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/*)

Phishing Attacks and Perceptions of Service Quality: A Content Analysis of Internet Banking in Turkey

First Author's Name: **Murat Hakan Altıntaş, PhD**
First Author's Title/Affiliation: **Assistant Professor, Uludag University, Faculty of Economics and Administration, Business Administration Department, Turkey**
Postal Address: **Uludag University, IIBF, Gorukle Campus, 16059, Bursa, Turkey**
Author's Personal/Organizational Website: ***iibf.uludag.edu.tr***
Email: ***mhakan@uludag.edu.tr***
Brief Biographic Description: M. Hakan Altıntaş is assistant professor of marketing in Uludag University, Turkey. His areas of interest are Consumer Behavior, Service Quality, Customer Equity and Export Marketing. His research publications include papers in journal such as Marketing Intelligence & Planning, Euromed Journal of Business.

Second Author's Name: **Necmi Gürsakal, PhD**
Second Author's Title/Affiliation: **Professor, Uludag University, Faculty of Economics and Administration, Econometrics Department, Turkey.**
Postal Address: **Necmi Gürsakal, IIBF, Gorukle Campus, 16059, Bursa, Turkey.**
Author's Personal/Organizational Website: ***http://homepage.uludag.edu.tr/~gursakal***
Email: ***gursakal@uludag.edu.tr***
Brief Biographic Description: Necmi Gürsakal is professor of Statistics in Uludag University, Turkey. His areas of interest are Chaos, Fractals, Six Sigma and Network Science.

Abstract

In Internet 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 200 bank customers. The present analysis only contains the customers who had experienced money transfer problems as

a result of Internet fraud. As a result of the study, the deficiencies in the service quality were classified into 41 basic groups, which were then arranged into and 6 dimensions. The importance of each dimension, as measured by the frequency of their occurrence, was then determined. The results obtained provide some suggestions for the banks on how to approach customers who have experienced such problems, and the things they should they provide in terms of customer care services.

Keywords: **Internet Banking; Phishing Attacks; Internet Fraud; Security, Turkey**

INTRODUCTION

A number of scales 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).

The dimensions of service quality can be observed and studied in different services fields. The banking sector is one such sector, and it is a field in which service quality is a very important part of the consumer experience. Other sectors may have different priorities for the dimensions involved in the customer service quality. Bahia and Nantel (2000) developed their own BSQ (banking service quality) scale and compared it with the SERVQUAL scale, and concluded that the model that they developed was more reliable and fits the validity criteria. The elements of their scale are: effectiveness and assurance, access, price, tangibles, service portfolio, reliability. Yavas et al. (1997) in their studies emphasized the importance of understanding the specific needs of the customers and the empathy factor in pleasing the customer. 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. The interpretation of service quality in conventional banking and Internet banking will differ. In particular, in Internet banking, dealing with serious problems and

complaints about the service quality dimensions is a determining factor. The interpretation of service quality goes hand-in-hand with the customers' expectations of the service. Therefore, the customers' expectations of Internet banking are the driving force behind service quality.

It has been shown that the users entering the Internet 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 Internet 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 Internet 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 Internet 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 Internet banking service quality dimensions in a negative way.

An extensive search of the literature failed to identify any previous article written in precisely this field.

This article aims examine which dimensions bank service quality 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 Internet banking within the security dimension. Consequently, the article is able to provide information on customer service elements that need specific attention in the future. 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.

LITERATURE REVIEW

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. Security is one of the most important issues, which can cause the customer to be in doubt even while using the Internet banking system (Patricio, 2003, p. 475) and it is correlated with the concept of trust. Jaruwachirathanakul and Fink (2005) advise that the customers' adoption of Internet banking may be increased by making them believe the system, and argue that this can be used as a push strategy. The e-trust level of the customers has an effect on the loyalty concept, although to a lesser degree than satisfaction (Ribbink et al., 2004). Such a relation expresses the conditional dependencies of customer's interpretation of Internet banking service quality.

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 online 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 Internet banking service quality. In this concept, phishing has a structure, which can change the customers' interpretation of service quality as far as Internet banking is concerned.

As mentioned earlier, the customers' trust of Internet 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 Internet 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. As far as this subject is concerned, it is necessary to pay attention to the fraud factor.

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. In particular, phishing attacks have shown a significant increase in recent years (For details, see www.antiphishing.org). 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). 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.

In the phishing attack, a typical phishing mail purporting to come from the bank asks for an update of personal information update. Although it may look legitimate, the mail is

controlled by the phisher. (Jakobsson, 2005, p. 13). 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).

Phishing is a problem of authentication for the banks. Fraudsters have two ways of evading authentication methods in Internet banking (Hiltgen et al., 2006, p. 21): offline credential-stealing attacks, and online channel-breaking attacks. 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 Internet 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.

The security aspect of Internet 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 Internet 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. Therefore, security is an important Internet banking concept, and it is one of the Internet banking quality factors.

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 Internet 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 a positive definer of

service quality (Liao and Cheung, 2005) and security control is a subject which should be worked on when the user continues to use online banking after an incident of identity theft (Smith, 2006).

Starting from this theoretical background, the research reported in the present article was carried out to show the failure points in the services in Turkey for customers using Internet banking, in the context of money transfer by identity theft.

QUALITATIVE RESEARCH

The online banking system is an active event whereby the customers make use of banking services at home or in their offices. Internet banking is generally provided by conventional banks. According to the data from the Turkish Union of Banks, the number of stable stations in the sector was 6.849 in December 2006. This number represents an increase of 15 per cent from 2003. Also, by December 2006 there were 17.441.926 people registered for Internet banking, and the active number of users was 3.367.857. Other important data from that report are shown in Table 1.

Table 1: Internet Banking Operations (2006 year - Turkey)

Operations	Number of Operations (thousand)	Operation Volume (Million YTL)
Money Transfer*	22.866	66.291
Payments	36.507	6.875
Investment	37.984	158.678
Credit Card	15.556	11.589
* Money Transfers made to third parties.		

There is a developing Internet banking sector in Turkey, and also phishing attacks are increasing. This increase in Internet banking raises the service quality of the banks, and produces improvements in customer service.

Data for the study was taken from an Internet website created by customers who had experienced Internet banking problems. The expressions of those customers who had stated that they had the problem of “money transfer from their accounts” were examined and subjected to content analysis. Certain measurement accumulations are present in content analysis. Kassarjian (1977) has identified these as word, character, item, theme and space-time. In the present research, the measurement units of ‘theme’ and ‘word’ are used as the basis for the content analysis. The expressions of 200 customers concerning the problems they had experienced were examined, taking data from 210 single spaced pages of expressions. From the analysis, 40 nodes were identified as a basis for classifying the themes and expressions (Table 2).

Table 2: Original Nodes

1. Not providing information
2. Forced answers
3. Not giving fast response
4. Not answering

5. Giving unintelligible answers
6. Not providing written answers
7. Not providing feedback
8. Not re-establishing connection
9. Making long examination of the problem
10. Not taking action on time
11. Leaving the operation unfinished
12. Slow operation time
13. Being late taking precautions
14. Inadequate operations
15. Not making examination that will please the customer.
16. Creating procedures
17. Not being able to maintain security
18. Not being helpful
19. Not helping adequately
20. Getting rid o the customer
21. Directing to other places
22. Not paying attention
23. Blaming the customer for the mistake
24. Not trusting the customer
25. Not paying enough attention to the customer
26. Insisting the customer is wrong
27. Detaining the customer
28. Leaving the customer alone with the problem
29. Blaming the customer
30. Being irresponsible to the customer
31. Making fun of the customer
32. Non-ethical behaviour
33. Insulting behaviour
34. Exhausting behaviour
35. Using wrong expressions
36. Delaying the problem
37. Not solving the problem
38. Ignoring the problem
39. Underestimating the problem
40. Not taking responsibility for the problem

The nodes identified are generally service quality factors that the customers interpret as being a contribution to the problem from the banks. Later on, these nodes were defined grouped into dimensions describing customers' interpretations of the quality of customer service (see Table III). Some of the expressions and themes examined in the research are illustrated by the following examples:

Dimension 1: Not giving information

" … I waited till evening", "… I couldn't get answer to my demands yet", "…they share the event but didn't help any more" .

Dimension 2: Working slow

"… maybe the problem will be solved but due to the

procedures…", " …also no inspection was made in the bank", " … but it was too late".
Dimension 3: Not helping
"... there is no need for me to explain about their ignorance.", " … they didn't pay attention to us".
Dimension 4: Approach to the customer
".. bank leads the problem to the customer", " .. they told me the problem might have been my fault and they couldn't help".
Dimension 5: Behaviour
"… in addition they gave me advice about the problem".
Dimension 6: Approach to the problem
"…bank stated that it didn't have any responsibility for the problem", "…they didn't take any responsibility for the problem".

The determined dimensions is a key showing in which service area the quality provided by the banks is inadequate. However, finding the relative weights of these dimensions will provide more meaningful results. If the frequencies of the six defined basic dimensions are studies, it is seen that 'approach to the customer' (25%) and 'slow working' (25%) and then 'not focusing on the problem' (21%) make up 71% of the total service quality complaints (Table 3). The percentages of 'not helping' and 'behaviour' are lower. In fact, 'behaviour' and 'not helping' are still important as far as service quality is concerned. This is due to the fact that, when the customer has a problem of Internet fraud, he or she wants the problem to be solved. Here, the customers focus on the dimensions of online system quality and customer service quality.

Table 3: Main Dimensions of Service Quality Problems

1.Information Flow (15.9 %)	**2. Approach to the customer (25.1%)**
1. Not giving information 2. Forced answers 3. Not giving fast response 4. Not answering 5. Giving unintelligible answers 6. Not providing written answers 7. Not providing feedback 8. Not re-establishing connection	1. Blaming the customer for the mistake 2. Not trusting the customer 3. Not paying enough attention to the customer 4. Insisting the customer is wrong 5. Detaining the customer 6. Leaving the customer alone with the problem 7. Blaming the customer 8. Being irresponsible towards the customer
3. Working slow (25.1%)	**4. Behaviour (7.7%)**
1. Long examination time 2. Uninviting operation 3. Slow operation time 4. Not taking action on time 5. Being late taking precautions	1. Making fun of the customer 2. Indirect threatening 3. Ineffective behaviour 4. Insulting behaviour 5. Exhausting behaviour

6. Inadequate operations 7. Not making examination 8. Giving thought to procedure 9. Security failure	6. Using wrong expressions
5. Not helping (6.2%) 1. Not being helpful 2. Not helping adequately 3. Getting rid of customer 4. Directing to other places 5. Not paying attention	**6. Not focusing the problem (20.0%)** 1. Delaying the problem 2. Not solving the problem 3. Ignoring the problem 4. Underestimating the problem 5. Not taking responsibility for the problem

CONCLUSIONS

This study aimed to study how the banks of the customers who had experienced Internet fraud problems approached those problems, from the point of view of the customers in Turkey. As a result of the content analysis made, 41 basic subjects of complaint were determined and they were classified into six factors. When the frequencies of these dimensions were observed, it was seen that 'slow working' (25.1%), 'approach to the customer' (25.1%) and the bank 'not focusing on the problem' (20%) dimensions make up of approximately 70% of the total. From this result it can be concluded that the banks should plan communications with customers relating to these dimensions, and reshape their approaches accordingly. Similarly, not providing the customer with information is another factor, which causes dissatisfaction. The customer complaints about 'not being helpful' and 'behaviour' also need to be addressed, even though these complaints are not excessive.

The security concept is a driving force for the customers of Internet banking, and at the same time is the basis of the trust concept. In this research, whether the problem is caused by the customer or by the bank, there is a customer population whose trust was damaged. Trust is also important for the loyally of the customer. Therefore, it is clear that in order not to damage the loyalty structures of the customers who had experienced Internet fraud problems, it is necessary for the banks to develop regulations about the dimensions expressed in complaints.

In Internet banking, customer awareness is a basic defence mechanism against fraud and identity theft. Therefore the financial foundations need to prepare education about the problems within this context (ffiec.gov). Also, as Gonzales et al. (2004) advise, action plans in the QFD context need to be developed, including evaluation teams, free telephone help lines, customer feedback and IT development. Internet banking is also an extension of the customers' online behaviour. Security has an important place within this behaviour. Within the online customer experience period, an effective behaviour model needs to contain the effects of "why the customers need, why the customers are scared and why the customers interpret" in the buying period (Smith and Rupp, 2003).

Banks should approach those of their customers having Internet fraud problems within

the complaint-handling context. However, since the deficiencies of the institutions are also important in the customer complaints (Lam and Dale, 1999), it is important that they should develop sub-applications that will overcome internal inadequacies (employee, culture, administration etc.). Therefore, from the point of view of buying and using the service, the customers' demands relating to security, what the customers are afraid of and what they interpret as their security needs to be taken into consideration. Customer communications and administration systems should be designed with this in mind. Banks can approach customers having problems personally. By showing that it sees the customer as a "person" with programmed personalization (Surprenant and Solomon, 1987) a bank can at least reduce the negative attitudes which customers have towards their bank.

References

Bahia, K. and Nantel, J. (2000). A reliable and valid measurement scale for the perceived service quality of banks. *International Journal of Bank Marketing*, 18 (2), 84-91.

Beaumier, C. M. (2006). Multifactor authentication: a blow to identity theft. *Bank Accounting & Finance*, February-March, 33-37

Brady, M. K. and Cronin, Jr. J. J. (2001). Some new thoughts on conceptualizing perceived service quality: a hierarchical approach. *Journal of Marketing,* 65 (3), 34-49.

Broderick, A. J. and Vachitapornpuk, S. (2002). Service quality in Internet banking: the importance of customer role. *Marketing Intelligence & Planning,* 20 (6), 327-335.

Claessens, J., Dem, V., Cock, D. D., Preneel, B. & Vandewalle J. (2002). On the security of today's online electronic banking systems. *Computers & Security*, 21 (3), 257-269.

Devlin, J. F. and Yeung, M. (2003). Insights into customer motivations for switching to internet banking. *Int. Rev. of Retail, Distribution and Consumer Research*, 13 (4), 375-392.

FFIEC (Federal Financial Institutions Examination Council, "Authentication in an internet banking environment", Retrieved March 20, 2007, from http://www.federalreserve.gov/boarddocs/srletters/2005/sr0519a1.pdf

Gonzalez, M.E., Quesada, G., Picado, F. & Eckelman, C. A. (2004). Customer satisfaction using QFD: an e-banking case. *Managing Service Quality*, 14 (4), 317-330.

Grönross, C. (1984). A service quality model and its marketing implications. *European Journal of Marketing*, 18 (4), 36-44.

Han, I. and Suh, B. (2002). Effect of trust on customer acceptance of internet banking. *Electronic Commerce Research and Applications*, 1 (3), 247-263.

Hicks, D. (2005). Phishing and pharming helping consumers avoid internet fraud. *Community & Banking*, Fall, 28-31.

Hiltgen, A., Kramp, T. & Weigold, T. (2006). Secure internet banking authentication. *IEEE Security & Privacy*, March-April, 21-39

Hutchinson, D. and Warren, M. (2003). Security for internet banking: a framework. *Logistics Information Management*, 16 (1), 64-73.

Jakobsson, M. (2005). Modeling and preventing phishing attacks. Phishing Panel of Financial Cryptography, Retrieved March 20, 2007, from http://www.gbtn.org/~chlee/research/phishing/phishing_jakobsson.pdf

Jaruwachirathanakul, B. and Fink, D. (2005). Internet banking adoption strategies for a developing country: the case of Thailand. *Internet Research*, 15 (3), 295- 311 .

Jayawardhena, C. (2004). Measurement of service quality in internet banking: the development of an instrument. *Journal of Marketing Management*, 20 (1/2),185-207

Joseph, M., McClure, C. & Joseph, B. (1999). Service quality in the banking sector: the impact of technology on service delivery. *International Journal of Bank Marketing*, 17 (4), 182-191.

Jun, M. and Cai, S. (2001). The key determinants of internet banking service quality: a content analysis. *International Journal of Bank Marketing*, 19 (7), 276-291.

Kassarjian, H. H. (1977). Content analysis in consumer research. *The Journal of Consumer Research*, 4 (1), 8-18.

Kaynak, E. and Harcar, T. D. (2005). Consumer attitudes towards online banking: a new strategic marketing medium for commercial banks. *Int. J. Technology Marketing*, 1 (1), 62-78.

Kirda, E. and Kruegel, C. (2006). Protecting users against phishing attacks. *The Computer Journal*, 49 (5), 554-561.

Laforet, S. and Li, X. (2005). Consumers' attitudes towards online and mobile banking in China. *International Journal of Bank Marketing*, 23 (5), 362-380

Lam, N. W. W. and Dale, B. G. (1999). Customer complaints handling system: key issues and concerns. *Total Quality Management*, 10 (6), 843-851

Liao, Z. and Wong, W-K. (2007). The determinants of customer interactions with internet-enabled e-banking services. National University of Singapore, Department of Economics, Working Paper, No. 0701, Retrieved April 2, 2007, from http://nt2.fas.nus.edu.sg/ecs/pub/wp/wp0701.pdf

Liao,Z. and Cheung, M.T. (2005). Service quality in internet e-banking: a user-based core framework. *IEEE International Conference on e-Technology,e-Commerce and e-Service (*EEE'05), pp.628-631. http://ieeexplore.ieee.org/iel5/9634/30444/01402370.pdf?arnumber=1402370

Litan, A. (2004). Phishing attacks victims likely targets for identify theft. *Gartner*, Research, Publication Date: 4 May 2004 ID Number: FT-22-8873, pp. 1-3

Mckenna, B. (2004), "Banks put customers on phishing alert. But whose pigeon is it?" *Info Security*, 30 January, Retrieved March 25, 2007, from http://www.compseconline.com/analysis/040130infosec_phishing.html

Newman, G. and Clarke, R.V. (2002). Etailing: new opportunities for crime, new opportunities for prevention. Produced For The Foresight Crime Prevention Panel by The Jill Dando Insitute of Crime Science, Ucl, February 2002, Retreived 24 March, 2007, from http://www.foresight.gov.uk/Previous_Rounds/Foresight_1999__2002/Crime_Prevention/Reports/Etailing%20New%20Opportunities%20Main%20Report/Index.html

Parasuraman. A., Zeithaml, V. A. & Berry, L. L. (1985). A conceptual model of service quality and its implications for future research. *Journal of Marketing*, 49 (Fall), 41-50.

Patricio, L., Fisk, R. P. & Cunha, J. F. (2003). Improving satisfaction with bank service offerings: measuring the contribution of each delivery channel. *Managing Service Quality*, 13 (6), 471-482

Polatoglu, V.N. and Ekin, S. (2001). An empirical investigation of the Turkish consumers' acceptance of internet banking services. *International Journal of Bank Marketing*, 19 (4), 156-165.

Ribbink, D., Van Riel, A. C. R., Liljander, V. & Streukens, S. (2004). Comfort your online customer: quality, trust and loyalty on the internet. *Managing Service Quality*, 14 (6), 446-456

Rose, S. (2000). The truth about online banking. *Money*, 29 (4), 114–122.

Rusch, J.J. (2002). The social psychology of computer viruses and worms", Paper Presented at INET 2002, Crystal Gateway Marriott, Crystal City, Virginia, June 21, pp. 1-20. Retrieved March 26, 2007, from http://vx.netlux.org/lib/pdf/The%20Social%20Psychology%20of%20Computer%20Viruses%20and%20Worms.pdf

Rusch, J.J. (1999). The Social Engineering of Internet Fraud. Paper Presented *Internet Society Annual Conference*, Retreived 26 March, 2007, from http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm

Schneier, B. (2004). Customers, passwords, and web sites. *IEEE, Internet Security & Privacy*, 2 (4), 88.

Sciglimpaglia, D.and Ely, D. (2002). Internet banking: a customer-centric perspective. Proceedings of the 35th Hawaii International Conference on System Sciences, 7-10 Jan., Retrieved March 20, 2007, from http://ieeexplore.ieee.org/iel5/7798/21442/00994179.pdf?tp=&isnumber=&arnumber=994179

Siu, N.Y.M., and Mou, J.C.W. (2005). Measuring service quality in internet banking the case of Hong Kong. *Journal of International Consumer Marketing*, 17 (4), 99-116.

Smith, A. D. (2006). Exploring security and comfort issues associated with online banking. *Int. J. Electronic Finance*, 1 (1), 18-48.

Smith, A. D. and Rupp, W.T. (2003). Strategic online customer decision making: leveraging the transformational power of the Internet. *Online Information Review*, 27 (6), 418-432

Snellman, K. and Vithkari, T. (2003). Customer complaining behavior in technology-based service encounters. *International Journal of Service Industry Management.* 14 (2), 217-231.

Surprenant C. F. and Solomon, M. (1987). Predictibility and personalization in the service encounter. *Journal of Marketing*, 51 (April), 86-96.

Tally, G., Thomas, R., & Vleck, T. V. (2004). Anti-Phishing: best practices for institutions and consumers. *McAfee Research ,Technical Report* # 04-004, pp.1-28 Retrieved 27 March, 2007, from http://www.mcafee.com/us/local_content/white_papers/ wp_anti_phishing.pdf

Türk Bankalar Birliği,(The Banks Association of Turkey), *Statistical Reports,* Retrieved March 28, 2007, from http://www.tbb.org.tr/turkce/bulten/3%20aylik/internet/haziran2006.zip

Türk Bankalar Birliği, (The Banks Association of Turkey) *Statistical Reports*, Retrieved March 28, 2007, from http://www.tbb.gov.tr.turkce/bulten/3%20aylik/subepersonel/aralik2006.zip

US Netizen (2005), "A new security threat – pharming", Retrieved March 27, 2007, from http://www.freedomfcu.org/pdfs/Pharming.pdf

Yan, G. and Paradi, J. C. (1998). Internet-the future delivery channel for banking services?. Thirty-First Annual Hawaii International Conference on System Sciences, 4, Retrieved March 10, 2007, from http://csdl2.computer.org/comp/proceedings/hicss/1998/8242/04/82420290.pdf

Yang, Z., Jun, M. & Peterson, R. T. (2004). Measuring customer perceived online service quality scale development and managerial implications. *International*

Journal of Operations & Production Management, 24 (11), 1149-1174.

Yavas, U., Bilgin, Z. & Shemwell, D. J. (1997). Service quality in the banking sector in a emerging economy: a consumer survey. *International Journal of Bank Marketing*, 15 (6), 217-233.

Yüksel, H. (2005). Quality dimensions of internet banking: an empirical study. 35th International Conference of Computers& Industrial Engineering,İstanbul ,Turkey, Retrieved April 9, 2007, from http://www.umoncton.ca/cie/Conferences/35thconf/CIE35%20Proceedings/PDF/039.pdf

Zin, A. N. M. and Yunos, Z. (2005). How to make online banking secure. The Star InTech on 21 April, Retrieved March 15, 2007 from http://www.niser.org.my/resources/how_to_make_online_banking_secure.pdf