Journal of Finance and Accounting
2016; 4(1): 1-8
Published online January 27, 2016 (http://www.sciencepublishinggroup.com/j/jfa)
doi: 10.11648/j.jfa.20160401.11
ISSN: 2330-7331 (Print); ISSN: 2330-7323 (Online)

Security of E-Banking in Bangladesh

Mohammad Shamsus Sadekin[1], Md. Abdul Hannan Shaikh[2]

[1]Department of Humanities, Chittagong University of Engineering & Technology, Chittagong, Bangladesh
[2]Department of Management, Islamic University, Kushtia, Bangladesh

Email address:
sadekinmba@yahoo.com (M. S. Sadekin)

To cite this article:
Mohammad Shamsus Sadekin, Md. Abdul Hannan Shaikh. Security of E-Banking in Bangladesh. *Journal of Finance and Accounting.* Vol. 4, No. 1, 2016, pp. 1-8. doi: 10.11648/j.jfa.20160401.11

Abstract: E-banking implies provision of banking products and services through electronic delivery channels. It permits anytime, anywhere and any how banking. It offers easy, faster, convenient, low cost banking services around the clock. Security has been recognized as a capital component of electronic banking industry. The main factor of e-banking practice and security are different from traditional banking services because of uncertain nature of the online environment. Every steps in the online banking activities are secured by one or more security mechanisms. This paper discusses the substantial cracks in existing knowledge about the internet banking security in Bangladesh. The typical data is collected both from the secondary and primary sources. In analyzing data, the statistical tools have used with the aid of SPSS software. The result shows that e-banking practice is not highly secured in Bangladesh. The users also have lack of awareness about e-banking security.

Keywords: E-Banking, Security, Password

1. Introduction

E-Banking is one of the major parts of e-finance. It can be applied to the banking operations, which done over World Wide Web. This is also known as electronic funds transfer (EFT) is simply to use of electronic transmissions money directly from one account to another, rather than by cheque or cash. It is also allowed bank customers to admittance accounts and common information on bank products and facilities through a personal computer (PC) or other intellectual device. On the other hand, IT products and services can be comprised extensive products for business clients as well as retail and fiduciary products for customers [1]. It involves individuals and corporate clients by including balance transfers, payments, transaction settlement, documentary collections, credits, corporate and domestic lending, card business and so on. It is well known that banking is essential for customers but not bank. The traditional bank branch is going to be disappeared in order to substitute electronic banking which continues to attract new users. The banking industry believes that the banks will be able to develop customer service level and tie their customers closer to the bank by adopting new technology [2]. Thus, the study on e-banking is more important topic for researcher now a day. The developed country is now using e-banking as a part and parcel of their economy. Salehi [3] have provided that a strong banking industry is important in every country and significant affects in supporting economic development through efficient financial services. Customer's identification is presented by access code, such as a password or Personal Identification Number (PIN), instead of a signature on a check or other physical document. Online banking is also referred as Internet banking, e-banking, virtual banking and by other terms. To access online banking, a customer would go to the financial institution's secured website, and enter the online banking facility using the customer number and password previously setup. Some financial institutions have set up additional security steps for access to online banking, but there is no consistency to the approach adopted [4]. Bank is a financial institution where peoples deposit their money for better security. From the very beginning of banking industry, every bank have given assurance of sufficient security to their customer. Recently, Chavan [5] has conducted a study on “Internet Banking- Benefits and Challenges in an Emerging Economy” and developed a new information technology for the development of financial services, especially banking sector transitions. Nattakant [6] have discussed the phishing that involves sending e-mails pretending in the form of legitimate financial institutions to recipients and asking personal information such as username and password. Biswas et. al. [7] have shown that the software, technology, infrastructure, skilled manpower and cyber law are not provided the proper security for the implementation of e-banking in Bangladesh.

Customers may be depended on security level of e-banking. They have deposited their valuable assets including cash in bank. Thus, the security of traditional and e-banking is very important for banking industry. The traditional bank transaction may be more secured rather than e-banking transaction. One can also benefit from physical security and use vaults to protect cash. However, the customer's financial information is very important for the case of e-banking security. Therefore, the aim of this article is to present the security status of e-banking in Bangladesh.

2. Background of the Study

E-banking is actually online service for bank customers. Computer is the main instrument for e-banking functions. But computer security doesn't cover total online security. Online security is more difficult than computer security. Online hackers always try to hack e-mail account, social network account and personal bank account. It may possible to collect cash from e-account by hacking. Till now these hackers chopped many bank's web site and collect hugs amount of money by using their technological efficiency. The online banking is fully dependent on e-transaction. So, e-banking security mainly depends on the protection of software, so called software security.

To understand the techniques for securing a computer system, it is important to protect various types of "attacks" that can be made against it. Wysopal and Eng [8] have classified in the following three types of attacks:

i. Backdoors are a method of by passing verification or other safety controls in order to admittance a computer system or the data contained on that system. Backdoors can occur at the system level, in a cryptographic procedure, or within an application.

ii. Denial of service attacks is not used to gain unauthorized access or control of a system. They are as an alternative designed to render it unusable. Attackers can deny service to individual victims, such as by intentionally entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. These types of attack are, in practice, very hard to prevent, because the behavior of whole networks needs to be analyzed, not only the behavior of small pieces of code.

iii. Someone who has gained access to a computer can install different types of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media, for instance CD-R/DVD-R, tape; or portable devices such as key drives, digital cameras or digital audio players.

2.1. Various Type of Attack on Internet

i. *Phishing:* Phishing is the e-mail deception method in which the perpetrator sends out legitimate-looking email in an effort to collect personal and financial information from recipients. Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

ii. *Spyware and Adware:* Ad supported software, often called Adware or Advertising Supported Software, is used when referencing any type of program that downloads or displays unwanted banner advertisements in the software being used. Adware is often bundled within software a computer owner purchases. The authors of a program sometimes include adware in their software to recover development costs, or to be able to provide the product for free or at a discounted price. Adware can be designed to collect data on which sites the user visits, send this data back to the company and deliver advertising based on the information. Though the advertisements produced by adware may be seen as an annoyance, a distraction, or an invasion of privacy to the user, the income the developer receives may help them to maintain, upgrade and continue to develop more products. Often, after using a free software product that includes adware, a user may opt to purchase a registered or licensed version without adware to remove the ads. This adware-free product may also have additional functionality. However, adware can also contain or be classified as spyware, a type of malware that is considered by many to be privacy-invasive. Spyware can steal a user's information or corrupt the user's system files. Though adware companies may have a Privacy Policy stating that no sensitive or identifying information will be collected, there is usually no way for the user to be completely sure that he or she remains anonymous. Therefore, because of privacy concerns and the prospect of malicious adware, antivirus software today detects and removes both adware and spyware.

iii. *Computer virus:* A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, logging their keystrokes, or even rendering the computer useless. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without user consent.

iv. *Trojans:* Trojans are malicious programs that perform actions that have not been authorized by the user. These actions can include:
- Deleting data.
- Blocking data.
- Modifying data.
- Copying data.
- Disrupting the performance of computers or computer networks.

v. *Key loggers:* A key logger, sometimes called a keystroke logger, key logger, or system monitor, is a hardware device or small program that monitors each keystroke a user types on a specific computer's keyboard. As a hardware device, a key logger is a small battery-sized plug that serves as a connector between the user's keyboard and computer. Because the device resembles an ordinary keyboard plug, it is relatively easy for someone who wants to monitor a user's behavior to physically hide such a device "in plain sight." (It also helps that most workstation keyboards plug into the back of the computer.) As the user types, the device collect each keystroke and save it as text in its own miniature hard drive. At a later point in time, the person who installed the key logger must return and physically remove the device in order to access the information the device has gathered.

vi. *Salami attack:* The most typical scheme portrayed by a salami attack is that which involves an automated modification to financial systems and their data. For example, the digits representing currency on a bank's computer(s) could be altered so that values to the right of the pennies field (< 0.01) are always rounded down (fair arithmetic routines will calculate in both directions equally). Since all this rounding down produces excess fractions of cents, they must be transferred elsewhere, and, carefully, so that no net loss to the system of accounts becomes apparent.

2.2. Computer Protection Against the Attacks on Internet

Security method [9, 10] is a vibrant issue for all business organizations. It is seen that banks which provide services to their client must confirm safety. So those clients are pleased to bank. In a sense, bank is a business organization so it is also their obligation to maintain everything firmly.

To safeguard the E-banking, there are some security doctrines that have to be provided by banks. Because in this case many transactions are occurring in electronic media, so without securing the banking activities banks cannot drive. Islam [9] has provided the following technique to protect the computer attacks for security purpose:

i. Authentication is the procedure of two parties' involvement in a discussion. This discussion assures that they are definitely relating with whom they think they are interacting. Authentication might be from both sides: i) server authentication and ii) client authentication. Most internet shopping places use username and password to confirm its users so called "password authentication". They are usually more concerned with the legitimacy of credit card than the identity of the user.

ii. Confidentiality deals with protecting the contents of message or data transferred over the internet from unapproved people. For example, anyone wants to safeguard his debit or credit card information when he purchases over the Internet.

iii. Data integrity is interconnected to inhibiting data from being reformed by an attacker. For example, only the debit or credit card number is protected while the contents do not provide the online order. Then, the attacker could potentially modify the instruction while it is being transmitted over the network by adding or deleting contents from the order.

iv. It is significant to assure that authentic users of an e-banking system will get service at any time. At times attacker might set up a database that uninterruptedly tries to be authenticated by the bank. But the authentication will repetitively fail. However, attacker would occupy expensive resources of the site. These resources become unavailable to the genuine clients of the bank.

v. Non-repudiation is an element of secure systems for preventing a message. This might very expensive for e-businesses such as online trading which want to safeguard that a customer will not be able to deny having requested to buy or sell securities.

3. Analysis of Data

Followings are the presentation of the result and analysis of data collected for the study. Responses from total 120 respondents consisting of 44 bankers and 76 bank customers, 98 male and 22 female, 34 married and 86 unmarried, and 28 from rural and 92 from urban areas selected for the study were considered.

It is provided from the Table 1 that among the respondents 34% from rural area, 40% from municipalities, 17% from various district town and 29% from different city corporations. Among the respondents 15% respondents from various locations mentioned that online banking is highly secured. Among the respondents 15% said e-banking in Bangladesh is highly secured and 31% respondents said e-banking security is not sufficient in Bangladesh. Out of the total respondents 11.5% do not know about the security status of e-banking in Bangladesh.

Table 1. *Security of E-Banking and Location of Respondents.*

Location of Respondents	**Highly Secured**	**Sufficient Secured**	**Not enough secured**	**Not secured at all**	**Don't know**	**Total**
No. (%)	**No. (%)**	**No. (%)**	**No. (%)**	**No. (%)**	**No. (%)**	**No. (%)**
Rural Area	5 (15)	13 (38)	11 (32)	0 (0)	5 (15)	34 (29)
Municipality	3 (7.5)	16 (40)	17 (42.5)	1 (2.5)	3 (7.5)	40 (33)
District town	3 (18)	7 (41)	5 (29)	0 (0)	2 (12)	17 (14)
City Corporation	7 (24)	14 (48)	5 (18)	0 (0)	3 (10)	29 (24)
Total	18 (15)	50 (42)	38 (31)	1 (.80)	13 (11.2)	120 (100)

It is evident from Table 1 that among the respondents 34% from rural area, 40% from municipalities, 17% from various district town and 29% from different city corporations. Among the respondents 15% respondents from various locations mentioned that online banking is highly secured. Among the respondents 15% said e-banking in Bangladesh is highly secured and 31% respondents said e-banking security is not sufficient in Bangladesh. Out of the total respondents 11.5% do not know about the security status of e-banking in Bangladesh.

Among the respondents 31.7% uses some digits as their password.13.3% uses only name or letter, 18.3% uses some digits and some letters and 28.33% respondents don't maintain e-banking accounts (see Table 2).

Table 2. *Type of Passwords Used by the Respondents for Maintaining E-Bank Account.*

Type of Passwords			
	Frequency	**Percent**	**Cumulative Percent**
Number	38	31.7	31.7
Letter	16	13.3	45
Number & Letter	22	18.3	63.3
Other	0	0	63.3
Mixed	10	8.3	71.7
N/A	34	28.33	100.0
Total	120	100.0	

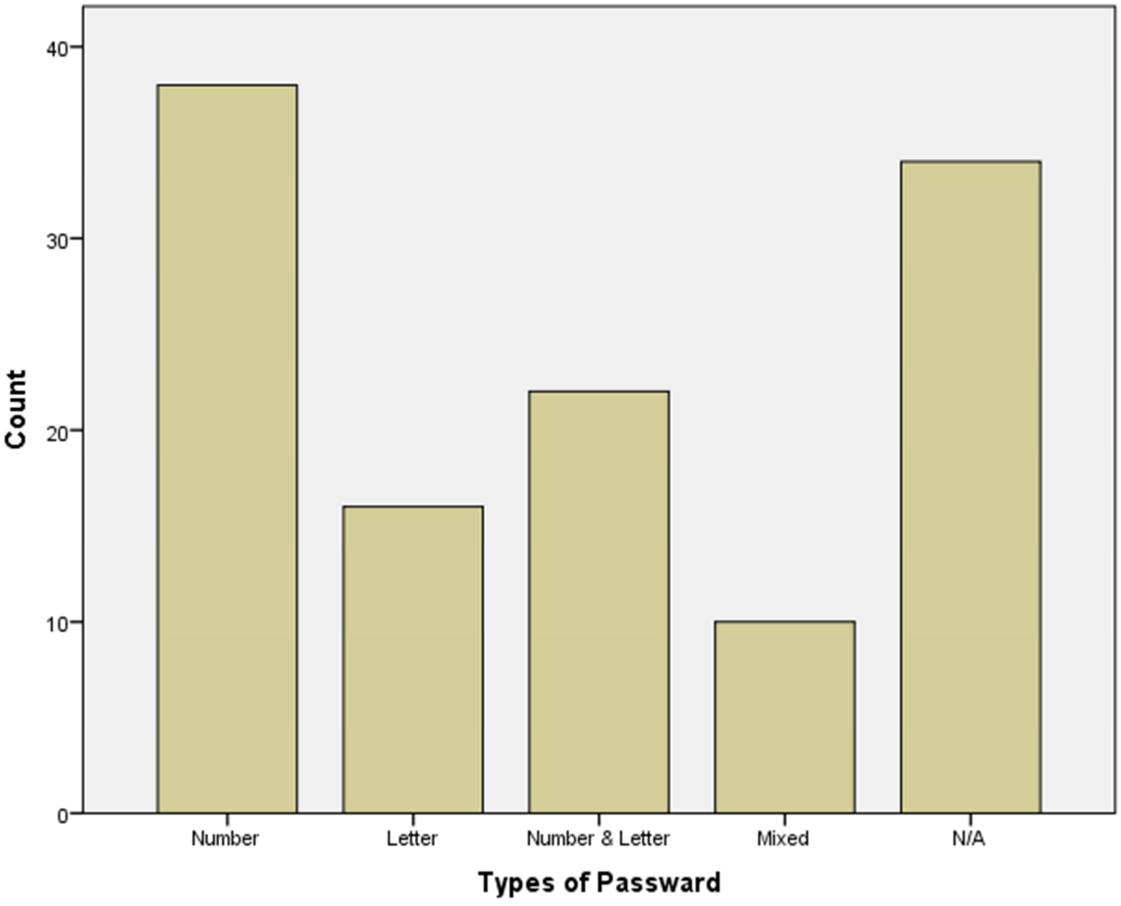

Figure 1. *Type of Passwords Used by the Respondents to Maintain E-Account.*

The figure 1 shows clearly that those who use e-banking majority of those respondents use some digits as their password. or combination of digit and letter for maintaining e-banking accounts.

Table 3 shows the inter correlation among some major variables such as types of password, trust on e-banking, security of e-banking, ATM booth's location, hacking online account, sharing password, speed quality of internet connection, availability of anti-virus, name of anti-virus, checking e-bank statement. From this table it is seen that

(i) There is a positive correlation between security of e-banking and location of ATM booths. That means the location of ATM booths will increase or decrease the security of e-banking. If the locations of ATM booths are in secured area the security of e-banking will increase and if the locations of ATM booths are in are in non-secured area the security of e-banking will decrease.

Table 3. *Inter Correlation Among Some Major Variables.*

		Types of Password	Trust on e-banking	Security of e-banking	ATM Location	Hack your account	Sharing password	Speed quality of connection	Anti-virus	Name of Anti-virus
Trust on e-banking	Pearson Correlation	-.013								
	Sig. (2-tailed)	.890								
Security of e-banking	Pearson Correlation	-.116	-.109							
	Sig. (2-tailed)	.206	.236							
ATM Location	Pearson Correlation	-.033	.060							
	Sig. (2-tailed)	.724	.514	.013						
Hack your account	Pearson Correlation	.130	.124	.068	.273**					
	Sig. (2-tailed)	.156	.178	.462	.003					
Sharing password	Pearson Correlation	.147	.067	.107	.114	.372**				
	Sig. (2-tailed)	.109	.468	.244	.217	.000				
Speed quality of connection	Pearson Correlation	-.001	-.004	-.095	.100	.161	.297**			
	Sig. (2-tailed)	.995	.969	.300	.279	.079	.001			
Anti-virus	Pearson Correlation	-.021	.180*	-.097	.182*	.277**	.263**	.435**		
	Sig. (2-tailed)	.820	.049	.290	.046	.002	.004	.000		
Name of Anti-virus	Pearson Correlation	.006	.155	-.028	.138	.174	.106	.226*		
	Sig. (2-tailed)	.950	.091	.761	.134	.057	.251	.013		
Check statement	Pearson	.148	.010	-.021	.247**	.213*	.334**	.390**	.347**	
	Sig. (2-tailed)	.107	.917	.817	.007	.020	.000	.000	.000	

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

(ii) There is a high degree of positive correlation between ATM location and hacking of e-banking. That means if the ATM location is not in secured area there is a big chance of hacking the online account.

(iii) There is a high degree of positive correlation between sharing password and hacking online account. That means those account holder who will share his password with others there is a big chance of hacking his account.

(iv) There is a positive correlation between speed quality of internet connection and sharing password. If the speed quality is low then account holder may close his account without sign out or without closing the browser or clearing the browser. Then who will first access he can easily hack this account.

(v) There is also a positive correlation among availability of anti-virus in PC with hacking e-account, sharing password, ATM location and speed quality of internet connection. Virus is very risky for computer and internet. IT is able to destroy all the security system of e-banking software. So the unavailability of anti-virus will reduce all the security point of e-banking. Anti-virus security is highly correlated with is brand. All anti-virus is not equally effective to destroy the risky virus.

(vi) Checking the bank statement is highly correlated with ATM location, hacking of e-account, sharing password, speed quality of internet connection, availability of anti-virus and name of anti-virus. Those account holders who check their account balance regularly, their account is comparatively more secured than that account holder who doesn't do this. Because he can easily informed about any accident.

Table 4. *E-Banking Security and use of Antivirus.*

	Number of Respondents Revealing Security Level	**Use of Anti-Virus**	
		Yes	**No**
		No. (%)	**No. (%)**
Security of E-Banking	Highly Secured (18)	13 (15)	5 (16)
	Sufficient Secured (50)	40 (45)	10 (31)
	Not Enough Secured (38)	27 (31)	11 (34)
	Not Secured at all (1)	0 (0)	1 (3)
	Don't Know (13)	8 (9)	5 (16)
Total		88 (73)	32 (27)

Among the respondents 73% use and 27% respondents do not use anti-virus. Among the respondents 45% anti-virus users said e-banking in Bangladesh is sufficient secured and 34% respondents who do not use anti-virus said e-banking not enough secured. (see Table 4).

Table 5. *Chi-Squire Table Showing Response Pattern on Safety of ATM Location (N=120).*

Safety of ATM Location	Observed No. (%)	Chi-squire	d. f.	P
Yes	42 (35%)	10.80	1	N. S.
No	78 (65%)			

The result of the Table 5 reveals that the respondents are not significantly associated. They differ significantly towards the safety and ATM location of e-banking in Bangladesh. Majority (65%) respondents agree that the locations of ATM booths are not in safe position.

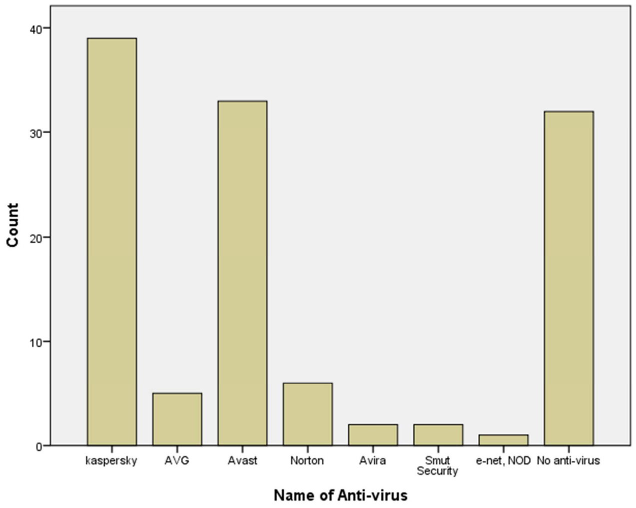

Figure 2. *Uses of Antivirus by the Respondents.*

Figure 2 shows that a large number of respondents do not use antivirus in their personal computer. Among the antivirus users majority of them use Avast or Kaspersky. Some respondents use AVG, Norton, and Avira etc.

Among the respondents 15% said e-banking is highly secured, 41.7% said sufficient secured, 31.7% said not enough secured 10.8% don't know about the security level of e-banking (see Table 6)

Table 6. *Security Level of E-Banking in Bangladesh.*

Security of E-Banking	Frequency	Percent	Cumulative Percent
Highly Secured	18	15.0	15.0
Sufficient Secured	50	41.7	56.7
Not Enough Secured	38	31.7	88.3
Not Secured at all	1	.8	89.2
Don't Know	13	10.8	100.0
Total	120	100.0	

Table 7. *Chi-Square Table Showing Response Pattern on Safety of ATM Location (N=120).*

Safety of ATM Booths	Frequency	Percentage	Chi-Squire	d. f.	P
Yes	42	35%	10.80	1	N.S.
No	78	65%			

The result of the Table 7 reveals that *the* respondents are significantly associated. They do not differ significantly towards security and ATM location of e-banking in Bangladesh. But majority (65%) respondents agree that the locations of ATM booths are not in safe position.

Table 8. *Sharing Password with Other by the Respondents.*

Do You Share Password?	Number of Respondents	Percent	Cumulative Percent
Yes	16	13.3	13.3
No	70	58.4	71.7
N/A	34	28.3	100

Table 8 shows that majority of the respondents (71.7%) do not share their e-banking password with others but among the respondents 13.3% share their secured password which is harmful for e-banking security.

Table 9 shows that 15.83% respondents use mobile banking. Among the mobile bank account holders 47.37% feel that e-banking in Bangladesh is not enough secured. Among the ATM card users 06 said, this is not enough secured. Among the respondents 28.34% respondents don not have online account. Table shows that majority of the mobile bank account holders feel that security of this type of account is not enough. Credit card users feel this account is highly secured.

Table 9. *Types of Online Account and E-Banking Security.*

Type of Online Account	Highly Secured	Sufficient Secured	Not Enough Secured	Not Secured at all	Don't Know	Total
	No. (%)	No. (%)	No. (%)	No. (%)	No. (%)	No. (%)
Mobile Bank Account	0 (0)	8 (42.11)	9 (47.37)	1 (5.26)	1 (5.26)	19 (15.83)
Credit Card Account	4 (66.67)	2 (33.33)	0 (0)	0 (0)	0 (0)	6 (5)
ATM Account	6 (13.96)	19 (44.18)	15 (34.88)	0 (0)	3 (6.98)	43 (35.83)

Type of Online Account	Highly Secured	Sufficient Secured	Not Enough Secured	Not Secured at all	Don't Know	Total
	No. (%)	No. (%)	No. (%)	No. (%)	No. (%)	No. (%)
Internet Bank Account	2 (15.38)	7 (53.86)	3 (23.07)	0 (0)	1 (7.69)	13 (10.83)
Other	0 (0)	1 (20)	3 (60)	0 (0)	1 (20)	5 (4.17)
N/A	6 (17.65)	13 (38.23)	8 (23.53)	0 (0)	7 (20.59)	34 (28.34)
Total	18 (15)	50 (41.67)	38 (31.67)	1 (.83)	13 (10.83)	120 (100)

Table 10. *Customer Log-out From Bank Web Site and Re-start Personal Computer.*

Log Out From Bank Web Site		Re-start Computer After Transaction
Yes	58 (48.33%)	17 (14.17%)
No	62 (51.67%)	103 (85.83%)

Table 10 shows that among the respondents 51.67% do not log out from bank web site and 85.83% do not re-start their computer after completing a transaction.

4. Findings of the Study

Security is very important and sensitive issue for e-banking practices. In Bangladesh the e-banking security is not in satisfactory position. Customers trust on e-banking depends on e-banking security. E-banking securities are not similar with traditional banking security. Software security is the major part of e-banking security. The following security related findings have been identified from the results and analysis of the study:

4.1. Security Status

It is grasped from the Tab. 6 that, E-Banking is not highly secured in Bangladesh. Among the respondents 41.7% said that e-banking security in Bangladesh is sufficient but 31.7% said, e-banking in Bangladesh is not enough secured. Only 15% said e-banking in Bangladesh is "highly secured". There have some e-banking security problems in Bangladesh; as a result some unwanted occurrences have been taken place.

4.2. Password

Simple passwords such as person's name or other real words are relatively easy for a user to remember but they are weak from security point of view because they are vulnerable to dictionary attacks. Strong passwords are mixed (e. g., x7h! t%C9) passwords are less vulnerable to attack but at the same time more difficult to remember. It is found from Tab. 2 that among the respondents 31.7% are using only some "digit" and 13.3% respondents' uses only some "letter" as their e-banking password though this type of password is not secured enough.

4.3. Sharing Password

Password should not be shared with the closest person in life but many users share this with their wife, friends and family members. Hacking may happen by those closely related persons by giving ATM or credit card to other to withdrawal money. There is a significant positive correlation between sharing password and hacking online account. It is attained from the Table 8 that 13.3% account holders' shared password with others.

4.4. Job Switch of IT Experts

The software developer and the IT expert of any bank know the security of the software clearly and they can easily find out the security gap of the relative software. If he changes his job he may help the hackers by providing information if he has ill intention.

4.5. Sharing Personal Information via E-mail

Some account holders share financial information through e-mail. The hackers may find out the confidential information from e-mail and may hack the account and manipulate. By using web site it is possible to send SMS to a client. This may be done by hackers. Hackers create a fake web site by the name of any specific bank and then demand account related information.

4.6. Log out From Bank Web Site and Re-start the Computer

It is obtained from the Table 10 that majority of the respondents do not log out from his account or from the bank web site. This may be a cause of e-banking security risk. If account holders use public computer then it is necessary to re-start or log off. Sign out is not sufficient from security point of view. Because the hackers are expert to sign in if users didn't log out from the web site or re-start the computer.

4.7. E-banking Security and ATM Booth's Location

It is grasped from Table 1 that there is a significant positive correlation between ATM booth's location and hacking of e-banking account. If the ATM location is not enough secured there is a chance of hacking of online account.

4.8. Antivirus

It is obtained from Table 3 that there is a significant positive correlation between antivirus in PC and hacking of e-account. Customers who do not use antivirus their account are less secured.

4.9. Checking Statement

Checking the statement is significantly positively correlated with hacking e-account. It is established from Table 3 that the account holders who check their account balance regularly; their accounts are more secured than those who do not.

4.10. Types of Online Account and Security

In Bangladesh, customers use Mobile Banking, Credit Card, ATM Card, and many other online accounts. It is achieved from the Table 9 that out of these ATM account are more secured than the Mobile Banking account.

5. Conclusions

E-Banking is a new concept in banking sector of Bangladesh. It becomes more popular in Bangladesh day by day. Bangladeshi banks offer many facilities of e-banking. Domestic private commercial banks and foreign commercial banks are in leading position. However, the state owned commercial banks may not be offered all the functions of e-banking. The customers may not be trusted on e-banking without providing top level of security. Many customers may be used either mobile bank account or ATM account in Bangladesh, which are not actually highly secured. All types of e-banking services have appreciated and applied for people at different walks in the case of activities. Thus, an attractive offer package have provided for e-banking which will popular everywhere very soon. But, the security concern should be maintained strictly to increase the trust of customers. The initiatives should be taken to make more secure. Furthermore, Bangladeshi customers have limited knowledge about e-banking transactions. They are not ready to accept any financial difficulties and will not trust on e-banking services. Bankers have to be sincere about e-banking security. Therefore e-banking may be secured by taking necessary initiatives, like using finger print, authentication of cash withdrawals, using close circuit camera, increasing internet speed, increasing awareness, using protective password and antivirus, formulation of e-banking supporting policies, close monitoring, legal provisions for controlling frauds etc.

References

[1] Al-Amin S and Rahman S, Application of Electronic Banking in Bangladesh: An Overview, *Bangladesh Research Publication Journal.* 4(2), 172-184 (2010).

[2] Graven M P, Electronic money. *PC Magazine,* 8 August, (2000).

[3] Salehi M, Ali M and Zhila A., Islamic Banking Practice and Satisfaction: Empirical Evidence From Iran. *ACRM Journal of Business and Management, Research.* 3(2), 35-41(2008).

[4] Cronin M J, *Banking and Finance on the Internet.* John Wiley and Sons (1997).

[5] Chavan J, Internet Banking-Benefits and Challenges in an Emerging Economy. *International Journal of Research in Business Management,* 1 (1), 19-26 (2013).

[6] Nattakant U, Online Banking Users in Western Australian of Phishing Attacks" *P. hd Thesis, Faculty of Computing, Health and Science, Edith Cowan University,* (2012).

[7] Biswas S et. al., Electronic Banking in Bangladesh: Security Issues, Forms, Opportunities and Challenges. *Canadian Journal on Scientific and Industrial Research.* 2(5), (2011).

[8] Wysopal C, Eng C, Static Detection of Application Backdoors". Veracode. (2015).

[9] Islam M M, Proposed ICT Infrastructure for E-banking in Bangladesh. *Department of Computer and Systems Sciences, Royal Institute of Technology (KTH)*, Stockholm, Sweden (2005).

[10] Parker D B, Fighting Computer Crime: A New Framework for Protecting Information. New York: *John Wiley & Sons*, Inc., (1998).