Online Banking in India: Attacks and Preventive Measures to Minimize Risk

Mrs. Rajeshree Khande
Associate Professor,
Sinhgad Institute of Management,
Off Sinhgad Road, Vadgaon, Pune-41

Dr. Yashwant Patil,
Associate Professor,
Vaikunth Mehta National Institute of Cooperative Management, Ganshkhind, Pune
yspatil@hotmail.com

Abstract--This paper presents Online banking attacks, security analysis of Internet banking. Several modern models are evolving and being applied to many banking systems for preventing and detecting online banking fraud s. However, they have no effective detection mechanism to identify valid users and trace their unlawful activities. Also they are not secure enough to prevent fraudulent users from performing fraudulent transactions over the Internet. This paper discusses the various types of online banking attacks and preventive measure to minimize the risk and to deal with these attacks.

Keyword: Online Banking, Internet Banking, security

I. INTRODUCTION

In 2012, attacks on online banking systems will be one of the most widespread methods of stealing money from bank and from users account. The number of crimes committed in this area is rising rapidly all over the world in spite of all the technical measures taken by banks.

Online banking fraud can be performed internally by staff or externally by fraudulent users or suppliers. Online banking is the delivery channel to conduct banking activity, for example, transferring funds, paying bills, viewing checking and savings account balances, paying mortgages, and purchasing. An Internet banking customer accesses his or her accounts from a browser - software that runs Internet banking programs resident on the bank's World Wide Web server. Any service can be selected by the customer. The traditional branch model of bank is now giving place to an alternative delivery channels with ATM network, Point of sale (POS), Internet banking and mobile banking. Once the branch offices of bank are interconnected through network or satellite links, there would be no physical identity for any branch. It would a borderless entity permitting anytime, anywhere and anyhow banking. Since Online Banking has become increasingly popular globally, because it is so easy and convenient for Internet users to manage their bank accounts from anywhere of the world at any time. Banks have encouraged for this trend for years, since Online Banking also saves lots of resources of the banks, increase profitability and customer volume. The banks had to set up the required infrastructure and need an investment for ATMs and branches interconnectivity, staff training, and other operations costs. The Internet enhanced the user experience of banking activities dramatically. However, since the Internet is not originally designed for Online Banking, Online Banking now is facing a wide range of security risks for both the banks and the Online Banking users such as brute-force attacks, distributed attacks, and social phishing. The banks have to increase their Online Banking security system constantly, which means the banks have to keep investing on the security systems all the time.

Compared with the possibility of the lost from the potential risks, the banks may not want to update their current security systems, because the cost of upgrading security is too expensive. Then this will leave the lots of security responsibilities to the Online Banking users. However, the customers' PCs actually are always the weakest link for the Online Banking security. The customers would rather to choose convenience and easy-to-use than complex login procedure for Online Banking.

A. ATTACKS THAT TARGET ONLINE BANKING

Several types of electronic fraud specifically target online banking. Some of the more popular types are described below [3]:

1 Phishing attacks

Phishing involves an e-mail message being sent out to as many internet e-mail addresses that the hoaxer can obtain. Usually, these e-mails claim to come from a bank. The e-mail request the recipient to update or to verify their personal and financial information, including date of birth, login information, account details, credit card numbers, PIN numbers etc. The e-mail will contain a link that takes you to a spoof website that looks identical or similar to the bank website. The hoaxer can then capture personal data like passwords as you type it in. Clicking on a link may also download malware onto your computer which will record your future use of the internet and forward even more information to the fraudster. The fraudsters will then use this information to compromise bank accounts, credit cards etc.

In some cases, pop-up windows can appear in front of a copy of an authentic bank web site. The real web site address is displayed, however, any information you type into the pop-up will go to unauthorized users. In a similar scheme, called

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE

"Vishing," a person calls you and pretends to be a bank representative seeking to verify account information.

2 Malware:

Malware is also referring as "malicious software". This is designed to penetrate a computer system without your permission. The term covers a variety of intrusive software/programmes, including Viruses, Worms, Trojan horses and Spyware. Attacks involving malware are a factor in online financial crime. In fact, it is possible for this type of malicious software to perform the following operations [4]

2.1. Spyware: These are programs/files that may already reside on your computer and often arrive as hidden components of free programs. Spyware monitors web usage and in its more extreme forms can include keystroke logging and virtual snooping on all your computer activity.

2.2 Trojan horse / Trojan: It is software that carries an unwanted application like a virus or spyware - typically used by hackers to gain unauthorized access to computer systems.

2.3 Virus: A computer program designed to replicate by copying itself into other programs stored in a computer. It may be not dangerous but usually has a negative effect, such as slowing your computer down or corrupting its memory and files. Viruses are now mainly spread by email and by file sharing services.

2.4 Virus hoax e-mail: Many e-mail warnings about viruses are hoaxes, designed purely to disrupt businesses. Such warnings may be genuine, so don't take them lightly, but always check the story out by visiting an antivirus site before taking any action or forwarding them to friends and colleagues.

2.5 Worm: This is a malicious programme that replicates itself until it fills all of the storage space on a computer drive or network. Worms may use up computer time, space and speed when replicating, with a malicious intent to slow or bring down entire web servers and disrupt internet use.

2.6 Account information theft: Malware can capture the keystrokes for your login information. Malware can also monitor and capture other data you use to authenticate your identity for example "magic words" you chose.

2.7 Fake web site substitution: Malware can generate web pages that appear to be legitimate but are not. They replace your bank's legal web site with a page that can look identical, except that the web address will vary in some way. Such a "man-in the middle attack" site enables an attacker to catch user information. The attacker adds additional fields to the copy of the web page opened in your browser. When you submit the information, it is sent to both the bank and the malicious attacker without your knowledge.

2.8 Account Hijacking: Malware can hijack your browser and transfer funds without your knowledge. When you attempt to login at a bank web site, the software launches a hidden browser window on your computer, logs in to your bank, reads your account balance, and creates a secret fund transfer to the intruder-owned account.

In addition to online infections, detections of malicious programs directly on user computers or removable media are also of interest. Removable media devices include USB drives, camera memory cards, mobile phone memory cards, and external hard drives.

2.9 Where malicious links are planted?

As per the study carried out by Kaspersky Security the Statistics show that malicious link are planted in most prominent sites such as search engines, entertainment sites, Social networking sites, 18+ materials sites and Advertisements. In this study it was stated that a variety of entertainment websites with video content, such as YouTube is at the first position one (31%) and Search engines it at second position (22%) to plant the malicious links. As users sometimes click malicious links directly from major search engine sites like Google and yahoo. Just one per cent behind were social networks in third place. Users should be extra cautious when using sites like Facebook and other social networking sites. These are the social networks that malicious users specifically target and where they spread harmful content. Fourth and fifth places were taken by different advertising sites mostly banner ads and adult content websites. Fig 1.0 show the top websites with the most frequent redirects via malicious links Percentage of redirects, 2011. [11]

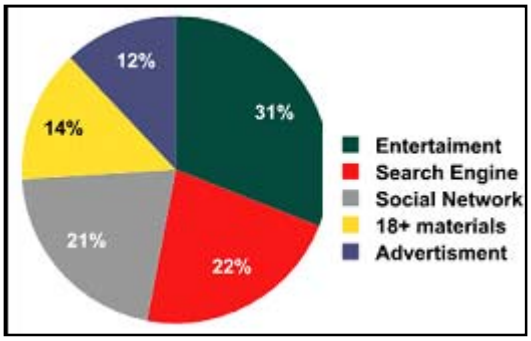

Fig 1: Websites with the most frequent redirects via malicious links Percentage of redirects, 2011 Source: Kaspersky Security Bulletin Statistics

a. **Pharming :**

Pharming attacks involve the installation of malicious code on your computer. With pharming attacks, you must open an email, or email attachment, to become vulnerable. You then visit a fake website and, without your knowledge, provide information that compromises your financial identity.

b. **Advance fee or '419 Fraud' :**

This involves unsolicited letters and e-mail messages offering the recipient a generous reward for helping to move large

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE

sums of money, usually in US dollars. These funds are said to be anything from corporate profits/accumulated bribes/unspent government funds to unclaimed money belonging to a deceased person. The transactions typically require the recipient of the letter or e-mail message to pay something like a fee/tax/bribe to complete the deal. This is the Advance fee. However, any fees paid will be lost.

c. Identity theft:

Identity theft is a crime in which a fraudster obtains key pieces of personal information, such as date of birth, bank details in order to impersonate someone else. The personal information discovered is then used illegally to apply for credit, purchase goods and services, or gain access to bank accounts.

d. Keystroke capturing/logging

Anything you type on a computer can be captured and stored. This can be done using a hardware device attached to your computer or by software running almost invisibly on the machine. Keystroke logging is often used by fraudsters to capture personal details including passwords. Some recent viruses are even capable of installing such software without the user's knowledge. The risk of encountering keystroke logging is greater on computers shared by a number of users, such as those in internet cafes. An up-to-date antivirus software programme and Firewall will help to remove the harmful software before it can be used.

e. Lottery fraud

This involves letters or e-mail messages which advise the recipient that they have won a prize in a lottery. To obtain the funds they are asked to respond to the letter or e-mail message. A request will then be made for the recipient to provide his/her bank account details to allow for funds to be transferred. The recipient may also be asked to pay a handling/processing fee. If paid, this fee will be lost. Also, any details given will probably be used to commit further fraud.

Apart from above attacks few more Security threats to on-line banking are listed below

- **Session Hijacking** – The session is hijacked by unauthorized use of the cookies deposited by the banking site.
- **Cookie tampering** – Information in the cookie is changed to allow an attack.
- **Form Tampering (read-only and hidden fields)** – Changes are made in hidden or read-only fields in the HTML form.
- **Outbound Data Theft** – Data sent from the web site are intercepted for use in attacks. For example, that may include data about the software installed at the site, version number etc.
- **Application Denial of Service** - Numerous types of attacks make use of the possibility of entering rogue information in input fields. Theses only highlight the major sources of attacks, which are constantly multiplying.
- **Cross-Site Scripting** – A script is injected to one web site or web log, but it is operated at a different web site.
- **Site Cloaking** – Cloaking fools search engines by disguising one web site as another.

I. CYBER CRIME STATISTICS

CERT-In is a functional organization of Department of Information Technology, Ministry of Communications and Information Technology, Government of India, with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

In the year 2010, CERT-In handled more than 10000 incidents. The types of incidents handled were mostly of Phishing, Malicious Code, Website compromise & propagation of malware and Network Scanning & Probing. CERT-In is tracking the defacements of Indian websites and suggesting suitable measures to harden the web servers to concerned organizations. In all 14348 numbers of defacements were tracked in the year 2010. Most of the defacements were done for the websites under .in domain. In total 9772 .in domain websites were defaced. [10]

Security Incidents	2004	2005	2006	2007	2008	2009	2010
Phishing	3	101	339	392	604	374	508
Network Scanning / Probing	11	40	177	223	265	303	477
Virus / Malicious Code	5	95	19	358	408	596	1817
Spam	-	-	-	-	305	285	981
Website Compromise & Malware Propagation	-	-	-	-	835	6548	6344
Others	4	18	17	264	148	160	188
Total	**23**	**254**	**552**	**1237**	**2565**	**8266**	**10315**

Table 1: The year wise summary of various types of Security Incident handled by CERT-In ***Source: CERT-In Annual Report (2010)***

3 WHAT BANKS CAN DO TO PROTECT AGAINST ONLINE BANKING CRIMES

With the growing cyber-crime threat and increasing institutional responsibility, there is no other option for banks but to be proactive. It has been observed from the literature review that more than 30 percent of successful crimes in online banking are committed by employees or related persons. However protection needs to start with Management, not the Information Technology (IT) Department. The concern, commitment, and control of management are critical to adopting funding, and enforcing an effective protection scheme that may be fully implemented in the online banking environment. That is not to say that internal IT or contract

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE

technology personnel have no role to play, but simply directing IT personnel to install a firewall or regularly changing the passwords would not be a medicine to cure all diseases. Like any other form of corporate security from sign-in sheets to identification badges to biometrics for protection. A bank simply cannot afford to make the mistake of deploying anything less than a comprehensive top-down strategy to enable a reliable system of computer network security.

a. A comprehensive approach and control information security:

Sr. No	Approach	Details
1	Preventive	Secure card readers, Encryption, Spyware, 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

Table 2: A comprehensive approach and control information security

A bank's goal is to adopt a customized set of IS policy procedures and a practice that enables control over critical information and technology assets in a cost-effective way. A comprehensive approach to physical, technical, and organizational security controls need to be follow to minimize the risk. Table 2 show the five controls Preventive, detective, Deterrent, Corrective and recovery.

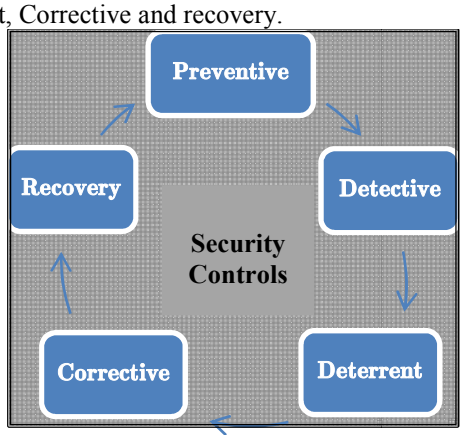

Fig 2: A comprehensive approach and security controls

b. Protection strategy

Banks also need to be practical for securing the information and Information system. Adopting procedures to deal with suspicious employees and implementing crisis teams are all basic issues that banks need to consider in addressing any comprehensive security system. On the other hand, banking industry can use some basic protection methods and perfect defensive tools to minimize their risks from online banking fraud. Basic protection strategy can start with an effective risk assessment and a review of the policies and procedures associated to information security. Some of the prevention strategies are mention below:

1. Risk assessment: Bank has to be analyzed all possible threats and risks associated with online banking and similar malicious activities. Management has to be priorities the risks with high probability and high impact or costs (if a crime occurs).
2. The bank can implement prevention techniques, tools and policies. The tools would include technologies to protect the bank's system and network from malicious objects and attacks, such as firewalls, intrusion detection system, anti-virus software and antispyware procedure. Banks can also conduct awareness and training program to minimize the risk of phishing and identification theft.
3. A bank should make sure it has a excellence business recovery plan in its policies and Procedures. A number of things can cause a bank to lose its computers and information systems, including system failures, man-made or natural disaster, hackers/crackers and other cyber criminals. An effective business recovery plan will allow a business to recover from any of these adverse measures. It is essential that the recovery system, in particular data recovery to be tested.
4. Develop an incident response plan as part of the policies and procedures. An incident response plan is developed at minimum risk. What if some cracker or cybercriminal attacked your bank successfully and did the one thing that has the highest public risk for the bank for example, stole thousands of credit card numbers and PINs, wiped out your hard drives, stole the corporate identity, etc. ? To monitor and recover from such activity bank has to implement incident response plan.
5. Training and awareness: Through training awareness program and seminars is essential of risks of online banking can be minimized. It includes both customer and employees, and their ability to recognize the types of cybercrimes and respond appropriately to each.
6. Banks can use some specific information technology (IT) or information systems (IS) countermeasures to mitigate the risk of cyber-crime.
7. Last but not least by developing a policy and procedure is not sufficient, bank should place appropriate security controls and Information security team in place to monitor the activity performed in the online banking environment.

4 CODE OF PRACTICE

The following practices can help to avoid common security problems associated with online banking:

- ✓ Banks should have documented and published IS policy, procedure and guideline in place which is

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE

approved by board of directors and communicated to end users.

- ✓ Review of information security policy and procedure on regular basis.
- ✓ Upgrade existing password single-factor authentication systems to two-factor systems.
- ✓ Use scanning software or tools to proactively identify and protect against phishing. Scanning tools are commercially available tools that can be used for identifying and analyzing security vulnerabilities in network, operating systems and database
- ✓ Implement adequate network security to block unnecessary network traffic to the systems.
- ✓ Set up adequate backup facility and recovery arrangements.
- ✓ Conduct training and awareness programs to help customer and employee to avoid online scams.
- ✓ Protect computer or information system from cyber attacks by implementing and monitoring the information security controls.
- ✓ Bank should establish disaster management site to recover form loss.

V. CONCLUSION

A bank, therefore, needs a broad strategy of prevention. "No one method can protect a bank against all types of cyber-crimes and cyber-enabled perpetrators." Because of the high-level of risk in banking related to cyber-criminal activities, banks must maintain constant monitoring and attention to be aware of the risks, assess and priorities the risks, and take appropriate actions to minimize the operational risks. There are a number of threats that spreads through a variety of channels in order to steal confidential banking information. Basic protection strategy can be start with an effective risk assessment and a review of the policies and procedures associated with information security. A bank should adopt a customized set of procedures and practices that enable control over critical information and technology assets in a cost-effective way. A comprehensive approach to physical, technical, and organizational security controls should be implemented to protect information system.

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.
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. 2. ed. 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
11. http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE