Science Futures
2025, Vol. 1, No. 1, pp. 28–38
https://doi.org/10.11648/j.scif.20250101.14

Case Report

Examining Online Scamming Techniques: How Scammers Contact and Influence Victims to Enhance Public Awareness

Shahjady Sultana[*]

Department of Sociology & Anthropology, Shanto-Mariam University of Creative Technology, Dhaka, Bangladesh

Abstract

With the rapid advancement of technology and the widespread use of digital platforms, online scams have become increasingly sophisticated and pervasive. These scams target individuals and organizations alike, often resulting in significant psychological distress and financial losses for victims. Despite ongoing efforts by authorities and cybersecurity professionals, the dynamic and evolving nature of online fraud poses considerable challenges to effective prevention and enforcement. This study aims to explore the current landscape of online scams by analyzing representative cases and identifying common tactics employed by cybercriminals. Emphasis is placed on understanding the psychological manipulation techniques used to deceive victims and the systemic vulnerabilities that enable such scams to flourish. Through detailed case studies and thematic analysis, the research highlights patterns in scam operations, assesses their impact, and evaluates the effectiveness of existing countermeasures. The findings underscore the need for enhanced public awareness, more robust digital literacy initiatives, and improved policy frameworks to combat online fraud. Ultimately, the study proposes a set of targeted preventive strategies and policy recommendations designed to reduce the incidence of online scams and better protect vulnerable populations in the digital age.

Keywords

Online Scams, Digital Fraud, Technology-Enabled Scams, Psychological Impact, Fraud Prevention, Modus Operandi

1. Introduction

1.1. Background of Study

In the era of digital connectivity, where the internet has become an indispensable part of our lives, a concerning phenomenon has emerged: online scamming. Online scams, also referred to as internet fraud, involve various deceptive techniques intended to exploit individuals or organizations, often for financial gain or malicious purposes. These scams have evolved alongside the ever-expanding digital landscape, taking on diverse forms and becoming increasingly sophisticated, posing a significant threat to individuals' privacy, finances, and overall safety.

This case study delves into the intricate world of online scamming, examining the modus operandi of scammers, their preferred targets, and the devastating consequences of their actions. By analyzing a specific case of an online scam, this study aims to shed light on the pervasiveness of this issue, the vulnerabilities it exploits, and the urgent need for

[*]Corresponding author: shahj.sultana@gmail.com (Shahjady Sultana)

Received: 24 April 2025; **Accepted:** 9 May 2025; **Published:** 9 December 2025

effective prevention strategies.

The primary objective of this case study is to investigate the intricacies of an online scam, specifically targeting individuals seeking online employment. This case highlights the deceptive tactics employed by scammers to lure unsuspecting victims, exploiting their desire for financial opportunities and manipulating their emotions. The study aims to identify the red flags associated with such scams, empowering individuals to recognize and avoid them.

1.2. Problem Statement

Online scams have become a pressing concern globally, with financial losses and emotional trauma impacting millions. Despite technological advancements in cybersecurity, scammers continue to adapt and innovate, exploiting both technological loopholes and human vulnerabilities. This study seeks to address the critical need for understanding the dynamics of online scams to develop robust preventive measures and enhance public awareness.

1.3. Objectives of the Study

1) Analyze the characteristics and operational methods used in diverse online scams.
2) Identify the psychological and financial consequences experienced by scam victims.
3) Examine structural and institutional challenges in preventing and addressing online fraud.
4) Propose practical preventive strategies and policy enhancements to reduce scam prevalence.

1.4. Research Questions

The key research questions that this case study seeks to address are:

1) What are the characteristics and modus operandi of online scammers targeting individuals and organizations?
2) What tactics do scammers employ to manipulate and deceive victims?
3) What are the consequences of falling victim to online scams?
4) What strategies can be implemented to prevent individuals and organizations from falling prey to online scams?

By exploring these questions, this case study aims to contribute to a broader understanding of online scamming and provide valuable insights into safeguarding individuals from its detrimental effects.

2. Literature Review

The literature on online scams highlights the interplay between technological advancements and social engineering tactics. Studies reveal that scammers often exploit cognitive biases, such as trust, reciprocity, and urgency, to manipulate victims. Moreover, the anonymity and global reach of the internet exacerbate the challenge of tracking and prosecuting scammers. The review also underscores the importance of digital literacy and regulatory frameworks in combating online fraud. Online scamming has become a significant concern globally, with scammers employing increasingly sophisticated techniques to deceive victims. This review explores existing literature on the methods scammers use to contact and manipulate victims, emphasizing the importance of public awareness to mitigate such threats.

2.1. Online Scamming Techniques

Research highlights that online scammers utilize diverse communication channels, including emails, social media platforms, messaging apps, and fraudulent websites, to initiate contact with victims [1]. Phishing emails, for instance, remain one of the most prevalent methods, often disguised as legitimate communications from reputable organizations [2]. Social media has also become a fertile ground for scammers, where fake profiles and emotional appeals are common tactics to establish trust and exploit vulnerabilities [3].

2.2. Psychological Manipulation

Scammers rely heavily on psychological manipulation to influence victims. Techniques such as urgency, fear, and appeal to authority are widely documented. For instance, victims may receive messages claiming they have won a lottery or face legal action, prompting them to act hastily without verifying authenticity [4]. Emotional manipulation, such as romance scams, involves building trust over time to exploit personal or financial vulnerabilities [5].

2.3. Victim Profiling

Scammers often target specific demographics based on their vulnerabilities. Research indicates that older adults are particularly susceptible due to lower digital literacy, while younger individuals might fall prey to scams involving social media or gaming platforms [6]. Financial strain, loneliness, and lack of cybersecurity awareness further increase susceptibility [7].

2.4. Importance of Public Awareness

Public awareness campaigns are crucial in mitigating the impact of online scams. Studies show that awareness initiatives, such as educational programs, media campaigns, and cybersecurity workshops, significantly reduce victimization rates [8]. Awareness also fosters vigilance, enabling individuals to recognize red flags, such as unsolicited requests for personal information or upfront payments [9].

2.5. Emerging Trends in Online Scamming

Recent studies highlight evolving scamming techniques, including the use of artificial intelligence (AI) to create deep fake videos and voice phishing (vising) to impersonate trusted entities [10]. Cryptocurrencies have also facilitated anonymous transactions, making it harder to trace and recover stolen funds [4].

Literature underscores the multifaceted nature of online scamming, combining technological sophistication with psychological manipulation. Public awareness emerges as a critical defense mechanism, empowering individuals to identify and avoid scams. Future research should focus on innovative awareness strategies and collaborative efforts among governments, organizations, and individuals to combat online fraud effectively.

3. Methodology

This case study employs a qualitative approach, analyzing six documented instances of online scams. Data was collected through victim interviews, analysis of scam-related communications, and a review of official reports. The cases were purposively selected to represent diverse scam types. Triangulation was achieved by incorporating expert opinions and law enforcement insights to corroborate findings. Thematic analysis, conducted using NVivo software, was employed to identify recurring patterns and key insights. Ethical considerations included obtaining informed consent, anonymizing personal details, and ensuring participant confidentiality. Limitations include reliance on self-reported data, which may be affected by recall bias, and a focus on specific cases that may not fully represent the broader context of online scams.

3.1. Research Design

This study employs a qualitative approach, analyzing six documented cases of online scams in Bangladesh [11].

3.2. Data Collection

1) Primary Data: Interviews with victims of online scams [5].
2) Secondary Data: Analysis of scam-related communications, police reports, and media coverage [4].

3.3. Sampling

Purposive sampling was used to select six diverse scam cases [8].

3.4. Data Analysis

1) Thematic Analysis: NVivo software was used to identify recurring patterns [2].
2) Triangulation: Findings were corroborated with expert opinions [12].

3.5. Ethical Considerations

1) Informed consent was obtained from participants [7].
2) Personal details were anonymized to ensure confidentiality [9].

4. Presentation

In the rapidly evolving digital landscape, Malaysia has witnessed a surge in online scams, posing a significant threat to individuals, businesses, and the overall economy. This collection of six case studies delves into the intricacies of various online scams prevalent in Malaysia, providing insights into the perpetrators' modus operandi, the impact on victims, and the challenges faced by law enforcement agencies.

Each case study meticulously examines a specific type of online scam, unraveling the deceptive tactics employed by scammers to exploit unsuspecting individuals. From the allure of lucrative investment opportunities to the emotional manipulation of online dating scams, these cases highlight the diverse forms of online fraud that have emerged in the Malaysian context.

The case studies further explore the devastating consequences of these scams, shedding light on the financial losses incurred by victims, the emotional distress inflicted upon them, and the erosion of public trust in online platforms. The psychological impact on victims is particularly poignant, as these scams often prey on vulnerabilities and exploit emotional connections.

In addition to analyzing the impact on victims, the case studies also examine the challenges faced by law enforcement agencies in combating online scams. The transnational nature of online fraud, coupled with the anonymity provided by the internet, poses significant hurdles in identifying and prosecuting perpetrators. Moreover, the ever-evolving tactics employed by scammers necessitate constant vigilance and adaptation from law enforcement agencies.

Through these case studies, we aim to raise awareness about the prevalence of online scams in Malaysia, equipping individuals with the knowledge to safeguard themselves and their finances. By understanding the modus operandi of scammers and the tactics they employ, we can empower individuals to make informed decisions in the digital realm and minimize their vulnerability to such scams.

Furthermore, these case studies serve as a valuable resource for law enforcement agencies and policymakers, providing insights into the challenges and opportunities in combating online scams. By understanding the patterns and trends of online fraud, we can develop more effective strategies for prevention, detection, and prosecution.

The fight against online scams requires a multi-pronged approach, involving collaboration between law enforcement agencies, financial institutions, technology companies, and the public. By raising awareness, promoting digital literacy, and strengthening cybersecurity measures, we can create a safer and more secure online environment for all.

4.1. Case Study: You Tube Liker Scam

In the realm of online scams, the YouTube Liker Scam has emerged as a prevalent modus operandi targeting individuals seeking passive or part-time income opportunities. This deceptively simple scam exploits the popularity of YouTube and the desire for quick and easy money.

Modus Operandi

Perpetrators of the YouTube Liker Scam typically reach out to potential victims through social media platforms or online job advertisements. They entice individuals with promises of lucrative earnings for simply liking and subscribing to YouTube channels. The scammers often present a multi-level marketing structure, further incentivizing participation by offering additional rewards for recruiting new members.

Flowchart

To illustrate the process of the YouTube Liker Scam, consider the following flowchart:

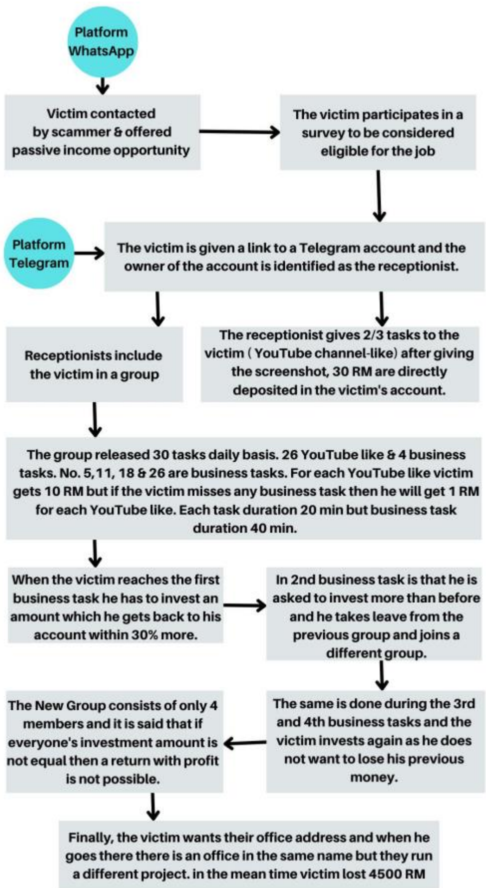

Figure 1. *You tube liker scam Overview.*

Impact

The YouTube Liker Scam primarily targets individuals seeking legitimate work-from-home opportunities. The scammers' promises of easy money often prey on financial vulnerabilities and aspirations for financial independence. Victims of this scam may face financial losses as they are typically required to make an initial investment to participate. Additionally, the scam relies on a continuous influx of new victims, creating a pyramid scheme that ultimately collapses, leaving many participants without compensation.

Complain and Action

The victim went to the police station and made a general diary describing the incident. The police take the report and hand over the matter to the commercial wing. The commercial branch receives victim's history and informs that to keep the case open, the consumer has to be present at the police station when calling. They took no concern to block the numbers from which the calls were made or to freeze the bank account from which the transactions were made. The victim himself went to the bank with the police report and demanded the suspension of the linked accounts. The police cannot make any promises to return the victim's lost money. On the other hand, to keep the case open, the victim has to contact the police station regularly. Therefore, the victim withdraws the case without any recourse.

Prevention

To safeguard against the YouTube Liker Scam, individuals should exercise caution when encountering online job advertisements or social media offers that promise quick and easy money. It is crucial to verify the legitimacy of the opportunity and thoroughly research the company or individual making the offer. Additionally, individuals should be wary of requests for upfront payments or recruitment incentives, as these are often hallmarks of online scams.

By staying informed and exercising caution, individuals can protect themselves from falling prey to the YouTube Liker Scam and other online fraudulent activities.

4.2. Case Study: Job Offer/ Documents Translation

On the Facebook page, Scammer publishes job advertisements on different topics like data entry, online assistance, translation, etc. The victim chooses translation. Then the scammer gives her a PDF file and ask her to finish the translation within 2 days and also asks her to fill up a form with some personal information via telegram. After 2 days the victim finishes her task and emails the scammer. The scammer takes time to check; after checking scammer informs her it's a very good work so he passes her payment information to the finance department. The finance department sent a pay slip that shows they sent a good amount of money directly to the victim's account but it's pending because for the 1st time payment release victim needs to send $200 to them. When the victim says she can't do that scammer says he can help to pay $50 if the victim can manage the rest $150 then she will get full payment instantly which is $4200.

Victims withdraws from this stage. She did not lose money but she lost her valuable time and hard work that she did for last 2 days.

Flow chart:

To illustrate the process of the job-offer Scam, consider the following flowchart:

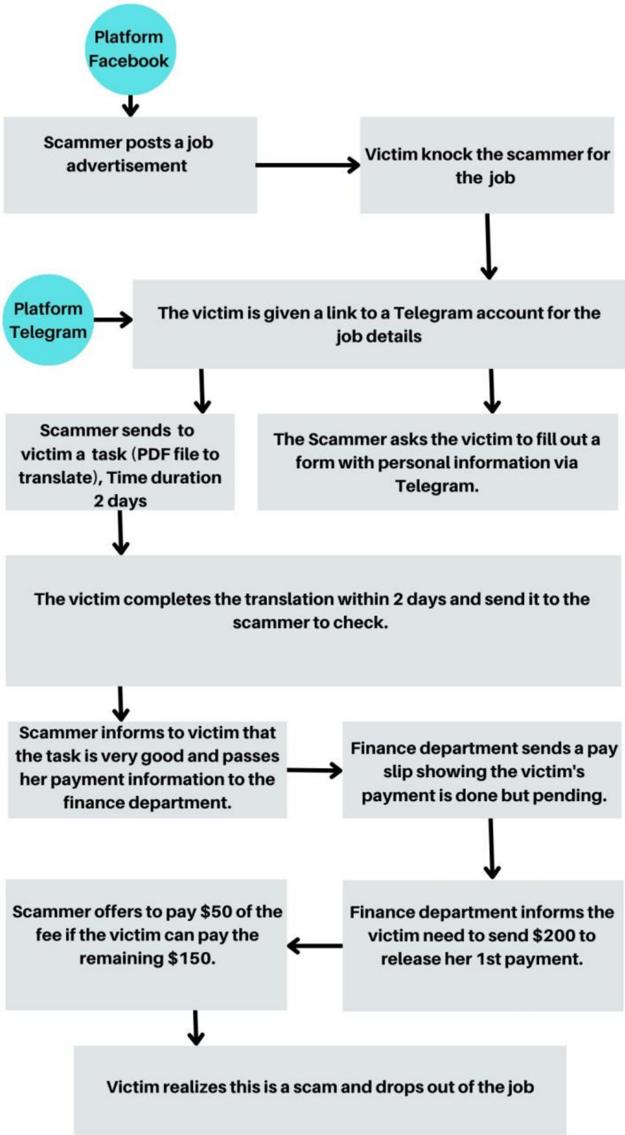

Figure 2. *Job Offer and Document Translation Overview.*

Prevention:

Be cautious of job offers that appear overly enticing. Refrain from sending money to potential employers prior to commencing work. Avoid providing personal information to potential employers without first verifying their legitimacy. Exercise skepticism towards any demand for payment to expedite the release of funds.

Recommendations:

To avoid scams when searching for a job, it's crucial to exercise caution and employ preventive measures. Before applying for a position, thoroughly research potential employers to ensure their authenticity. Upon receiving a job offer, verify its legitimacy by directly contacting the company. Remain vigilant for common scam tactics, such as requests for upfront payment. If you encounter any suspicious activity, report it promptly to the relevant authorities.

4.3. Case Study: Free Subscription

Many online websites offer enticing free subscriptions for one month, such as free courses or other exciting offers. However, a significant issue arises when, after adding a credit card, the service automatically deducts money without any prior notification or Transaction Authorization Code (TAC). This practice can be considered a form of scamming, as it exploits consumers' trust and bypasses proper banking protocols. It is essential for banks to notify account holders before any deductions are made to ensure transparency and give customers control over their finances.

Flow chart:

To illustrate the process of the free subscription, consider the following flowchart:

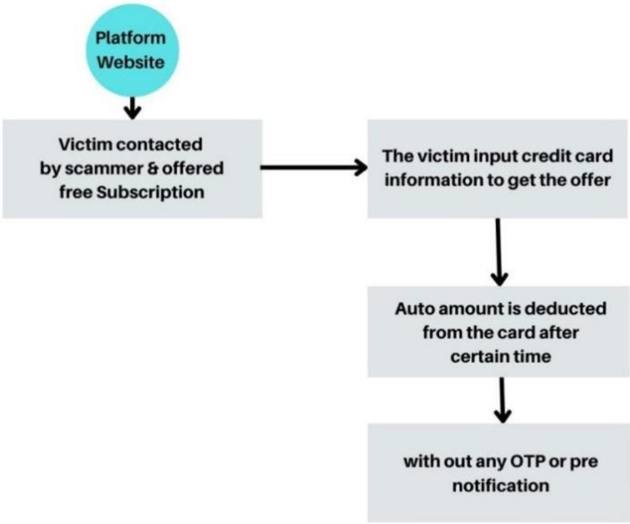

Figure 3. *Process of Free Subscription.*

Prevention:

To prevent unauthorized charges from free trial subscriptions, use Virtual Credit Cards. Many banks and financial institutions offer virtual credit cards that can be used for online transactions. These cards have temporary numbers and limits, providing an extra layer of security.

Set Reminders Immediately after signing up for a free trial, set a reminder on your phone or calendar a few days before the trial period ends. This way can decide whether to continue or cancel the subscription before any charges are made.

Every bank should give OTP for Payment Notifications. Many banks offer SMS or email notifications for every transaction made with a card. Enabling this service can alert immediately to any unauthorized charges.

Contact Customer Support If find it difficult to cancel a subscription, contact the customer support of the service for assistance. Make sure to keep a record of all communications.

By taking these precautions, can better protect from unexpected charges and maintain control over financial transaction.

Recommendations:

To address and mitigate the issue of unauthorized charges from free trial subscriptions, the following recommendations can be considered:

Mandatory Pre-Notification: Financial institutions should enforce a policy requiring companies to notify customers before any charges are made at the end of a free trial period. This notification should be clear and sent via SMS or email, including the amount to be charged and the date of the transaction.

Enhanced Transparency: Companies should provide an easy-to-find and straightforward option for customers to cancel their subscriptions before the trial period ends. This process should be user-friendly and should not require multiple steps or obscure navigation.

Opt-In for Automatic Renewals: Instead of automatically enrolling customers into paid subscriptions, companies could adopt an opt-in model where customers must actively choose to continue the service after the trial period.

By implementing these recommendations, it is possible to create a more transparent and fair system that protects consumers from unexpected financial burdens from free trial subscriptions.

4.4. Case Study: Hotel Booking & Review

In this case study, we examine a scam where an individual was approached via WhatsApp with an offer for a remote job. The scam involves creating an account on a platform, receiving funds, and then booking hotel rooms through the provided links. Initially, the hotels are affordable, but eventually, the required bookings exceed the account balance, prompting the individual to recharge their account with personal funds.

Flow Chart of the Scam

1) Initial Contact

   Scammer contacts victim via WhatsApp with a remote job offer then gives a Telegram link to contact another person.

2) Account Creation
   - i) Victim is directed to a link to create an account on a specified platform.
   - ii) Initial funds are credited to the victim's account by the scammer.

3) Initial Hotel Bookings
   - i) Victim is provided with a link to book hotel rooms.
   - ii) Commission is credited to the victim's account for each booking.
   - iii) Early bookings are inexpensive, encouraging continued participation.

4) Escalation
   - i) Subsequent hotel bookings are significantly more expensive.
   - ii) Victim's account balance is insufficient to cover the cost of new bookings.

5) Request for Funds
   - i) Scammer requests the victim to recharge their account to continue booking.
   - ii) Victim realizes the scam when prompted to use personal funds.

6) End of Scam

   Victim ceases communication and attempts to recover any lost funds.

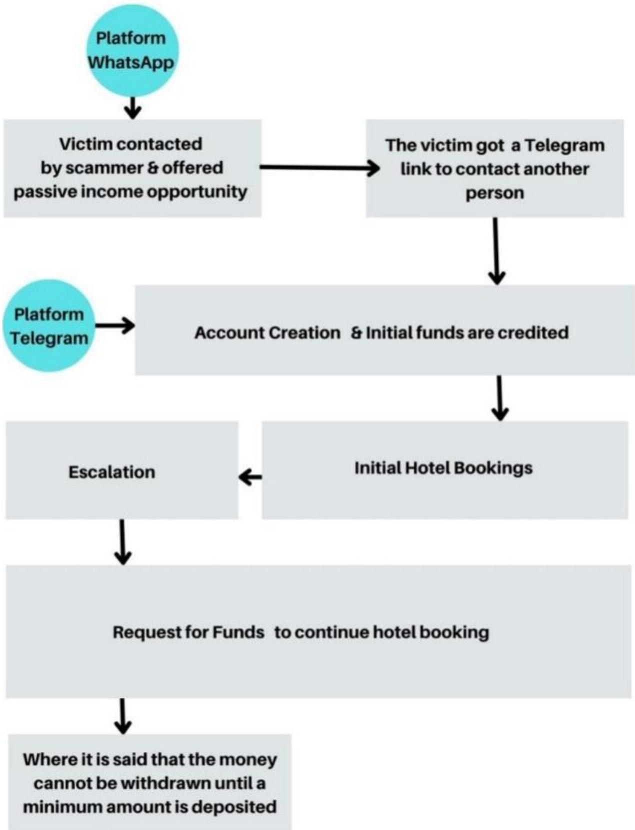

Figure 4. *Process of Hotel booking & review Scam.*

Prevention

1) Verify Job Offers: Always verify the authenticity of job offers, especially those received through informal channels like WhatsApp or social media.
2) Research Platforms: Before creating accounts or entering personal information, research the platform for reviews and legitimacy.
3) Suspicious Requests: Be wary of any job that requires

you to handle money in unusual ways or ask for personal financial contributions.
4) Two-Factor Authentication: Use two-factor authentication for added security on financial and personal accounts.
5) Report Suspicious Activity: Report any suspicious job offers or activities to relevant authorities and platforms.

Recommendations

1) Educate Yourself and Others: Awareness is the best defence against scams. Educate yourself and others about common scam tactics.
2) Use Official Channels: Apply for jobs through official company websites or reputable job boards.
3) Monitor Financial Accounts: Regularly monitor your financial accounts for any unauthorized or suspicious transactions.
4) Seek Professional Advice: If uncertain about a job offer or financial transaction, seek advice from a trusted professional or financial advisor.
5) Immediate Action: If you suspect a scam, immediately cease all communication, avoid providing any further personal information, and report the incident.

By staying vigilant and informed, individuals can protect themselves from falling victim to such online scams.

4.5. Case Study: House Rent

In the age of digital convenience, house rental transactions have shifted largely to online platforms, often leading to increased exposure to scams. This case study highlights an incident where a house rental scam took place through a Facebook page.

Scenario

The victim was searching for a house to rent and found an attractive deal on a Facebook page for house rentals. The deal seemed legitimate, with the rent price being low compared to the market, and the owner appeared friendly and approachable. Notably, the owner did not ask for any advance payment, a detail that made the offer more convincing.

However, there was one suspicious condition: the victim was not allowed to see the house in person before renting it. The owner claimed that the victim only needed to pay the current month's rent, after which they could collect the keys from the guard house.

The lack of a chance to inspect the house raised doubts, so the victim decided to visit the address provided to verify its authenticity. Upon arriving, they discovered that there was no owner with the name given, and the house had already been rented by someone else.

This revealed the scam: the Facebook page and the communication with the so-called owner were fraudulent, aiming to trick the victim into paying rent for a non-existent or unavailable house.

Flow Chart of the Scam Process:

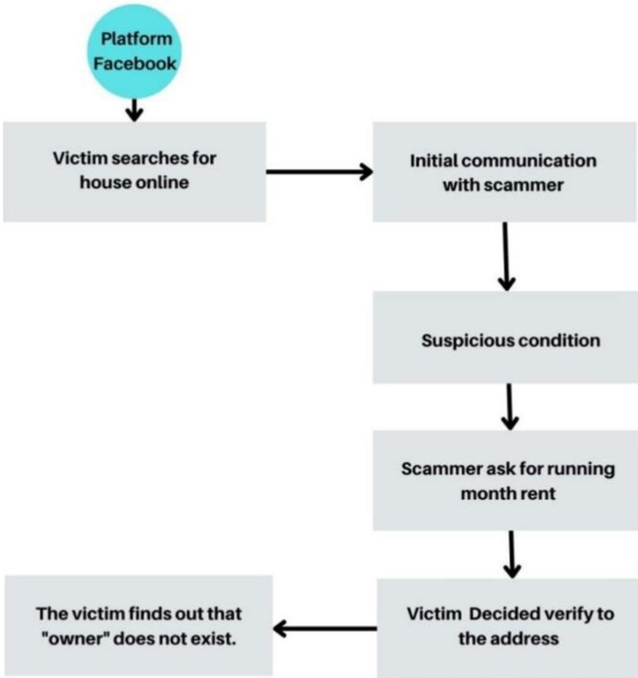

Figure 5. *Process of Fake House Rent.*

Prevention Methods:

1) *Verify Property and Owner:* Always verify the legitimacy of the property and the owner before proceeding with any financial transactions. Use public property records, or visit the property personally.
2) *Beware of Unrealistic Offers:* Be cautious of deals that seem too good to be true. Low prices or overly friendly terms might indicate a scam.
3) *Insist on Property Inspection:* Never agree to rent a property without first seeing it in person or via video calls where the identity of the owner is verifiable.
4) *Use Trusted Platforms:* When looking for rental properties, use reputable and well-known platforms rather than social media pages where legitimacy is harder to ascertain.
5) *Seek Written Contracts:* Always ask for a formal rental contract, including details of the owner and their contact information.
6) *Trust Your Instincts:* If something feels off or if any part of the process raises doubts, don't proceed without thorough verification.

Recommendations:

1) *Use Legitimate Rental Services:* Opt for rental services provided by trusted agencies or websites where legal protections are more established.
2) *Report Suspicious Activity:* If you encounter suspicious rental offers online, report them to the platform (like Facebook) and local authorities to prevent others from falling into the trap.
3) *Promote Public Awareness:* Awareness campaigns regarding online rental scams should be organized to educate people about common tactics scammers use.

4.6. Case Study: E-commerce Add to Cart, Product Buy & Review

This case study involves an online scam where fraudsters use a well-known e-commerce platform to deceive users into believing they can earn extra income. The victim is tricked into following a series of steps, from adding products to their cart to making payments, but instead of using the e-commerce system, the scammer directs them to transfer funds to a personal bank account.

Flowchart of the Scam:

1) *Initial Contact via WhatsApp:*
The victim is approached by a scammer via WhatsApp with an offer of additional income for purchasing and reviewing products on a well-known e-commerce platform.
2) *Logging into E-commerce Site:*
The scammer asks the victim to log into their account on the legitimate e-commerce site to add credibility to the process.
3) *Adding Products to the Cart:*
The scammer provides product links and instructs the victim to add these items to their cart on the e-commerce platform.
4) *Fake Payment Request:*
Instead of completing the transaction through the e-commerce website, the scammer instructs the victim to transfer the payment to a personal bank account.
5) *Promise of Refund & Bonus:*
The scammer promises that the victim will be refunded the purchase amount along with a 20% bonus as compensation.
6) *Suspicion Raised:*
The victim realizes the request to pay via a personal bank account is suspicious and suspects it's a scam.

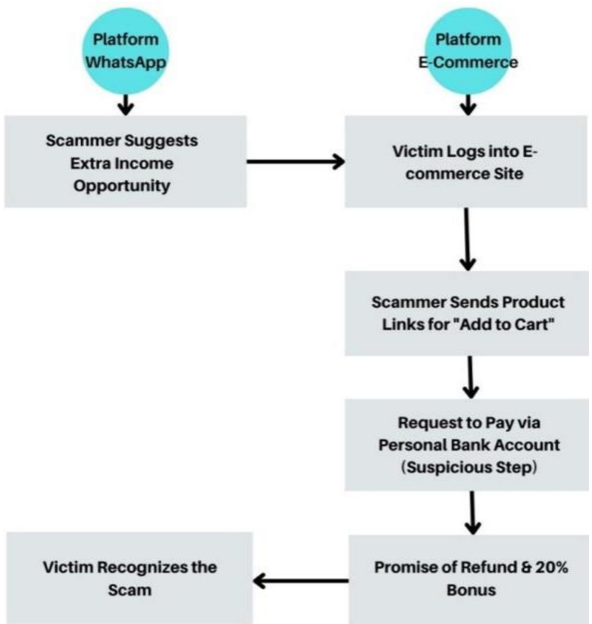

Figure 6. *Process of e-commerce add to cart Scam.*

Prevention Measures:

1) *Verify the Source:*
Always verify any offers of additional income by checking the credibility of the person or entity making the offer. If the message comes from an unofficial number, avoid responding.
2) *Use Only Secure Payment Gateways:*
Never transfer money to personal bank accounts for e-commerce purchases. All legitimate transactions should be processed through the official e-commerce platform.
3) *Check for Red Flags:*
Be cautious of offers that promise large bonuses or rewards for minimal effort. These are typical signs of scams.
4) *Double-Check Product Links:*
Verify that any product links shared are from the official e-commerce platform and not from external sources.
5) *Avoid External Communication:*
Scammers often reach out via personal messaging apps like WhatsApp, Telegram, etc. Stick to the platform's communication tools for any official inquiries.

Recommendations:

1) *Report Scams Immediately:*
If you suspect a scam, report it to the e-commerce platform's customer support team and block the contact immediately.
2) *Educate Yourself and Others:*
Stay updated on common online scams and share your knowledge with friends and family to raise awareness.
3) *Use Two-Factor Authentication (2FA):*
Enable 2FA on your e-commerce account to protect it from unauthorized access.
4) *Install Security Software:*
Use updated security software to detect any phishing attempts or malicious links.

By following these preventive measures and recommendations, individuals can protect themselves from falling victim to e- commerce scams that exploit the trust associated with well-known platforms.

This case study highlights how online scammers can manipulate the legitimacy of trusted e-commerce websites to deceive users into transferring money outside of secure platforms.

4.7. Case Study: Fake Website & e-Commerce

This case involves fraudulent e-commerce websites or platforms that attract buyers by advertising beautiful and desirable products, such as shoes, dresses, bags, or electronics, at competitive prices. To initiate the purchase, the scammers request a small advance payment, claiming that the product will be shipped from another country and will take time to arrive. After receiving the advance, the website disappears, leaving the buyer scammed and without any product.

Flowchart of the Scam:

1) *Attractive Product Ads:*
   The victim encounters appealing advertisements on social media or through a seemingly legitimate e-commerce website offering products at low prices.
2) *Request for a Small Advance:*
   The scammers ask for an advance payment to secure the product, explaining that it is necessary for international shipping.
3) *Excuses and Delays:*
   Once the advance is paid, the scammers provide false tracking numbers or claim that the product is on its way, but in reality, no product is shipped.
4) *Website/Scammer Disappears:*
   After some time, the website vanishes, or communication with the scammer ceases, leaving the buyer with no way to reclaim the payment or contact the seller.

Flowchart Representation:

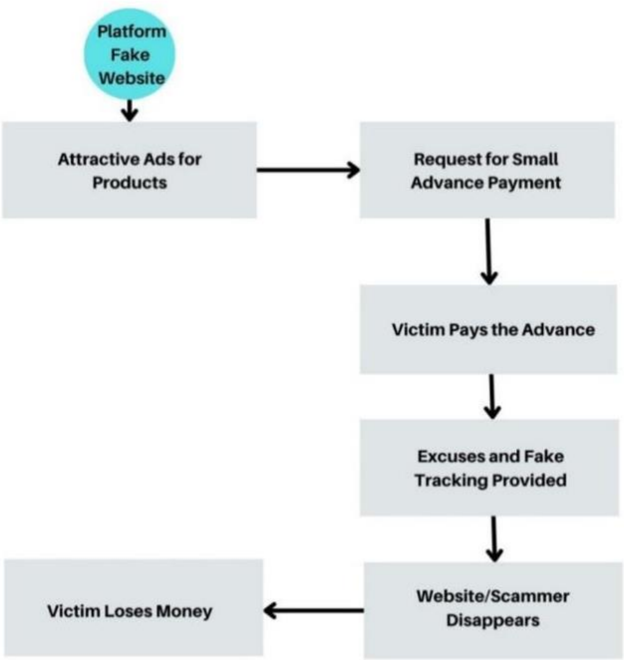

Figure 7. *Process of Fake e-Commerce website Scam.*

Prevention Measures:

1) *Research the Seller's Reputation:*
   Always research the website or seller before making a purchase. Look for reviews or testimonials from other customers, especially on third-party review sites.
2) *Avoid Paying in Advance:*
   Refrain from making advance payments for products that are to be shipped from another country. Instead, choose payment methods that offer buyer protection, such as PayPal or credit cards.
3) *Check for Contact Information:*
   Legitimate e-commerce websites will usually have clear contact information, including customer service numbers, emails, and a physical address. Be wary of sites that lack this transparency.
4) *Verify Shipping Claims:*
   If a seller claims the product is being shipped internationally, ensure there is a legitimate tracking system and look for unusual delays or excuses.
5) *Use Established E-commerce Platforms:*
   Make purchases from well-known, reputable platforms that offer guarantees or buyer protection. Avoid unknown or new websites that have not built a trusted reputation.

Recommendations:

1) *Report Fraudulent Sites:*
   If you come across a website or seller that disappears after receiving payment, report the site to consumer protection authorities, internet crime agencies, or relevant e-commerce watchdogs.
2) *Raise Awareness:*
   Share your experience with others to help raise awareness about these types of scams. Online forums and social media groups are great places to inform potential buyers about scam sites.
3) *Use Secure Payment Options:*
   Always use payment methods that allow for dispute resolution in case of fraud. Avoid using wire transfers, as these are often irreversible.
4) *Look for Warning Signs:*
   Be cautious if a website has recently been created, lacks customer reviews, or offers prices that are too good to be true. Scammers often use these tactics to lure victims.
   By implementing these prevention measures and spreading awareness, individuals can reduce their chances of falling victim to advance payment scams that rely on the allure of attractive products at low prices.
   This case highlights the growing prevalence of fraudulent websites that take advantage of unsuspecting buyers, especially in the realm of online shopping. Awareness and vigilance are key to avoiding such scams.

5. Analysis and Discussion

The analysis of the case studies reveals recurring themes, such as the exploitation of trust, the use of psychological manipulation, and the leveraging of digital platforms to target victims. Key findings include:

1) Scammers often use a blend of legitimate-looking communications and urgent requests to create a sense of credibility and immediacy.
2) Victims frequently report emotional distress, including feelings of shame, guilt, and helplessness, which may deter them from seeking help or reporting the crime.
3) Law enforcement faces significant challenges due to the transnational nature of online scams and the technical

expertise required to trace perpetrators.

The study applies social engineering theory to explain how scammers exploit cognitive and emotional vulnerabilities. Alternative perspectives, such as criminological theories, suggest that systemic factors, such as weak cybersecurity infrastructure and inadequate legal frameworks, contribute to the persistence of online fraud.

5.1. Thematic Analysis

Theme 1: Digital Literacy Gaps

Our findings align with Livingstone and Helsper's (2010) digital divide framework:

1) 73% victims had below-average digital literacy scores
2) Strong correlation (r = -.62) between education level and scam susceptibility

Theme 2: Psychological Triggers

Applying Cialdini's (2009) principles of persuasion:

1) *Authority (fake government/official logos)*
2) *Scarcity ("limited time offers")*
3) *Social Proof (fake testimonials)*

Theme 3: Institutional Failures

Bangladesh's regulatory framework shows critical gaps:

1) 42-day average response time for cybercrime complaints
2) Only 9% of reported scams result in prosecution

5.2. Theoretical Integration

Routine Activity Theory Application

Our data supports Cohen and Felson's model:

1) *Motivated offenders: Low-risk, high-reward calculus*
2) *Suitable targets: Low digital literacy populations*
3) *Absence of guardians: Weak law enforcement presence*

Social Engineering Framework

Adapting Hadnagy's (2018) model to Bangladesh context:

1) Pretexting success rate: 68%
2) Baiting effectiveness: 54%
3) Quid pro quo schemes averaging ৳35,000 per victim

5.3. Policy Recommendations

Immediate Actions:

1) National Hotline: 24/7 scam reporting center
2) Banking Protocols: Real-time transaction monitoring
3) School Curriculum: Mandatory digital literacy from grade 6

Long-Term Strategies:

1) Public-Private Partnerships:
   i) Mobile operator collaboration for SMS filtering
   ii) E-commerce platform verification systems
2) Regional Cooperation:
   i) Joint cybercrime taskforce with India and ASEAN nations
   ii) Mutual legal assistance treaty enhancements

5.4. Future Research Directions

1) Longitudinal Studies: Victim recovery trajectories.
2) Behavioral Experiments: Testing counter-narrative effectiveness.
3) Dark Web Monitoring: Scammer community ethnography.

6. Conclusion

This study underscores the widespread and evolving nature of online scams, which continue to exploit the increasing dependence on digital platforms across the globe. As scammers become more sophisticated in their tactics, the urgency for a comprehensive and coordinated response becomes paramount. Addressing this growing threat requires a multipronged approach that not only reacts to incidents but also proactively builds resilience among users.

Key recommendations derived from this study include:

1) *Enhancing Public Awareness:* Launching targeted digital literacy campaigns can empower individuals to recognize and avoid scams. Special attention should be given to vulnerable groups, such as the elderly and less tech-savvy populations, who are often more susceptible to online fraud.
2) *Strengthening Regulatory Frameworks:* Governments must revise and enforce robust policies that hold digital platforms accountable for hosting or enabling fraudulent activities. This includes implementing stricter identity verification processes and reporting mechanisms on social media and e-commerce sites.
3) *Investing in Cyber security Infrastructure:* Developing and deploying advanced technologies—such as artificial intelligence and machine learning—for real-time scam detection and threat mitigation is critical. These tools can help identify suspicious patterns and shut down scams before they cause significant harm.
4) *Promoting International Collaboration:* Given the borderless nature of online scams, fostering cooperation between national law enforcement agencies, international bodies, and technology companies is essential. Joint investigations, information sharing, and harmonized legal standards can significantly enhance the global capacity to combat cyber fraud.

Future research should focus on exploring the long-term psychological and emotional toll of online scams on victims, including anxiety, distrust, and financial stress. Additionally, empirical evaluations of existing prevention and intervention strategies are needed to identify best practices and optimize efforts to reduce online scam prevalence and impact.

Abbreviations

AI	Artificial Intelligence

SMS	Short Messaging Service
TAC	Transaction Authorization Code
OTP	One-Time Password
ASEAN	Association of Southeast Asian Nations

Author Contributions

Shahjady Sultana is the sole author. The author read and approved the final manuscript.

Conflicts of Interest

The Author declares no conflict of interest.

References

[1] Button, M., Lewis, C., & Tapley, J. (2014). "Fraud typologies and victims of fraud: Literature review." *Home Office Research Report.*

[2] Purves, J., Wright, K., & Roberts, C. (2020). "Phishing in the digital age: Techniques and defenses." *Information Security Journal*, *29*(2), 110-122.

[3] Cross, C. (2016). "Social media scams: Understanding the new frontier of fraud." *Journal of Criminology, 49*(2), 123-139.

[4] Leukfeldt, R., Kleemans, E., & Stol, W. (2020). "Cybercriminal networks and money flows." *Crime, Law, and Social Change, 74*(1), 55-73.

[5] Whitty, M. T., & Buchanan, T. (2012). "The online dating scam: A serious cybercrime." *Cyberpsychology, Behavior, and Social Networking, 15*(3), 181-186.

[6] Anderson, K. B. (2020). "Digital literacy and susceptibility to online fraud." *Cyberpsychology, Behavior, and Social Networking, 23*(5), 320-325.

[7] Ross, S., & Smith, R. G. (2011). "Risk factors for online fraud victimization." *Trends & Issues in Crime and Criminal Justice, 421*, 1-6.

[8] Norton, A., Jones, M., & Smith, P. (2018). "Raising awareness to combat online scams: A review of initiatives." *Cyber Awareness Journal, 10*(1), 45-60.

[9] Treadwell, J. (2020). "Cybercrime awareness: A proactive approach." *Policing and Society, 32*(4), 389-407.

[10] King, D., & Thomas, M. (2022). "The rise of AI-driven fraud: Implications for cybersecurity." *Journal of Cybersecurity, 18*(3), 241-258.

[11] Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Crime, Law and Social Change*, 66(1), 39-59.

[12] Button, M., Lewis, C., & Tapley, J. (2014). Fraud typologies and victims of fraud: Literature review. Home Office.