



Journal of Internet Banking and Commerce

An open access Internet journal (<http://www.arraydev.com/commerce/jibc/>)

Journal of Internet Banking and Commerce, August 2007, vol. 12, no.2
(<http://www.arraydev.com/commerce/jibc/>)

Online Frauds in Banks with Phishing

First Author's Name: **N. P. Singh, PhD**

First Author's Title/Affiliation: **Professor, Management Development Institute, Gurgaon, India**

Postal Address: **Mehrauli Road, Sukhrali, Gurgaon -122001, India**

Author's Personal/Organizational Website: **www.mdi.ac.in**

Email: **knpsingh(at) mdi.ac.in.**

Brief Biographic Description: Dr. N.P. Singh is a Professor of Information Technology Management at Management Development Institute, Gurgaon, India His current research interests are Business Intelligence, Data Warehouse, Data Mining, Enterprise Systems, Application of information Systems in Banking & E-commerce. He has published sixty plus research papers in prestigious journals. He is working on consulting assignments in relation to evaluation of MIS projects, E-governance Projects, Corporate strategy etc.

Abstract

Hi-tech fraudsters have urbanized a new way of tricking on line banking customers. One such most well known and fast growing technique is phishing. Latest in phishing is application of Trojan horse program. Trojan horse" program insinuates itself into a user's computer via an email and directs the user of the system to website which is exactly similar to financial institution web site. Crooks pick up passwords and account numbers as soon as customer logon to these sites. As it evident from table 1 phishing causes maximum loss to the customers/ institution in comparison to other similar techniques. Keeping in view, the serious threats of phishing attacks author analyzed the trends of major activities of the phishing across globe specifically in the banking sector. In addition, author analyzed the reasons for increase in fishng activities, types of phishing techniques, and process of phishing. Further author has presented recent cases of phishing specifically in banking/ financial sector. Towards the end it author has studied the measures to combat the fishing in online banking.

Keywords: Online Frauds, Phishing Techniques, Anti-phishing tools, Dual factor

authentication, Banks.

© N. P. Singh, 2007

INTRODUCTION

Online banking is designed mainly to achieve two objectives. First increased convenience for the consumer and second reducing the cost of operations to the banks. Numerous benefits such as lower fee to go online, higher interest rates, online viewing of account details and statement information, pay bills, transfer money between accounts, scheduling automatic periodic payments such as rent or loan payments, applying for accounts or loans and managing loyalty points to achieve first objective. In the process banks are able to reduce cost of operations to some extent. But steep rise in online banking crimes had undermined its success as few bank customers want to return to boring bank queues for secure transactions. Opponents of online banking say that online banking involved heavy risk to the consumers (86% of all attacks are directed at the home users' against 14% at the financial houses, Zvomuya (2007)) and industry has rushed to get online without appropriately confronting issues that could compromise its integrity.

The common online banking frauds are (i) Hoax emails (A hoax¹ is an attempt to trick an audience into believing that something false is real), (ii) Computer viruses (A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user), (iii) spyware² (a computer software that is installed surreptitiously on user computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent), (iv) Email employment scams / Internet Job Scams (people are lured by the scammers to visit some websites such as social security statement website³ with a view to steal your information with respect to social security number etc), (v) Identity theft (Identity theft⁴ is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else), (vi) Phishing (explained in the next sections), (vii) Vishing (a variant of phishing), and (viii) Eavesdropping⁵ (Unauthorized, real-time access to intelligence) when using a wireless connection.

In the recent past, according to the UK payments association Apacs⁶, the huge rise in online banking fraud coincides with an upsurge in the number of phishing scams being run on the web and demonstrates the importance of educating bank customers about this type of crime. The similar concern is raised by Financial Services Authority (FSA), UK

¹ <http://en.wikipedia.org/wiki/Hoax>

² <http://en.wikipedia.org/wiki/Spyware>

³ http://www.identitytheftfixes.com/identity_theft_can_cost_you_more_than_just_your_credit_score.html

⁴ http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci801871,00.html

⁵ http://www.spybusters.com/eavesdropping_definition.html

⁶ <http://www.bcs.org/server.php?show=conWebDoc.10452>

regulator. FSA recorded 8.000% increase in online banking frauds and identified phishing as major instrument (OUTLAW News (2006)). Jaques (2006) reported that a quarters of Britons have disclosed their PIN to some one else, exposing themselves to risk of fraud. Another facts revealed by users that they use similar PIN for all their on average four cards. Young (2006) mentioned that online bank fraud losses rose by 55 per cent from £14.5m in the first six months of 2005 to £22.5m in the same period in 2006 as per the release of Apacs and phishing scams are major contributor. Miller (2007) identified trends of phishing in 2006. He pointed out six innovations of phishing. These are (i) Plug and Play Phishing Networks (phishers perfected techniques to rapidly deploy entire networks of phishing sites on cracked web servers. The software used are known as Rockphish and R11) (ii) Phlashing (Flash-based phishing sites) (Attackers have begun using Flash animation to create spoof sites as a strategy to defeat automated anti-phishing services), (iii) Two-factor Authentication (able to defeat two-factor authentication tactics using a man-in-the-middle attack), (iv) Hacked Bank Sites (Several attacks in 2006 saw phishers hack into bank web servers and use them in attacks), (v) Continued XSS Vulnerabilities (exploiting financial institutions web site vulnerability to attacks using cross-site scripting (XSS)), (vi) MySpace Phishing (targeting social networks). With the growth of phishing customers are realizing that online transactions in particualar e-commerce transactions are not safe. Phishing is becoming so widespread, its variations are taking on cute names. In the initial years it used to be limited to the largest banks, but a new twist, called 'puddle phishing' has the fraudsters going after the customers of regional banks or credit unions. Phishing which targets small groups or individual companies is known as 'spear phishing'. In addition, vishing, pharming, man-in-the-middle attacks variants of phishing are also becoming common to the victims.

This article is an attempt to analyse various facets of phishing with the help of secondary data available on internet and in the literature. Various views of phishing are explained in the definitions of phishing presented in the next section of the article. The four major phishing techniques are briefed in section 3. The main reasons for increase in fishng activities are detiled in section 4. Recent statistics/ cases of phishing in general and phishing for banking frauds are detailed in section 5 of this article. Short duration historical analysis of Indian financila institutions is detailed in section 6. Towards the end, section 7 incudes the various measures to combat the phishing in online banking followed by concluding remarks. The article is based on secondary data mainly collected from the internet or from published reoprt. Conclusions are the result of qualitative analysis in temrs of new development of phishing domain and couter measures by the victims.

WHAT IS PHISHING?

It is derived from fishing. Phishing (also called brand spoofing) is a term used for a short of fraud where phishers send out spoof email to a random database to fool the recipient in to divulging personal information like credit cards details, usernames and passwords, that can be used for identity theft. Phishing is one of the most well known and fastest growing scams on the Internet today. The typical phishing scam involves an e-mail that appears as though it came from a reputable and known service institutions or company. The e-mail appears to be legitimate and the actual one. The message generally indicates that, due to problems in the institution (bank in this case) such a database updates, problem occurred in server, security/identity theft concerns, the recipient is

required to update personal data such as passwords, bank account information, driver's license numbers, social security numbers, Personal Identification Numbers (PIN), and so forth. The e-mails include warning to the users that failure to immediately provide the updated information will result in suspension or termination of the account etc. Some of explanations of the word in the form of definition are listed in the following:

Definition 1⁷: In computing, **phishing** is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. eBay and PayPal are two of the most targeted companies, and online banks are also common targets.

Definition 2⁸: The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft

Definition 3⁹: Phishing means sending an e-mail that falsely claims to be from a particular enterprise (like your bank) and asking for sensitive financial information.

Definition 4¹⁰: Phishing is a type of fraud that is designed to trick individuals into disclosing confidential and financial information for the purpose of identity theft.

Another variant of phishing is Vishing (voice-phishing). It is the practice of sending fraudulent email to consumers that appears to be an email from a local bank, credit union or other financially related web site and contains what appears to be a local phone number. The fraudulent email will appear to inform the consumer of some type of problem with their account and instruct them to dial a local phone number. Consumers who are used to calling automated tellers are being tricked into using their phone keypad to type in vital account numbers, pin numbers, and other financial information into overseas computers (Baker (2007)).

PHISHING TECHNIQUES

There are mainly three techniques of phishing as mentioned by ITU (2005). However, one more technique is reported by Chawki (2006). These techniques are briefed in the following:

- i. **Dragnet Method:** This method involves the use of spammed emails, bearing falsified corporate identification (e.g., trademarks, logos, and corporate names), that are addressed to a large class of people (e.g., customers of a particular financial institution or members of a particular auction site) to websites or pop-up windows with similarly falsified identification to trigger immediate response.

⁷ <http://en.wikipedia.org/wiki/Phishing>

⁸ <http://www.webopedia.com/TERM/P/phishing.html>

⁹ <http://inhome.rediff.com/money/2004/dec/20spec.htm>

¹⁰ <http://www.rbc.com/security/bulletinPhishing.html>

- ii. **Rod-and-Reel method:** This method targets prospective victims with whom initial contact is already made. Specific prospective victims so defined are targeted with false information to them to prompt their disclosure of personal and financial data.
- iii. **Lobsterpot Method:** It consists of creation of websites similar to legitimate corporate websites which narrowly defined class of victims by phishers. Smaller class of prospective victims identified in advance, but no triggering of victim response. It is enough that the victims mistake the spoofed website as a legitimate and trust worthy site and provides information of personal data.
- iv. **Gillnet phishing:** In gillnet phishing; phishers introduce malicious code into emails and websites. They can, for example misuse browser functionality by injecting hostile content into another site's pop – up window. Merely by opening a particular email, or browsing a particular website, Internet users may have a Trojan horse introduced into their systems. In some cases, the malicious code will change settings in user's systems, so that users who want to visit legitimate banking websites will be redirected to a look alike phishing site. In other cases, the malicious code will record user's keystrokes and passwords when they visit legitimate banking sites, then transmit those data to phishers for later illegal access to users' financial accounts.

REASONS FOR THE INCREASE IN PHISHING

- i. The tool such as "Universal man-in-the-middle phishing kit" which automatically creates sophisticated phishing site is available on underground online market places for about \$1000. (Evers (2007) & Dunn (2007)).
- ii. Availability of key-logging software which can surreptitiously record key-stroking activity and collect computer usernames and passwords. (News (2003).
- iii. Customers are lured by fictitious rewards for participating in bogus surveys and handover sensitive account information to phishers (Leyden (2006) and Miller (2006)).
- iv. Some of the organizations employ lax password requirements. For example eBay allowed combinations such as user ID of james34231 and a password of james34. The similar combinations are also allowed by Google mail (Goodin (2007)).
- v. Another reason for increase in phishing is very high return on investment. According to Lohman (2006) "The return on investment in phishing is phenomenal." "It costs about \$160 to set up a phishing scam to send 10,000,000 emails a month. Even if only 0.001 percent of the emailed people respond, it nets about \$125,000."

PHISHING CASES:

Globally, about 30,000 phishing attacks are reported each month, of which over 80% are directed at financial institutions. Statistics presented in table 5 is an ample proof of sharp increase in phishing activities. Phishing attackers have targeted at financial entities such as Citibank, Wells Fargo, Halifax Bank, eBay, and Yahoo as reported by Secure Science Corporation (2003). The details of top 10 brands affected by phishing are presented in

table 8 indicates that eBay and Paypal are favorite of phisher during the last five years. According to assureconsulting.com¹¹, phishing is a complex and converging security threats facing businesses. The methods used by spammers have become more sophisticated, and spam is now increasingly combined with malware and used as a tool for online fraud or theft, or to propagate malicious code. Assureconsulting.com reported a set of three examples using phishing for financial frauds targeted on financial entities, internet service providers, retailers such as Citibank, U.S. Bank, Paypal, Visa, AOL, Nationwide, Chase, MSN, and Yahoo. McAfee¹² says that phishing schemes and identity theft will continue to be a problem among the consumer community until further education and widespread acceptance of proactive protection occurs. According to Thomas (2006), the survey by RSA Security reveals that 62 per cent of all phishing scams were aimed at US banks and credit unions, while the number of identity fraud attacks against European and other financial institutions dropped. Table 1 embodies a brief description of few phishing cases as reported in the literature with respect to financial institutions along with general statistics of phishing. These cases includes only those cases wherein amount stolen by phishers is mentioned.

Table 1: Recent Statistics of Banking Fraud using phishing techniques

Country	Facts/ Description
UK	<p>General Statistics: The number of recorded phishing incidents was 312 and 5059 between January to June, 2005 and January to June 2006 respectively, the Lords science and technology committee was told. UK was among top 10 phishing site hosting countries from Jan 2005 to Jan 2007. The amount of cash stolen in the first half of 2006 was £23.2m, the committee was told, and was likely to be £22.5m in the second half of the year. Chip-and-pin cards were introduced by the banking industry in 2004 in an attempt to combat the rapid rise in fraud using plastic cards. Credit and debit fraud peaked in 2004 at just over half a billion pounds. With introduction of chip-and –pin cards it fell by 13% during the whole of 2005 and these latest figures show a further decline. Despite this, losses due to cards being used in telephone, online or mail order fraud continued to increase. This type of fraud, where the legitimate card holder is not present, rose by 5% in the first half of the year to £95m. And fraud using counterfeit cards rose even faster - up by 16% to £53m. APACS said the main factor behind this was the fact that criminals continue to copy the details of people's magnetic strips - known as skimming - to create fake cards. Online Banking fraud in 2004 was £12.2 million and it was increased to £33.5 million during 2006. Number of bogus websites was 1713 in 2005 which reached a figure of 14,516 in 2006 (BBC (2006a,b), Rupert (2007), Jeremy (2006)),</p> <p>Unkown Bank case: In the UK, one single bank took £30m of the £35m phishing losses sustained in 2006. According to investigators, the phishermen target this bank because of its lax internal controls, and above all its poor record of asset recovery: apparently it recovers only about 60% of stolen money compared with 75–95% for its competitors (Anderson (2007)).</p>

¹¹ <http://www.assureconsulting.com/articles/phishing.shtml>

¹² <http://www.networkmagazineindia.com/200409/securitywatch01.shtml>

	Douglas Havard and Lee Elwood Case: Douglas Havard and Lee Elwood were sentenced to six years by Leeds Crown Court for stealing 6.5 million pounds as a part of identity frauds (Thomas (2005)).
USA	General Statistics: It is evident from the table 6,7, and 8 that US is leaders of top 10 phishing sites hosting countries and also experienced large number of phishing attacks. Gartner study (May, 2004)- At least 1.8 million consumers had been tricked into divulging personal information in phishing attacks, most within the past year. Phishers cost US consumers US \$ 1.2 Billion in 2003 according to Gartner ¹³ . (Sullivan, Bob (2004).) Financial institutions are tight-lipped about fraud losses (Sullivan (2004a)). The average loss per phishing attack was \$1,244 in 2006, up from \$256 in 2005. Gartner estimates that the total financial losses attributable to phishing will total \$2.8 billion in 2006. In 2005, 80% of victims got their money back. In 2006 that number dropped to 54%. Gartner estimates that 3.5 million Americans will give up sensitive information to phishers in 2006, up from an estimated 1.9 million in 2005. High income group reported receiving an average of 112 phishing e-mails during 2005 versus 74 e-mails per consumers across all income brackets ¹⁴ (McMillan (2006)).
	Wachovia Bank ¹⁵ customers receive e-mails with contents as “Wachovia Internet Banking, is here by announcing the New Security Upgrade. We've upgraded our new SSL servers to serve our customers for a better and secure banking service, against any fraudulent activities. Due to this recent upgrade, you are requested to update your account information by following the reference below”.
	Bank of America: Lopez and his wife, Farah lost \$90,000 to Riga Latvia (Costello (2004) & Sullivan (2004b)). Lopez' computer was infected by a keylogging Trojan, which captured his login details. His money were soon transferred to a bank in Latvia. When Bank of America refused to cover the loss, Lopez sued for negligence, saying the bank failed to warn him about the Trojan.
Sweden	General Statistics: A rouge anti spam program (rakin.zip or raking.exe infected with haxdor.ki Trojan) stolen the identities of 250 plus customers and \$ 1.5 million from Sweden largest bank during October 2005 to December 2005 (PC Tools News (2006)).
	Nordic Bank Case: Phishing gangs have managed to steal about €900,000 from accounts at Swedish bank Nordea since last autumn using a Trojan horse. At least 250 customers have been affected; the accounts of another 121 customers are under investigation. Nordea, the largest bank in Nordic countries, have confirmed the attacks, but didn't inform the public until now. (Libbenga (2007)).
Germany	General Statistics: According to a-i3 survey ¹⁶ (2006, January, 554 respondents) 20% are getting more than 20 phishing e-mails/ month and 3

¹³ <http://sify.com/news/infographics/onlinescams/scam2/index.php>

¹⁴ http://www.sda-india.com/sda_india/psecom,id,24,site_layout,sdaindia,analysis,201,p,0.html

¹⁵ <http://www.svbizlaw.com/phishing.wachovia.htm>

¹⁶ http://www.eco.de/servlet/PB/show/1858849/Schwenk_ai3.pdf

	<p>respondents claims financial losses more than 3000 euro. In 2006, the damage caused by phishing in Germany¹⁷ amounted to around \$6 million.</p> <p>Post Bank: The gang, made up of five men, are said to have stolen around 30,000 Euros (Norah (2004)). Two clients of Germany's Postbank lost 21,000 euros between them. The money was diverted to eastern Europe by phishers. Deutsche and Postbank are the only two banks affected in Germany (Reuters (2007)).</p>
Malaysia & Hong Kong	General Statistics: In the last 18 months, the DBS Bank, HSBC, Citibank, Standard Chartered, UOB (Malaysia), and OCBC (Hong Kong) have been hit by phishing scams (News (2004) ¹⁸).
South Africa	<p>General Trends: The number of bank customers falling prey to thieves through "phishing" is on the rise, largely because of people using Internet cafes for their online banking (Vusumuzi (2007)). Standard Bank, FNB and ABSA have confirmed that some of their online clients' accounts have been breached in the past few days (Rondganger (2007)).</p> <p>First National Bank: (100% increases in phishing attacks). R 6000 was transferred from an account but canceled by the bank due to SMS notification on the account (Mtshali (2007)).</p> <p>Standard Bank: The fraudsters were able to siphon R200 000 from an individual's account, but it was recovered later on. Most of phishing attacks are high tech (Rondganger (2007)).</p> <p>Nedbank¹⁹: Ned bank is not affected by phishing attacks since it uses a number of brand protection services to monitor potential phishing</p>
Australia	<p>General Trends: According to the Australian Securities and Investments Commission (ASIC), the number of phishing attacks is increasing at a very growth rate. The targets are becoming much smaller and more localized. "The success rate of phishing is usually around 3 percent²⁰. Australia has 7 million online bankers. That means there is a potential response of 210,000 people. If they all lost AU\$1,000 that is AU\$210 million," said Rodney Mills detective sergeant of the fraud strategy project team for the Victoria Police. 200 million AUS\$ in 2003²¹.</p> <p>Westpac Bank case: En-masse e-mail to Westpac bank customers, represents the latest example of "phishing scams," designed to fool them into divulging their online banking security details. According to anti-virus vendor Sophos phishing techniques used in Westpac was of highest order of sophistication (Colley (2004)).</p>
France	General Statistics: In France, there are attacks of small scale, 30 000 to 400 000 e-mail in 2005 (Devillard (2006)).
Ireland	Bank of Ireland Case: Some of the customers of Bank of Ireland had lost more than €110,000 to the scammers. One customer claims to have lost more than €49,000 and other reported losses between €5,000 to €16,900 (O'Brein (2006a)). Bank had agreed to refund about €160,000 to the

¹⁷ http://www.chosensecurity.com/solutions/anti_phishing.htm

¹⁸ <http://computertimes.asiaone.com.sg/news/story/0,5104,2808,00.html>

¹⁹ http://www.ioltechnology.co.za/article_page.php?iSectionId=2885&iArticleId=3751820

²⁰ http://domainsmagazine.com/Domains_14/Domain_2780.shtml

²¹ <http://www.cs.tau.ac.il/tausec/lectures/AntiPhishingil.pdf>

	customers to compensate their losses (O'Brein (2006b)).
Brazil	General Statistics: Valdir Paulo de Almeida gang had looted between 50 and 100 million reais (\$18m and \$37m) during 2003 & 2004 (Leyden (2005)). According to other sources , banks targeted by the Trojan horses included Banco do Brasil, Bradesco, Caixa Economica Federal, HSBC, Itau, and Unibanco and about \$30 million during 2004.
China	<p>General Statistics : Ranked second in the world for hosting phishing attacks, and accounting for 13 percent of the world's total phishing websites. In 2004, 1,350 online fraud and spam cases. In the first quarter of 2005, 543 phishing incidents were identified with 1,361 illegal websites closed by Chinese authorities (Frederick Stakelbeck, Jr.(2005)).</p> <p>Hong Kong and Shanghai Banking Corporation Case: It is believed to be the first known local cases where customers have fallen prey to a syndicate purporting to be a Hong Kong bank. An amount of HK\$660,000 siphoned off from their accounts over three weeks (September 17 to October 6). A total of 12 bank customers received "phishing" emails purporting to be sent by their bank (Chan (2004)).</p> <p>Industrial and Commercial Bank of China (ICBC) case: In Guiyang, capital of Southwest China's Guizhou Province, Song Chenglin, a 23-year-old Harbin college student had stolen 770,000 yuan (US\$93,000) by hacking into the ICBC (Chan (2004)).</p>
Russia	Citibank Case: The financial losses of Russian businesses caused by "carder" reached \$20'000'000. Carders specialized on counterfeiting plastic cards use Internet for receiving information on card holders and card's numbers. Phishing Messages are received by customers of Citibank. The Russian message reads as "Your personal account has accepted wire transfer in foreign currency more than \$ 2'000. According to the agreement of CitibankR Online you have to confirm you data for successful accepting money to the account. To confirm this operation it is necessary to run program of account management and fallow proposed instruction. In case of un-confirmation wire transfer will be returned to sender". SAYTARLY (2004).
South Korea	A 20-year-old school dropout has broken into an online banking system and stolen some 50 million won (\$A66,111), causing alarm over the security of South Korea's widely-used internet banking services. According to police, Lee ²² attached hacking software to a message he planted on a community internet site. The woman clicked on it, inadvertently downloading the "key stroke" logging program which enabled Lee to gain the passwords and security code for her account. Police said internet users must avoid downloading unfamiliar programs on the internet and install protection software provided by the banks.

²² <http://www.theage.com.au/news/Breaking/Phishing-attack-nets-over-60000/2005/06/06/1117910220131.html>

As mentioned earlier phishing is not only confined to the banking institutions but targets other organizations which are involved in e-commerce, mobile commerce and money transfer activities. Few popular cases are described in table 2.

Table 2: Recent Statistics of phishing with respect to non-banking institutions.

Country	Facts & description
UK	<p>eBay Phishing Case²³: More than 160 people were duped in the scam in 12 months between July 2003 and July 2004. The total fraud was almost £200,000.</p>
	<p>Douglas Havard and Lee Elwood Case: they have netted over 6.5 million pounds during 2003-04 in UK (Roberts (2005)). They reportedly received large groups of stolen credit card information and passwords from unnamed individuals in Russia, then used those to purchase goods online and resell them, pocketing the proceeds and passing a cut along to their counterparts in Russia through money exchanges. They also trafficked in stolen identity information and documents, including driver's licenses, passports and birth certificates, NHTCU said.</p>
USA	<p>AOL Case: ISP is seeking damages of \$18 Million against unnamed groups who have targeted AOL and Compuserve members with phishing e-mails (Leyden (2006)).</p>
	<p>Forcellina²⁴ Case (2004): Husband, 23, accessed chat rooms, used device to capture screen names of chat room participants; then sent e-mails pretending to be ISP requiring correct billing information, including current credit-card number. Used credit-card numbers and other personal data to arrange for wire transfers of funds via Western Union, but had others pick up funds from Western Union.</p>
	<p>Hill Case (2003)²⁵: He operated AOL and PayPal phishing scheme, used fraudulently obtained credit-card numbers to obtain goods and services costing more than \$47,000. Sentenced to 46 months.</p>
	<p>Kathy Prati Case²⁶: Kathy a graphic designer in Sonoma valley bought truffle shampoo on a web site and within 24 hours some one had used her card to order \$ 900 in merchandise from Eddie Bauer and ship it to Russia.</p>
	<p>Carr Case²⁷: Helen Carr was accused of sending fake email messages to AOL customers in the U.S and several foreign countries. The emails advised the customers that they must update their credit card and personal information on file with AOL to maintain their accounts. She was found guilty of conspiracy to possess unauthorized access devices and sentenced in January 2004 to 46 months imprisonment.</p>

²³ http://news.bbc.co.uk/2/hi/uk_news/england/lancashire/4396914.stm

²⁴ <http://www.abanet.org/adminlaw/annual2004/Phishing/PhishingABAAug2004Rusch.ppt#10>

²⁵ <http://www.abanet.org/adminlaw/annual2004/Phishing/PhishingABAAug2004Rusch.ppt#10>

²⁶ http://www.businessweek.com/magazine/content/05_22/b3935009_mz001.htm

²⁷ http://findarticles.com/p/articles/mi_pjus/is_200311/ai_1464826283/pg_14

	<p>Yetter Case²⁸: Yetter offered for sale on the Internet motor vehicles, motor vehicle parts, television equipment, or other merchandise for sale, and fraudulently obtained more than \$10,000 from victims with no intention of providing the purchased items.</p> <p>Matthew Guevara Case²⁹: Guevara 21, of Chicago, Illinois, created false e-mail accounts with Hotmail and unauthorized website with the address www.msnbilling.com through Yahoo!. Then sent MSN customers e-mail messages, purporting to come from MSN that directed customers to fraudulent www.msnbilling.com website and asked them to verify their accounts by providing name, MSN account, and credit card data. Website automatically forwarded each customer's data to one of Guevara's false Hotmail accounts; Guevara used stolen credit card information himself and provided it to another person as well. He was sentenced to 5 year probation and 6 months home confinement.</p> <p>Shelly S. Perry Case³⁰: Perry operated an "Internet Business" having a website address of "www.paylessfurniture.com" from her private residence in Memphis, Tennessee. Perry defrauded many individuals, located throughout the country, who were attempting to purchase furniture via the said Internet website, auction sites, and personal contact with her. More than 70 citizen victims sent her \$110,000.00 in access.</p> <p>More Statistics³¹: There are many more such cases from USA. To mention, Shwan Kalin case of DealerTrack, Inc. (Lobsterpot phishing), Alba Julia, Romania case with total loss of \$5000,000 (Rod-and –Reel Phishing), Isaac Gebrezehir case of counterfeiting IRS forms (Rod-and –Reel Phishing with a loss of \$700,000), and Juvenile case of AOL and Paypal accounts (Dragnet Phishing).</p>
India	<p>Kingfisher Case: More than 15,000 online ticket of Kingfisher Airline were purchased by fraudsters who got credit card information of Indian and foreign nationals. The loss to the carrier was Rs.17 Crores (Business News (2007)).</p> <p>NASSCOM Case: Ajay Sood and Others (Operators of a placement agency involved in head-hunting), composed and sent emails to third parties in NASSCOM's name in order to obtain personal data. They agreed to pay Rs 1.6 Million to NASSCOM as damage for violating NASSCOM trademark right a compromise in the suit proceedings. (Titus and Roy (2005)).</p> <p>Kobayashi-Hillary Case: Kobayashi-Hillary (2006) pointed out that he suffered identity theft last year when his debit card was cloned and £2,000 cleaned out of his account. That wasn't from a call centre thief in Mumbai, it was from a card skimmer in Mayfair.</p>
Australia	<p>eBay Phishing Case: Dov Tenenboim, 21, of the Sydney suburb broken in to at least 90 different eBay accounts during 2006 and stolen AU\$ 42,000 (Goodin (2007)).</p>
Japan	<p>UFJ Card Co. case: Eight customers of UFJ Card Co. lost a total of 1.5 million yen to swindlers using forged cards to make illegal withdrawals (Shimbun (2006)),</p>

²⁸ http://findarticles.com/p/articles/mi_pjus/is_200311/ai_1464826283/pg_15

²⁹ http://www.itu.int/ITU-D/e-strategies/e-legislation/Doc/Cybercrime_M_Menting.pdf

³⁰ http://findarticles.com/p/articles/mi_pjus/is_200311/ai_1464826283/pg_15

³¹ <http://www.abanet.org/adminlaw/annual2004/Phishing/PhishingABAAug2004Rusch.ppt#12>

	Sunao Koizumi Case ³² : He had stolen user IDs and passwords of Yahoo Auction users and using these IDs and passwords won about 300 bids for a total of about 5.5 million yen worth of book vouchers and travel coupons on Internet auctions and resold the products (Kyodo News (2007)).
	Akio Usami Case ³³ : The Tokyo-based group headed by Akio Usami has stolen from approximately 700 people a total of 100 million yen (approximately \$900,000) by drawing victims to a fake Yahoo Japan auction website.
	Yahoo Case ³⁴ : In 2006 eight people were arrested by Japanese police on suspicion of phishing fraud by creating bogus Yahoo Japan Web sites, netting themselves 100 million yen (\$870 thousand USD).

PHISHING IN INDIA

In India there have been several cases of attacks³⁵ on genuine websites. Financial institutions are the main targets of phishers, particularly, private banks. The major incidents are reported about ICICI, HDFC, UTI, and Stat bank of India. Many elderly customers who have just begun using online facilities of the financial institutions are falling prey to phishers. The messages send to customers are similar to as one given in the following which was sent to ICICI customers.

“The mail reads that the ICICI bank is upgrading to a new SSL Server to insulate customers against online Identity Theft and other criminal activities. Users are told to confirm their personal banking information following the link given in the mail. It also warns that if the user does not complete the form, the online bank account will be suspended till further notification³⁶”.

As mentioned in the beginning phishing incidents are increasing around the world in all aspect. May it be number of phishing e-mail reported, number of phishing hosting sites, amount lost in phishing attacks etc. The analysis of these parameters of phishing with respect to India is presented in the following. These facts are about for the year 2005 to 2007.

It is evident from the data presented in table 3 and 4 that India had figured six times/months among top 10 phishing hosting countries in the 25 months that is from January, 2005 to January, 2007. However percentage contribution is not very high in comparison to leaders USA and China in this domain. In addition specific researches are available with respect to phishing attacks on Indian financial institutions. Kaur (2005) pointed out that over 1,000 cases of phishing are reported in three months-from Dec '04 to March '05 in spite of RBI guidelines on Internet banking which enforces the adoption of internationally accepted state-of-the-art minimum technology standards for access control, encryption/decryption (minimum key length), firewalls, verification of digital

³² <http://asia.news.yahoo.com/060207/kyodo/d8fk4i588.html>

³³ <http://www.sophos.com/pressoffice/news/articles/2006/05/jpphishgang.html>

³⁴ http://en.wikipedia.org/wiki/Phishing#_note-76

³⁵ <http://www.ciol.com/content/search/showarticle1.asp?artid=84504>

³⁶ http://www.mwti.net/products/pdfs/theitshield_ICICI%20Bank%20Phishing%20Scam%20Targets%20Customers%20In%20India.pdf

signature, and Public Key Infrastructure (PKI). There are lots of investments by banks in security domain. According to the 2005 DQ-IDC Mega Spenders survey, Punjab National Bank topped the investment list. Its web servers are provided with Digital Certificates and are SSL enabled. Customers are forced to change the passwords at periodic intervals and a virtual keyboard feature has been provided for Internet Banking login, whereby the customer uses mouse clicks instead of typing using the keyboard. This minimizes the risk of keyboard grabbing but still many phishing are reported. '2005 India Web@work', a survey conducted by Websense Inc revealed that 32% of employees in India admitted to have given out their confidential data such as credit card numbers and corporate network passwords as a result of phishing attacks and 62% of IT managers believe that a security breach would put their jobs at risk (corporate Bureau (2005)).

Banking sources indicate that besides SBI, three other international banks have informed Computer Emergency Response Team- India (CERT-In) about attempts at phishing during 2006. CERT-In reported that phishing incidents in 2006 were 180 per cent higher than 2005, and that trend has carried through into 2007 (Gold (2007)) and it has reports that 335 sites were targeted in 2006. Incidentally, 256 out of 335 were from the e-commerce segment (Cherian (2007)). Interestingly, CERT-In said it has recorded more consistent phishing incidents in the second half of 2006. The agency said there were close to 30 incidents recorded every month between July to October, 2006, 62 per cent of which involved phishing (against 25 per cent in 2005) and 32 per cent of which involved network scanning (against 30 per cent in 2005).

Kumar (2006) pointed out that it has been six months since the phishing attack on ICICI bank customers became public, and during that period, two more such attacks were reported on customers of financial institutions in India, one of UTI Bank and the other, State Bank of India. He had mentioned, considering that 'phishing' was pretty much unheard of in India a year ago, this frequency is something to be concerned about. Paul (2006) reported that in addition to ICICI, UTI, and SBI, the other financial organizations such as IDBI, ICICI Bank Home loans, HSBC, Standard Chartered, ABN personal loans, Bank of India and Kotak-Mahindra too have their phishing sites.

According to statistics presented by Espiner (2007) phishing attacks have outnumbered e-mails infected with viruses and Trojan horse programs during January 2007. Survey³⁷ conducted between January and March 2007 by Websense, Inc., reveals that 57% of the Indian enterprises have received phishing lures during the last one year and over a third of Indian companies (38%) were attacked by spyware. This is based on a sample of 450 Indian CIOs. Ghosh (2007) mentioned that more than 74% of IT managers across India report that their employees have received phishing attacks via email and about 52% say that their PCs have been infected by phishing. RSA Consumer Solutions reported that globally, phishing attacks have grown by 41% in the past 12 months and Phishers could convince up to 5% of recipients to respond. Few cases of phishing of major three banks (State Bank of India (SBI), ICICI, Unit Trust of India (UTI Bank)) of India are given in table 3.

³⁷ <http://www.moneycontrol.com/india/news/pressnews/60-india-inc-believed-to-have-recd-phishing-lureswebsense/281565>

Table 3: Popular Phishing Cases in Financial Sector In India

Name of The Bank	Facts & Description
State Bank of India,	Websense® Security ³⁸ Labs™ has received reports of a phishing attack that targets customers of State Bank of India. This phishing site is hosted in the United States. The content of the e-mail were as “Dear Valued SBI® Netbanking Customer, SBI's Internet Banking, is hereby announcing the New Security Upgrade. We've upgraded our new SSL servers to serve our customers for a better and secure banking service, against any fraudulent activities. Due to this recent upgrade, you are requested to update your account information by following the reference below”. (November, 15, 2006). Banking sources indicate ³⁹ that besides SBI, three other international banks have informed CERT-In about attempts at phishing. The Reserve Bank of India (RBI) ⁴⁰ has instructed banks to furnish data on frauds, thefts and burglaries on a quarterly basis to the regional offices of the Urban Banks Department.
ICICI	<p>General Statistics: According to Nair (2004) attempts were made by e-crooks for phishing ICICI customer accounts but no financial loss was reported. In February 2006⁴¹, there was a phishing scam where the ICICI bank website was cloned. According to Mulherkar (2006) in ICICI phishing scam the link in the email took the user to http://www.iciciibank.net while the bank's official address is http://www.icicibank.com. Based on the analyses of large number of reports at Internet, it can be concluded that there are large number of attempts by phishers at ICICI customers but success was very less. On February 7, 2006, ICICI Bank filed a complaint with Bandra Kurla Complex police station, Mumbai when its customers are asked to confirm their account details through an e-mail ID (icici@icicibank.com). When the cyber crime cell began investigating, they found that a scamster had managed to get hold of customer details and used it to purchase goods on the Internet. ICICI Bank website, this time cloned to www.iciciibank.net (Hossain (2007)).</p> <p>Phishing Victim Case: Sukhwinder Singh, phishing victim of ICICI Bank lost Rs. 41,000/- to a phishers Harpreet Chauhan (Moneycontrol.com⁴²)</p>
UTI	UTI Customers from Thane, Delhi, Vishakapatnam, Nasik and Ahmedabad had replied to an e-mail from the bank. The damage: 30 customers who lost Rs 20 lakhs (Kasbekar (2007)). UTI ⁴³ bank customers have lost more than

³⁸ <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=702>

³⁹ http://infotech.indiatimes.com/Enterprise/Be_web_wary_Phishing_hits_SBI_3_other_banks_/articleshow/461978.cms

⁴⁰ <http://www.realinformationsecurity.com/general/rbi-seeks-data-from-banks-on-frauds.html> (2007, March)

⁴¹ http://www.pegasusinfocorp.com/resources/articles/what_is_phishing.html

⁴² <http://www.moneycontrol.com/india/news/investigation/phishingpeoples-accounts/08/14/260119>

⁴³ http://www.mouthshut.com/review/UTI_Bank-116456-1.html

	<p>one crore of their hard earned money, because of fake online website, used by scamasters {Nigerian nationals⁴⁴} to withdraw money from customer accounts. In January, 2006, phishers⁴⁵ have crafted a URL on geocities that is nearly a version of home page of UTI bank and send it to customers via e-mail with intentions to get personal information of more than 100,000 customers of UTI.</p>
--	--

HOW TO COMBAT BANK FRAUD:

There are many methods to combat bank frauds in general and phishing in particular. In India alert and conscious customers could avoid phishing attacks. Most of the financial institutions are educating their customers of regular basis about phishing websites. In addition to these educative e-mails from the institutions the following three category measures can reduce frauds with phishing. Category I includes measures for customers, category II includes induction of new technology, and last category III includes measures on part of the institutions.

Category I

- i. Never share your password (Security related information) under any circumstance. (Standard Bank, Zvomuya (2007))
- ii. Never click on an e-mail that is purportedly from a bank advising you for updated antivirus software, and which can be downloaded from the bank's website. (Standard Bank, Zvomuya (2007))
- iii. Browse the bank's notification system on regular basis so that one can see the activities of his/her account. (Standard Bank, Zvomuya (2007)).
- iv. When ever one wants to visit the website of the bank, type full URL or web address. It is secure. It will avoid the logon to spoof sites such as <http://www.citbank.com> for <http://www.citibank.com>, and www.idbiibank.com for <http://www.idbibank.com>. (Standard Bank, Zvomuya (2007)).
- v. It is not safe to do internet banking in wireless internet environments or at Internet café. (Standard Bank, Zvomuya (2007)). It should be avoided out rightly.
- vi. Continuously read the posting of your banker for security updates. For example Zion bank⁴⁶ postings
- vii. Never access Online Banking via a link⁴⁷. Rather type the address directly into the browser address bar.

Category II

- i. Use browsers such as Firefox 2, Opera and Internet Explorer 7 (all latest versions) which include phishing shields (Kurup (2007)) and has better anti-fraud features in comparison to others (Matthew (2006)).

⁴⁴ <http://www.dqindia.com/content/industry/focus/2007/107051005.asp>

⁴⁵ <http://www.spamrazor.net/news.htm>

⁴⁶ http://www.zionsbank.com/online_fraud.jsp

⁴⁷ <https://www.fnb.co.za/>

- ii. Banks must implement anti-phishing programs as implemented by HSBC in Hong Kong⁴⁸. Security firms such as Symantec and McAfee are marketing anti-phishing software's. Bank must install security software's from Symantec Corp and McAfee Inc⁴⁹. There are many more companies which either developing or marketing anti-phishing solutions. These solutions can safeguard banks /financial institutions against fishing. Few of these solutions providers are mentioned in the following for the sake of examples.
 - a. NTT Comware⁵⁰ said Tuesday it has begun marketing PHISHCUT, a solution method for preventing phishing.
 - b. India's premier customized software solutions company, HQ, New Delhi⁵¹ partnered with Cloudmark Inc., to provide ant-spam and anti-phishing products/ solutions to Indian SMB's and ISPs.
 - c. Aladdin Knowledge Systems⁵², the leader in Software DRM, USB-based authentication, and secure Web gateways, today announced that Mumbai-based SecureSynergy Pvt Ltd is the first managed security service provider in India to deploy the Aladdin eSafe SecureSurfing solution for its customers.
 - d. Sendmail⁵³, leading global provider of trusted messaging has launched Domain Keys Identified Mail (DKIM) authentication technology in the company's Sentrion security appliances, and also in the commercial Sendmail Switch and Open Source mail servers. Sendmail's latest announcement concurs with the Internet Engineering Task Force (IETF) approval of DKIM as an Internet Standard. By verifying incoming messages organizations can remove targeted spoofing and phishing threats, cut on the number of false positives and remove identifiable spam.
 - e. Replace username and password login with stronger Hardware-based authentication solutions that are still current and viable as suggested by majority of customers in USA (Bennett (2006)). Similar suggestions are reported by the online survey, conducted in December 2006 by RSA. They also suggested risk based authentication. The sample size was 1,678 adults from eight countries including India (Pradhan (2007)). In fact Bendigo Bank is the first Australian banks to offer customers strong authentication protection for Internet banking using password generating tokens, in a move to thwart Internet banking fraudsters (Dinham (2004)). The cost of the tokens is AU\$16.50 each.

⁴⁸ <http://www.chinatechnews.com/2005/06/16/2618-hsbc-starts-anti-phishing-program-for-hong-kong-customers/>

⁴⁹ http://www.businessweek.com/magazine/content/05_22/b3935009_mz001.htm

⁵⁰ <http://www.japantoday.com/jp/news/402016>

⁵¹ <http://www.synapse.co.in/cloudmark/cloudmark-anti-spam-phishing-india.html>

⁵² <http://www.google.co.in/search?q=phishing+in+india&hl=en&start=250&sa=N>

⁵³ <http://www.techshout.com/security/2007/24/new-standard-combating-email-fraud-and-phishing-being-adopted-by-sendmail/>

- iii. Fast-moving, adaptable threats require equally agile, multi-faceted security responses. There are different technologies that provide multi-factor authentication, and banks must seriously consider the implications of each in terms of cost, ease of deployment and potential impact on usability (Bennett (2006)).
- iv. Introduction of electronic signatures to all email correspondence with its customers to curb phishing as it was done by German bank Postbank (Libbenga (2006)).
- v. Password shall be replaced with can be replaced with biometric technology.

Category III

- i. Transfer malicious mails to government agencies⁵⁴, which take care of such e-mails. For examples- uce@fte.gov, spam@uce.gov in USA. (Hall (2006), Indian Computer Emergency Response Team (CERT-In)
- ii. Citibank recently reduced the amount of money it allows customers to transfer out of checking accounts in response to the phishing epidemic. Daily limits on the institution's Global Transfers program, which allows customers to move money to any Citibank account for \$5 or \$10 per transfer, were reduced to \$500 per day and \$1,000 per week in October. This practice can be followed by others.
- iii. Minimize or eliminate the risks by instead using a virtual card with a virtual number for one-time use, with a specified limit and validity period—in many ways, this option is even safer than using a physical credit card in the real world. I've found that HDFC Bank's NetSafe⁵⁵ facility serves this purpose quite adequately, and in the rare event that your virtual card does get misused, your liability, if any, would be a very limited one indeed.
- iv. Banks should monitor every online transaction—not just log-in, but throughout the entire online banking session and telephone banking sessions (Bennett (2006) and (Pradhan (2007)).

In India, ICICI bank had adopted a dual factor authentication practice and remodeled its debt cards which now have 8X2 grid of numbers on the back of their debit cards. HDFC bank adopted a three pronged approach to tackle phishing (i) continuous education of customers about online transactions security, (ii) setting up a robust incident response process to render attacks harmless, (iii) implementing state of art technology solutions to thwart phishing attacks.

Table 4: Leading Online Hazards in the US 2006 (Frequency of incidence, cost per incident and cost of the total damages)

S.N.	Hazards	Frequency	Cost per incident per person	Total damages countrywide
1	Spam	1 in 2 People	-	-
2	Viruses	1 in 4 People	\$109	\$5.2. billion

⁵⁴ <http://blogcritics.org/archives/2005/03/02/101711.php>

⁵⁵ <http://www.expresscomputeronline.com/20040823/opinion01.shtml>

3	Spyware	1 in 8 People	\$ 100	\$ 2.6 Billion
4	Phishing	1 in 115 People	\$ 850	\$ 630 Million
Source: Consumer Reports "State of the Net", August 2006, www.marketer.com and				
http://www.user-groups.net/safenet/0608-21_phishing.html				

Table 5⁵⁶: Phishing E-Mail Reports

Month	Number of Reports		
	2005	2006	2007
January	12845	17877	29930
February	13468	17163	23610
March	12883	18480	24853
April	14411	17490	23656
May	14987	20109	
June	15050	26571	
July	14135	23670	
August	13776	26150	
September	13562	22136	
October	15820	26877	
November	16882	25816	
December	15244	23787	
	175068	268132	

⁵⁶ <http://www.antiphishing.org/>

Table 6⁵⁷: Top 10 Phishing Sites Hosting Countries

Country	2005											
	Jan.	Feb	Mar	Apr	May	June	July	Aug	Sep.	Oct.	Nov.	Dec.
USA	32.0 0	37.0 0	34.0 0	26.3 0	34.00	35.5 0	30.0 0	27.1 9	31.2 2	28.7 5	32.9 6	34.6 7
China	13.0 0	28.0 0	12.0 0	22.0 0	15.00	11.2 0	10.0 0	12.1 5	12.1 3	9.96	8.04	8.98
Korea	10.0 0	11.0 0	9.00	10.0 0	9.00	10.1 0	14.0 0	9.60	10.9 1	8.40	11.3 4	9.83
Germany	2.70	2.95	2.99	2.71	3.30	3.20	3.50	3.23	3.16	3.70	3.85	3.78
Australia	2.10	-	-	-	-	-	5.00	3.05	-	3.65	-	-
Canada	2.10	2.28	2.97	1.94	2.30	2.80	1.76	2.21	2.97	3.60	2.42	1.85
Japan	3.10	2.46	2.48	2.87	2.60	2.40	3.00	3.65	2.44	3.00	2.23	3.33
UK	-	-	-	-	-	-	-	-	-	2.75	2.91	3.40
Italy	-	-	-	1.30	2.02	1.76	-	-	-	2.22	-	-
India	-	-	-	1.70	-	-	1.50	-	-	2.10	-	-
France	2.70	1.74	-	2.10	3.94	5.60	6.00	4.07	2.31	-	1.83	1.96
Russia	-	-	-	-	-	-	-	2.40	-	-	1.96	-
Poland	-	-	-	-	-	-	-	-	2.24	-	-	-
Romania	2.20	1.45	2.50	-	-	1.72	-	-	1.98	-	1.96	1.96
Venezuela	-	-	-	-	-	-	-	-	-	-	-	-
Brazil	2.70	3.97	2.39	-	1.60	-	-	-	1.98	-	-	-
Sweden	-	-	-	-	-	-	-	2.04	-	-	-	-
Thailand	-	-	-	-	-	-	1.50	-	-	-	-	-
Malaysia	-	-	-	-	2.60	-	-	-	-	-	-	-
Spain	-	-	2.45	-	-	-	-	-	-	-	-	-
Argentina	-	1.78	2.36	-	-	-	-	-	-	-	-	-
Netherlands	-	-	-	1.50	-	1.65	-	-	-	-	-	-
Taiwan	-	-	-	-	-	-	-	-	-	-	-	2.19

⁵⁷ <http://www.antiphishing.org/phishReportsArchive.html>

Table 7⁵⁸: Top 10 Phishing Sites Hosting Countries

Country	2006												07
	Jan.	Feb	Mar	Apr	May	June	July	Aug	Sep.	Oct	Nov.	Dec.	Jan
USA	36.57	37.48	35.13	26.30	34.10	35.57	29.85	27.88	31.22	28.87	24.20	24.70	24.5
China	8.98	18.14	11.93	21.20	15.00	15.00	12.00	14.00	12.00	11.96	15.42	14.24	17.2
Korea	7.70	8.89	8.85	7.20	8.17	10.17	13.34	9.59	8.90	8.40	14.88	15.72	11.0
Germany	3.75	2.95	3.57	2.80	3.38	3.20	3.32	3.23	3.17	3.70	5.27	4.08	3.64
Australia					-	-	4.56	3.06	-	3.64	-	-	-
Canada	2.06	2.29	3.52	1.90	2.37	2.84	1.78	2.22	2.97	3.60	-	3.06	4.05
Japan	2.80	2.47	2.39	2.90	2.65	2.34	3.04	3.66	2.44	3.01	-	1.74	2.41
UK	2.10				-	-	-	-	-	2.75	2.04	2.71	1.67
Italy	-			1.40	2.02	1.73	1.52	-	-	2.22	-	1.67	-
India	-			1.70	-	1.66	-	-		2.11	-	-	-
France	2.37	1.75		2.20	3.94	5.67	5.87	4.07	2.31	-	1.83	2.15	2.33
Russia	-				-	-	-	2.46			2.64	1.67	2.15
Poland	-		-		-	-	-	-	2.24	-	-	-	-
Romania	1.62		2.29		-	1.72	-	-	1.98	-	2.84	-	-
Venezuela	-		-		-	-	-	-	-	-	1.81	-	-
Brazil	-	3.19	1.97		1.70	-	-	-	1.98	-	1.43	-	1.90
Sweden	-		-		-	-	-	2.04	-	-	-	-	-
Thailand	-		-		-	-	1.59	-	-	-	-	-	-
Malaysia	-		-		2.59	-	-	-	-	-	-	-	-
Spain	-		2.13										
Argentina	-	1.75	1.92										
Netherlands	-	-	-	1.50									
Taiwan	2.68	-	-										

⁵⁸ <http://www.antiphishing.org/phishReportsArchive.html>

Table 8: List of 10 top brands affected by Phishing during Number of 2003, 2004, 2006, 2007

Company	2003		2004		2006			2007				
	No v	De c	Ja n	Feb	Oct.	Nov.	Dec.	Jan	Feb	Mar	Apr	May
eBay	06	33	51	104	1210	852	1020	1423	796	986	2002	5310
Citibank	06	17	35	58	-	48	30	120	-	-	-	-
Paypal	04	06	10	42	1493	1043	2223	2693	2511	2227	4556	2934
AOL	04	16	34	10	-	-	-					
Fleet Bank	01	02	02	9	-	-	-					
EarthLink	02	04	09	8	-	-	-					
VISA	01	02	02	8	-	-	-					
Barclays	00	01	01	6	321	1733	1334	1972	421	335	227	78
Yahoo	00	01	02	4	-	-	-					
Bank One	00	00	00	3	-	-	-					
Fifth Third Bank					203	458	834	1302	1182	-	91	-
Bank of America Corporation					188	161	780	1048	507	536	292	226
Volksbanken Raiffeisenba nken					191	117	311	379	208	-	-	-
Wells Fargo					133	399	299	233	97	161	88	41
JP Morgan Chase & Co					104	308	153	643	167	161	84	70
HSBC Group					---	-	132	149	-	-	-	-
US Bank							61	-	-	209	32	-
Key Bank					111	28	-					
Regions Bank	-	-	-	-	-	-	-	-	150	-	-	143
Capital One								-	91	96	-	-
Branch Banking & Trust Company	-	-	-	-	-	-	-	-	-	221	471	131
Wachoria	-	-	-	-	-	-	-	-	-	139	47	-
National City	-	-	-	-	-	-	-	-	-	-	-	183
Poste Italiane	-	-	-	-	-	-	--	-	-	-	-	146

Source: <http://www.phishtank.com/stats/2007/01/>

CONCLUSION

There is a sharp rise in phishing statistics as it evident from the values in various tables. May it be number of hosting of phishing sites, or mails received about phishing, monetary loss either of the customers or of organizations. The main reason for losses/success of frauds is ignorance on part of customer as well as service providers (bankers,

ISPs, retailers etc). It requires stringent methods of educating customers and regular review of security related information of individual customers. For example:

- i. Customer should not be allowed to be the customer of financial institutions unless they read security related concern properly and provide a proof to the institutions that they are aware of security concerns. This could be done by pushing terms and conditions of being customer in pieces and unless customer runs through all pieces of information his/her application should not be accepted for being a customer. It will certainly act as an stumbling block to have more customer but new innovative methods can be devised so that customer did feel heat of these measures.
- ii. Let us take an example of ICICIdirect.com web sites in India. It has policy, which forces its clients changing of password after 15 days. It start reminding the customer that within next two days customer had to change password otherwise transactions will not be allowed. It is being followed at ICICIdirect.com religiously. But at the same time if one operate his/her saving bank account with ICICI Bank, he/she can continue with his/her password, which is only of four digits for ever. The question is why not the same policy for saving bank or any other account of the bank.
- iii. There are many cases reported in the past with reference to inadequate characters of password in terms of sequencing and number. The institutions may devise a policy of secure password in terms of sequencing the characters or characters it self. In addition, policy must take care of size of the security related data. In addition, institution may analyze the pass word data base on regular interval for inadequacy and it may be communicated to the customers on real time basis.
- iv. International fund/ large fund transfers should not be on real time basis. As a part of term and conditions, customers must be informed before the transfer take place. Duration of execution of the transaction may be 24 hours/36 hours or as deemed fit by the financial institution.
- v. The information on incidents of phishing or similar serious crime should be made available to the citizens as early as possible and also out come of judicial process. In addition, new regulations must be made available through electronic means to all the citizens/ customers.
- vi. Many organizations (Software developers or implementers) have developed anti-phishing solutions, the usage of these security tools may be encouraged through regulations. In addition, small organizations should be supported by states in making their electronic transactions secure.
- vii. There is a need for better, easy to use and cost effective methods of authentication of customer transactions.
- viii. To fight phishing, institutions must adopt a multi-pronged approach with minimum four components. (a) usage and development of new technologies to counter frauds, (b) educating customers with riders every where, (c) helping law reinforcement agency by way of providing information of the incidents, and (d) proper and regular stringent audit of online systems.

References

Anderson, R. (2007). Closing the Phishing Hole – Fraud, Risk and Non-banks, <http://www.cl.cam.ac.uk/~rja14/Papers/nonbanks.pdf>

Baker, T.D. (2006). New email-based bank fraud via VOIP services, 07/21/06, http://www.xeal.com/blog/index.php/2006/07/21/new_email_based_bank_fraud_via_voip_serv

BBC (2006a). Online banking fraud rises fast, Tuesday, 7 November 2006, 00:04 GMT, <http://news.bbc.co.uk/1/hi/business/6122116.stm> (Accessed on 07.04.07).

BBC (2006b), Online banking fraud 'up 8,000%', Wednesday, 13 December 2006, http://news.bbc.co.uk/2/hi/uk_news/politics/6177555.stm, (Accessed on 07.04.07).

Bennett, N. (2006). Need for stronger authentication, June, 2006 <http://www.networkmagazineindia.com/200606/vendorvoice01.shtml>

Business News (2007). India in the list of 10 top countries hosting phishing websites, <http://in.news.yahoo.com/070216/203/6c73r.html>

Chan, T. (2004). HK\$660,000 stolen in e-bank scam, October 8, http://www.chinadaily.com.cn/english/doc/2004-10/08/content_380368.htm

Chauki, M. (2006). Phishing in Cyberspace: Issues and Solutions, <http://www.crime-research.org/articles/phishing-in-cyberspace-issues-and-solutions/>

Cherian, J. (2007). Phishing up 180% in India, <http://www.allheadlinenews.com/articles/7006315133>

Colley, A. (2004). "Most devious" bank email phishing scam discovered, 4 March, <http://www.silicon.com/software/security/0,39024655,39118902,00.htm>

Corporate Bureau (2005). 74% IT managers receive phishing attacks, http://www.financialexpress.com/fe_full_story.php?content_id=98848 (Accessed on 08.04.07).

Costello, T (2004). Crooks clean out couple's online bank account, December, 14, <http://www.msnbc.msn.com/id/6713753/>

Devillard, A. (2006). The "phishing" in France, few victims but a growing threat, <http://translate.google.com/translate?hl=en&sl=fr&u=http://www.01net.com/article/311785.html&sa=X&oi=translate&resnum=1&ct=result&prev=/search%3Fq%3DPhishing%2Bin%2BFrance%26hl%3Den>

Dinham, A. (2004). AU regional bank signs up for anti-phishing tokens, <http://www.zdnet.com.au/news/security/soa/AU-regional-bank-signs-up-for-anti-phishing-tokens/0,130061744,139152762,00.htm>

Dunn, J.E. (2007). Do-it-yourself phishing kit available online, January,15, <http://www.pcworld.in/news/index.jsp/artId=4915203>

Espiner, T. (2007). Phishing overtakes viruses and Trojans, January, 31, <http://zdnetindia.com/news/security/stories/169631.html>

Evers, J. (2007). New tools enables sophisticated phishing scams, January 11, <http://zdnetindia.com/news/security/stories/167392.html>

Frederick Stakelbeck, Jr. (2005). China and e-Banking, www.inthenationalinterest.com/Articles/November2005/November2005Stakelbeck.html

Ghosh, A. (2007). Banks alert to online fraud, to stay ahead of phishers, The Economic Times, New Delhi Friday 6 April, 2007.

Gold, S. (2007). Phishing incidents soaring - in India, January, 31, <http://securityblog.itproportal.com/?p=698>

Gooden, Dan (2007). Man hijacks 90 eBay accounts, March 21st, http://www.theregister.co.uk/2007/03/21/ebay_hijack_plea/

Hall, B. (2007). Phishing Out Internet Banking Fraud, January 29, <http://ezinearticles.com/?Phishing-Out-Internet-Banking-Fraud&id=435269>.

ITU (2005). Research On Legislation In Data Privacy, Security And The Prevention Of Cyber-crime, http://www.itu.int/ITU-D/e-strategies/e-legislation/Doc/Cybercrime_M_Menting.pdf

Jaques, R. (2006). Phishing scams push up web banking fraud losses, 8 November 2006, <http://business.pcauthority.com.au/news/67988,phishing-scams-push-up-web-banking-fraud-losses.aspx>

Jeremy Kirk (2006). Online banking fraud dramatically jumps in the U.K, November 08, 2006, http://www.computerworld.com/action/article.do?Command=viewArticleBasic&articleId=9004889&intsrc=article_more_bot.

John, P. (2006). Other banks caught in phishing net too, February 12, http://www.indusfaceconsulting.com/corporate/12feb06_news.htm

Kasbekar, M. (2007). How thieves rob you online, January 20, <http://inhome.rediff.com/money/2007/jan/20thief.htm>

Kaur, J. (2005). Are You Being Phished?, <http://www.dqindia.com/content/enterprise/2005/105060702.asp>

Kobayashi-Hillary, M. (2006). Data theft scandal - what we can learn from India, <http://services.silicon.com/offshoring/0,3800004877,39163049,00.htm?r=2>.

Krupp, P. (2007). Banks should divulge phishing details to the customers, January 4, http://www.cxotoday.com/India/Editors_Speak/Banks_should_divulge_phishing_details_to_customers/551-78253-904.html

Kumar, D. (2007). `Phishing' for trouble, Jan 20, 2007, <http://www.hindu.com/thehindu/mp/2007/01/20/stories/2007012000380200.htm>

Leyden J. (2005). Brazilian cops net 'phishing kingpin', March 21, http://www.theregister.co.uk/2005/03/21/brazil_phishing_arrest/

Leyden, J.(2006a). AOL sues mystery phishers for \$18m, March 1, http://www.theregister.co.uk/2006/03/01/aol_phishing_lawsuits/.

Leyden, J. (2006b). Phishing fraudsters offer cash reward, 14th March, <http://play.tm/wire/click/824881>

Libbenga, J. (2006). German Postbank uses e-signatures to curb phishing, April, 7, http://www.theregister.co.uk/2006/04/07/postbank_curbs_phishing/

Libbenga, J. (2007). Phishers haul in money from Nordic bank, January, 19, http://www.theregister.co.uk/2007/01/19/phishers_attack_nordea/

Lihle Mtshali (2007). Rise in online banking fraud, 29 March 2007, <http://www.sundaytimes.co.za/News/Article.aspx?id=424637>.

Lohman, T. (2006). NAB hit by phishing scam, March 9, <http://www.itnews.com.au/newsstory.aspx?CIaNID=30742>

Matthew B. (2006). Firefox 2 Tops IE 7 in Anti-Phishing Study, November, 16 <http://www.pcworld.in/news/index.jsp/artId=4685844>

McMillan, R. (2006). Consumers to Lose \$2.8 Billion to Phishers in 2006, November 09, <http://www.pcworld.com/article/id,127799-pg,1-RSS,RSS/article.html>

Miller, R. (2006). Chinese Bank's Server Used in Phishing Attacks on US Banks, InfoSec News, Sun, 12 Mar 2006, http://news.netcraft.com/archives/2006/03/12/chinese_banks_server_used_in_phishing_attacks_on_us_banks.html.

Miller, R. (2007). Phishing attacks continue to grow in sophistication. http://news.netcraft.com/archives/2007/01/15/phishing_attacks_continue_to_grow_in_sophistication.html

Mulherkar, J. (2006). How to escape phishing in online banking, February 15, 2006, <http://in.rediff.com/getahead/2006/feb/15bank.htm>

Nair, V.P. (2004). However careful you are..., Jul 12, 2004, <http://www.blonnet.com/ew/2004/07/12/stories/2004071200010100.htm>

Nayak, A. (2007). Identify thefts & "phishing" within Indian BPO employees, <http://www.bpoindia.org/research/identity-theft-indian-bpo.shtml>

News (2003). Spyware bank frauds uncovered in US and South Africa, <http://www.finextra.com/fullstory.asp?id=9511>

Norah, L. (2004). Phishing gang arrested in Germany, December, 18, <http://itvibe.com/news/3094/>

O'Brien, C. (2006a). BoI Customers fall victim to phishing scam, August, 17, http://www.theregister.co.uk/2006/08/17/boi_phishing_attack/

O'Brein, C. (2006b). Bank of Ireland coughs up for phishing victims, September, 8, <http://www.silicon.com/financialservices/0,3800010322,39162206,00.htm>

OUT-LAW News (2006). FSA blames phishing for growth of online banking fraud, 18/12/2006 <http://www.out-law.com/page-7582>.

PC Tools News (2006). PC tools issues Internet fraud warning after Swedish bank loses \$ 1.5 Million, Janury, <http://www.pctools.com/news/view/id/159/>

Pradhan, P. (2007). Survey shows on line banking needs changes, January, 29 <http://www.tech2.com/india/news/general/survey-shows-online-banking-needs-changes/3987/0>

Reuters (2007). Online banking fraud soars 44 per cent – APACS, March, <http://www.pcpro.co.uk/security/news/107226/online-banking-fraud-soars-44-per-cent-apacs.html>

Reuters (2004). "Phishing" scam now lures German banking clients, August, <http://in.tech.yahoo.com/040826/137/2fpm6.html>

Robert, P.F. (2005). UK Phishers Caught, Packed Away, <http://www.eweek.com/article2/0,1895,1831960,00.asp>

Rondganger. L. (2007). Online bank fraud hits three banks, 27 March 2007 at 11h00, http://www.ioltechnology.co.za/article_page.php?iSectionId=2885&iArticleId=3752066 (Accessed on 07.04.07).

Rupert J. (2007). Good catches for 'phishing' fraudsters as losses through fake bank websites leap 44% to £34m, March 14, 2007, <http://business.guardian.co.uk/story/0,,2033243,00.html>

Saytarly, T (2004). Phishing costs \$20 000 000 for Russian businesses, October 14, <http://www.crime-research.org/news/14.10.2004/707/>

Secure Science Corporation (2003). Banking Scam Revealed, November 13, <http://www.securityfocus.com/infocus/1745>

Sullivan, B. (2004a). Survey: 2 million bank accounts robbed, ET June 14, 2004
<http://www.msnbc.msn.com/id/5184077/>

Sullivan, B. (2004b). Online bank fraud concerns consumers, ET Dec. 14, 2004
<http://www.msnbc.msn.com/id/6713033/>

Thomas D. (2005). Phishers jailed over £6.5m identity fraud, June,
<http://www.vnunet.com/computing/news/2139095/phishers-jailed-identity-fraud>

Thomas, D. (2006). Phishing attacks against Europeans drop, 14 June, 2006,
<http://www.computing.co.uk/computing/news/2158229/phishing-attacks-against>

Titus, D. and Roy, S. (2005). Phishing on the Net,
<http://www.asialaw.com/default.asp?page=14&ISS=16853&SID=518004>

Vusumuzi Ka Nzapheza (2007). Number of 'phishing' victims jumps 20%, 08 March 2007
at 05h00, [http://www.ioltechnology.co.za/article_page.php?iSectionId=2885 &
iArticleId=3720753](http://www.ioltechnology.co.za/article_page.php?iSectionId=2885&iArticleId=3720753), (Accessed on 07.04.07).

Young, T. (2007). Online fraud losses increase 55 per cent, 07 November,
<http://www.computing.co.uk/computing/news/2168086/apacs-figures-show-rise-online>.

Zoheb, Hossain (2007). Hook, line and sinker- Beware of phishing,
www.indlaw.com/publicdata/articles/article218.pdf

Zvomuya, P. (2007). How to combat bank fraud, [http://www.mg.co.za/personalfinance/
articlePage.aspx?articleid=297928&area=/personal_finance/pers_fin_banking/](http://www.mg.co.za/personalfinance/articlePage.aspx?articleid=297928&area=/personal_finance/pers_fin_banking/)