Preventing Crimes of Online Scams Across Countries: A Comparative Study Between Bangladesh and Singapore

Khandaker Farzana Rahman[1]
Hee Jhee Jiow[2]
Brenda Lee[3]

ARTICLE INFO

Article history:
Date of Submission: 21-11-2024
Date of Acceptance: 19-01-2025
Date of Publication: 30-10-2025

Keywords: Scam, Crime Prevention, Bangladesh, Singapore, Online fraud

ABSTRACT

Scams are commonly taking place globally, and the consequences of such fraudulent activities take a toll on individual privacy and national security. Financial scams in Bangladesh are on the rise, as numerous financial institutions continue to exploit political power to siphon public money through deceit. Although limited preventive measures are in place, but realistic methods have yet to be employed to recover money from these scammers. In contrast, Singapore, despite being highly ranked in many global indexes, suffers from a variety of scams, including purchase scams, credit for sex, and internet romance scams. By analyzing the available literature and secondary sources, this study aims to conduct a comparative analysis of different types of scams and their preventive mechanisms in Bangladesh and Singapore. The study finds that both countries have strict implementations of laws to prevent online fraud. Still, each country suffers from numerous obstacles to eliminating such crimes. However, Bangladesh has yet to develop a rigorous control mechanism for such crime, whereas Singapore has been quite advanced in dealing with various patterns of scams through its community interventions. Data collection and analysis were conducted to understand the current situation of scams in Bangladesh and Singapore, and the review was undertaken by deploying qualitative methods. However, the study acts as a crucial starting point for formulating comprehensive policies to combat the rising threat of online scams in Bangladesh. It highlights the urgent need for Bangladesh to establish robust regulatory frameworks and promote community-driven initiatives, while also drawing inspiration from Singapore's sophisticated and effective strategies for scam prevention as a model. By encouraging international partnerships, and emphasizing data-driven policymaking, both nations can work together to tackle the dynamic and continually evolving nature of online scams with greater efficacy.

[1] Associate Professor (on study leave), Department of Criminology, University of Dhaka. Email: kfrahman@du.ac.bd (Corresponding Author)

[2] Associate Professor, Singapore Institute of Technology, Singapore. Email: jhee.jiow@singaporetech.edu.sg

[3] Graduate student, Singapore Institute of Technology, Singapore. Email: brenda.Lsh@hotmail.com

Social Science Review [The Dhaka University Studies, Part-D], Vol. 42, No.1, June 2025
DOI: https://doi.org/10.3329/ssr.v42i1.85321

Introduction

Scams or online frauds are no longer standalone incidents today; they have taken over private and public spheres in their ubiquity. The magnitude of these fraudulent activities has swelled to such an extent that the costs affect the global market, consumers, and society. Despite this prevalence, little academic work has been devoted to understanding its deriving or facilitating factors. However, if the magnitude and impact of these scams are to be perceived, acknowledging and investigating the phenomenon is the first way to address the issue.

Scams exploit people online through modus operandi (Norris. et al., 2019). Even a few years ago, scams took the form of fake phone calls or deception in financial transactions, lottery, and sweepstakes. However, now, with the era of digitalization, scammers have kept committing fraudulent activities in far greater forms and places. Even in many cases, scams are carried out using almost untraceable methods (Ketchell, 2019). Fake romantic relationships online, phishing, bitcoin, or credit card scams have proliferated with the increased ease and access to the internet. Phishing, in particular, has been emerging as a severe threat to the trading security of the blockchain ecosystem (Wu. et al., 2020). The greater pervasiveness of scams accounts for more significant net worth and impact costs. Even though developing and developed countries continue to suffer irrespectively, their economic and societal ramifications are much more critical for developing countries. The growing trend of scams is rising, especially financial scams in Bangladesh and love or investment scams in Singapore. Though the pervasiveness of online scams in reality between the two countries is slightly different, their preventive mechanism is far more different from each other.

In Bangladesh, financial institutions often are alleged to commit scams through deceit. Scammers take advantage of higher political affiliations and the absence of any regulatory framework in the country to supervise these gross financial transactions. Even though a few preventive measures and investigations have started, they are functioning at turtle speed and have a long way to go in protecting the public and their money from these scammers. In this regard, Iftekharuzzaman, the Executive Director of Transparency International, Bangladesh (TIB), notes that ‘Delays in trials had become a common practice in Bangladesh. For instance, the Anti-Corruption Commission (ACC) is deliberately delaying the investigation related to the swindle of Basic Bank.’ (Karim, 2020). Basic Bank has been one of the most notorious scam cases that misappropriated more than TK 4500 crore, and the reluctance and inefficiency of its investigative process are symbolic of the prevalence of financial scams in the country.

In contrast, Singapore also encounters diverse forms of scams, including purchase scams, sex credit, and internet love scams. Though both countries experience different kinds of scams and have strict implementation of laws to prevent online fraud, each

country still suffers from numerous obstacles to eliminating such crimes. In many cases, Bangladesh has yet to integrate community-based prevention mechanisms for combating fraud.

It is important to note that there is a significant gap in academic literature concerning Bangladesh, while there are existing studies on the trends of online scams in Singapore. However, both countries lack comprehensive literature on the mechanisms for preventing online scams. This highlights the need to identify gaps and develop improvements in the prevention strategies for online scams. The study aims to discuss common types of online scams occurring in Bangladesh and Singapore. It will explore the differences between these scams, examine the available prevention mechanisms for online fraud in both countries, and identify lessons that Bangladesh can draw from Singapore to enhance its prevention strategies against online scams. Given the fact of limited literature on existing patterns of online scams in both Bangladesh and Singapore, data collection and analysis were done by reviewing relevant reports published by national and international agencies from 2018 to 2022 and existing scholarly works.The reports included data also from law enforcement organisations and research institutions both in Singapore and Bangladesh.

The article is structured as follows: the first section will define the crime of online scams and discuss various types of this offense. Subsequently, it will concentrate on the legal and existing frameworks for preventing such crimes in both countries. The final section will conclude with a comparative analysis, highlighting the lessons Bangladesh may draw from Singapore in its efforts to prevent online scams.

Online Fraud: Hard to Detect?

The relentless march of technology and the limitations of traditional analytics frameworks continually push fraud prevention to evolve. Fraudsters' adaptive techniques drive technology solutions towards a future-proof extensive data ecosystem. Despite consistent efforts in crime prevention, why do fraud detection and resolution pose such a formidable challenge in a country? Singapore, a country that effectively reduces overall crime rates, may still encounter several difficulties when dealing with the prevalence of scams within its borders.

Historically, identifying fraud after the fact and attempting to recoup payments has been ineffective. Many organisations combating scams in a specific country contend with significant data sharing and communication obstacles, often hindered by language barriers. Unidirectional information flow creates inconsistencies between agencies, compounded by labour-intensive manual data reconciliation processes. Adapting to these challenges is undeniably tough, given the demand for diverse expertise, budget constraints, shrinking headcounts, and rapid technological advancements. The skills

required have expanded to encompass data scientists, domain experts, software developers, and cloud engineers. National agencies must implement an agile staffing model and a flexible, scalable analytics framework to overcome these hurdles.

Thus, detecting and prosecuting online fraud is challenging due to the constantly evolving tactics used by fraudsters, the global nature of online criminal activities, and the difficulties in gathering digital evidence that can stand up in court. Despite limitations, Singapore's remarkable success in preventing national crimes and its strides in developing a framework to combat scams may make it a compelling model for Bangladesh to learn from. Through a comprehensive comparative study, Bangladesh can glean valuable insights from Singapore's institutional frameworks and apply them to enhance its efforts to prevent scams.

Data and Methods

The research method encompasses the systematic approaches the researcher employs to gather, analyse, and interpret data throughout the study (Creswell, 2009). In the process of conducting research, the specific area of investigation and the research objectives and questions play a crucial role in guiding the researcher towards an appropriate methodology (Opoku et al.,2016). This involves selecting suitable techniques for data collection, whether through surveys, observations, or case studies, and then applying appropriate analytical tools and frameworks to derive meaningful insights from the data. Ultimately, the chosen method not only influences the reliability and validity of the findings but also shapes the overall understanding of the research focus.

The method used in this study is a qualitative research approach that aims to uncover and analyse recurring patterns and themes found within textual data. This technique is particularly effective for delving into the intricate content of articles, research papers, and reports spanning a wide range of disciplines (Castleberry & Nolen,2018). By systematically examining the language, concepts, and underlying messages in these texts, researchers gain valuable insights and a deeper understanding of the subject matter across diverse fields. Due to the complicated nature of crimes, there has been a dearth of available literature on existing patterns of online scams both in Bangladesh and Singapore. Considering both countries' contexts, in addition to reviewing scholarly articles and existing literature, information was collected reports by national and international agencies, such as law enforcement organisations banking institutions and research organisations. Though updated data from law enforcement were considered in Singapore, the Bangladesh police force has a shortage of annual data regarding the pattern and trends of scams in the last decades. Thus, the study concentrates on scholarly articles and reports to understand the patterns of scams and the challenges of preventing such crimes in Bangladesh.

A thematic coding analysis of secondary data was done in this paper. The researchers begin by reviewing existing documents and reports to understand the context and content of the research topic. As the authors become familiar with the data, initial codes are recorded that highlight significant features pertinent to the research questions. These codes are subsequently organized into potential themes, which capture meaningful patterns related to the research (Lochmiller, 2021). These themes are consistently reviewed and refined to ensure they accurately represent the coded data as well as they are checked for any overlaps or redundancies. After each theme is clearly defined and given a name that encapsulates its essence, the findings are compiled into a report and the draft research is developed.

This small-scale paper solely depends on law enforcement agencies' primary and secondary scholarships and works, reports of national and international organisations. A major disadvantage of using secondary data is that the researcher did not participate in the primary-level data collection and lacks knowledge about how it was conducted (Johnston, 2014). To address these concerns, researchers may seek information from consultations with the original researchers and statisticians, which was not done in this study, as this was based on the available contents found on the prevention of online scams in Bangladesh and Singapore. Though this dependency on existing secondary sources is the prime limitation of this work, this paper can foster paths to superior and further studies and new approaches toward preventing scam prevention.

Literature Review

The world has come together closer than before, leading to increased scams and fraudulent activities and the scam was traditionally started through conventional means such as physical mail and fax, and more recently through electronic mail (Mokhtari et al., 2008). The phenomenon of online scams in Bangladesh however has been rising in the context of globalization and enhanced connectivity. Another feature of scams in Bangladesh is that this trend is attributed to the exploitation of political power by various financial institutions, which engage in fraudulent activities to embezzle public funds. Fraudsters exploit the presence of strong political affiliations and the lack of regulatory oversight in the nation to engage in these egregious financial dealings. Despite initiating some preventative measures and investigations, their efficacy has been limited, and progress needs to be faster in safeguarding the public and their finances from fraudulent activities.

Scams are prevalent in virtually all sectors today, such as banking, government grants, lottery, telephone, investment, census, etc. Today's most common scams include advanced fees for specific products or services, fake check overpayment, false employment promises, lottery sweepstakes, internet purchases, or fraud in internet relationships (Western Union, n.d.)

The scam has been gradually defined in the existing literature from a broader perspective. Of the significant classifications of scams, Pouryousefi and Frooman (2019, p. 3) identify consumer scam as the "intention to deceive an individual who chooses to participate in an exchange on the promise of receiving tangible or intangible goods, services, or financial returns that are never to be provided or are grossly misrepresented." Chua and Wareham (2008) expound upon product scams, a prevalent form of criminal activity wherein intangible commodities are marketed with the assurance that they will yield miraculous cures, lucky draws, lotteries, sweepstakes, and the like. A prevalent type of scam activity is the financial scam, which guarantees substantial monetary gains in exchange for a specified investment amount that is ultimately misused.

If we consider the case of Singapore, despite having a diverse range of cultures and influences, it is considered one of the lowest crime rates in the world. Singapore has portrayed many success stories in Asia in preventing crime through public-policy engagement, building effective formal institutions such as the Crime Prevention Division and National Crime Prevention Council, and implementing mutual collaboration. The achievement of a low crime rate has been attributed to the utilization of deterrence, enforcement, and rehabilitation strategies, which have been effectively implemented and supervised by a proficient criminal justice system. In Singapore, deterrence is achieved through implementing stringent laws advocated by a powerful executive and ratified by a highly legislative body. This is complemented by a highly resilient and effective judicial system that is recognized globally and a police force that strives to attain world-class standards in its comprehensive policing capacities. This also includes a strong emphasis on community policing, which is characterized by a mutually beneficial relationship with the communities it serves, rigorous enforcement by officers who are beyond reproach, and a correctional system that is austere yet compassionate.

Bangladesh, on the other hand, is relatively prone to different social crimes. According to the Bangladesh Police, 17484 criminal cases have been filed in 2019 (Bangladesh Police, 2020). In Bangladesh, crime prevention strategies are primarily reactive, and there needs to be more theoretical frameworks for crime prevention. Crime prevention encompasses a range of strategies implemented both institutionally and non-institutionally. These strategies include community-oriented policing and various security measures. Different offices of law enforcement, such as, Police Headquarters, Crime Investigation Department, Police Bureau of Investigation, Detective Branch, and specialized units are responsible for crime prevention. It is worth mentioning that the Bangladeshi policing system still needs more institutional efficiency as well as though the practice is recently in place, community-oriented policing has faced many challenges related to infrastructure and resources (Islam, 2018).

Sources from Bangladesh government often say Bangladesh would be Singapore in terms of development and economic stability (Hasan & Islam, 2020). In addition, in maintaining law and order, Singapore has become a role model to Bangladesh and South Asia and could be taken as an example to prevent such kind of digital crime. Considering the reported crimes of online scams, over the past decade, Bangladesh has experienced a significant increase in incidents of online scams. The available statistics represent a notable increase in online fraud of 7.44% in 2019 from the preceding year (Babu, 2022). Nevertheless, a significant number of occurrences frequently go unreported for various reasons.

On the other hand, according to Iau's (2021) report, there was a significant increase of 65.1% in the number of reported scams in Singapore last year, which reached a record high. As Singapore has successfully developed a rigorous framework of policing, including public and awareness campaigns, their case would offer ample lessons for Bangladesh, which is initially struggling to develop a comprehensive prevention mechanism for scam prevention.

Findings

The prevalence of financial scams and corruption has reached a point where it impacts the financial industry and significantly influences the global economy. Financial institutions are being subjected to substantial fines, which testify to the extent of these illicit activities. Bangladesh has encountered pervasive financial fraud in numerous financial establishments. According to a report published by the Centre for Policy Dialogue, over several decades, fraudulent activities have resulted in a total loss of approximately 22,502 crore BDT across 14 banks (Major scams cost banks Tk 22,502cr: CPD, 2018). The ACC has initiated legal proceedings against several prominent financial institutions, including BASIC Bank, Hallmark Group, Crescent Group, Bismillah Group, and Farmer's Bank (now known as Padma Bank) (Karim, 2020).

According to Islam's (2017) research, seven factors contribute to the growing prevalence of financial scams in the nation. The individual asserts that the perpetuation of fraudulent activities in recruitment is facilitated by a confluence of factors, including political pressure, the exertion of power by government-supported collective bargaining agreement (CBA) leaders, political interventions, the attainment of political power, inadequate regulation, and inefficiencies in documentation and field surveying. The complexity of online scams, such as fraudulent service providers, lotteries, and sweepstakes, renders them difficult to trace. Many e-commerce platforms in Bangladesh have been charged with fraud

for their inability to provide services to their clients (Chowdhury et al., 2022; The Dhaka Tribune, 2021). In addition to vulnerability to scams in banking, mobile banking and financial sector and e-commerce, mass-market-level consumer fraud was reportedly committed exploiting legal financial channels to defraud thousands of people in various districts (Amin, 2023).

By contrast, Singapore experiences similar types of criminal activities of online frauds. It has been identified by the Singapore Police Force (2019) and Scam Alert (2020) that five predominant scams exist in Singapore. The prevalent types of scams include E-commerce or online purchase scams, internet love scams, impersonation scams, investment scams, and credit-for-sex scams. Singapore Police Force (2019, p.1) (SPF) reports that the most common scams were found to make up 80% of those reported in the first half of 2019. Each of the top scam types identified will be briefly discussed.

Online Purchase Scams

The perpetuation of fraudulent activities in e-commerce, including online purchase scams, targets unsuspecting individuals who engage in online transactions on e-commerce platforms, lured by the prospect of attractive product deals (Scam Alert, 2020). Frequently, discounted gadgets and amusement park tickets are vented to potential buyers who subsequently transfer payment to the purported seller with the expectation of receiving the promised items (Scam Alert, 2020). Following that, certain vendors may require additional payment for shipping expenses or other fees after the initial payment.

In the first half of 2018, 1,013 cases of online purchase scams were reported, with a total loss of $870,000. In the first half of 2019, however, 1,435 reported cases were recorded, resulting in a $1.2 million loss (SPF, 2019). The top five e-commerce sites where scams occur include Carousell (1,239 cases), Facebook (602 cases), Lazada (197 cases), and Instagram (103 cases) (OSAC, 2020).

Credit-for-sex Scams

Credit for sex scams are operated by posing as attractive women on social media platforms. Scammers will convince targets to buy them gift cards or money with the promise of sexual services (OSAC, 2020). Based on the 2019 mid-year report by SPF (2019), there were 456 cases between January 2019 and June 2019 and 209 cases during the same period in 2018. The total loss in 2018 was $464,000; in 2019, it was $1.1 million. 2019, the most significant sum loss was $80,000 (SPF, 2019).

Through victim submissions on Scam Alert (2020), scammers chat with victims on online platforms such as Line, Tinder, and other dating applications. The girls offer

services in exchange for Google cards or bank transactions. Upon the first transaction, scammers introduce the second person as a friend or agent who requests the victim extra money as insurance or a security deposit (Scam Alert, 2020).

Internet Love Scam

The proliferation of social media and dating apps has given rise to a contemporary type of fraud known as online romance scams, which has become prevalent in Western cultures (Coluccia et al., 2020, p. 16). Romance scams involve the fabrication of fraudulent online profiles on dating and social networking platforms, such as Facebook, Skype, and LinkedIn, by malevolent actors who aim to lure unsuspecting individuals into relationships with the ultimate goal of extorting money from them (Whitty, 2019). While both genders are represented in the demographic of scammers, most individuals who engage in scamming activities are male, as reported by Scam Alert in 2020.

Through the victim's anecdotes, scammers will typically chat with them for a period to gain their trust. Scammers have an attractive profile and claim a successful business or career. After this, the scammer will provide a story that requires monetary assistance, such as lawsuits or building collapses. The trusting victim will be asked to transfer money multiple times before realizing something is amiss. Another commonly reported method requires the victim to pay off a considerable sum of money for a gift package stuck at customs. The victims may later be threatened if they refuse to pay more (Scam Alert, 2020). Fortunately, many victims acted cautiously and refused to help the scammers when they requested monetary assistance. However, those who fell for the scam typically suffer a substantial financial loss, with one case that amounted to 15,000 euros.

Impersonation Scam

The proliferation of technological advancements has led to the emergence of fraudulent activities, thereby necessitating a critical examination of job scams and phishing scams (Neo & Lee, 2022). According to Scam Alert (2020), impersonation scams involve a deceptive phone call in which the perpetrator assumes the identity of a government official, an employee of a Chinese bank, or a courier company. The caller may claim that the intended recipient's identity has been compromised and may proceed to solicit the divulgence of confidential personal information, such as bank account or passport particulars or login credentials for online banking. The Scam Alert report (2020) also reveals that 455 cases were reported, and $21,100,100 was reported lost due to fraudulent activities between 2018 and 2020.

Based on online victim submissions via Scam Alert (2020), scammers often pose as employees from telecommunication companies such as Singtel or Ministries. They

inform victims that their identity has been stolen and require them to follow a few instructions. Many victims identify the scam during the initial stages of the process and may hang up the phone or call the police.

Investment Scam

Investment scams represent the final and most prevalent form of online fraud in Singapore. In these scams, victims typically receive messages from scammers claiming to be stockbrokers or bank employees on social media. Scammers initially ask their victims for their personal information and then subsequently charge them administrative fees so that they can obtain the earnings and returns. Between 2018 and 2020, 508 cases were reported, and $36,900,000 was scammed (Scam Alert, 2020).

Most often, the perpetrators start their contact through an online chat platform and subsequently inspire them in discussions regarding future investment opportunities. Upon gaining the victims' trust, scammers send them bogus trading or cryptocurrency websites. After noticing growth in their investments, victims will continue investing more but are unaware they cannot withdraw any of their money (Scam Alert, 2020).

Discussion on Preventive Framework of Scams

As previously mentioned, financial fraud is currently the most common kind in Bangladesh. Apart from the cases relating to Basic Bank and Hallmark discussed above, several multi-level marketing companies have made headlines in the past two decades, shocking thousands. Destiny Group and Jubo Karmasangsthan Society (Jubok) are two such companies that managed to make millions using a "Ponzi scheme" method. According to the Harvard Law Review (2020), the "Ponzi scheme" is a kind of investment scheme that uses a series of frauds where the fraudsters assure higher than market amount returns on investments while aiming to increase the number of investors. The earlier investors are paid profits using the money invested by the new ones, affirming the legitimacy of their business. According to the Daily Star, Destiny Group sold trees worth 4,200 crore, allegedly planted in a property far away from 17.5 lac investors by showing them photos of the trees. Anti-Corruption Commission later found that although they claimed to plant 6.18 crore saplings, only 32 lac trees were planted. (51 indicted in Destiny, 2016) Jubok sold non-existent lands to 2.67 lac clients, owing them a mammoth taka 2,147 crore. Jubok started its activities in 1994 and, after 22 years of operating, was charged with illegal banking activities by Bangladesh Bank in 2006 (Byron, 2011).

As there were no definite laws to prevent or charge such cases, the Anti-corruption Commission had to file cases against them using laws that fit the best. One such law is the Money Laundering Prevention Act 2012, which states that any activity that launders

or attempts to launder money derived from fraud is considered a "predicate offense." This allows the perpetrators to use loopholes in the legal system to their advantage. In 2013, a multi-level marketing specified law was passed to prevent similar frauds from happening in the future. The Multi-level Marketing (MLM) Control Act 2013 (Act No xxxiv of 2013) requires companies to acquire licenses before conducting business. The law provides three to five years in jail or a fine of up to 50lacs for those without a license or conducting forgery. Moreover, under this law, anyone caught scamming under the banner of MLM can be punished with one to five years in jail and pay double the amount of money scammed by the victim.

The condition of the banking sector in Bangladesh has deteriorated over the past decade due to multiple loan and credit cards scam events that managed to cause a considerable amount of damage and are surviving only due to the additional support provided by the government. Even though the law required the investigation to be completed within 180 days, ACC, using special permission, continued it for years. However, the investigation results remain inconclusive because of the lack of substantial evidence and loopholes due to the lack of specified laws, allowing the perpetrators to stay far from being punished. Similarly, in the hallmark group's loan scam that managed to steal around tk. 474 crore, ACC filed 11 cases based on forged documents against the responsible persons in 2012. The charge sheets were submitted in 2013, and the cases were framed against them in 2015 and 2016, indicating sluggish progress. (Karim, 2020) Several other similar cases, including the case of Framers Bank (now Padma Bank), Bismillah Group, and Crescent Group, all remain identical due to the absence of necessary measures.

Devising precautionary models to prevent and detect such unwanted events in due time is essential. Some countries consider the audit division the most important, as keeping an eye on the situation every step of the way drastically decreases the chance of disasters. Inventory observations are also required to follow up with the customers' actions and verify the claims' legitimacy. In addition to this, a reference check on each employee and a hotline for information regarding fraud can help security measures go a long way (Rahman & Anwar, 2014). Regarding fraud detection methods in Bangladesh, internal audits rank as the most effective, closely followed by employee notifications. Through regular internal audits, any irregular activity is bound to attract attention. Other effective methods include external audits, anonymous notifications or letters, accidental discovery, and specific investigations by management. (Ghazali, et al., 2014) However, a crucial factor in maintaining the credibility of these detection and prevention techniques is to ensure quick and fair legal action against the wrongdoers. With exemplary actions of justice, all these models retain their authority over the people.

On the other hand, Singapore uses various prevention methods to reduce the number of cybercrimes, such as the availability of helplines and information and police investigations. Helplines and information promote community policing, in which citizens are educated and made responsible for crime prevention (Garland, 2001). As such, inner-city neighborhoods, schools, hospitals, families, and online social networking sites are forms of community policing responsible to a certain degree for promoting *self-responsibilization* (Low, 2012, p.11). However, Singapore Police Force (SPF) and Ministry of Home Affairs (MHA) empowered the Computer Misuse and Cybersecurity Act (CMCA) under the Cyber Security Agency (CSA) to properly investigate and prosecute cybercrimes (Cyber Security Agency, 2020) which is considered the basic framework of prevention of scams.

Comparison of Prevention of Scams in Bangladesh and Singapore

If we look at the comparisons of scams and preventive measures between Bangladesh and Singapore, we see some parallels and differences (figure 1). Bangladesh and Singapore experience diverse online scams, including e-commerce, online shopping, internet love, and investment. Scams involving money or the banking industry are significantly more common in Bangladesh. In addition, Bangladeshi people are frequently the victims of online shopping fraud, much like Singaporeans are (Emon, 2020). This is because they see a lot of enticing adverts and significant discounts on products even when they do not purchase them.

Table 1: Similarities and differences among scams in Bangladesh and Singapore

Bangladesh	Singapore
Banking Fraud (loan fraud, credit card scams)	Job & Phishing scams
Mobile banking scams	Investment scams
E-commerce scams	E-commerce Scams
Multi-Level Marketing business fraud	Credit for sex scams, Online love scams

Sources: Rahman (2023); DBS Bank (2023)

When examining the current situation in Bangladesh, it becomes pretty clear how flimsy and ineffective the available models and procedures are in stopping fraud. Bangladesh must also catch up with its neighbours and the global economy regarding corporate governance (Mahmood & Islam, 2015). Given the pace of technological innovation and the evolution of fraud schemes, our judicial system seems archaic and unable to keep up with modernization. Because of lack of specific laws, ineffective organisational preventive models, crooked public servants, and a lax judicial system, fraudsters can engage in such activities and get away with them, leaving the victims defenceless. Bangladesh passed the Digital Security Act 2018

(replaced with Cyber Security Act 2025) punishes offenders with various prison sentences to prevent any crime from occurring on an internet platform. Ironically, Bangladesh does not have legislation that deals only with online scams. In addition to this problem, victims of online scams frequently cannot identify the offenders or choose not to pursue justice because of a tradition of impunity in similar cases. Due to the lengthy legal process, victims of scammers frequently do not feel motivated to report the incident. If any claimed disclosure of personal information to the police occurs, victims generally choose to remain silent out of fear or embarrassment.

After an online crime is reported, the court frequently releases the accused due to a lack of witnesses, evidence, or the prosecution's inability to establish the case. The Bangladeshi police still mainly focus on reactive crime prevention when dealing with electronic crimes. Furthermore, the problem of digital fraud in Bangladesh has not yet been adequately addressed by community police. However, the central police departments like the Crime Investigation Department and Detective Branch deal with cybercrime. Despite lacking a formal framework for public-police engagement in the fight against online fraud, developing financial literacy and awareness among citizens through community policing may enhance current online scam prevention methods.

On the other hand, in Singapore, although community policing is an effective prevention method, scam prevention is executed through a stringent framework of agencies. However, CMCA was initially limited to cybercrimes committed wholly or partly in Singapore. This limitation is problematic as cross-border cybercrimes become increasingly common. As such, CMCA amended its policies in April 2017 and allowed the police to investigate cybercrimes committed by overseas scammers, especially if they were deemed high-risk and very harmful to Singapore (Cyber Security Agency, 2020).

To tackle the limitations of policing online scammers, SPF set up an anti-scam centre in June 2019 to disrupt scam operations and reduce monetary loss. Since its formation, the centre has received 3,312 scam reports and a $10.6 million loss. Following the reports, the police froze 2,600 bank accounts and recovered 35% of the amount scammed (Mahmud, 2020). The police have also arrested 112 individuals responsible for 1,223 cases (Mahmud, 2020).

Simultaneously, the importance of the awareness campaign in Singapore is to create more awareness to promote an environment that reduces cybercrime (Okorie et al., 2020). A combination of automated techniques and multi-level barrier applications is also widely suggested to prevent phishing scams (Miller et al.,2020). Singapore police force, along with the assistance of community policing, engaged different stakeholders to avoid scams. Importantly, under a stringent legal mechanism, perpetrators are still

investigated and prosecuted accordingly. However, implementing the law in case of extra-territorial jurisdiction of crime committed over cyberspace is still challenging.

The study also reveals the mortifying degree of alertness among the general population, which is a supplier of never-ending naive victims, ready to fall prey to the waiting fraudsters. Even though national, international, private, and public organisations are working to spread knowledge regarding such issues, thousands of uninformed people still need to catch up on the common traps every year. Creating massive awareness among the general population is as important as creating up-to-date policies and implementing preventive measures when battling against fraudsters. In this case, Singapore has initiated different awareness creation programs through offline and online media, while Bangladesh still needs to catch up in disseminating knowledge about preventing such scams. To frame its policy of avoiding scams, Bangladesh should take lessons from Singapore as it has been ranked consistently high in maintaining law and order and reporting crime. Since Bangladesh needs to set up a full-fledged prevention mechanism for scams, policymakers should consider Singapore's best practices in eliminating online crimes.

Conclusion

Financial scams are a common phenomenon in the present global economy (Amir et al., 2022). Considering the urgency of preventing such crime, the study aimed to analyse, discuss, and dissect the phenomenon of scams and frauds in Bangladesh and Singapore. It also sheds light on the legal status quo and its effectiveness in different sectors, along with the need of awareness among the general public on such traps.

In Bangladesh, online scams are predominantly financial scams by different institutions and groups, while Singapore faces multi-dimensional scams affecting public and private life. The prevention mechanism is still developing, and a full-fledged law is missing in Bangladesh, so grievances might be overlooked. It is important to note that a lack of relevant literature also can be held partially responsible for weak preventive policies. While in Singapore, the prevention mechanism is much more proactive and systematic, Scam Alert Singapore aims to create public awareness against such fraud and strict implementation of legislation and regulations by law enforcement.

Comparing the two countries' scam prevention strategies results from developing different policies and mechanisms that indicate one's capacity, willingness, and resources. Singapore developed the prevention mechanism of online fraud through active government policies, scam awareness campaigns, and community- based policing, while the Bangladeshi government could adopt a systematic punitive intervention through law enforcement. Additionally, community police can launch proactive initiatives aimed at increasing public awareness about the various frauds and

scams that pose a threat to citizens. These efforts would not only inform individuals about the tactics used by scammers but also emphasize the importance of reporting suspicious activities to law enforcement. By fostering a culture of vigilance and open communication, community police can help empower citizens to protect themselves and contribute to the overall safety of the community.

One common scenario is that both governments, considering the crime pattern, still face various barriers to prevention. As different kinds of online fraud and their new patterns are emerging in both countries, it is apparent that there is a vast opportunity for further research and studies on online fraud prevention in Bangladesh and Singapore.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The authors received no financial support for the research, authorship and/or publication of this article.

References

Amin, K.M, (2023, August 31). Is MLM fraud back in disguise?.*The Daily Star*. https://www.thedailystar.net/opinion/editorial/news/mlm-fraud-back-disguise-3401836

Amir, M. K. B., Amir, M. Z. B., & Islam, M. A. (2022). Phenomenon of bank scams in Bangladesh: Analysis on behavioral issues. *International Journal of Research in Business and Social Science*, *11*(7), 189-200

Babu, M.U. (2022, October 19). Digital economy grows fast leaving consumers exposed to frauds. *The Business Standard.* https://www.tbsnews.net/economy/digital-economy-grows-fast-leaving-consumers-exposed-frauds-516390

Bangladesh Police. (2020). Crime Statistics 2019. https://www.police.gov.bd/en/crime_statistic/year/2019

Byron, R. K. (2011, January 30). Jubok owes Tk 2,147cr, not Tk 37cr, to people. *The Daily Star*. https://www.thedailystar.net/news-detail-172259

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds?. *Currents in pharmacy teaching and learning*, *10*(6), 807-815.

Chowdhury, M. S. A., Bappi, M. A. U., Imtiaz, M. N., Hoque, S., Islam, S., & Haque, M. S. (2022). The Transition of E-Commerce Industry in Bangladesh: Added Concerns & Ways of Recovery. *International Journal of Economics and Finance*, *14*(7), 1-18.

Chua, C. E. H., & Wareham, J. (2008). Parasitism and Internet auction fraud: An exploration. *Information and organisation.* https://doi.org/10.1016/j.infoandorg.2008.01.001

Coluccia,A., Pozza,A., Ferretti, F., Carabellese, F., Masti,A., & Gualtieri, G. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. *A Scoping Review. Clin Pract Epidemiol Ment Health*, *26*(16), 24-35. doi: 10.2174/1745017902016010024.

Creswell, J. W. (2009). Research design: Qualitative and mixed methods approaches. *London and Thousand Oaks: Sage Publications*.

Cyber Security Agency. (2020). *Investigation of cybersecurity threats and incidents.*

DBS Bank (2024). Top 5 latest types of scams in Singapore. https://www.dbs.com/livemore/money/types-of-scams-singapore.html

Garland, D. (2001). *The* Culture of Control. Oxford University Press.

Ghazali, M. Z., Rahim, M. S. M., Ali, A., & Abidin, S. (2014). A preliminary study on fraud prevention and detection at the state and local government entities in Malaysia. *Procedia - Social and Behavioral Sciences, 164*, 437–444. https://doi.org/10.1016/j.sbspro.2014.11.100

Hasan, K., & Islam, M.T. (2020). Consolidating democracy or accelerating development:a comparative study between Bangladesh and Singapore. The Jahangirnagar Review, 44, 399-416.

Iau, J. (2021, February 9). Record number of scams in 2020 pushed overall crime rate in S'pore to highest in more than 10 years. The Straits Times. https://www.straitstimes.com/singapore/courts-crime/record-number-of-scams-in-2020-pushed-overall-crime-rate-in-spore-to-highest

Islam, S. (2018). Community Policing (CP): Challenges on preventing crime and human security in Bangladesh. *Review of Public Administration and Management*, *6*(3), 1-9.

Islam, S. (2017, December 7). 7 reasons behind loan scams in state-owned banks. *Dhaka Tribune*. https://www.dhakatribune.com/business/banks/2017/12/07/7-reasons-behind-loan-scams-in-state-owned-banks

Johnston, M. P. (2014). Secondary data analysis: A method of which the time has come. *Qualitative and quantitative methods in libraries*, *3*(3), 619-626.

Karim, R. (2020, March 4). Big bank scams, slow actions. *The Business Standard*. https://tbsnews.net/bangladesh/court/big-bank-scams-slow-actions-51496

Ketchell, M. (2019, December 20). Inside the mind of the online scammer. *The Conversation*. https://theconversation.com/inside-the-mind-of-the-online-scammer-127471

Lochmiller, C. R. (2021). Conducting thematic analysis with qualitative data. *The Qualitative Report*, *26*(6), 2029-2044.

Low, M. G. (2012). Community policing in Singapore. University of British Columbia. https://doi.org/10.14288/1.0105176

Mahmood, R., & Islam, M. M. (2015). Practices of corporate governance in the banking sector of Bangladesh. *International Journal of Managing Value and Supply Chains*, *6*(3), 17-29.

Mahmud, A. (2020). Why Scam Cases Continue To Rise And What Is Being Done About Them. *Channel News Asia*. https://www.channelnewsasia.com/news/singapore/singapore-scam-cases-on-the-rise-crime-rate-12395936

Major scams cost banks Tk 22,502cr: CPD. (2018, December 9). The Daily Star. https://www.thedailystar.net/business/news/major-scams-cost-banks-tk-22502cr-cpd-1671175

Miller, B., Miller, K., Zhang, X., & Terwilliger, M. G. (2020). Prevention of phishing attacks: a three-pillared approach. *Issues in Information Systems*, *21*(2), 1-8.

Mokhtari, M., Saraee, M. H., & Haghshenas, A. (2008). A novel method in scam detection and prevention using data mining approaches. *Proceedings of IDMC2008*, 1-11.

More e-commerce scams exposed: 6 officials of Tholay.com, WeCoom.com detained. (2021, October 11). *The Independent*. https://www.theindependentbd.com/post/268947

Neo, H. X. C., & Lee, Y. (2022). How to Survive the Worst Phishing Scam?: Case Study of Singapore OCBC Bank's Management of Its Phishing Scam Crisis. *AJPR*, *5*(1), 37-47.

Norris, G., Brookes, A., & Dowell, D. C. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology, 34*(3), 231–245. https://doi.org/10.1007/s11896-019-09334-5

National Crime Prevention Council Singapore. (2020). [Facebook Page]. Facebook.https://www.facebook.com/ncpc.sg/photos/a.146829248684077/3484215378278764/?type=3&theater

Okorie, E. J., Adaka, S. S., & Orji, B. O. (2020). Crime prevention campaign and development: A participant observers report on social media scam prevention in Singapore, *International Journal of Research and Sustainable Development, 7*(2), 20-29.

Opoku, A., Ahmed, V., & Akotia, J. (2016). Choosing an appropriate research methodology and method. In *Research methodology in the built environment* (pp. 32-49). Routledge.

OSAC. (2020). *Singapore 2020 Crime & Safety Report*. https://www.osac.gov/Content/Report/7f0cc2bc-ba9b-4485-b58b-1861aa0f8fc3

Police investigating 190 suspects after victims report more than S$1.8million lost in scams. (2020, July 18). *CNA*. https://www.channelnewsasia.com/news/singapore/scam-cases-police-investigating-suspects-enforcement-operation-12943836

Pouryousefi, S., & Frooman, J. (2019). The Consumer Scam: An Agency-Theoretic Approach. *Journal of Business Ethics, 154*(1), 1–12. https://doi.org/10.1007/s10551-017-3466-x

Rahman, M. (2023). Prevention of E-Commerce Fraud in Bangladesh: A Critical Study on Legal and Institutional Framework. *Available at SSRN 4477507*.

Rahman, R. A., & Anwar, I. S. K. (2014). Effectiveness of Fraud Prevention and Detection Techniques in Malaysian Islamic Banks. *Procedia - Social and Behavioral Sciences, 145*, 97–102. https://doi.org/10.1016/j.sbspro.2014.06.015

Singapore Police Force (SPF). (2020). Annual Crime Brief 2019. *Singapore Police Force*, 1-18.

Scam Alert - Bringing You The Latest Scam Info. (2020). *Scam Alert*. https://www.scamalert.sg/

Harvard Law Review. (2023). The Future of Restitution and Equity in the Distribution of Funds Recovered from Ponzi Schemes and Other Multi-Victim Frauds. https://harvardlawreview.org/2020/04/the-future-of-restitution-and-equity-in-the-distribution-of-funds-recovered-from-ponzi-schemes-and-other-multi-victim-frauds

Western Union. (n.d.). Common Scams using Western Union. *Western Union Money Transfer*. https://www.westernunion.com/bd/en/fraud-types.html

Whitty, M. T. (2019). Who can spot an online romance scam?. *Journal of Financial Crime, 26*(2), 623-633.

Wu, J., Yuan, Q., Lin, D., You, W., Chen, W., Chen, C., & Zheng, Z. (2020). Who are the phishers? phishing scam detection on ethereum via network embedding. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52*(2), 1156-1166.

51 indicted in Destiny scam cases. (2016, August 25). *The Daily Star*. https://www.thedailystar.net/backpage/51-indicted-destiny-scam-cases-1274986/