Customers’ perception of information security in internet banking

Nikola Milosavljević  
Quality Management and Standardization  
Student of Faculty of Organisational Sciences  
Belgrade, Serbia  
nikola97ks@gmail.com

Sara Njagojević  
Quality Management and Standardization  
Student of Faculty of Organisational Sciences  
Belgrade, Serbia  
sara.njagojevic@gmail.com

Abstract—Information Security is one of the key segments for every organization that gathers customers’ information. This paper reviews customers’ perception of information security in internet banking, their needs regarding security of information and their familiarity with some of the concepts related to Information Security. Online questionnaire was used in this paper as method for collecting data that will be used in this research. After conducted questionnaire, statistical analysis was performed using SPSS 23, and various tests (T-test, ANOVA) were used in order to get most precise data.

Keywords—Information Security, Internet banking, Customers’ perception

1. INTRODUCTION

As technology has developed and evolved, the reliance by every organization upon Information and Communication Technology (ICT) has increased dramatically [1], and ICT have affected all the industries such as insurance, health, banking, transportation, private organization, military and government [2].

One of the most important resource that company can possesses is information [3,4], and because of that modern world, society, institutions and organizations are becoming dependent on information technology [3]. With the advent of globalization and ever changing technologies the need for information security is becoming more and more vital [3]. Information security and security in general is an issue of increasing importance [2,5]. Areas such as physical, platform, communication, network and application all have impact on security and they all have their own specific threats, risks and solutions [2]. Maintaining the security of information requires serious effort and approach involving managers, employees, and support personnel, no matter in which sector of organization they work. [6].

Secure and safe information environment is crucial to most of the organizations. Information that information system provides must be with the highest feasible level of:

- Confidentiality by making sure only people who have legitimate right can have an access
- Integrity for securing the information from being malevolently or purposely changed
- Availability by making information accessible to authorized staff when and where it is needed [7, 8].

Security incidents are happening almost every day, and they are caused by hackers, spam, viruses, spyware, zombie networks and many other threats. These incidents can have significant impact on the economy and society by violating human rights and a lot of organizations have suffered failures, serious losses and extinction due to lack of security, privacy and governance of this asset [9, 10].

Many people hesitate or reject to accept new technologies such as internet banking systems or new IT appliances because of security and privacy issues and whether that will happen depends not only on its actual security level, but it also depends on perceived security [11]. Despite that, not a lot of research has been done to study people’s perception of information security [10]. Perceived information security is defined as the consumer’s opinion about likelihood with which their personal information will not be manipulated, viewed or stored during transmission or storage by improper participants [12]. Once customers expose personal information and lose control over it, they naturally feel worried about what will happen with their information[13].

In the field of services, in order to increase customer repurchase intention, it is important to improve service quality. Improving service quality requires boosting customer satisfaction which can be achieved through awareness of real customer perception of service experience. In order to understand customer perception, the key determinants of customer expectations must be identified [14].

There have been many research studies regarding customer expectations in a various context, but it have been usually analyzed from the aspect of customer satisfaction and dissatisfaction, and service quality [15].

The gaps between customer expectations and their perceptions of the service they get which are established depending on service provider’s services and behavior is recognized as service quality [9]. The roots of information security can be found in total quality management. In Total Quality Management (TQM) customers requirements and expectations and the objectives of the organizations are achieved in an competent and cost-effective way. According to some
research studies, service quality is a essential
determinant of customers’ satisfaction, positive word-
of-mouth, buying decisions and long-term loyalty
[15].

The banking sector, as one of the fastest growing
industries, has embraced internet banking as a delivery
channel for their services. The point of e-banking is to
provide the banking services electronically instead of
the traditional banks’ branches. Online banking is
delivering all the services offered by the banks at the
customers’ home computer, tablet or mobile phone.
Customer can use most of the banking services online,
like balance reporting and transactions of funds
without going to the bank at all [16].

Online banking has many benefits over traditional
banking because the service is available 24h per day,
branch operating hours is reduced and queues are
being eliminated, etc. It helps banks to keep existing
customers, increase customer’s satisfaction and banks’
market share, while decreasing administrative and
operational cost and improve banks’ competitiveness
[17].

Internet banking is now widespread around the
world due to its convenience and low cost. As reported
by American Bankers’ Association (ABA) survey done
in August 2014, internet banking is America’s most
popular banking method with 31% of customer
preferring it.

In the context of Internet banking, security and
privacy are specified as “a potential loss due to fraud
or a hacker compromising the security of an online
bank user”. Security and privacy and confidentiality of
personal information are among the biggest concerns

Financial Fraud Action UK (FFA) stated that
losses related to internet banking frauds in the UK
reached £40.9m in 2014.

Many studies have been conducted regarding this
problem, but at the same time, most of these
researches consider employee security awareness in
organizations, while only few of them have been
analyzing customer awareness of internet banking
security [18].

II. LITERATURE REVIEW

Information security has become a major problem
and concern for both organizations and customers, so
it is very important to learn more about people’s
perception of information security [10]. Some authors
suggested that further research should be concentrating
on the connection between people’s perception of
information security and their viewpoint toward
information technology, and the factors that contribute
to the perceived information security [10].

Reference [9] showed that information security
governance as one of the parts of corporate
governance urges information security service. This
can help organizations to deal with information
security risks through providing stable service quality
meeting the expectations of their customers, learning
about customer expectations and reducing the gap
between customer perception and expectations.

Reference [5] is focusing on consumers’ problems
related to online privacy in Germany. According to
their results consumers’ views about internet privacy
and online behaviors are mostly influenced by their
views related to privacy generally and their opinion
about the role of the government and companies in
protecting consumer privacy.

Reference [4] conducted a research where
customers were exposed to three security related
scenarios (negative, neutral and positive) in the hotel
industry and then measured different effects on
customers’ perception of service quality, customers
satisfaction, referral likelihood, and revisit intentions.
In the first two scenarios where breach happened, no
matter if the customers’ credit card data were stolen,
the results of the research showed negative outcomes.
Third scenario, where customers were told that hotel
had just passed a comprehensive information system
security check, resulted in increased satisfaction and
revisit intentions.

Reference [19] researched how confidentiality,
integrity, availability, privacy and verification effect
perceived information security in internet banking
systems. Confidentiality and privacy have substantial
positive effect on perceived information security,
while availability, integrity and verification are not
viewed as important factors by the customers.

Reference [12] proposed a set of antecedents
(assembly, protection, verification and
authentication) to perceived security from visible
technology mechanisms and for this reason perceptible
to the consumers. Protection, which insinuates
consumers’ perceptions of how secure their stored
information are, and encryption, which shows how
their information was handled during transmission
were proved to be influential factors of perceived
security.

Reference [20] indicated that privacy and security
are main issues of dissatisfaction with the use of
mobile and internet banking while possibility of losing
money to fraud is what consumers are mostly
concerned about. It is also stated that the lower the
perception of risk associated with using mobile
banking, the more likely it will be accepted. Reference
[21] concluded that security and standardization of
services are the crucial issues and challenges in mobile
banking today which need to be dealt with, according
to consumers.

Reference [18] conducted a research study about
customer awareness of internet banking security in
which are presented his illuminating findings:

- Customers are not very familiar with internet
  banking security
- Customers are not familiar with basic
technologies and main threats of internet
  banking
Customers are concerned about internet banking security
- Customers don’t actively care about internet banking security
- The existing security information is not very useful
- Every channel has its own benefits for customers
- The utilization of advanced devices may backfire.

While over 60% of customers either agree/strongly agree that internet banking is secure, over 50% of non-users disagree/strongly disagree [18].

III. RESEARCH METHODOLOGY

A. Aim of this research
The aim of this research is to examine the needs of internet banking customers regarding security of information. As well the aim of this study is to examine how familiar they are with information security, how much security of their information is important to them and how different kinds of security breaches affect their attitude towards internet banking.

B. Research questions and hypothesis
- Research Question 1: How familiar are customers with basic technologies and the main threats of internet banking
- Research question 2: Customers are concerned about internet banking security
- Research question 3: Customers consider internet banking is secure

Hypothesis 1: There is a difference in familiarity with basic technologies and the main threats of internet banking between sexes.
Hypothesis 2: Internet banking customers know the correct web address of their banks

C. Population and sample characteristics
The population of this research are people from Serbia, both users and non users of internet banking. Online questionnaire was used in this paper as method for collecting data that will be used in this research. The sample size is 118 respondents. We can see more about respondents from the graphs below.

D. Research instrument
Questionnaire was created and distributed online. It was consisted of five parts. First one was related to basic demographic questions including sex, age, the purchasing power and level of education. Second part included questions about their usage of internet banking, while third one contained the questions about importance of information security to the respondents, and how familiar they are with some technical aspects of IS. Questions in the fourth part examined the needs of the internet banking customers. Last part was consisted of questions sorted in different scenarios regarding security breaches.

E. Data Analysis Methods
After conducted questionnaire, statistical analysis was performed using SPSS 23, and various tests (T-test, ANOVA) were used in order to get most precise data.

IV. RESULTS

A. Research Question 1: How familiar are customers with basic technologies and the main threats of internet banking
There were four questions regarding how much are customers familiar with some of the basic technologies and the main threats of internet banking (SSL, phishing, digital certificates and dynamic security).
passwords). As it can be seen from the tables below, most of the respondents never heard of these technologies or they only heard about them, but they don’t know what these are.

### TABLE I. FAMILIARITY WITH IS DYNAMIC PASSWORDS

<table>
<thead>
<tr>
<th>Familiar with dynamic passwords</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never heard of it</td>
<td>59</td>
<td>50.0</td>
</tr>
<tr>
<td>Just heard of it</td>
<td>27</td>
<td>22.9</td>
</tr>
<tr>
<td>Know what it is</td>
<td>25</td>
<td>21.2</td>
</tr>
<tr>
<td>Totally familiar</td>
<td>7</td>
<td>5.9</td>
</tr>
<tr>
<td>Total</td>
<td>118</td>
<td>100.0</td>
</tr>
</tbody>
</table>

### TABLE II. FAMILIARITY WITH IS PHISHING

<table>
<thead>
<tr>
<th>Familiar with phishing</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never heard of it</td>
<td>68</td>
<td>57.6</td>
</tr>
<tr>
<td>Just heard of it</td>
<td>14</td>
<td>11.9</td>
</tr>
<tr>
<td>Know what it is</td>
<td>21</td>
<td>17.8</td>
</tr>
<tr>
<td>Totally familiar</td>
<td>13</td>
<td>11.0</td>
</tr>
<tr>
<td>Total</td>
<td>116</td>
<td>98.3</td>
</tr>
<tr>
<td>Missing</td>
<td>2</td>
<td>1.7</td>
</tr>
<tr>
<td>Total</td>
<td>118</td>
<td>100.0</td>
</tr>
</tbody>
</table>

### TABLE III. FAMILIARITY WITH IS SSL

<table>
<thead>
<tr>
<th>Familiar with SSL</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never heard of it</td>
<td>71</td>
<td>60.2</td>
</tr>
<tr>
<td>Just heard of it</td>
<td>15</td>
<td>12.7</td>
</tr>
<tr>
<td>Know what it is</td>
<td>17</td>
<td>14.4</td>
</tr>
<tr>
<td>Totally familiar</td>
<td>13</td>
<td>11.0</td>
</tr>
<tr>
<td>Total</td>
<td>116</td>
<td>98.3</td>
</tr>
<tr>
<td>Missing</td>
<td>2</td>
<td>1.7</td>
</tr>
<tr>
<td>Total</td>
<td>118</td>
<td>100.0</td>
</tr>
</tbody>
</table>

### TABLE IV. FAMILIARITY WITH IS DIGITAL CERTIFICATES

<table>
<thead>
<tr>
<th>Familiar with digital certificates</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never heard of it</td>
<td>51</td>
<td>43.2</td>
</tr>
<tr>
<td>Just heard of it</td>
<td>28</td>
<td>23.7</td>
</tr>
<tr>
<td>Know what it is</td>
<td>32</td>
<td>27.1</td>
</tr>
<tr>
<td>Totally familiar</td>
<td>7</td>
<td>5.9</td>
</tr>
<tr>
<td>Total</td>
<td>118</td>
<td>100.0</td>
</tr>
</tbody>
</table>

**B. Research question 2: Customers are concerned about internet banking security**

This is proven not to be true. It seems like customers are not really concerned about their internet banking security because most of the respondents said that they strongly disagree/disagree.

**C. Research question 3: Customers consider internet banking is secure**

Results have shown that this is mostly true. 93% of the answers were that they agree/strongly agree.

**D. Hypothesis 1: There is a difference in familiarity with basic technologies and the main threats of internet banking between sexes**

Using t-test it can be proven that this is right for every of the four questions that was asked regarding this issue. Significant influence does exist and it is less than 0.05. The results of this research are given in the table.
E. Hypothesis 2: Internet banking customers know the correct web address of their banks

Using ANOVA test this is shown only partially. Only 56% of the internet banking customers knows the correct Web address of their. Significant influence does exist and it is less than 0.05.

V. DISCUSSION AND CONCLUSION

Information systems are something that is constantly evolving, and because of that security of information is becoming more and more important. With the developing of information systems, banks are following trends and there are constant growth of the internet banking customers. In order to use the internet banking, customers should be familiar with the security of their information and threats that can invade their privacy and their bank accounts. Due to the importance of this topic, we decided to take a closer look at the needs of the internet banking customers.

Based on the results of first research question, it can be concluded that customers are not really familiar with the basic technologies and the main threats of internet banking. Reference [18] conducted a research study about customer awareness of internet banking security and concluded the same thing, that customers are not really familiar with internet banking security and they are not acquainted with basic technologies and the main threats of internet banking.

This is something that can be very dangerous, both for the customers and for the banks, because customers should know how to properly use their internet banking account in order to keep their information private and secure.

Regarding our second research question, it can be seen that customers are not really concerned about the security of their internet banking accounts. Reference [18] concluded the opposite. This can be explained with the difference between cultures, and that internet banking in Serbia is still developing, so customers may have not yet had problems with the security.

In third research question, we examined if internet banking customers consider that internet banking is safe and secure for using.

Most of the respondents (93%) answered that they agree/strongly agree that internet banking is secure, while [22] concluded that only 60% of the customers agree with this statement.

In first hypothesis, it can be concluded that there is significant difference between sexes about how familiar they are with information security. Man are shown to be more familiar with information security and dynamic passwords).

Results from the second hypothesis are very interesting. It is shown that only 56% of the respondents who use internet banking knows the correct internet address of their banks. Combining this with the results from the research questions 1, especially with the familiarity with the phising where 56.7% of the respondents said that they never heard about it, it can be concluded that internet banking customers can be very vulnerable. The best way to avoid phishing attacks and fake sites is to know how to
recognize them, so both internet banking customers and banks should work on this issue.

REFERENCES