Phishing Attacks and Perceptions of Service Quality: An Analysis of Virtual Banking in India

*Amitabh Verma

*Assistant Professor, Department of Management, Birla Institute of Technology, Mesra, Ranchi (Jharkhand), India

Abstract

Virtual banking has revolutionized the banking industry making transactions faster and more convenient. But security issues present a pressing concern. Even with the best supervisory and security devices losses may occur. This article will present and discuss Virtual banking service quality and a relationship to their customers. It examines which dimensions bank service qualities are problematic and/or inadequate, in cases where customers are having Internet fraud problems. The basic contribution of this article is to present facts about the areas where the basic actions of the banks are insufficient when customers have identity theft problems in virtual banking within the security dimension. The article consists of two main sections. In the first section, the terms and concepts used in the study are explained; security, phishing attacks and Internet banking. In the second section, a content analysis is made to reach the determined goal and the results are evaluated. The article is based on interviews with representatives from the Indian banks and theories from researches within the field. The result from the studies indicate several aspects showing that the interviewed bank branches have implemented the main part of the theories but may further improve their virtual banks. If banks wish to maintain high service quality online they must put more effort into their Virtual banks. These statements should be investigated further to assess the most suitable and applicable measurements for each banks specific situation and need. In virtual banking, which is a trust-based system, phishing attacks and Internet fraud can affect the customers’ view of the service quality provided by the banks. Theft of the customers’ personal identity information can cause the customers to lose their confidence in the system and their banks. Within this context, content analysis was used to develop an examination of the complaints of 100 Indian bank customers. The present analysis only contains the customers who had experienced money transfer problems a result of Internet fraud. The results obtained provide some suggestions for the banks on how to approach customers who have experienced such problems, and the things they should provide in terms of customer care services. Consequently, the article is able to provide information on customer service elements that need specific attention in the future.

Keywords: Internet Banking; Phishing Attacks; Internet Fraud; Security

1. Introduction

Virtual banking was first introduced in the United States of America (USA) in the early 1990s and it has since extended globally gradually. Virtual banking is a product of e-commerce in the field of banking and financial services. It offers different online services like balance enquiry, requests for cheque books, recording stop-payment instructions, balance transfer instructions, account opening, settlement of online credit card transactions resulting from online shopping and other forms of traditional banking services. Mostly, these are traditional services offered through internet as a new delivery channel. But, in the process it has thrown open issues which have ramifications beyond what a new delivery channel would normally envisage and, hence, has compelled regulators world over to take note of this emerging channel. Phishing action has important implications for
security, which is an important sub element of service quality. Although security is normally thought of in terms of the bank's system, the failure of the customer's Internet usage can also produce security problems. Therefore security has a two-sided structure. Information technology has been one of the driving forces in the changes that have occurred in trade and economy. Global trade is fifty times bigger today than 1950 and it continues to grow. Information Technology, IT, is the use of computer hardware and computer software to store, convert, process, retrieve, transmit and protect information. Technology has become more accessible, cheaper and easier to use, which has had a significant impact on the world's trade and commerce. With the introduction of the Internet and the World Wide Web companies acknowledged IT as a tool to do business while consumers acknowledged it as not only an opportunity to purchase goods and services but also to obtain information. This has led to the development of the new phenomenon of the 21st century, which is known as the electronic commerce. "Electronic commerce, e-commerce, is simply any business transaction that takes place via digital processes over a network.". E-commerce is a rapidly growing industry, which has and still changes economy, markets and industry structures. It has also altered products and services and their supply chains, but also consumer behaviour and the labour market. Many service industries have changed their ways of doing business because of the e-commerce; one of these service industries is the banking industry. Banks have made most parts of their services and business accessible online, called Virtual Banking. It is the term used for new age banking system. It is also called as online banking and it is an outgrowth of PC banking. Virtual banking is a result of explored possibility to use internet application in one of the various domains of commerce. It is difficult to infer whether the internet tool has been applied for convenience of bankers or for the customers' convenience. But ultimately it contributes in increasing the efficiency of the banking operation as well providing more convenience to customers. Without even interacting with the bankers, customers transact from one corner of the country to another corner. Virtual Banking has had great impact on the banking industry and the online competition between the banks has increased. Banks need to develop creative solutions of how to make full use of the new technology and how to provide their customers with high online service quality. When lacking face to face interaction banks must increase the experienced online service quality among customers in order to attain and sustain competitive advantages and customer relationships.

There are many advantages of Virtual Banking. It is convenient, it isn't bound by operational timings, there are no geographical barriers and the services can be offered at a minuscule cost. Virtual banking has experienced explosive growth and has transformed traditional practices in banking (Gonzalez et al., 2008). Private Banks in India were the first to implement virtual banking services in the banking industry. Private Banks, due to late entry into the industry, understood that the establishing network in remote corners of the country is a very difficult task. It was clear to them that the only way to stay connected to the customers at any place and at anytime is through internet applications. They took the internet applications as a weapon of competitive advantage to corner the great monoliths like State Bank of India, Indian Bank etc. Private Banks are pioneer in India to explore the versatility of internet applications in delivering services to customers.

As per prediction of Broadie et al (2007) Virtual banking is leading to a paradigm shift in marketing practices resulting in high performance in the banking industry. Delivery of service in banking can be provided efficiently only when the back ground operations are efficient. An efficient back ground operation can be conducted only when it is integrated by an electronic system. The components like data, hardware,
software, network and people are the essential elements of the system. Banking customers get satisfied with the system when it provides them maximum convenience and comfort while transacting with the bank. Internet enabled electronic system facilitate the operation to fetch these result.

An in-depth analysis would help to understand that internet enabled electronic bank system differentiates from traditional banking operation through faster delivery of information from the customer and service provider. Additionally, it has to be noted that the banking operations does not transfer physical currencies instead it transfer the information about the value for currencies. Virtual Banks enable transfer of information more swiftly on-line. In service organizations like banks, information flows more than physical items. In the commercial world, especially in most advanced societies today, money is rather carried in information storage medium such as cheques, credit cards and electronic means that in its pure cash form. According to Christopher et al (2006), E banking has become an important channel to sell the products and services and is perceived to be necessity in order to stay profitable in successful.

The perception is the formed as a result of interpreting the experience. There is a growing interest in understanding the users’ experience (Hiltunen et al., 2002 ); as it is observed as a larger concept than user satisfaction. From this perspective, assessing the user experience is essential for many technology products and services (Wilson & Sasse, 2004).

2. Service Quality

Customers have started perceiving the services of bank through internet as a prime attractive feature than any other prime product features of the bank. Customers have started evaluating the banks based on the convenience and comforts it provides to them. Bankers have started developing various product features and services using internet applications. A number of scales available for measuring service quality. When the design and application of those scales is examined (Grönroos, 1985; Parasuraman et al., 1985) ten main elements of technical and functional service quality can be identified – access, communication, competence, courtesy, credibility, reliability, responsiveness, security, tangibles, understanding/knowing the customer. This kind of analysis of service quality into elements also has a highly dimensional and hierarchical aspect. Grouping these elements together, the customer interprets the service quality in terms of outcome, interaction and environmental dimensions (Brady and Cronin, 2001). These are ways of showing personal attention to the customer. Displeasing the customer in relation to service quality will naturally increase negative responses from customers and put pressure on the complaint mechanisms. Once the formal complaint mechanism has been invoked, the feedback mechanism is important. The feedback and complaint mechanisms can be seen as part of the convenience/accuracy dimension (Joseph et al., 1999), and this dimension is expected to develop appropriate answers to customer problems. It should be noted that conventional and technological service quality dimensions can change. Complaints about the service quality dimensions are a determining factor. The interpretation of service quality goes hand-in-hand with the customers’ expectations of the service. Therefore, the customers’ expectations of Virtual banking are the driving force behind service quality.

It has been shown that the users entering the Virtual banking system want to have more financial control of economic factors (Devlin and Yeung, 2003), and that an important proportion of the customers using electronic banking would switch to Virtual Banking provided that appropriate incentives, such as interest rates, are
provided (Sciglimpaglia and Ely, 2002). Broderick and Vachirapornpuk (2002) reported in their narrative analysis that the expectations of the customers from virtual banking are based on earning money, effective and fast money transfer and price tolerance, and also that the organization should be proactive in the context of service encounters. On the other hand, Yan and Paradi (1998) argued, on the basis of their studies, that the banks should activate their transaction based services as part of their Internet services, and at the same time the customers should respond quickly to technological developments, otherwise they will lose their compatibility strengths. Snellman and Vithkari (2003) compared conventional service encounters with technology-based service encounters and Internet banking; they found that complaints were much higher than in conventional encounters, and the complaints about SST are made up complaints relating to failure of the service period and customer-based failures. In their studies of the service quality in Virtual banking, Siu and Mou (2005) identified four factors; credibility, security, problem solving and efficiency.

In particular, where the comments relate to the perceived inefficiency of the bank, the dissatisfaction of the customer during the service period may change his or her entire perception of the bank. Illegal actions like phishing, which is an external effect which cannot be controlled by the customer, will affect the customer’s view of his or her bank and virtual banking service quality dimensions in a negative way.

3. Security Issues

Security is one of the most important issues of service dimensions, which can cause the customer to be in doubt even while using the virtual banking system (Patricio, 2003, p. 475) and it is correlated with the concept of trust. The security aspect of Virtual banking consists of three systems: the bank, the Internet and the user’s own computer (Hutchinson and Warren, 2003). These systems illustrate the distribution of service quality. Jun and Cai (2001) argue that Virtual banking service quality can be based on three main elements (customer service quality, online system quality and banking service product quality) and they show reliability is an aspect which can cause dissatisfaction for the user. There is a strong relationship between a secure operation, protection of personal information, and a low level of perceived risk (Yang et al., 2004). Polatoglu and Ekin (2001) in their research observed that customers using Virtual banking for a long period of time without experiencing problems (reliability, security and privacy) have a higher degree of satisfaction. Liao and Wong (2007) argued that perceived security has a positive effect on customers’ relations with e-banking, and that in order to remove the security risk it is necessary to create personal confidence and continuously to improve the banks’ security system. Rose (2000) has also dealt with security and customer service aspects of online banking systems Therefore, security is an important Virtual banking concept, and it is one of the Virtual banking quality factors.

Laforet and Li (2005), in their studies, discovered significant security differences between those using online banking and those who are not, and emphasized that the hackers and fraud aspects are important for the non-users. Kaynak and Harcar (2005) observed that security problems are the most important reason given for not using Virtual banking. Their results show that security problems, like hackers and fraud, are determining aspects in Internet service presentation. In this concept, trust and security are factors supporting a positive view of virtual banking service quality. As mentioned earlier, the customers’ trust of virtual banking is important and is a variable which has an effect on their view of service quality (Jayawardhena, 2004; Yüksel, 2005). Trust is a variable which has a significant
effect on the customer’s approach toward virtual banking and tendency to use Internet banking (Han and Suh, 2004). Therefore when this trust is reduced, whether or not this is the customer’s own fault, his or her attitude toward his or her bank will change in this concept, phishing has a structure, which can change the customers’ interpretation of service quality as far as virtual banking is concerned.

However, today the term Phishing has evolved to encompass a variety of attacks that target personal information. Along with an increase in the number of potential targets, there are three major factors that criminals have been able to take advantage of:

**Unawareness of threat** - If users are unaware that their personal information is actively being targeted by criminals, they may lack the perspective needed to identify phishing threats and may not take the proper precautions when conducting online activities.

**Unawareness of policy** - Phishing scams often rely on a victim’s unawareness of organizational policies and procedures for contacting customers, particularly for issues relating to account maintenance and fraud investigation. Customers unaware of the policies of an online merchant are likely to be more susceptible to the social engineering aspect of a phishing scam, regardless of technical sophistication.

**Criminals’ technical sophistication** - Criminals conducting phishing scams are leveraging technology that has been successfully used for activities such as spam, distributed denial of service (DDoS), and electronic surveillance. Even as customers are becoming aware of phishing, criminals have responded with technical tricks to make phishing scams more deceptive and effective.

4. Authentication Mechanisms

The banks’ authentication mechanisms are fixed passwords, dynamic passwords, digital signature, challenge/response scheme, and hardware token applications (Claessens et al., 2002, 259-261). The customer can do his or her Virtual banking operations from anywhere using a password; and a password does not maintain sufficient protection from Internet frauds like phishing. Therefore two more authentication systems are needed (Zin and Yunos, 2005). For those customers who have lost their identity due to phishing, a loss of confidence will take place, and therefore the service encounters need to find solutions for protecting the user (Litan, 2004; Schneier, 2004). When bank administrators are interviewed about this subject, they think that it is important to make the customers more aware of the problem, and since the attackers keep changing their methods, banks should take a more active role to find solutions (McKenna, 2004). Kirda and Kruegel (2006) state that one of the reasons for the increase in phishing attacks is the lack of experience and lack of sophistication of the Internet user. If looked at from a social-physiological point of view, the customers are convinced by the phishing attackers (Rusch, 1999). If one thinks of this period where the customer is convinced as one of thoughtlessness, six basic factors can be seen (Rusch, 2002): flow, context confusion, arousal and repetition, distraction, claims of authority, and confirmation bias. An important factor here is the existence of, and connection to, an exchange of messages between the user and the foundation. Therefore, although
it is due to his or her own fault or technology, his or her attitude towards the foundation will change.

5. Account Hijacking: Phishing

At this point, it is important to deal with the subject of illegal approaches to users’ Internet accounts. Account hijacking involves the unauthorized access to and misuse of existing bank accounts and this action includes the following (Beaumier, 2006:34): **Hacking, Phishing, Pharming and keystroke logging**. Among the illegal actions threatening the banks, the most important one is **Phishing Actions** and related activities. The act of tricking individuals into divulging their sensitive information and using it for malicious purposes is not new. The term “phishing” has origins in the mid-1990s, when it was used to describe the acquisition of internet service provider (ISP) account. Before widespread use of the internet, criminals used the telephone to pose as a trusted agent to acquire information. In particular, phishing attacks have shown a significant increase in recent years ([www.antiphishing.org](http://www.antiphishing.org)). It is a problem of authentication for the banks. Fraudsters have two ways of evading authentication methods in virtual banking (Hiltgen et al., 2006, p. 21): offline credential-stealing attacks, and online channel-breaking attacks. In the phishing application, an email claiming to be from the customer’s bank is sent to the user and he or she is asked to approve personal information (Hicks, 2005, p. 29). Pharming directs the person to a website which looks like the bank’s official site, and obtains information from the person. Even those who do not provide the information are under threat because the e-mail contains a virus ([US Netizen, 2005](http://www.usnetizen.org)). A phishing period starts with an e-mail sent to the user. The incoming mail may be filtered using a spam filter, but if it is not filtered three options are open to the one doing the phishing (Tally et al., 2004); trojan software, a decoy asking for some operations to be done, and using spy ware which blocks the operations between the customer and the company, and collects user information instead. These actions are computing environment crimes. Within these crimes, electronic funds may be transferred, or identities may be stolen; in both situations the user’s computer is both a target and a tool (Newman and Clarke, 2002).

6. Attack Techniques

Nowadays, the nature of attacks is more active rather than passive. Previously, the threats were all passive such as password guessing, dumpster diving and shoulder surfing. Here are some of the techniques used by the attackers today:

• **Trojan Attack.** The attacker installed a Trojan, such as key logger program, on a user’s computer. This happens when users visited certain websites and downloaded programs. As they are doing this, key logger program is also installed on their computer without their knowledge. When users log into their bank’s website, the information keyed in during that session will be captured and sent to the attacker. Here, the attacker uses the Trojan as an agent to piggyback information from the user’s computer to his backyard and make any fraudulent transactions whenever he wants.

**Man-in-the-Middle Attack:** Here, the attacker creates a fake website and catches the attention of users to that website. Normally, the attacker was able to trick the users by disguising their identity to make it appear that the message was coming from a trusted source. Once successful, instead of going to the designated website,
users do not realize that they actually go to the fraudster's website. The information keyed in during that session will be captured and the fraudsters can make their own transactions at the same time.

7. Phishing Today

Originally, phishing was identified as the use of electronic mail messages, designed to look like messages from a trusted agent, such as a bank, auction site, or online commerce site. These messages usually implore the user to take some form of action, such as validating their account information. These messages often use a sense of urgency (such as the threat of account suspension) to motivate the user to take action. Recently, there have been several new social engineering approaches to deceive unsuspecting users. These include the offer to fill out a survey for an online banking site with a monetary reward if the user includes account information, and email messages claiming to be from hotel reward clubs, asking users to verify credit card information that a customer may store on the legitimate site for reservation purposes. Included in the message is a URL for the victim to use, which then directs the user to a site to enter their personal information. This site is crafted to closely mimic the look and feel of the legitimate site. The information is then collected and used by the criminals. Over time, these fake emails and web sites have evolved to become more technically deceiving to casual investigation. Recently the definition of phishing has grown to encompass a wider variety of electronic financial crimes. In addition to the widespread use of these fake email messages and websites to lure users into divulging their personal information, I have also observed an increase in the amount of malicious code that specifically targets user account information. Once installed on a victim's computer, these programs use a variety of techniques to spy on communications with web sites and collect account information. This method differs from the technical subterfuge generally associated with phishing scams and can be included within the definition of spyware as well. It is important to include them in a discussion on phishing trends for the following reasons:

Social component – Criminals often use social engineering along with vulnerabilities in applications such as web browsers or email clients to trick users into installing malicious code on their computer.

Common infrastructure – We have observed the use of common tools and techniques for delivering phishing emails and distributing malware. These include the use of botnets, open mail relays, and compromised web sites to host phishing sites and malware.

The big picture - As countermeasures are implemented to thwart one method of stealing information, criminals still have additional opportunities available to them. It is important to understand the technical capabilities available to these criminals so that more effective measures for protecting customer information can be developed and law enforcement personnel tasked with tracking down and prosecuting criminals conducting phishing scams can be more effective.

Brands and Legitimate Entities Hijacked by Email Phishing Attacks-1st Half

Phishers continue to expand the number and kind of brands they attack – and to employ fast-flux schemes to relocate phishing servers from one compromised host to another. Both techniques seek to maximize the longevity of phishing attacks: the
former to prey on companies inexperienced in neutralizing campaigns and the latter to continually relocate phishers’ counterfeit web sites and make them harder to take off line.

**Most Targeted Industry Sector**

The proportion of phishing campaigns directed against the Payment Services sector continued increasing through Q2, up some 16 percent from quarter to quarter, while the Financial Services sector’s proportion dropped more than 10 percent during the same period. Generally, over the half, the proportion of crimeware-specific malicious code (designed specifically against financial institutions’ customers) and data-stealing malware receded as the proportion of other kinds of malware rose during this period.

### 8. Internet Banking Security

<table>
<thead>
<tr>
<th>Scanned Computers</th>
<th>20,399,717</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infected Computers</td>
<td>11,118,809</td>
</tr>
<tr>
<td>Non Infected Computers</td>
<td>9,280,908</td>
</tr>
<tr>
<td>Banking Trojans / Password</td>
<td>507,295</td>
</tr>
<tr>
<td>Downloaders</td>
<td>133,223</td>
</tr>
</tbody>
</table>

The most important part for ensuring security while banking online is to keep your password and pin number a secret. The information pertaining to the pin number of your internet bank account and the password should not be disclosed to any unknown individual. It is also important to change your password at regular intervals. Besides this, do not respond to any e-mail or telephone call inquiring about the details of your card or card number, as no bank will contact you directly for information about your card.

The security of your personal computer is very important for safe internet banking. Therefore, always install antivirus software and software to remove spyware. Spyware can obtain information from your computer without your knowledge or consent and spread it on the net. This can compromise the security of your computer and allow hackers to access your internet bank account for carrying out unauthorized and criminal transactions. Also install updated versions of the operating system you are using. You can also install firewalls that can protect your computer from crackers by creating a barrier between your computer and the internet or network.

Checking your bank statements regularly will help you detect any transaction that has taken place without your knowledge. Any unknown transaction can indicate that someone might have access to your internet bank account. You need to be more vigilant while accessing the Internet from someone’s computer or from an Internet cafe.

While banking through the Internet, make sure that the banking session is secure. You will often get indicators like presence of ‘https://’ in the URL. Sometimes, a digital certificate can be viewed if you click on a certain key displayed in the window. In addition, always remember to completely log off, after completing the banking session. If you do not log off properly, the banking session may not be
closed, which can enable the crackers to acquire details about your internet banking.

Nowadays, the banking institutions have come up with a number of safety measures for ensuring secure internet banking. Therefore, before conducting any financial transaction with banks through the Internet, you can evaluate these security measures. Always beware of those mails that extend some lucrative offers for making easy money. Do not disclose any private information, especially related to your internet banking, unless you are sure about the authenticity of such organizations. So, following some simple and easy precautionary measures, you can ward off the threat posed by vicious crackers to the security of your internet bank account.

9 Virtual Banking in India – Guidelines

Reserve Bank of India had set up a ‘Working Group on Internet Banking’ to examine different aspects of Virtual Banking. The Group had focussed on three major areas of Virtual Banking i.e,

(i) Technology and security issues,
(ii) Legal issues and
(iii) Regulatory and supervisory issues.

RBI has accepted the recommendations of the Group to be implemented in a phased manner. Accordingly, the following guidelines are issued for implementation by banks. Banks are also advised that they may be guided by the original report, for a detailed guidance on different issues. The Reserve Bank of India has decided that the Group’s recommendations as detailed in the circulars should be adopted by all banks offering Virtual banking services, with immediate effect. Even though the recommendations have been made in the context of Virtual banking, these are applicable, in general, to all forms of electronic banking and banks offering any form of electronic banking should adopt the same to the extent relevant.

All banks offering Virtual banking are advised to make a review of their systems in the light of this circular and report to Reserve Bank the types of services offered, extent of their compliance with the recommendations, deviations and their proposal indicating a time frame for compliance. The first such report must reach us within one month from the date of this circular. Banks not offering any kind of Virtual banking may submit a ‘nil’ report.

Banks who are already offering any kind of transactional service are advised to report, in addition to those mentioned in paragraph above, their business models with projections of cost / benefits etc. and seek our post-facto approval.

Many proposals for stopping phishing attacks rely on a security toolbar that displays warnings or security-related information in the web browser’s interface. Some existing security toolbars:

11. Striking a Balance

Presently, Internet banking customers only need a computer with access to the Internet to use Virtual banking services. Customers can access their banking
accounts from anywhere in the world. Each customers is provided a login ID and a password to access the service. It is indeed easy and convenient for customers.

However, the use of password does not provide adequate protection against Internet fraud such as phishing. The problem with password is that when it has been compromised, the fraudsters can easily take full control of online transactions. In such cases, the password is no longer works as an authentication token because we cannot be sure who is behind the keyboard typing that password in.

However, easy access and convenience should not be at the expense and mercy of the security of information. This is important in order to ensure the confidentiality of information and that it is not being manipulated or compromised by the fraudsters.

There are several methods of ensuring a more secure Internet banking:

(1) Minimum Requirement: Two Factor Authentication

Based on the above method, the security measures in place are not adequate to prevent fraud. The current method of using only one factor of authentication definitely has its weaknesses. The security aspects of Internet banking need to be strengthened. At minimum, a two-factor authentication should be implemented in order to verify the authenticity of the information pertaining to Internet banking services.

The first authentication factor can be the use of passwords and the second authentication factor can be the use of tokens such as a smartcard. MyKAD is a good avenue to introduce the second factor.

The above security measures will greatly minimise incidents of Internet banking fraud. The smartcard here provides a second layer of authentication. This will stop a perpetrator even if he manages to obtain the user's password.

Intercepted passwords cannot be used if fraudsters do not have the Smartcard. Besides addressing fraudulent activities, this can instil customers' confidence in Internet banking.

Additional Requirement: Three Factor Authentication

However, for a better security, a three factor authentication process should be considered. The third authentication factor is the use of biometric such as iris or thumbprint recognition. This ascertains who one is, biologically. This method of authentication has been introduced by the Employee Provident Fund (EPF) for it members, but is limited to getting the latest statements of a member.

With a three-factor authentication a more secure method can be implemented - a password to ascertain what one knows, a token (smartcard) to ascertain what one has, and biometric recognition (for example fingerprint or thumbprint) to ascertain who one biologically is.

As such, if passwords have been compromised, fraudsters need to get through another two levels of authentication to access a customers account. Thjs would be difficult, if not totally impossible.
10. The Future

The issue of banks not being ready to realize the full benefits of Internet banking was aptly summed up by a critic, "Much of what is now on display at bank websites is an embarrassment, to put it politely. The average site has information about certain products, e-mail contacts of bank department, perhaps the Chairman's annual general meeting speech as well. A mere information booth. This is definitely not Internet banking." However, banks are working towards addressing these problems. The security issues can be tackled by having the bank's systems technologically equipped to evade operational and security risks. Reputational risks can be prevented by testing of the system before implementation, developing contingency plans (to handle system disruptions, system hackers, security lapses and virus attacks) and creating back-up facilities. Legal and cross-border risks can be avoided through proper customer identification devices, information screening techniques, periodic reviews on compliance with various laws, and gaining knowledge of various national laws (applicable) and guide the customers through their cross-border dealings. Apart from ensuring the security of the Internet-based transactions, ICICI is taking steps to overcome the other hurdles. The bank is tying up with computer manufacturers to make PCs available to customers at low prices. The bank also plans to tie-up with Sify to place its ATMs in Sify cybercafés. In 2000, ICICI opened Internet kiosks (cabins) at its ATMs to enable easy Internet access to its customers for banking. Many other banks are also adopting such practices. Analysts claim that Internet banking holds lots of potential with the emergence of growing Internet awareness among customers, integration of banking services with e-commerce service, the increasing reach of the Internet and the entry of global players in the banking sector. Even the Reserve Bank of India has come out with Internet banking related guidelines (Refer Exhibit II). With ICICI already having decided to make the Internet an integral part of its future business plans and other banks reportedly following suit, Internet banking seems poised to become an important part of the Indian banking sector in the years to come.

11 Conclusion

Phishing is a highly profitable activity for criminals. Over the past two years, there has been an increase in the technology, diversity, and sophistication of these attacks in response to increased user awareness and countermeasures, in order to maintain profitability. Users have become more aware of phishing crimes and how to identify unsophisticated phishing sites. In response, criminals are using web browser vulnerabilities and obfuscation techniques to create phishing scam pages that are more difficult to differentiate from legitimate sites; thus users can become victims even if they are aware of phishing scams. In reaction to increasing response from service providers and law enforcement, criminals are using increasing technical sophistication to establish more survivable infrastructures that support phishing activities. The key building blocks for these infrastructures are the botnets that are used to send phishing emails and host phishing sites.

References


www.aeph.in


www.aeph.in