Article

Not peer-reviewed version

Investigation into Online Banking and its Prevailing Fraud Factors: A Comprehensive Analysis

Richard Kalu *

Posted Date: 24 March 2025

doi: 10.20944/preprints202503.1711.v1

Keywords: Online Banking; Fraud; Data Integrity; Biometric Authentication; Fraud Prevention; Cybersecurity

Article

Investigation into Online Banking and Its Prevailing Fraud Factors: A Comprehensive Analysis

Richard Kalu

Independent Researcher; richard.kalu01@hotmail.com

Abstract: This study explores the investigation of security concerns surrounding online banking, the prevailing fraud factors that affect banks and customers and aim to discuss effective precautionary steps towards preventing fraudulent activities. Employing a qualitative research approach, data was collected through online interviews during the pandemic lockdown and restrictions. Findings reveal that while online banking has transformed financial transactions by offering unprecedented convenience and efficiency, it has simultaneously exposed both banks and customers to significant fraud risks. The study discusses user perceptions of online security, the impact of fraud on reputation and customer trust and recommends integrated fraud detection, prevention, and resolution measures. These insights provide a critical contribution to the ongoing development of robust online banking security protocols.

Keywords: online banking; Fraud; data integrity; biometric authentication; Fraud prevention cybersecurity

Subject: computer science; information systems security; risk management and Fraud analysis; financial technology (FinTech) and digital banking

1. Introduction

Online banking has evolved exponentially since its inception. Initially conceived as an experimental service in the early 1980s, online banking has grown from a niche-offering to a mainstream financial service. Prior to the advent of the internet, banking activities were confined to physical branches. Customers had to travel to bank buildings even for simple tasks such as checking an account balance. However, with the emergence of digital technologies, home banking was introduced in New York City in 1981 by several leading banks. In the UK, the Bank of Scotland pioneered the online banking experience in 1983 using rudimentary systems involving televisions and telephones [1,2].

The rapid evolution of online banking has brought significant benefits such as increased convenience, reduced operational costs, and enhanced transaction efficiency. A typical scenario is the availability of internet aided technologies that allow customers take a picture of a cheque using a mobile device and depositing it into a bank account as well as receiving text/email alerts confirming transaction accordingly [3].

Today, online banking has evolved as technology continues to grow and has become the most popular way of creating access to banking activities, even on the go [4]. The evolution of internet banking and its success is still being celebrated on the 8th of October every year, signifying the National Online Bank Day around the world. Yet, it has also introduced new vulnerabilities, exposing both banks and customers to fraud and cyber-attacks.

This article provides a comprehensive analysis of online banking security issues, drawing from extensive qualitative data collected via online interviews. It examines the evolution of online banking, evaluates current security measures, and discusses the persisting challenges in fraud detection and prevention in modern day banking [28,30]. The insights gained offer recommendations for improved security protocols and future research directions.

2. Related Work

2.1. Evolution of Online Banking

The literature on online banking highlights a significant transition from traditional brick-and-mortar systems to digital platforms. Early experiments in online banking began in the early 1980s, when customers were first given the opportunity to perform banking transactions from home. This initial phase was met with considerable skepticism; customers were unsure if remote banking could provide the same level of security as physical bank visits. Conducting day to day banking activities over the internet has increased the experience and effect of banking as well as increased accuracy of data [5], compared to traditional brick-and-mortar banking.

The evolution continued as banks adopted increasingly sophisticated technologies [25]. From the use of dial-up connections and primitive user interfaces [6], online banking platforms evolved into modern systems with advanced graphical interfaces, secure mobile applications, and real-time transaction processing. The rapid technological growth has been celebrated annually on National Online Bank Day, which underscores both the historical significance and the ongoing relevance of digital banking innovations. [7] Reported that from a bank's perspective, internet banking not only simplifies the process of banking using the internet, but also creates an effective robust transactional platform as well as providing an enhanced timeless delivery of banking services

2.2. Security Concerns in Online Banking

As online banking evolved, so too did the security challenges. Financial institutions now face a dual burden: while they strive to offer seamless and convenient services, [36] with some offering refunds, [26] they must also safeguard sensitive customer data and financial transactions against an ever-growing array of cyber threats.

The processes involved in online banking kickstarts from the attempt by a user to log into their bank account online, using a device (PC or any mobile device) to access the bank's server via the bank's website or application, depending on the level of activity being carried out by the user. Figure 1 shows an example of the layout of processes and stages involved [8].

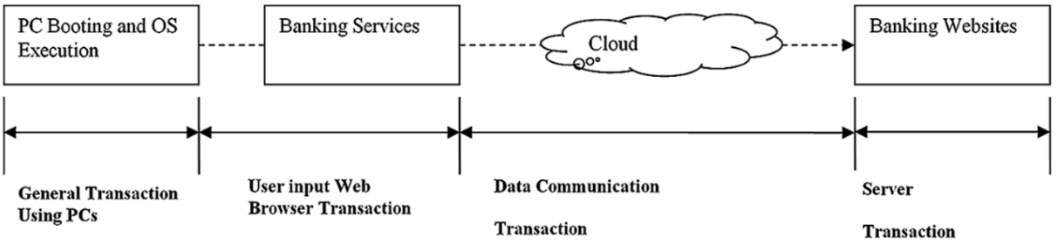
PC Booting and OS Execution
Banking Services
Cloud
Banking Websites
General Transaction Using PCs
User input Web Browser Transaction
Data Communication Transaction
Server Transaction

Figure 1. Layout of Online Banking System.

Studies have shown that there are 3 major issues challenging the security of online banking. [9] This report shows that these issues are results of various limitations or factors including poor configuration of operating systems, limitations of web browsers and servers and weakness of web security technologies. Hence the three main security challenges are as follows:

- **Authentication:** Ensuring that only authorized users gain access to their accounts is a primary concern [38]. The use of usernames, passwords, personal identification numbers (PINs), and security questions forms the basis of most authentication processes. However, any weakness in these systems can lead to unauthorized access and fraud.
- **Data Integrity and Confidentiality:** Protecting customer data from unauthorized alteration or disclosure is critical. Banks must implement robust encryption and data integrity measures to ensure that sensitive information remains secure.

doi:10.20944/preprints202503.1711.v1

- **System Design and Access Control:** The architecture of online banking systems must be designed with security in mind from the ground up. This includes implementing firewalls, antivirus systems, and continuous monitoring to detect and thwart potential breaches.

Studies [10] indicate that despite the implementation of various security measures such as one-time passwords (OTP), digital certificates, and biometric authentication fraudsters continue to find new ways to exploit vulnerabilities in online banking systems. Research has shown that in September 2012, 73% of websites in the United States of America experienced phishing attacks [11,23]. Figure 2 shows a chart of the various industries and the percentage of attacks they experienced.

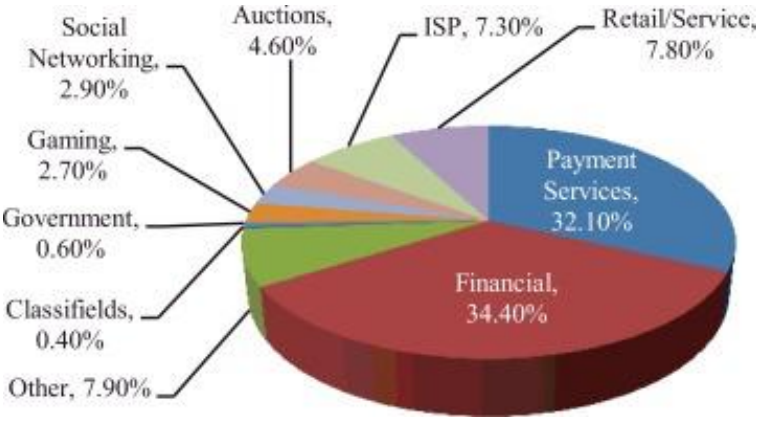

Figure 2. Different industries affected by phishing in 2012.

2.3. Prevailing Fraud Factors and Attack Techniques

Online banking fraud encompasses a wide range of fraudulent activities aimed at gaining unauthorized access to customer accounts and financial assets. The literature categorizes these fraudulent methods into several types:

- **Phishing, Vishing, and Smishing:** Fraudsters use emails (phishing), phone calls (vishing), and text messages (smishing) [34] to trick customers into divulging sensitive information [12]. These scams are designed to mimic legitimate bank communications, thereby deceiving unsuspecting users and stealing their identity, which encompasses identity fraud [31].
- **Malware and Trojan Attacks:** Malicious software such as keyloggers, viruses, and trojans are employed to capture login credentials and other confidential data from infected devices.
- **Man-in-the-Middle and Fraudulent Website Attacks:** Attackers create counterfeit websites that resemble official bank portals to capture user information as it is entered. These methods exploit the trust that customers place in familiar banking interfaces [24].
- **Trojan Attack:** in this case the attacker installs a Trojan in form of key logger computer program on an unsuspicious users' computer. [13] This often kick starts when a user visit compromised websites, downloads and installs infected programme on their electronic device.

The increasing sophistication of these attack vectors necessitates continuous innovation in security protocols. While banks have deployed multiple layers of security, the dynamic nature of cyber threats requires ongoing vigilance and adaptation.

2.4. Security Measures and Recommendations

Financial institutions have responded to the threat of fraud by implementing a range of security measures. Some of the commonly adopted models include:

- **One-Time Passwords (OTP):** Often used as a secondary authentication factor, OTPs provide a temporary code that enhances security during online transactions. One-time passwords could be static or could change periodically [14].
- **Digital Certificates and Public Key Infrastructure (PKI):** These technologies help verify the identities of both the user and the bank's server, ensuring secure communication channels.

However, reports [15] that several attacks on digital certificates recently involving hackers breaking into 2 digital certificates out of 3, has led to doubts regarding the safety of the models of digital certificates.

- **Device Registration and Recognition:** By identifying and authorizing trusted devices, banks can limit access to known endpoints.
- **Biometric Verification:** Technologies such as fingerprint scanning and facial recognition have become increasingly prevalent in safeguarding online banking systems.
- **Pass-Phrase Verification:** Often referred to a second level security method used by banks to verify transactions being carried out by users online, enabling the authorization of transactions to go through.
- **CAPTCHA** (Completely Automated Public Test to tell Computers and Humans Apart): as the name implies is an automated verification tool widely used in the prevention of online automated system attacks. [16] CAPTCHA is commonly used in solving Artificial Intelligence (AI) problems online by generating and grading tests that are humanly solvable but not bot solvable [33].

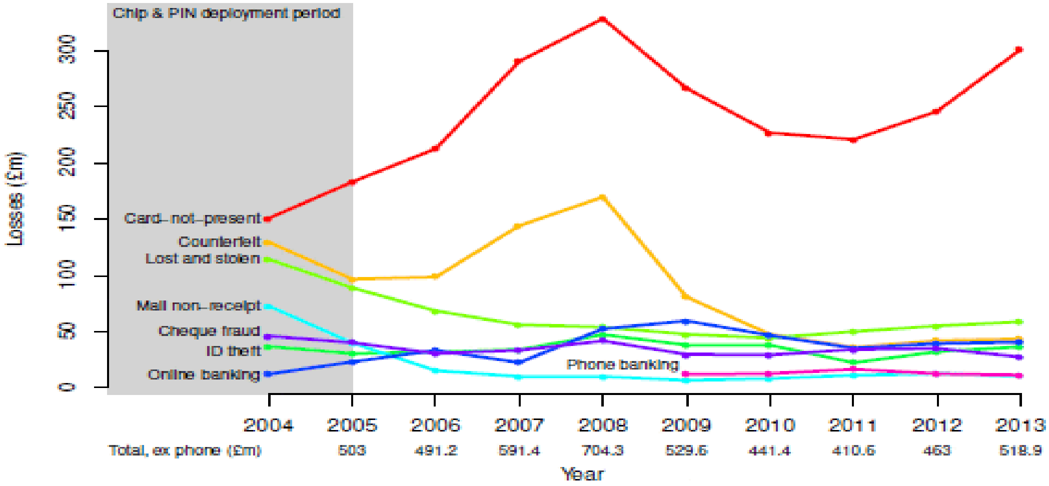

Figure 3. Financial fraud levels on UK payment systems 2004 - 2013.

Despite these measures, the literature emphasizes that no single solution is entirely foolproof. The challenge lies in integrating multiple layers of security to create a comprehensive defense strategy. Recommendations from recent studies [17] suggest that banks should invest in advanced monitoring systems, user education programs, and more adaptive security protocols that can evolve alongside emerging fraud techniques.

3. Methodology

3.1. Research Design and Rationale

The adoption of qualitative and quantitative research methodologies in this study aimed at exploring the lived experiences of online banking users with respect to security and fraud. Given the sensitive nature of the topic and the dynamic environment of digital banking, qualitative methods are deemed most suitable to capture nuanced insights and personal perspectives [35]. A mixed method allows researchers to delve into the complex interplay between user trust [37], perceived security and the effectiveness of current fraud prevention measures [27].

3.2. Data Collection: Online Interviews

In this study, online interviews were used to capture the views and experiences of the respondents. Due to the global COVID-19 pandemic and ensuing social distancing measures at the time of this research, traditional face-to-face interviews were not feasible. Instead, online interviews were conducted using platforms such as Zoom and Skype. Using semi-structured questionnaires, interviews can be guided to provide participants the flexibility to elaborate on their experiences while ensuring that key points are captured. Questionnaires for this study addressed several areas, including:

- General usage of online banking services
- Perceived benefits and convenience
- Experiences with and perceptions of online fraud
- Trust in the security measures implemented by banks

Considering the pandemic state of the world at the time of this study, a total of 112 potential participants were contacted, out of which 46 responses were received. After excluding incomplete responses, 40 complete interviews were used for data analysis. This sample provided a diverse cross-section of online banking users, including personal and business account holders, thereby offering a representative view of current online banking practices and challenges.

3.3. Data Analysis

The collected data were analyzed qualitatively, focusing on recurring themes and patterns that emerged from the interviews. The analysis involved coding responses to identify common issues such as trust deficits, concerns about data security, and personal experiences of fraud. Triangulation was employed to enhance the validity of the findings, combining insights from the interviews with secondary data from existing literature. This approach ensured that the study's conclusions were well-grounded in both empirical evidence and theoretical frameworks.

3.4. Ethical Considerations

Research projects are expected to be completed and carried out in an ethical manner. This implies researchers must ensure that research projects are conducted within the law and proper guidance is followed to meet ethical standard requirements. Some research projects require researchers gaining appropriate approval from ethics committee, demonstrating that the interests of participants and anonymity are put into consideration and protected, as was the case in this study.

4. Results

4.1. Overview of Collected Data

Interviews and questionnaires generate valuable insights in research, in this study, data collected captured the security practices and fraud experiences of online banking users. Out of the 112 individuals contacted, 46 agreed to participate, and 40 provided complete responses.

Table 1. Overview of Interview Data Gathered.

Classification of Responses	Percentage of Findings
1. Online banking users	40
2. Business Account	12
3. Savings Account	10
4. Current Account	18
5. Fraud victims	23 (57%)
6. Fraud with loss victims	15 (37%)
7. Incomplete responses	6

The data revealed the following key findings:

- **User Demographics:** The sample included both personal and business account holders with a range of experiences in online banking. A significant proportion of respondents had been banking with their institutions for over three years, indicating a well-established customer relationship.
- **Usage Patterns:** Younger users were found to be more comfortable and reliant on online banking services, whereas older users tended to maintain a preference for in-person banking. This divergence was particularly evident in responses related to the frequency of physical branch visits.
- **Fraud Experience:** Approximately 57% of the respondents reported having been victims of some form of online fraud. Among these, 37% experienced direct financial losses, underscoring the severe impact that fraudulent activities can have on customer finances.
- **Security Perceptions:** Despite the availability of multiple security measures, a significant number of respondents expressed concerns regarding data integrity and unauthorized access. The findings suggest that while users appreciate the convenience of online banking, they remain conscious of its security concerns.

4.2. Detailed Findings

4.2.1. Convenience and Efficiency

The interviews consistently highlighted the convenience that online banking offers. Respondents noted that the ability to conduct transactions from home or on-the-go significantly reduces the need for physical branch visits. This was particularly important during the pandemic, when social distancing measures further accentuated the value of remote banking. However, a subset of older customers reported continuing to visit bank branches due to concerns over online security.

4.2.2. Fraud Incidence and Impact

The data revealed that online fraud remains a critical issue for many users. Respondents described various forms of fraud, including phishing scams, unauthorized transactions, and malware infections.

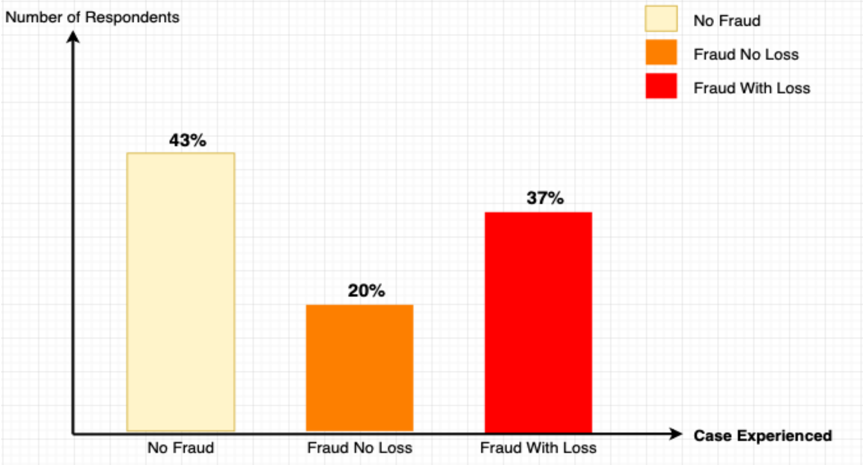

Figure 4. Classification of Fraud Cases.

Some interviewees recounted experiences where fraudulent activities not only resulted in financial losses but also eroded their trust in their banking institutions. The psychological impact of fraud was also significant, with some customers expressing long-lasting concerns about the security of their personal information.

4.2.3. Trust and Customer Relationship

Trust emerged as a central theme in the interviews. While online banking is praised for its efficiency, the recurring incidence of fraud has created a trust [18] deficit between banks and their customers. The respondents indicated that even when banks offer guarantees such as refunding fraud losses, the breach of trust is difficult to fully repair. This underscores the need for banks to adopt more transparent and proactive security measures, as well as to invest in educating customers about safe online practices.

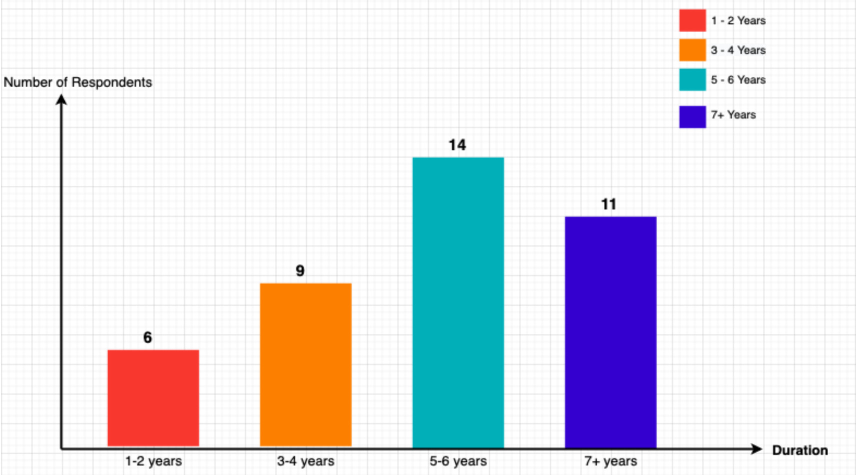

Figure 5. Longevity of banking relationship (Question 06).

4.2.4. Effectiveness of Current Security Measures

This study agrees that while many banks implement advanced security techniques such as one-time passwords, digital certificates, and biometric verification, these measures are not entirely foolproof []. Fraudsters continually adapt their tactics, finding new ways to bypass even sophisticated security systems. Respondents expressed a desire for more robust, multi-layered security approaches that can address both known and emerging threats.

5. Discussion

5.1. Interpreting the Findings

The results of the study provide a comprehensive picture of the current state of online banking security. The evolution of online banking has undeniably brought substantial benefits in terms of convenience and efficiency [19]. However, the same digital landscape that enables these benefits also creates opportunities for fraudsters. The high rate of fraud incidence reported by the respondents is a stark reminder that security remains a paramount concern for both banks and its customers.

The data indicate that while younger users are generally more comfortable with digital transactions, there remains a segment of the population—primarily older users—that is hesitant to fully embrace online banking due to security concerns. This generational divide suggests that banks must not only invest in technological solutions but also in targeted communication and awareness strategies to bolster customer confidence across all age groups.

5.2. Security Versus Convenience

An inherent tension in online banking remains the balance between security and convenience. On one hand, robust security measures such as multifactor authentication and encryption are essential for protecting customer data and preventing fraud. On the other hand, overly complex security protocols can hinder user experience and discourage customers from having a smooth customer journey within the system. The findings from this study suggest that while customers appreciate the convenience of online banking, they are also keenly aware of its vulnerabilities. Hence, banks must strike a delicate balance that ensures both usability and security without compromising one for the other.

5.3. Evolving Fraud Tactics and the Need for Adaptive Security

The study reinforces the notion that fraud tactics are continually evolving. Despite the implementation of numerous security measures, fraudsters remain persistent and innovative. This study reveals that many security breaches are not due to a single point of failure but rather a combination of factors including poor user practices, outdated security protocols, and sophisticated attack [20,21] methods. To address these challenges, financial institutions must adopt a dynamic security framework that continuously adapts to emerging threats and vulnerability trends [29,40]. This might include investing in artificial intelligence–driven monitoring systems that can detect unusual transaction patterns in real time, as well as developing more effective mechanisms for biometric authentication and device recognition.

5.4. Recommendations for Future Practice

Based on the findings, several recommendations can be made to enhance the security of online banking systems:

- **Enhanced Customer Awareness:** banks must implement comprehensive educational programs that inform customers about the risks associated with online banking and provide guidance on how to protect themselves. This includes awareness campaigns on phishing, safe password practices and the importance of updating their software.
- **Integrated Security Solutions:** Financial institutions are encouraged to adopt a multi-layered security approach that integrates various authentication and monitoring tools. Combining traditional methods (such as OTPs and digital certificates) with emerging technologies (like biometrics and AI-based fraud detection) [22,32] can create a more resilient security environment.
- **Regular Security Audits and Updates:** Given the rapid evolution of cyber threats, regular security audits are critical. Banks must routinely assess the effectiveness of their security measures and update them to counter emerging vulnerabilities. Engaging with external cybersecurity experts to conduct these audits can also provide an independent perspective on potential weaknesses.
- **Improved Communication and Transparency:** To rebuild and maintain trust, banks should enhance their communication strategies regarding security practices. Transparent reporting on security breaches, along with clear explanations of the steps being taken to mitigate risks, can help restore customer confidence.
- **Research and Collaboration:** Finally, there is a need for continued research and collaboration between financial institutions, cybersecurity experts, and academic researchers. Joint efforts can foster innovation in security technologies and create industry standards that are better equipped to handle the evolving landscape of online fraud.

These recommendations, drawn from this study and the existing literature, emphasizes the importance of a holistic approach to online banking security that addresses both technological and human factors.

6. Conclusions

The investigation into online banking security and its prevailing fraud factors reveals a complex landscape where technological advancements and cybersecurity challenges coexist. On one side, the evolution of online banking has revolutionized the financial sector by offering convenience, cost efficiency, and enhanced transactional capabilities. On the other, these benefits have been accompanied by a persistent risk of fraud, which has significant implications for both banks and their customers.

The qualitative data collected during this study provided insights into user experiences and perceptions. While many respondents appreciated the convenience of conducting transactions remotely, a significant portion expressed concerns about security breaches and the reliability of current fraud prevention measures. The findings underscore that fraud not only results in financial losses but also has a profound impact on customer trust and the overall reputation of banking institutions.

The study highlights that the current security measures, although comprehensive in many respects, are insufficient to address the dynamic and evolving nature of online fraud. As fraudsters continually refine their methods, banks must adopt adaptive, multi-layered security strategies that combine advanced technology with robust user education and transparent communication. The recommendations outlined in this article ranging from enhanced fraud awareness to the integration of AI-driven monitoring systems—offer a roadmap for strengthening online banking security in the face of emerging threats.

In conclusion, while online banking remains an indispensable service in the modern financial landscape, its full potential can only be realized if security concerns are addressed in a proactive and holistic manner. Future research should focus on developing innovative solutions that integrate technology, policy, and human factors to create a more secure and trustworthy digital banking environment. This investigation serves as a call to action for financial institutions, policymakers, and researchers to collaborate in fortifying the defenses of online banking systems against an ever-evolving fraud landscape.

References

1. Pilcher, J. (2012). *Infographic: The History of Internet Banking (1983 – 2012)*. Retrieved from: https://thefinancialbrand.com/25380/yodlee-history-of-internet-banking/
2. Sarreal, R., Segal, B., Woods, L. (2019). *History of Online Banking: How Internet Banking went Mainstream.* Retrieved from: https://www.gobankingrates.com/banking/banks/history-online-banking/
3. Sarreal, R. (2017). *History of Online Banking: How Internet Banking went Mainstream*. Retrieved from: http://www.neville-associates.com/blog/history-online-banking-how-internet-banking-went-mainstream
4. Woods, L. (2014). *How Online Banking Evolved into a Mainstream Financial Tool*. Retrieved from: https://www.fool.com/investing/general/2014/11/09/how-online-banking-evolved-into-a-mainstream-finan.aspx
5. Kesharwani, A., & Bisht, S. S. (2012). The Impact of Trust and Perceived Risk on Internet Banking Adoption in India: An Extension of Technology Acceptance Model. In *International Journal of Bank Marketing* (Vol. 30 Iss: 4, pp 303 – 322). Retrieved from: https://www.researchgate.net/publication/243459780_The_impact_of_trust_and_perceived_risk_on_Internet_banking_adoption_in_India doi: 10.1108/02652321211236923
6. Singh, S. (2013). *Service Quality Gap Issues in Online Banking*. In *International Conference on Management and Information Systems* (pp. 616). Retrieved from https://www.researchgate.net/publication/308746656_Service_Quality_Gap_Issues_in_Online_Banking
7. Emefiele, C., Obim, E. N., & Nkamare, S. E. (2018). Impact of Electronic Banking on Detection of Fraud in Nigerian Banking. In *International Journal of Research in Finance and Marketing (IJRFM)*, Vol. 8 Issue 9. Retrieved from https://www.academia.edu/37850988/IMPACT_OF_ELECTRONIC_BANKING_ON_DETECTION_OF_FRAUD
8. Nagar, N., & Suman, U. (2017). Prevention, Detection, and Recovery of CSRF Attack in online banking system. in aljawarneh, s. a. (ed.), Online Banking Security Measures and Data Protection (pp. 172-188). Retrieved from https://www-igi-global-com.ezproxy.napier.ac.uk/gateway/chapter/full-text-html/166871 doi:10.4018/978-1-5225-0864-9.ch0116
9. Kassim, N. M., & Ramayah, T. (2013). Security Policy Issues in Internet Banking in Malaysia. In Management Association, I. (Ed.), IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications

(pp. 1274-1293). Retrieved from https://www-igi-global-com.ezproxy.napier.ac.uk/gateway/chapter/full-text-html/75078 doi: http://doi:10.4018/978-1-4666-2919-6.ch057

10. Khande, R., & Patil, Y. (2014). Online Banking in India: Attacks and Preventive Measures to Minimize Risk. In *International Conference on Information Communication and Embedded Systems (ICICES2014),* Chennai, 2014 (pp. 1-5). Retrieved from https://ieeexplore-ieee-org.ezproxy.napier.ac.uk/document/7033940 doi: 10.1109/ICICES.2014.7033940
11. Moghimi, M., & Varjani, A. Y. (2016). New Rule-Based Phishing Detection Method. In *Expert Systems with Applications*, Vol. 53 (pp. 231-242). Retrieved from: https://www.sciencedirect.com/science/article/pii/S0957417416000385#bbib0013 doi: https://doi.org/10.1016/j.eswa.2016.01.028
12. Drolet, M. (2019). Smishing and vishing: How These Cyber Attacks Work and How to Prevent Them. In *Infosec At Your Service*. Retrieved from: https://www.csoonline.com/article/3411439/smishing-and-vishing-how-these-cyber-attacks-work-and-how-to-prevent-them.html
13. Khrais, L. T. (2015). *Highlighting the Vulnerabilities of Online Banking System*. In *Journal of Internet Banking and Commerce*. Retrieved from: http://www.icommercecentral.com/open-access/highlighting-the-vulnerabilities-of-online-banking-system.php?aid=61518
14. Nilsson, M., Adams, A., & Herd, S. (2005). *Building Security and Trust in Online Banking*. In *CHI '05 Extended Abstracts on Human Factors in Computing Systems* (pp. 1701–1704). Retrieved from https://dl.acm.org/doi/epdf/10.1145/1056808.1057001 doi: 10.1145/1056808.1057001
15. Leavitt, N. (2011). Internet Security Under Attack: The Undermining of Digital Certificates. In *Computer* Vol. 44 (12), pp. 17-20. Retrieved from https://ieeexplore.ieee.org/abstract/document/6096548 doi: 10.1109/MC.2011.367
16. Yan, J., & Ahmad, A. S. E. (2008). Usability of CAPTCHAs or Usability Issues in CAPTCHA Design. In *Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS '08)* pp. 44-52. doi: 10.1145/1408664.1408671
17. Reurink, A. (2016). Financial Fraud: A Literature Review. In *MPIFG Discussion Paper 16/5*. Retrieved from https://www.mpifg.de/pu/mpifg_dp/dp16-5.pdf
18. Aboobucker, I., & Bao, Y. (2018). *What Obstruct Customer Acceptance of Internet Banking? Security and Privacy, Risk, Trust and Website Usability and the Role of Moderators*. In *Journal of High Technology Management Research*. Vol. 29 (1) pp. 109–123. doi: https://doi.org/10.1016/j.hitech.2018.04.010
19. Aljawarneh, S. A. (2017). Emerging Challenges, Security Issues, and Technologies in Online Banking Systems. In Aljawarneh, S. A. (Eds.), *Online Banking Security Measures and Data Protection* (pp. 90-112). Retrieved from https://www-igi-global-com.ezproxy.napier.ac.uk/gateway/chapter/166866 doi: 10.4018/978-1-5225-0864-9.ch006
20. Bond, M., Choudary, O., Murdoch, S. J., Skorobogatov, S., & Anderson, R. (2014). Chip and Skim: Cloning EMV Cards with the Pre-play Attack. In *2014 IEEE Symposium on Security and Privacy*, San Jose, CA, 2014, pp. 49-64. Retrieved from https://ieeexplore.ieee.org/abstract/document/6956556 doi: 10.1109/SP.2014.11.
21. Buchanan, T., & Whitty, M. T. (2014). The Online Dating Romance Scam: Causes and Consequences of Victimhood. In *Psychology, Crime & Law* Vol. 20 (3), pp. 261-283. Retrieved from https://www.tandfonline.com/doi/full/10.1080/1068316X.2013.772180?src=recsys doi: 10.1080/1068316X.2013.772180
22. Chen, J., & Guo, C. (2006). *Online Detection and Prevention of Phishing Attacks*. In *First International Conference on Communication and Networking* in China, Beijing. pp 1-7. Doi: 10.1109/CHINACOM.2006.344718
23. Coffee, J. C. (2015). *What Went Wrong? An Initial Inquiry into the Causes of the 2008 Financial Crisis*. In *Journal of Corporate Law Studies*. Vol. 9 (1) pp. 1-22. Doi: https://doi.org/10.1080/14735970.2009.11421533
24. Hoffman, A. O. I., Birnbrich. C. (2012). *The Impact of Fraud Prevention on Bank-Customer Relationships – An Empirical Investigation in Retail Banking*. In *International Journal of Bank Marketing*. Vol. 30 (5), pp. 390-407 doi: http://arvidhoffmann.nl/Hoffmann_Birnbrich_2012.pdf
25. Lin, W., Wang, Y., & Hung, Y. (2020). *Analysing the Factors Influencing the Adoption of Internet Banking: Applying DEMATEL-ANP-SEM Approach*. Doi: https://doi.org/10.1371/journal.pone.0227852

26. Mermod, A.Y. (2012). Fraud in Modern Banking: Highlights on Online Internet Banking Fraud. In Çaliyurt, K., & Idowu, S. (eds) *Emerging Fraud* (pp. 149-161). doi: 10.1007/978-3-642-20826-3_10
27. Ohman, A. (2005). *Qualitative Methodology for Rehabilitation Research*. Retrieved from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.451.9315&rep=rep1&type=pdf
28. Özkul, F. U., & Pamukçu, A. (2012). Fraud Detection and Forensic Accounting. In Çaliyurt, K., & Idowu, S. (eds) *Emerging Fraud* (pp. 19-41). Retrieved from https://link.springer.com/chapter/10.1007/978-3-642-20826-3_2 doi: 10.1007/978-3-642-20826-3_2
29. Peotta, L., Holtz, M. D., David, B. M., Deus, F. G., & Timóteo, D. S. R. (2018). A Formal Classification of Internet Banking Attacks and Vulnerabilities. In *International Journal of Computer Vision and Machine Learning (IJCVML),* Vol. 1 (3), pp. 186-197. Retrieved from https://www.academia.edu/39010214/A_FORMAL_CLASSIFICATION_OF_INTERNET_BANKING_ATTACKS_AND_VULNERABILITIES doi: 18.5121/ijcst.2018.3113
30. Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit Card Fraud Detection Using AdaBoost and Majority Voting. In *IEEE Access*, vol. 6, pp. 14277-14284. doi: 10.1109/ACCESS.2018.2806420
31. Saunders, K. M., & Zucker, B. (2010). Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. In International Review of Law, Computers & Technology (pp. 183-192). doi: https://doi.org/10.1080/13600869955134
32. Vanhoeyveld, J., Martens, D., & Peeters, B. (2020). *Value-added Tax Fraud Detection with Scalable Anomaly Detection Techniques*. In *Applied Soft Computing*. doi: https://doi.org/10.1016/j.asoc.2019.105895
33. Yan, J., & Ahmad, A. S. E. (2008). Usability of CAPTCHAs or Usability Issues in CAPTCHA Design. In *Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS '08)* pp. 44-52. doi: 10.1145/1408664.1408671
34. Adams, J. (2009). FRAUD: *A Text Alert for Community Banks: Small Banks Bear the Brunt of 'smishing' Attacks*. In *Bank Technology News*, *22* (9), 1. Retrieved from https://search-proquest-com.ezproxy.napier.ac.uk/docview/208165966?rfr_id=info%3Axri%2Fsid%3Aprimo
35. Bergman, M. M. (2008). *Advances in Mixed Methods Research*. Retrieved from: https://books.google.co.uk/books?hl=en&lr=&id=hWT6mWbnGC0C&oi=fnd&pg=PR5&dq=mixed+methods+research&ots=Tnzbq77RrB&sig=c9ahUPlGhZGvqocQcJ4Ye4jLlz0&redir_esc=y#v=onepage&q=mixed%20methods%20research&f=false
36. Cavaglieri, C. (2020). Best Banks for Dealing with Bank Fraud. In *How Does Your Bank Handle Fraud? Exclusive Data by Which? Money reveals the best and Worst Firms for Handling Fraud Complaints*. Retrieved from https://www.which.co.uk/money/banking/banking-security-and-new-ways-to-pay/online-banking-security/best-banks-for-dealing-with-bank-fraud-a8qp45d23x3l
37. Creswell, J. W. (2015). *A Concise Introduction to Mixed Methods Research*. Retrieved from: https://books.google.co.uk/books?hl=en&lr=&id=51UXBAAAQBAJ&oi=fnd&pg=PR1&dq=mixed+methods+research&ots=69LrS8StIw&sig=3aiOqlIJXKk0ovJWda2szOX6nj0&redir_esc=y#v=onepage&q=mixed%20methods%20research&f=false
38. Dolma, K. (2020). A Study on the Impact of Online Banking Fraud: Customer's Perspective. Retrieved from https://www.academia.edu/27182517/_A_Study_on_The_Impact_of_Online_Banking_Frauds_Customers
39. Drolet, M. (2019). Smishing and vishing: How These Cyber Attacks Work and How to Prevent Them. In *Infosec At Your Service*. Retrieved from: https://www.csoonline.com/article/3411439/smishing-and-vishing-how-these-cyber-attacks-work-and-how-to-prevent-them.html
40. FNB. (2017). FNB Warns Against New Online Banking Scam. In *Financial Services Monitor Worldwide*. Retrieved from https://search-proquest-com.ezproxy.napier.ac.uk/docview/1975913855/fulltext/27413BD0FA334968PQ/1?accountid=16607

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.