Aftab *et al. (IJECI)* 2024

(IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2024.0801186

Research Article

Vol. 8 issue 1 Jan-Mar 2024

Online shopping, Cyber frauds and Fraud prevention Strategies

Aftab Ahmad Malik[1], Waqar Azeem[2] and Mujtaba Asad[3]

[1]Department of Computer Science, University of Engineering and Technology Lahore.
[2]Faculty of Computer Science, South Eastern Regional College, Down Patrick Ireland, United Kingdom.
[3]Department of Automation and Control, Shanghai Jiao Tong University, Shanghai, China.
Corresponding author: dr_aftab_malik@yahoo.com

Received: December 22, 2023; **Accepted:** January 10, 2024; **Published:** March 15, 2024

ABSTRACT

Online shopping is increasingly being targeted by hackers and cyber criminals, who exploit the anonymity of the internet to deceive unsuspecting shoppers. These scams involve fake websites or ads, posing as legitimate sellers, damaging innocent citizens' bank accounts and databases, and causing damage to customers. Online shopping fraud involves using stolen credit or debit cards for purchases, while identity theft involves stealing personal information for fraudulent purposes like credit or illegal purchases. We discuss, the safety tips to avoid online shopping scams, using these safety tips before making a purchase. In United states a government agency FTC has been entrusted the task of implementation the civil law related to anti-trust; it also indorses and promotes the protection of consumers rights while working with Justice Department. Online shopping scams were the second most common fraud category in 2021, according to the FTC. To avoid them, use safety tips to identify and avoid scams. Cybercriminals steal and can use personal information to make unauthorized purchases or engage in fraudulent activities. Identity theft is a crime involving capturing and the misuse of another's personal identifying information like Id-card, credit card and bank account information. Fraudsters often use stolen credit cards to purchase items, return them for refunds, and then sell the refunded money or goods. Machine learning is a rapidly evolving technology that can significantly enhance online shopping security and user awareness which is coupled with artificial intelligence

Keywords: Cyber threats, Cyber frauds, Common Scams, Forgery, Identity theft.

1. INTRODUCTION

The consumers should be aware of potential scams in online shopping, including common types of frauds spreading in society; to protect themselves from potential scams such as Account Takeovers, Fake Websites and Stores, Identity Theft, Payment Frauds, Phishing Scams, Refund Fraud, Social Engineering and Unsecure Wi-Fi Networks. Online shopping fraud can be minimized by adopting a proactive approach, shopping from

reputable websites, and checking for reviews and customer feedback before making a purchase to ensure a secure transaction. Secure websites use encrypted connections, ensuring transactions are processed securely and efficiently. We must double-check the website's legitimacy by verifying the URL, checking for contact information, and examining spelling errors or unusual design elements. Online shopping dodges involve fraudulent activities where criminals pretend to be genuine sellers through fake websites or advertisements on genuine venders' sites. Scammers exploit the anonymity of the internet to create fake online retailers, using advanced technology, sophisticated designs, stolen logos, and domain names to steal unsuspecting shoppers from legitimate online sellers. Websites often sell luxury items like clothing, jewelry, and electronics at low prices, but customers may receive fake or nothing at all.

2. USE OF SOCIAL MEDIA AND ELECTRONIC DEVISES

Online shopping scams are increasingly using social media to set up fake online stores, often selling counterfeit clothing or jewelry. These scammers advertise their fake websites on social media, so trusting a site based on its appearance is not enough. To detect these scams, search for reviews before making a purchase. shopping.

According to [1], it is recommended that electronic devices and software can be very effectively used for detection and Control of the offences of online frauds, white collar crimes, cybercrimes, hacking of others information. According to [2], the frauds in Banking and entrepreneurs may be eradicated and minimizes by implementing software for Network Security with electronic devices and creating a demilitarized Zone in Network consisting of two fire walls, first is software firewall and the second a hardware firewall. The role of legislation and need of strong Legal Framework and Procedures has been discussed in [3]. According [4] to Technology has significantly impacted human life, particularly in the realm of buying and selling. The internet has significantly facilitated this process, offering more convenient and less stressful options. Online shopping and e-commerce have enabled consumers to access products from distant stores, eliminating distance and long queues. The paper [5] recommends to contest effectively with Cybercrime and Money Laundering; and discusses the threats and consumer perceptions of online shopping, emphasizing the need for awareness on cyber security issues. It provides tips on protecting users and merchants from data breaches and attacks, including phishing and adware.

3. HOW TO AVOID FRAUDS REGARDING ONLINE SHOPPING?

The research paper [6], stresses and worry about the requirement of calibration of forensic evidence its attaining preservation and presentation in court. It further advises the using FBI techniques must be used by FIA Pakistan. Online shopping allows consumers to access products from distant stores without long queues. However, it is susceptible to threats, such as data breaches and security compromises, making consumers uncertain about their trust in online shopping is convenient but crucial to avoid scams. By

following these tips, you can identify scam signs and feel more confident in your online shopping experience. It's better to be cautious and risk losing deals than losing money. Report any scams to your bank and the Federal Trade Commission. Frequently occurring Bank Frauds Using Digital Devices in Pakistan and the Role of Business Ethics has been elaborated and expounded in [7]. Some safety measures are given below:

- Avoid sellers contending on immediate payments via apps like Zelle®, Venmo, Cash App, or online wire transfers of money.
- Avoid sellers using pressure tactics for immediate purchases.
- Avoid sharing sensitive information like bank account number, PIN, or access code.
- Be cautious of social media ads leading to unfamiliar sites.
- Be doubtful of deals with low prices.
- Be watchful of fake websites and secure websites.
- Research the seller and use the term "scam" before sending money.
- Set up account alerts for unusual activity.
- Trust your instinct and walk away if something feels off.
- Use credit cards, especially if unfamiliar with the seller.

4. THE LEGAL PROVISIONS ON ONLINE FRAUDS

Fraud in Pakistan can occur at anytime, anywhere, and is defined as "fraudulently" under section 25 PPC, if done with intent to defraud. A fraud occurs when someone deceives you into parting with your property under false pretenses, including cash, personal information such as property car, house, phone number, or consent to use the information. There are few legal instruments, we would like to refer on the subject matter like “fraud in Pakistan on online shopping “.

- Consumer Protection Laws
- Electronic Transactions Ordinance, 2002,
- Intellectual Property Laws
- Procedures of Federal Investigation Agency (FIA),
- Pakistan Penal Code PPC relevant Clauses.

The Electronic Transactions Ordinance in Pakistan establishes a legal framework for electronic transactions, including online shopping, and acknowledges electronic documents and digital signatures. Pakistan has consumer protection laws to protect consumer rights and address fraud in online transactions. The Pakistan Penal Code includes provisions for cheating, criminal breach of trust, and forgery, which may apply in online shopping fraud cases. The FIA in Pakistan investigates and combats cybercrimes, including online fraud, and may use specific laws to protect brand owners' rights in cases of counterfeit or pirated goods involved in online shopping. According to [8], the internet has transformed the shopping experience, offering convenience and less stress.

5. THE PROCEDURE FOR TRIAL IN COURT

For the offences related to Frauds and Cyber

Crime is identical with other crimes as shown in the steps given below.

- Arrest warrant
- Arrest
- Initial appearance
- Investigation
- Identification of suspect
- Decision of charging the offender
- Court proceedings of the trial
- Fines, probation, or imprisonment
- Sentencing

The suspect is initially seen by a judge, where charges are read and bail may be set. Prosecutors review evidence and decide whether to file formal charges based on the crime's severity. A judge initially sees the suspect, reads charges, and sets bail. Prosecutors review evidence and decide on filing formal charges based on the crime's severity. Jurisdictional laws and procedures for online shopping-related crimes can vary, and the nature and severity of the crime can impact arrest steps. Legal representation is crucial for protecting individuals' rights during legal proceedings. The court determines the appropriate punishment for a suspect's conviction, which may include fines, probation, or imprisonment.

6. ONLINE SHOPPING FRAUDS IN PAKISTAN

According to [8], legal concerns arise when dealing with online shopping fraud in Pakistan. It's advisable to consult with a legal professional or contact relevant authorities like the Federal Investigation Agency for guidance on current legal provisions and actions. Pakistan's Payment System and Electronic Fund Transfers Act, 2007 establishes a legal framework for online payment transactions. According to [9], Online shopping offers convenience and reduced stress compared to traditional methods, eliminating the need for physical stores and allowing more informed product selection. However, it is susceptible to malicious attacks that compromise data safety, security, and integrity. According to [10], technology developments have significantly impacted business operations, forcing companies to adapt to global dynamics and customer demands. Understanding the roles of technologies in constructing innovative business models, particularly in ecommerce, is crucial. A survey based on secondary research results and an evaluation matrix were developed to summarize technologies and identify gaps in current research. A study conducted and reported in [11] assesses the consumer perceptions and attitudes towards healthy and environmentally friendly foods, focusing on reducing overconsumption, low-nutrient consumption, plant-based diets, and food waste, highlighting the importance of multilevel policies for promoting sustainable food practices.

According to [12] the media industry is experiencing rapid shifts in consumer spending, with consumers shifting towards digital services and media products. Gartner reports show a gradual increase in IT services, making the industry the third-largest IT spender. The study aims to investigate research on Information Systems (IS) in the media industry, particularly in management and economic areas.

In Pakistani FIR is required to be lodged with Police about the occurrence of fraud cases and if the matter is related to online or significant cybercrime, to the FIA, The FIR initiates a criminal investigation, requiring evidence at every stage. Attach screenshots, private conversations, or websites used for fraud. Pakistan has implemented the Payment Systems and Electronic Fund Transfers Act, 2007 to establish and operate Payment System Operators and Providers for online payment systems. Its purpose is to regulate payment systems and electronic fund transfers, providing consumer protection standards and determining financial institutions' rights and liabilities, ensuring efficient and secure financial transactions. Mostly the online shopping fraud cases can be minimized using knowledge of academic databases like PubMed, IEEE Explore, Science Direct, JSTOR, or Google Scholar, and search for relevant papers using keywords like "online shopping fraud", "e-commerce security" and "consumer protection." The FIA advises individuals facing fraud to seek legal assistance, inform relevant organizations and relevant agencies, lodge an FIR and effectively pursue the case. The authors of [13], use online product reviews to extract consumer brand associations and their interconnections, utilizing a network-based understanding of brand image. This approach measures brand image, using consumer-generated content which is tested in an empirical study.

7. RECOMMENDATIONS

i. To ensure online safety, avoid making purchases on unsecured Wi-Fi networks and use a VPN for added security.

ii. Maintain secure online accounts by shopping from reputable websites, using unique passwords.

iii. keep devices and antivirus software updated, being cautious of unauthorized emails, and

iv. Regularly review bank and credit card statements. Before making a purchase, review the seller's ratings and feedback, especially those with a negative track record.

v. Choose secure payment methods like credit cards or reputable online services, and avoid wire transfers or payment methods with limited dispute resolution options.

vi. Immediately report alleged fraudulent activity to online platforms, banks, and authorities.

vii. Arrange caution and verify website legitimacy before making online purchases.

viii. Ensure that the website uses secure and encrypted connections, specifically "https://" in the URL, when processing payments.

ix. Secure websites utilize encrypted connections to ensure efficient and secure transaction processing.

x. Enable “multi-factor authentication” whenever possible to enhance the security of your online accounts.

xi. The suspicious online links must be

ignored and not do not download the attachments of doubtful links and don't download anything from unwanted emails or messages, particularly those requesting for personal or financial information.

xii. It is advisable to consult with a legal professional or the Federal Investigation Agency for guidance on current legal provisions and actions. The legal landscape may change, and enforcement effectiveness may vary.

xiii. Research on consumer protection laws and cybersecurity measures in online shopping is being conducted to address fraud and ensure consumer safety. This study will enable to explore the implementation of cybersecurity measures to prevent online shopping fraud.

xiv. Exploration of recently developed methods and having knowledge about the detection of frauds in the processes of e-commerce is indeed very important as well as the role of electronic technology for the prevention of online frauds.

xv. Machine learning is a rapidly evolving technology that can significantly enhance online shopping security and user awareness which is coupled with artificial intelligence.

xvi. To ensure a fair and reliable online shopping experience, find out first the genuineness of that website/social media page that it has announced a just refund or returns policy, detailed complaint handling processes, and a clear understanding of the company you are dealing with.

xvii. It is recommended that the research published in "Computers & Security," "Journal of Cybersecurity," " and "Journal of Consumer Affairs" is very effective and notable. Therefor the reader must look into it.

xviii. Familiarize yourself with online store refund and return policies, and be cautious if unclear. Implementing these practices can reduce fraud risk and create a safer shopping experience.

xix. According to [4], Secure online payments with a secure service, 'https' URL, and padlock symbol. Verify URLs and consider virtual currencies like bitcoin, as they lack protections and cannot be refunded once sent.

8. CONCLUSION

Online shopping revolutionizes the shopping experience by eliminating long queues and limited options, allowing for more informed selection of preferred models or products without frequent store searches, thereby enhancing the overall shopping experience. Phishing and adware attacks have led to numerous data breaches affecting reputable firms like Amazon and Google. Online shopping offers convenience and reduced stress, but it also exposes users to malicious attacks that compromise data safety and integrity. Online shopping faces threats from fraud and lack of proper information. Enhancing knowledge on cyber security

threats can enhance security and reduce negative perceptions, making it a more appealing option for consumers. Online shopping has faced numerous data breaches due to cyber security threats, including phishing and adware techniques. This has led to reluctance among consumers to adopt online shopping due to concerns about fraud and lack of proper information. Enhancing cyber security awareness can help mitigate these risks.

9. ACKNOWLEDGEMENT

The authors express gratitude for Mr Kaukab Jamal Zuberi and Dr Syed Mona Hassan, Chief Editor for encouragements.

REFERENCES

[1] A. A. Malik, M. Asad and W. Azeem, “Detection and Control over the offences of White Collar Crime, Fraud and Hacking of information by using effectively the relevant software and Electronic Devices”, International Journal for Electronic Crime Investigation, vol. 7, no. 1, pp. 1-8, 2023.

[2] A. A. Malik, M. Asad and W. Azeem, “Frauds in Banking and entrepreneurs by electronic devices and combating using Software and employment of demilitarized zone in the Networking”, International Journal for Electronic Crime Investigation, vol. 6, no. 4, pp. 1-8, 2022.

[3] A. A. Malik, W. Azeem and M. Asad, “Role of Legislation, need of strong Legal Framework and Procedures to Contest Effectively with Cybercrime and Money Laundering”, International Journal of Crimes investigation, vol. 6, no. 2, pp. 1-8, 2022.

[4] A. A. Malik, W. Azeem and M. Asad, “Requirement of strong legal frame work and procedures to contest with Cybercrime in Pandemic Situation”, International Journal for Electronic Crimes Investigation, vol 5, no. 1, pp. 3-12, 2021.

[5] A. A. Malik, M. Asad and W. Azeem, “To Combat White Collar Crimes in Public and Private Sector and Need for Strong Legislation and Ethics”, International Journal for Electronic Crimes Investigation, vol. 4, no. 3, pp.1-8, 2020.

[6] A. A. Malik, “Standardization of forensic evidence its procurement preservation and presentation in court of using FBI techniques by FIA”, International Journal for Electronic Crimes Investigation, vol. 4, no. 1, pp. 1-6, 2020.

[7] A. A. Malik, "Bank Frauds Using Digital Devices and the Role of Business Ethics", International Journal for Electronic Crimes Investigation, vol. 2, no. 4, pp. 1-9, 2020.

[8] Pakistan's Payment System and Electronic Fund Transfers Act, 2007.

[9] A. Aseri, “Security issues for online

shoppers", International Journal of Scientific and Technology Research, vol. 10, no. 3, 2021.

[10] U. Doloto and Y. H. Chen-Burger, "A Survey of Business Models in eCommerce, In Agent and Multi-Agent Systems: Technologies and Applications", 9th KES International Conference, KES-AMSTA, pp. 249-259, 2015.

[11] A. Hoek, D. Pearson, S. James, M. Lawrence and S. Friel, "Shrinking the food-print: A qualitative study into consumer perceptions, experiences and attitudes towards healthy and environmentally friendly food behaviors", Appetite, pp. 117-131, 2017.

[12] A. Lugmayr and J. Grueblbauer, "Review of information systems research for media industry–recent advances, challenges, and introduction of information systems research in the media industry", Electronic Markets, vol. 27, no. 1, pp. 33-47, 2017.

[13] S. Gensler, F. Volckner, M. Egger, K. Fischbach and D. Schoder, "Listen to your customers: Insights into brand image using online consumer-generated product reviews", International Journal of Electronic Commerce, vol. 20, no. 1, pp. 112-141, 2015.