IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, September 2024

A Review on Securing Indian Online Banking: Threats and Countermeasures

Adarsh S Naik, Aishwarya, Akash Goud, Amulya NM

Department of Computer Science & Engineering (IoT & Cybersecurity including Blockchain Technology)
Alvas Institute of Engineering and Technology, Mijar, Karnataka, India
naikadarsh303@gmail.com, aishwaryaanchan2810@gmail.com
akashgoudkalalakash@gmail.com, amulyanmgowda@gmail.com

Abstract*: The paper mainly discusses the various online banking vulnerabilities and focuses on the current security models' weaknesses, leading to the detection failures and prohibition of genuine passageways for illegal actions online. Areas of vulnerability are many, and so the paper considers a number of online banking attacks, as well as suggesting measures that can be put in place in order to reduce the vulnerabilities and fraud activities related to unauthorized transactions to improve an overall internet banking system.*

Keywords: online banking, security analysis, fraud prevention, user identification, preventive measures.

I. INTRODUCTION

Another one of the extremely famous and rather open ways of making money on the banks and clients all over the globe in 2012 when the incidents increased was the attacks on the online banking systems. Also, few of the banks' activities were very timely ad hoc. In particular, despite the fact that the banks have been able to incorporate efficient technological tools to their operations, informational burglaries have progressively risen. Recently, there is a threat from internal fraudsters and external fraudsters and thus the risk of online banking fraud.

Payments of funds, payments of bills, checks of balance, e-mortgages and purchase are all done with the help of the online banking-a function that forms the online banking's core. Clients attach a browser that uses the software installed and managed on the banks' WWS to execute operations on their Internet bank accounts. A new banking delivery channels such as; Automated Teller Machines (ATMs), Point of Sale (POS);Internet banking, mobile banking contributed to the ''Anytime, Anywhere, Anyhow'' banking due to a shift in the branch model. The most popular facility in the world of banking, the internet banking empowers the users to carry out operations banking from the comfort of their homes anytime of the day. It is in this trend that banks have actively followed, in increasing costs saved and higher profitability through online banking.

The dynamics presented by Internet banking, though, contain a spectrum of security risks: from the brute-force ones through distributed and to the latest social phishing. Paradoxically, although banks relentlessly improve security measures for online banking, the evolving dynamics of cyberspace crime indirectly call for even more investment in this area. The banks have the really challenging task of balancing the need of upgradation of security against the costs associated with such upgrades. Consequently, there is a great onus on the individual users of online banking security, which might tend to value convenience over more set, complex security procedures at logins. One of the key areas to work on would be personal computers belonging to customers, which might easily turn out to be the security deficiency in any online banking transaction. Ensuring this means finding the right balance between security measures and user-friendly interfaces in safeguarding online banking transaction integrity.

ATTACKS TARGETING ONLINE BANKING

Online banking is the particular target of several types of electronic fraud. Below is a description of some of the more well-liked varieties:

DOI: 10.48175/IJARSCT-19505

1. Phishing Attacks

Phishing orchestrates a deceptive symphony, where carefully constructed emails flood thousands of Internet addresses, apparently coming from reputable banks. Cloaked in legitimacy, the emails cajole targets into updating or verifying a slew of personal and financial information - anything from birthdates and login credentials to account details, credit card numbers, and PINs. Then, via a link embedded in the email, it whisks them off to an artfully constructed spoof site that perfectly emulates the interface of a bank. In that mirage, there are opportunities for malignant actors to grab sensitive information, e.g. passkeys, that users input unwittingly. Moreover, the danger is not fastened with deceit only because in the run of time, those links are able to transfer some malware into your computer. This insidious program secretly logs your surfing behavior, all the information is sent to the fraudster, and it is routed to him. In some cases, this threat disguises itself in the form of something that appears real, such as pop-up windows that are well-designed to look like legitimate banking websites.

Although the real window displays the real address of the website being accessed, all data myA Next Generation Enterprise Electronic Health thoroughly type information into the pop-up windows surreptitiously goes to unauthorized data recipients. A related technique, "Vishing," is more direct: it involves robocalls. In such an instance, a caller would impersonate as a bank officer and, with his expertise, seek to recover and confirm secret account details and carry out the scam. In such a deceitful transaction, caution is paramount to prevent the depletion of bank accounts and credit cards.

II. MALWARE

Malware, a colloquialism for "malicious software," is a clandestine threat devised to compromise a computer system without the owner's consent. The term also describes an entire category of intrusive programs, which include Viruses, Worms, Trojan horses, and Spyware; these are responsible for financial crimes online.

2.1 Spyware: These are covert apps that track a user's online activity and typically come attached to free software. They reside on a user's PC. In the worst case scenario, spyware might record keystrokes and then monitor every action made on a computer.

2.2 Trojan Horse / Trojan: This is a form of cunning software structure that may be exploited by hackers to gain access to computer systems. It typically contains an unwanted program, like a virus or spyware.

2.3 Virus: A virus is a program designed to spread to other computer programs. This might potentially destroy information and memory on a computer, as well as severely impair its performance. Email as well as file-sharing software have made the distribution of viruses easy.

2.4 Virus Hoax Email:

A number of email virus warnings are hoaxes that are specifically intended to waste the time of business and other organizations. There are some genuine threats, and such warnings should always be checked on antivirus sites before acting or passing them on.

2.5 Worm:

Malicious program that replicates itself. It may take up so much storage space on your computer drive or network that no more files can be saved. Worms may also 'hijack' your computer resources and carry out a malicious attack on web servers with the aim of slowing them down or closing them down to prevent use of the Internet.

2.6 Stealing Account Info: This can be accomplished by keystroke capturing of login information and surveillance of other authentication data. This will compromise user identity.

2.7 Substitution of Website: The malware creates a fake website of out of an official site, substituting the legitimate site of a bank. What this will do is that it will intercept user information by adding fields to the fake page—a "man-in-the middle attack.".

2.8 Hacking of Account:

Malware could hijack a browser and conduct fund transfers without the knowledge of the user. The software first creates a hidden window of the browser to access the bank, then reads the balances from the accounts, and finally, manages the transfer of funds to the attacker's account without the user's knowledge.

Planting of Malicious Links into popular sites like search engines, entertainment, social 18+ advertisements, etc. The frequent targets of most hackers are the entertainment sites, especially video content like YouTube, and search engines. This thus serves to sensitize the user to be more careful.

Topping in the list of the distribution of malicious links are the social networks and advertising websites, adult content websites, etc. One must be vigilant in order to protect online interactions, as well as removable media devices, against such advanced threats.

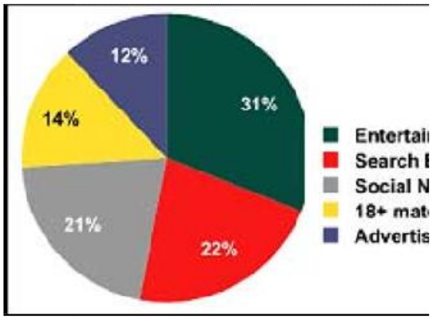


Fig 1: websites that experience fraudulent link redirects the most frequently 2011 percentage of redirection (Source: Kaspersky Security Bulletin Statistics).

a. Pharming

Pharming assaults are sneaky, entailing the covert installation of harmful software onto your system. Phamaling does not rely on user-initiated actions such as opening attachments and emails, unlike phishing. This indicates that people inadvertently browse fraudulent websites and divulge personal information that jeopardises their financial identity. **b. Advance Fee**, often known as "419 Fraud," is a scam in which several recipients are deluged with unsolicited letters or emails promising enormous quantities of money in US dollars to those who help transfer larger amounts of money. In order to access the money, victims must pay fees, taxes, or bribes. Any funds that are purportedly given to pay these fictitious costs end up being lost forever.

c. Identity Theft:

Identity theft is a crime whereby fraudsters obtain vital information, like date of birth or banking details, to impersonate another individual. Stolen information is utilized in the crimes of applying for credit, purchasing a number of items, or even accessing the bank accounts of the respective individual without their knowledge.

d. Keystroke Capturing/Logging:

Every keystroke one makes on a computer can be caught and recorded, whether by hardwiring devices or through very quiet software. Keystroke logging is one of the most common methods for collecting personal data from passwords to other personal information. This definitely requires caution, especially on shared computers, with updated antivirus software and firewalls in order to allow early warning and prevention.

e. Lottery Fraud:

Lots of people are becoming victims by false claims that they have won multimillion-dollar lottery prizes. Victims respond to letters or email, and afterwards, they are told to provide the bank account details so that money can be transferred, but for processing and handling, a certain fee needs to be paid in advance. The fee is then used for further fraudulent activities, as is the personal information.

Other E-Banking Security Risks

- **Session Hijacking:** Cookies deposited by banking websites may be used in hijacking an active session.
- **Cookie Tampering:** Information within cookies is altered to conduct an attack on websites.
- **Form Tampering:** A hidden or read-only field in an HTML form is tampered with and altered with unauthorized alterations.
- **Outbound Data Theft:** Data from a website is intercepted, such as data from installed software, to be utilized in executing attacks.
- **Application Denial of Service:** Exploiting the entry of rogue information in input fields to disrupt web applications.
- **Cross-Site Scripting:** The injection of scripts into one website, but the operation takes place on another site different from where it originated.
- **Site Cloaking:** Deceiving search engines into recognizing one website as another.

I. Statistics of Cyber Crime:

- In 2010, more than 10,000 instances were recorded, according to the Ministry of Communications and Information Technology's Computer Emergency Response Team-India.
- The majority of these reported occurrences involve malware dissemination, phishing, malicious code, compromised websites, and network scanning.
- The various initiatives taken to minimize defacements; 14,348 incidents monitored, which affected 9,772 \".in\" domain websites.
- CERT-In continues to be at the core of incident prevention, response services, and security quality management, truly reflective of continuing challenging issues in securing India's cyberspace.

III. ACTIONS BANKS CAN TAKE TO GUARD AGAINST ONLINE BANKING CRIMES

Preventive Steps Banks Can Take to Protect Against Online Banking Crimes

With increased threats of cybercrime and a heightened sense of institutional responsibility, banks must take an upfront approach. Literature reviewed substantially supports that it is the management, rather than the IT Department, that should initiate strong protective measures. Informed that it forms one of the primary lines of defense, the following are some of the most important strategies for strengthening bank defenses against crimes related to online banking:

Comprehensive Training of Employees:

Establish training programs at regular intervals for all employees. The main aspects of the training would be on cybersecurity, vigilance, and awareness.

Establish a culture of security awareness where employees are trained to become more cautious of threats and the need to respect the set security protocols.

Robust Access Controls:

Run a tight access control and permission system that permits only authorized personnel to have access to sensitive information.

Employees' access privileges should be reviewed and updated regularly in accordance with their role and responsibility within the organization.

Improved Authentication Mechanisms:

Implement multi-factor authentication for customers and staff, adding another layer of security besides conventional usernames and passwords. Adopt at the same time biometric authentication and enhanced token systems to improve methodologies of identity verification.

Continuous Monitoring and Analysis

Implement advanced monitoring tools that allow for constant observation of network activities and transactions to identify unusual patterns or behavior that might indicate the presence of an intruder.

Conduct frequent security audits and risk assessments to detect vulnerabilities before they are exploited, and implement measures to mitigate potential risks.

Encryption of Sensitive Data

Use robust encryption protocols for data in transit and at rest for sensitive customer information, making them unintelligible to unauthorized entities.

Mandate the use and necessity of end-to-end encryption to ensure that information is protected while in motion, at rest, or in use.

Collaboration with Law Enforcement:

Foster strong relationships between law enforcement agencies to promote the sharing of information and coordination in reacting to cyber threats. Establish a clear communication channel for incident reporting and solving issues quickly.

Incident Response Plan:

Develop a comprehensive incident response plan detailing procedures to be followed during a security breach clearly. Conduct regular drills and simulations to ensure that the response plan is effective and areas of improvement.

Customer Education Initiatives:

Organize customer education campaigns about online banking risks and educate your customers on how to bank safely. Offer security tips and best practices for account safety.

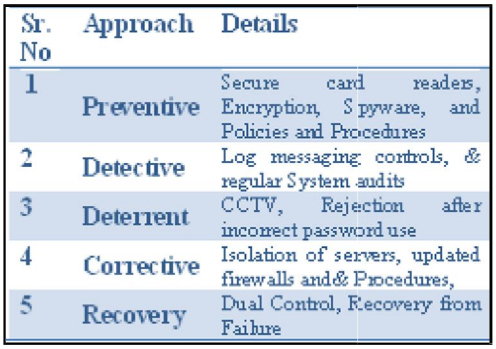
Integrated Artificial Intelligence (AI) and Machine Learning (ML):

Use AI and ML technologies to analyze terabytes of data for anomalies and predict security threats at the early stages before flaring up. Introduce AI-driven fraud detection systems that can support real-time monitoring and real-time response capabilities.

Regulatory Compliance Adherence:

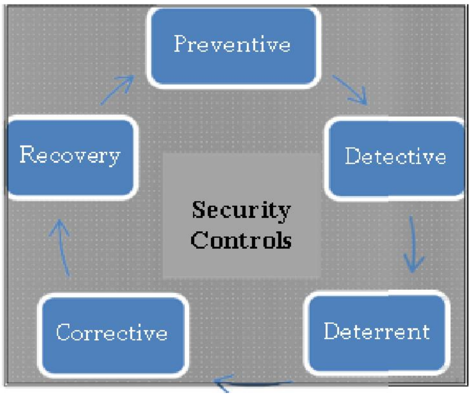
Stay up to date with the evolving regulatory environment and ensure rigorous adherence to compliance norms in the financial sector. Coordinate various regulators in benchmarking security practices with the best practices in the industry.

This holistic and proactive approach will significantly harden banks against the risks and thus help in staying at least one step ahead in this ongoing struggle against cyber-crimes related to online banking. Management commitment and its active involvement in building a strong framework for resilience in the security of the financial ecosystem is the very essence of the deliverable.



Sr. No	Approach	Details
1	Preventive	Secure card readers, Encryption, S pyware, and Policies and Procedures
2	Detective	Log messaging controls, & regular System audits
3	Deterrent	CCTV, Rejection after incorrect password use
4	Corrective	Isolation of servers, updated firewalls and& Procedures,
5	Recovery	Dual Control, Recovery from Failure

Information Security with Comprehensive Approach and Control.



A totally comprehensive approach with security controls.

IV. PRACTICE CODE

The following good practices will help in avoiding the common security problems related to online banking:

- The information security policy, method, and guidelines must to have been duly recorded and disseminated by the bank. The board of directors should provide their approval before informing the end users.
- Regularly reviewing information security policies and procedures.
- Modern password authentication systems should be upgraded to two-factor authentication.
- Employ scanning software or techniques to detect and safeguard against phishing attempts. Commercially accessible scanning technologies can be used to find and analyse security flaws in operating systems, databases, and networks.
- Adequately secure the network to prevent extraneous network traffic from reaching the systems.
- Establish sufficient backup infrastructure and contingency plans.
- Provide education and awareness campaigns to assist clients and staff in avoiding internet fraud.
- Information security controls protect the computer or the information system against cyber attack. The implementation and the monitoring are checked.

V. CONCLUSION

The proactive approach enables banks to safeguard against a host of cyber threats. Since any one measure cannot be considered completely safe, monitoring and risk assessment are required on a continuous basis. An overall policy review and a customized framework of control over information and technology assets in an effective and economical manner is what cybersecurity relies on.

A holistic defense must incorporate physical, technical, and organizational controls. The comprehensive approach would deal with the current but burgeoning threats and also be ready for changing landscapes. With proactive measures, assessment of the risks, and reinforcement of security controls in place, the banks will confidently stride through the dynamic landscape of cyber threats by securing information and ensuring operational integrity.

REFERENCES

[1]. Dandash, o. , srinivasan b. ,monash univ., clayton ,phu dung le “security analysis for internet banking models “,volume: 3 ,page(s): 1141 - 1146 , software engineering, artificial intelligence, networking, and parallel/distributed computing, 2007. snpd 2007. eighth acis international conference

[2]. Laerte Peotta, Marcelo D. Holtz, Bernardo M. David, Flavio G. Deus, Rafael Timóteo De Sousa Jr. “A Formal Classification Of Internet Banking Attacks And Vulnerabilities”, International Journal Of Computer Science & Information Technology (Ijcsit), Vol 3, No 1, Feb 201

[3]. Banking Securely Online, Produced 2006 by US-CERT, a government organization. Updated 2008.

DOI: 10.48175/IJARSCT-19505

[4]. CAVUSOGLU, Hasan e Cavusoglu, Huseyin. Emerging Issues in Responsible Vulnerability Disclosure. Workshop on Information Technology and Systems (WITS 2004). Barcelona, Spain, 2004

[5]. Banking Securely Online, Produced 2006 by US-CERT, a government organization, 2008

[6]. ISO/IEC 27002 Code of practice for information security management. Rio de Janeiro: ABNT,2007.

[7]. WEEKS, Stephen. Understanding Trust Management Systems. IEEE Symposium on Security and Privacy. 2001

[8]. http://www.hsbc.com/1/2/online-security/main-types-attack

[9]. http://made4biz-security.com/IDentiWall/on- line_banking_security_threats.html

[10]. http://www.asianlaws.org/brochures/cyber-law-police-brochure.pdf

DOI: 10.48175/IJARSCT-19505