dates of the document, encryption method and other details are listed. Every browser provides steps on how to view the certificate of a site. Users can search online and follow the steps provided to view the certificate of a website. Conventionally, risky sites do not have valid certificates; thus, users should be wary of these sites as possible scams, and hence, take appropriate steps to protect themselves by avoiding such sites. Also, if it is a transaction involving a user's bank or organization, the user needs to report it through the provided information channels.

iii. Launch Phishing Attack

Normally, users are unaware that they are being phished through fake phone calls and spam mails, for example. Under this circumstance, it is necessary for online users to be wary of suspicious mail, phone calls and other tools that may be used by attackers. Some steps at this stage could involve heeding the following steps by users and their organizations:

- Sensitizing customers/users with awareness materials on social engineering attacks and the techniques used by attackers.
- Provision of supporting materials like news reports to buttress the seriousness of social engineering attacks and their trends.

- For fake phone calls from attackers, users need to be adequately sensitized by their organizations to recognize potential attackers. A general rule of thumb is for them to never give out personal and sensitive details like pin code and credit card number under any circumstances.

As a way of making sure that other users are aware, a report of such incidents should be made by the user to their organization and possibly to law enforcement responsible for such fraud.

iv. Capture Information

Online users can receive unsolicited messages and phone calls. This, therefore, necessitates the use of a good anti-spamming and ant-phishing defense systems on a user's computer and phone. This will help filter fake mail messages received. Although some genuine mail may also be classified as such, users should always run through their spam mail to ensure that there is no important mail in the spam box before deleting them.

v. Attack Culmination and Victim Exploitation

Data protection software can be utilized by users to store their sensitive information, including passwords, credit card number, pin codes, and social security number. Even when an attacker gains remote access to a user's computer system, it is unlikely the attacker will be able to mine important data from the victim's system since the victim is using data protection software that encrypts all data and passwords stored.

4.1. Ensuring the Success of the User-Reflective Model

The success of the proposed user-reflection model hinges on the staff members of an organization adhering to the specifics of the model. In the following sections, we provide a system to ensure staff take a continuously reflective stance while performing their activities online.

4.1.1. Education and Awareness

Educating and making staff aware is a necessary action that every organization hoping to combat social engineering attacks should engage in. Every training programme should make it clear to staff that they should never divulge sensitive information such as personnel records, passwords or even sensitive office details. It should be made clear to staff that when they are being asked for sensitive information, whether via email, in person, or over the phone, they are probably being subjected to a social engineering attack and should refer to the proposed model (Figure 8) to avert the attack. Finally, staff members or victims, while maintaining a reflective stance of their activities online, should seek the advice of the relevant department should they suspect any situation they are uncomfortable with.

4.1.2. Monitoring

To ensure that staff adhere to the need for continuous reflection that they may be subjected to a social engineering attack while online, and that they also utilize the user-reflection model to evaluate their activities, a monitoring system is required to ensure this. To achieve this, the IT department of the organization could periodically run a simulated social engineering attack on staff members during their routine work. Simulated and targeted social engineering attacks like vishing and phishing emails and generic spam emails may be used. The results should be observed and evaluated, following up staff members who fail to identify the simulated malicious attacks. These staff members should be further educated and sensitized to the need to be aware and stay safe while conducting their duties online. In addition, staff members who are able to identify attacks should be acknowledged and rewarded in some way. Figure 9 provides a framework summary for the deployment and monitoring of simulated social engineering attacks in an organization.

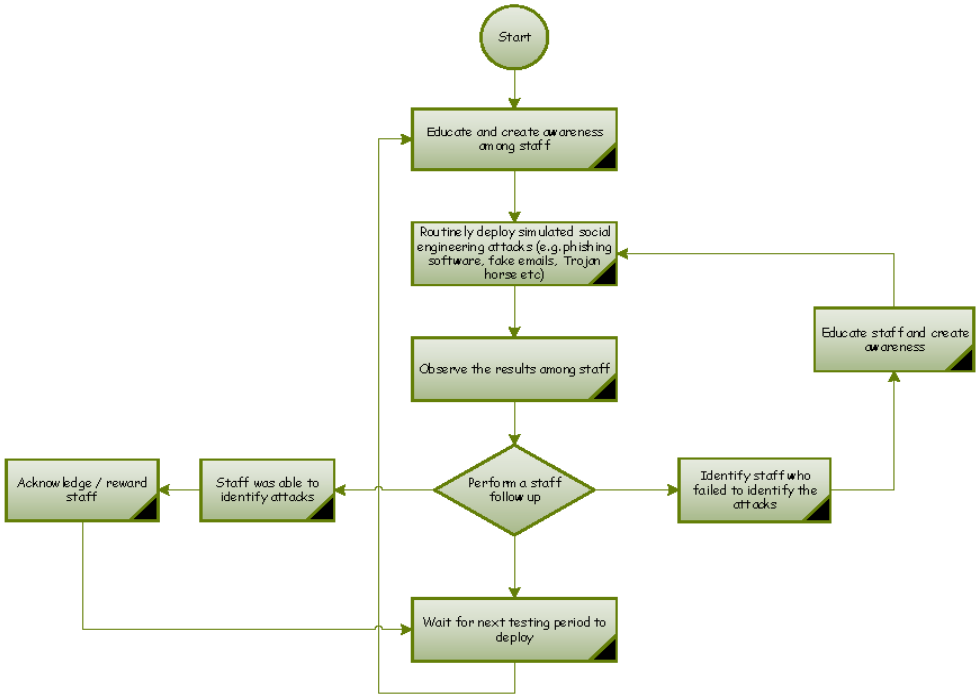

Figure 9. A monitoring system for ensuring staff adherence to a continuous reflective stance to avert social engineering related attacks.

5. Conclusions

The evolution in technology offers both opportunities and challenges to the financial sector. However, cybercriminals are also becoming ingenious and creative in their attacks, especially as they exploit on human emotions. To improve the cyber security stance of banks, new ways and tools need to be developed and deployed to fill the existing gaps created by these clever criminals and to counter the attacks they present. A holistic approach towards cyber threats is needed to elevate the threats to an operational level, which could help in making better decisions quickly and effectively. Not all threats can be analyzed and prioritized as the same, but by examining the analytics of threats retrospectively, banks could foresee attack patterns, and predict the possibility of an attack before it even happens.

We conclude with two remarks. Firstly, the New Zealand banking sector still faces, like the rest of its counterparts around the world, social engineering attacks, and this threat is becoming a growing concern. This study has discussed the effectiveness of current anti-social engineering strategies deployed by New Zealand banks and the gaps that need to be addressed. The situation is no different for other banks in the global arena. The global financial sector has found itself on a continuum of an attack platform due to its relevance to the economy of any nation, and cybercriminals will never stop at perpetrating attacks, but will continue to evolve ingenious ways to sabotage banks and their customers. Secondly, the model we have proposed is poised to give users a continuous reflection while online that the possibility always exists that they may already have been compromised, and hence, are part of a social engineering scheme that they may not be aware of. Our model, therefore, helps users avert or minimize the effect of perpetrated attacks.

As individual data are becoming increasingly compromised due to subtle attacks that appeal to human emotions, perhaps the time has come for targeted investment into education and training. This will no doubt reinforce the human firewall, with the aim of making users self-reflective of the fact that they may already be part of an elaborate social engineering attack or may be subjected to attacks while conducting their activities online.

Author Contributions: For research articles with several authors, a short paragraph specifying their individual contributions must be provided. The following statements should be used "Conceptualization, N.V.N. and D.A.; Methodology, D.A.; Validation, D.A., N.V.N. and S.M.; Formal Analysis, D.A. and N.V.N.; Investigation, N.V.N.; Resources, D.A. and S.M.; Writing-Original Draft Preparation, D.A. and N.V.N.; Writing-Review & Editing, D.A. and S.M.; Visualization, S.M.; Supervision, D.A. and S.M.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. PriceWaterhouseCoopers. *Adjusting the Lens on Economic Crime*; PriceWaterhouseCoopers (PWC): Auckland, New Zealand, 2016.
2. US Department of the Treasury. *Financial Services Sector-Specific Plan*; US Department of the Treasury: New York, NY, USA, 2015.
3. Software Engineering Institute. *Unintentional Insider Threats: Social Engineering*; IEEE Security and Privacy Workshops: San Jose, CA, USA, 2014.
4. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced Social Engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122. [CrossRef]
5. Janczewski, L.J.; Fu, L.R. Social Engineering Attacks: Model and New Zealand Perspective. In Proceedings of the 2010 International Multiconference on Computer Science and Information Technology (IMCSIT), Wisla, Poland, 18–20 October 2010.
6. World Economic Forum. *Understanding Systemic Cyber Risk*; World Economic Forum: Cologny, Switzerland, 2016.
7. Vrancianu, M.; Popa, L.A. Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests. *Amfiteatru Econ. J.* **2010**, *12*, 388–403.
8. The Hong Kong Economic Journal. *Cryptocurrency Exchange: Coincheck loses US$530 Mlllion in Hack*; The Hong Kong Economic Journal: Hon Kong, China, 2018.
9. Reserve Bank New Zealand, Register of Registered Banks in New Zealand. 8 June 2017. Available online: http://www.rbnz.govt.nz/regulation-and-supervision/banks/register (accessed on 2 March 2018).
10. Du, J. *An Empirical Analysis of Internet Banking Adoption in New Zealand*; Lincoln University: Canterbury, UK, 2011.
11. Taylor, K. *Bank Customers Logging on*; The New Zealand Herald: Auckland, New Zealand, 2002.
12. Canstar. Online Banking. Canstar: Auckland, New Zealand, May 2013. Available online: https://cdn.canstar.co.nz/wp-content/uploads/2014/03/nz-online-banking-apr-2013.pdf (accessed on 3 May 2018).
13. Hadnagy, C. *Social Engineering: The Art of Human Hackin*, 1st ed.; Wiley: Indianapolis, Indiana, 2010.
14. SANS Institute. *Glossary of Security Terms*; SANS: Boston, MA, USA, 2016.
15. Mitnick, D.S.W. *The Art of Deception: Controlling the Human Element of Security*; Wiley: Hoboken, NJ, USA, 2003.
16. Papazov, Y. *Social Engineering, North Atlantic Treaty Organization*; Science and Technology Organization: New York, NY, USA, 2016.
17. Molia, H.K.; Gohel, H.A. Protection of Computer Networks from the Social Engineering Attacks. *Int. J. Adv. Eng. Technol.* **2015**, *1*, 1.
18. Abu-Shanab, E.; Matalqa, S. Security and Fraud Issues of E-banking. *Int. J. Comput. Netw. Appl.* **2015**, *2*, 179–187.
19. Brar, T.P.S.; Sharma, D.; Khurmi, S.S. Vulnerabilities in e-Banking: A Study of Various Security Aspects. *Int. J. Comput. Bus. Res.* **2012**, *6*, 127–132.
20. Workman, M. Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. *J. Am. Soc. Inf. Sci. Technol.* **2008**, *59*, 662–674. [CrossRef]
21. Symantec. *Internet Security Threat Report*; Symantec: Sydney, Australia, 2016.
22. Radio New Zealand. *108 Cyber-Crime Attacks per Day in NZ*; RadioNZ: Wellington, New Zealand, 2016.
23. Pallavi, P.P.R.; Dudhe, D. Detection of Websites Based on Phishing Websites Characteristics. *Int. J. Innov. Res. Comput. Commun. Eng.* **2015**, *3*. [CrossRef]
24. VASCO. *Social Engineering: Mitigating Human Risk in Banking Transactions*; Vasco Data Security: Chicago, IL, USA, 2015.

25. Security Scorecard. *2016 Financial Industry Cybersecurity Report*; Security Scorecard: New York, NY, USA, 2016.
26. Proofpoint. *Human Factor*; Proofpoint: Chicago, IL, USA, 2017.
27. Australian Cyber Security Centre. *Australian Cyber Security Centre: 2017 Threat Report*; Australian Cyber Security Centre: Canberra, Australia, 2017.
28. Conference of State Bank Supervisors. *Cybersecurity 101: A Resource Guide for Bank Executives*; Conference of State Bank Supervisors: Washington, DC, USA, 2016.
29. Aburrous, M.; Dahal, H.M.A.K.; Thabatah, F. Experimental Case Studies for Investigating E-Banking Phishing. *J. Cogn, Comput.* **2010**, *2*, 242–253. [CrossRef]
30. E-Security Planet. *Social Engineering Attack Nets $2.1 Million from Wells Fargo Bank*; e-Security Planet: Foster City, CA, USA, 2012.
31. VASCO Data Security. *Social Engineering: Mitigating Human Risk in Banking Transactions*; VASCO Data Security: Oakbrook Terrace, IL, USA, 2015.
32. Longitude Research. *Cyberrisk in Banking: A Review of the Key Industry Threats and Responses Ahead*; SAS: Chicago, IL, USA, 2015; Available online: https://www.kroll.com/media/pdf/white-papers/cyberrisk-in-banking-106605.pdf (accessed on 3 May 2018).
33. Mithil Vasani, B.P.C.C. Android Based Total Security for System Authentication. *J. Eng. Res. Appl.* **2015**, *5*, 115–119.
34. ANZ New Zealand. ANZ New Zealand Facts, 07 2017. Available online: https://www.anz.co.nz/about-us/our-company/anz-new-zealand/ (accessed on 24 January 2018).