Internet Banking: Frauds and Prevention

Dr. Manish N. Moharil
Department of Commerce & Management
Mungasaji Maharaj Mahavidyalaya, Darwha
Email : manishmoharil@gmail.com

Abstract

Internet banking gives customers a lot of satisfaction in terms of getting a better service quality; it also gives banks a competitive advantage over the other players in the sector. However, the security of Internet banking has received attention due to the fraudulent behaviour of fraudsters; the absence of adequate Internet banking security has kept many people away from the service till today. In this paper, a review of the security challenges associated with Internet banking has been presented. Equally, the challenges and characteristics of Internet banking fraud have been mirrored. This paper also reviewed different types of fraud as well as some preventive measures in place to secure Internet banking services. The different techniques and models used for Internet banking security were ranked in this study based on an expert opinion. This paper is prepared into two parts; the first part introduced the topic Internet banking of the paper while the second part presented that type of common Internet banking Frauds and how to prevent Internet banking frauds. The literature review was presented in the third part of the paper.

Key words: Internet banking, Internet banking frauds, Virtual banking, prevention banking frauds

Introduction

Online banking, also known as **Internet banking**, virtual banking, web banking or home banking, is a system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website or mobile app. Since the early 2000s this has become the most common way that customers access their bank accounts. The online banking system will typically connect to or be part of the core banking system operated by a bank to provide customers access to banking services in addition to or in place of historic branch banking. Online banking significantly reduces the banks' operating cost by reducing reliance on a physical branch network and offers convenience to some customers by lessening the need to visit a branch bank as well as being able to perform banking transactions even when branches are closed, for example outside the conventional banking hours or on weekends and holidays.

Internet banking provides personal and corporate banking services offering features such as making electronic payments, viewing account balances, obtaining statements, checking recent transactions and transferring money between accounts. Some banks operate as a "direct bank" or "neobank" that operate entirely via the internet or internet and telephone without having any physical branches relying completely on their online banking facilities.

Common Internet Banking Frauds

Here are the top 10 most common types of online frauds in banking services

1) Identity Theft

Identity theft is one of the most common forms of Internet banking fraud. Here, cybercriminals steal personal information such as usernames, passwords and other confidential data to impersonate the victim.

2) Malicious Software

Malicious software, also commonly known as malware, is software that is designed to infiltrate or damage computer systems. Malware can be used by fraudsters to gain unauthorised access to the net banking credentials of a person.

3) Employee Initiated Fraud

Employee-initiated fraud is a type of net banking fraud where employees of a financial institution misuse their access to sensitive information and banking systems for personal gain. They can use this information to conduct embezzlement, insider trading and other forms of fraud.

4) Fraudulent Email (Phishing)

Phishing is a common tactic used by fraudsters to trick individuals into sharing their personal information. This is usually done through fraudulent emails that appear to be from legitimate financial institutions. They ask for confidential information such as usernames, passwords and account numbers.

5) e-Transfer Interception Fraud

e-Transfer interception fraud occurs when cybercriminals intercept and redirect legitimate e-transfers intended for a victim's bank account to their own account. They may use various tactics, such as social engineering, malware or hacking.

6) Vishing

Vishing is another common online banking fraud where cybercriminals use voice calls to deceive victims into sharing their personal information. The fraudster usually represents themselves as an executive from a legitimate financial institution and asks the victim to provide their confidential information over the phone.

7) Opening an Account in the Victim's Name (Application Fraud)

Application fraud is a type of Internet banking fraud where cybercriminals open bank accounts in the victim's name without their consent. They may use stolen identities and other fraudulent documents to open these accounts. These bank accounts are then used for illegal activities such as money laundering or transferring stolen funds.

8) SIM Swap

SIM swap is a type of e-banking fraud where cybercriminals trick a victim's mobile service provider into transferring the victim's mobile phone number to a SIM card in their possession. Once they have control of the victim's phone number, they can use it to bypass two-factor authentication measures. Through this, they gain unauthorised access to the victim's online banking accounts.

9) Automatic Transfer System (ATS)

ATS is a serious type of online banking scam that increases financial losses over time if not rapidly solved. Here, fraudsters set up automatic transfers to their own accounts without the victim's knowledge or consent. These automatic transfers may occur at regular intervals automatically.

10) Fake Apps

Fake applications are malicious application copies that are designed such that they mimic legitimate banking apps. These fake applications deceive users into providing their personal information. They are often downloaded from unofficial app stores or websites. In most cases, they contain malware or other malicious software.

How to Prevent Internet Banking Frauds?

Online frauds in banking are getting more and more common. Being aware and careful is necessary to avoid internet banking fraud. As a safety measure, one should take the following precautions:

- **Use Strong Passwords:** One should create strong and unique passwords for their online banking accounts. They should avoid using easily guessable passwords like birthdates or name-surname combinations and update their passwords regularly.
- **Enable Two-Factor Authentication (2FA):** Two-factor authentication adds an extra layer of security to online banking accounts. It typically involves using something one knows (such as a password) and something one has (such as a fingerprint or an OTP sent to their mobile) to verify their identity.
- **Be Cautious with Emails and Links:** One should be cautious with emails, especially those asking for personal information or urging one to click on suspicious links. One should always verify the authenticity of emails and links before providing any confidential information and avoid clicking on links or downloading attachments from unknown sources.
- **Keep Software Updated:** One should keep their computer, mobile device and all software, including antivirus and anti-malware programs, up-to-date with the latest security patches. This helps protect against known vulnerabilities that cybercriminals may exploit.
- **Be Wary of Public WiFi:** One should avoid conducting online banking transactions on public WiFi networks, as these networks may not be secure and can be easily intercepted by hackers.
- **Check Bank Statements Regularly:** One should review their bank statements and transaction history regularly. One should report the bank immediately in case of any suspicious activity.
- **Be Sceptical of Unsolicited Calls:** One should be sceptical of unsolicited phone calls or messages asking for personal or banking information. Legitimate financial institutions will never ask for confidential information over the phone or through messages.

References:

1. THE PRAGMATIC REVIEW ON INTERNET BANKING AND ASSOCIATED SERVICES IN INDIA Link-https://www.ijccr.com/July2014/20.pdf
2. Rishi, Om Prakash (2017). *Maximizing Business Performance and Efficiency Through Intelligent Systems*. IGI Global. p. 169. ISBN 9781522522348.
3. https://www.bankofbaroda.in/banking-mantra/digital/articles/common-internet-banking-frauds-and-prevention-tips