“Internet Banking Security Software” Proposed Model

Prof. Minakshi Dattatraya Bhosale
Head, Faculty of MCA, YTC, Yashoda Technical Campus Satara

ABSTRACT

Today’s world is a world of globalization, industrialization and Information Technology (IT). This beginning of the Internet and the popularity of personal computers offered both; an opportunity and a challenge for the banking industry. The accessibility and dynamism of the Internet bring both benefits and risks. Insufficient knowledge of Internet banking technology and fear about security risk, customers was avoided to use Internet banking services. Hence, took these things into consideration researcher developed web based “Internet banking security software” guide for customers those are doing Internet banking transactions. If the customer uses these all stages properly, then this software provides an extremely secure environment to the customer. This software provides guidelines for the customer to update the operating system, antivirus, Ms-office, Adobe acrobat reader and Flash software. Provide guidelines for removal of spyware like Trojan, malware, key logger, viruses. Before doing Internet banking transactions, the customer checks password strength. Keep a backup of all Internet banking transactions through the mail, provide a demo of encryption, decryption of connection string and a query string. The software provides the facility to customers through that customer directly connects to any bank in the Satara district. Hence the problem of fake URL and fake site is avoided. It will help to avoid phishing. At the end software provide facility of removing sessions and cookies. Through this facility session created by particular customer during Internet banking transactions is removed hence problem of hacking is controlled. Hence this software is the best guide of customer those are using Internet banking service.

Keyword: - Internet banking, hacking, phishing, query string, connection string.

1.1 INTRODUCTION

Due to the speedy development in information technology, the money transfer services industry has come across enormous developments achieved by the collaboration between competitive pressure, customer needs, and technological innovation. The customer moves to innovation-based organization toward oneself as a substitute to the conventional banking. This gives profits to both the bank, as it reduces the expenses of every transaction, and to the customer, who is offered, increased convenience. Thus, today's banking takes place increasingly through electronic channels. Automated teller machines (ATMs), telephone banking, Internet banking, and mobile banking are the electronic channels used by the customer. Customers are unaware the importance of Internet banking, they put more concern about the security and privacy of the Internet banking usage. Hence researchers develop “Internet banking security software” for Internet banking customer. This software provides guidelines to the customer how to perform Internet banking transactions securely is really useful for the customer when the customer follows all specified steps when doing Internet banking transaction.

1.2 REQUIREMENT SPECIFICATIONS

1.2.1 Proposed Environment
Front end: ASP.Net, C#.Net, JavaScript
Back end: SQL server 2008

1.2.2.1 Hardware Requirements:
Processor: P-IV and above
RAM: 512 MB or Above
HDD: 80GB or more

1.2.2.2 Software Requirements:
Operating System: Windows XP and above.
1.3 TECHNOLOGY USED:

1.3.1 The .NET Platform
Due to the software development world is in constant change. One of the most recent and largest changes was the unleashing of .NET, a platform that provides a common runtime environment that can be targeted by any programming language. Programmers can be used by several languages that support .NET, making the application logic easier to reuse in other environments. For examples, logic of a .NET application that manages inventory could be seamlessly integrated into other applications, including web based applications or programs written in other languages.

1.3.2 ASP.NET is integrated with the .NET Framework:
The .NET Framework is divided into an almost painstaking collection of functional parts, with a staggering total of more than 1,000 types (the .NET term for classes, structures, interfaces, and other core programming ingredients).

1.3.3 ASP.NET is compiled. Not Interpreted:
One of the major reasons for performance degradation in ASP scripts is that all ASP webpage code uses interpreted scripting languages.

1.3.4 ASP.NET runs inside the Common Language Runtime:
Perhaps the most important aspect of ASP.NET to remember is that it runs inside the runtime engine of the CLR. The whole of the .NET framework that is, all namespaces, applications, and classes are referred to as managed code.

1.3.5 The C# Language:
C# is a programming language developed by Microsoft. Because it uses the .NET platform, it has an extensive set of software components, making it a highly productive programming tool. With C#, anyone can quickly create Windows based applications, web based applications, Console applications, network programs, database applications, or programming libraries that can be used by other applications. C# is an object oriented language, which means that a C# program consists of a set of objects that communicate with each other at runtime. These objects are described by classes that you define when you write your program.

1.3.6 ADO.NET:
ADO.NET is a large set of .NET classes that enable us to retrieve and manipulate data, and update data sources, in many different ways. As an integral part of the .NET framework, it shares many of its features. Features such as multi-language support, garbage collection, just-in-time compilation, object-oriented design, and dynamic caching, and is far more than an upgrade of previous versions of it. ADO.NET is set to become a core component of any data-driven, .NET application or Web service, and understanding its power will be essential to anyone wishing to utilize.NET data support for maximum effect.

1.3.7 SQL Server 2008:
The SQL Server simplified database administration, its tight integration with the operating system's security subsystem and error logging capability and its compatibility with Windows services provides a broad-spectrum information service provider. Also, its tight integration with the operating system provides highly tuned enterprise solution for almost all database requirements. SQL Server 2008 is the back end of the .Net framework. It is used to build a database for the technology. The data can be bind with creating the new connection to the server. On the SQL server, researchers can build his query and can fire it

1.3.8 Communication Interfaces:
HTTP, SMTP protocol is used for communication interface
1.4 SCREENSHOTS OF “INTERNET BANKING SOFTWARE”

Internet banking security software is the application developed by the researcher to provide control of illegal access. Through this software customer is aware of the preventative measures before using Internet banking technology. Through this software chances of fraud are reduced. This software provides the facility to know the steps obligatory to update the software’s which control unauthorized access of banking transaction. The researcher provides backup facility through Email ending, check password strength; avoid phishing, removes sessions and cookies. This software is admiration to all customers gives the assistance to control psychological, security, Money transfer, and operational risk.

1.4.1 Login page: - Login page is important to be in command of illegal access. Through this login page, only authorized user can use the system, hence it will provide security to the user application. By using this page customer can login the Internet banking security software.

Screenshot no: - 1.4.1 Loginto “Internet banking security software”

![Login Window](image1)

Internet banking Security Software

1.4.2 Home Page: - This home page provides a guideline for customersto do secure Internet banking transactions, provides information about Internet banking services and views the latest news regarding hacking. If the user follows all these steps, then he securely does the Internet banking transaction.

Screenshot no: - 1.4.2 Home page
1.4.3 About us: - This web page provides required steps for secure Internet banking transactions. The user must follow these steps to avoid hacking. Screenshot no: 1.4.3 About us page
First facility is the software updating facility customer update his/her computer to stop the use of a computer with an insecure operating system. Also update Microsoft Windows, antivirus software. The password strength facility helps to prepare strong passwords because for secure transactions, customer require to change the password at least every 3 month and never reuse an old password. Phishing is another type of attack in this attack similar websites of banks is prepared by a hacker. Customer unfortunately logon to the fake website then full transaction is hacked by the hacker. Hence researcher provides facility to only click on the bank website and system directly connects to the bank website. For keeping transaction backup, data are sent to the e-mail through this website. Cookies are saved in the browser side and sessions are saved on the server side. The server uses cookies for tracking the user’s sessions. A hacker can easily track the user therefore removal of cookies is important. If a user deletes cookies, the server loses track of the client and hence it will automatically terminate the connection.
sessions. The researcher provides ‘Clean’ option through this option cookie and sessions are removed from the site.

1.4.4 Operating system updating guideline:

The operating system is the most important part of the software because it vulnerabilities such as viruses, worms, bugs and other bad things affect the entire machine. Protecting computer system with available data on it, the customer must need to update the software regularly. This webpage search user computer operating system and displays a name of the operating system. In the next step software provides a guideline for users to update the operating system. The user must perform the above described steps and update operating system regularly.

1.4.4.1 Find OS:-

During this step user click on ‘Help Desk’ option, then click on ‘OS updates’ after that ‘find OS’ option is available. The user just clicks on this option then immediately software gives message regarding available operating system for customer computer.

Screenshot no: - 1.4.4.1 Find OS

![Image of Operating System](https://example.com/image.png)

1.4.4.2 Updation of Windows 7 and Vista: -Screenshot no 1.4.4.2 provides steps to Windows 7 and Vista updation. The user follows these steps for Windows installation

Screenshot no: - 1.4.4.2 Updation of Windows 7 and Vista OS
1.4.4.3 Updating Windows XP Operating System: - Windows XP update steps are described here.
Screenshot no: - 1.4.4.3 Steps for updating Windows XP Operating System
1.4.5 **Antivirus updates:** - Computer viruses are malicious programs written in order to damage another person’s computer and steal information or cash during the transaction. Worms, Trojans and malware these three are hazardous virus damage the computer system. Antivirus is the software which protects the computer system from incoming threats and seeks out, destroys and warns of possible threats to the system. Antivirus protects the computer system. The virus-related code exploits the loophole to elevate its own privileges and as a result, improvements full access to the computer. Hence, performing updates of computer software regularly is the inevitability of evading hacking. In this software, the researcher provides a facility to find antivirus available in the computer system. Antivirus is periodically updated by the system, hence no need to update antivirus. Whenever a user performs an Internet banking transaction must check the updating status of antivirus.

Screenshot no: - 1.4.5 Find Antivirus of user’s computers
1.4.6 Removal of Spyware: Spyware is software that can install automatically or run on your computer without any intimation. Spyware can monitor customer online behaviour or collect information about the customer (including personally identifiable or other sensitive information), change settings on your computer, or cause your computer to run slowly. Hence this software provides guidelines about how to overcome these spyware.

1.4.6.1 Removal of Key logger: Keylogger is a computer program that records each keystroke made by a computer user, mainly with the intention of increasing in fraudulent access to passwords and supplementary trustworthy information. It will record instant message, e-mail, any e-mail addresses, customer use and visited website URLs. Keylogger can also be embedded in spyware permitting customer data to be spread to any mysterious third party. Hence the removal of Keylogger is an important task. Screenshot no 1.4.6.1 provide guideline to remove Keylogger from customer computer.

Screenshot no: 1.4.6.1 Steps for removing Keylogger spyware
1.4.6.2 Removal of Trojan, malware and other threats. Malware is software aimed at violence and harm, inactivate, or interrupt computers, computer systems, or networks. Hackers often take benefit of website safety faults, also known as vulnerabilities, to inject malware into existing software and systems. Such types of malware are Trojan, worms, viruses. Worms are malicious programs that create replicas of themselves again and again on the local drive, network shares, etc. The merely determination of the worm is to replicate itself again and again. It doesn’t destroy any data or file on the computer. Trojans are malicious programs that accomplish activities that have not been authorized by the user. Such as deleting, blocking, modifying, copying data, disorder the performance of computers or computer networks. Hence this software provides guidelines to remove these malwares. Screenshot no 1.4.1.2 shows guidelines for eliminating malware from customer computer.

Screenshot no: - 1.4.6.2 Steps for removing Trojans, malware and other threats.
To improve the security of Internet banking transaction, the customer needs to update application software regularly. Updates can fix vulnerabilities in software. If vulnerabilities aren’t fixed, they might allow malware to use an exploit to get on to the customer computer. Hence updating software can help to protect the customer against threats.

### 1.4.7 Updating MS-office, Adobe Acrobat reader and Flash application S/W

To ensure the security of Internet banking transaction, the customer needs to update application software regularly. Updates can fix vulnerabilities in software. If vulnerabilities aren’t fixed, they might allow malware to use an exploit to get on to the customer computer. Hence updating software can help to protect the customer against threats.

**Screenshot no:** - 1.4.7.1 Steps for updating MS-office software
Steps for Installation

1. Insert the Microsoft Office media disc into the DVD drive. Click "Start" followed by "Computer." Double-click the disc drive if Windows fails to launch setup automatically.

2. Enter your product key when prompted and click "Continue." Read the license terms and then check "I Accept the Terms of This Agreement." Click "Continue."

3. Click "Customize." Select the first program or tool from the list and then choose "Run From My Computer." "Run All From My Computer," "Installed on First Use" or "Not Available" from the options.

4. Repeat the previous step for each application or feature. Click "Install Now" to install Microsoft Office to the laptop.
1.4.7.3 Steps for updating Flash software

1.4.8 Encryption/Decryption: - In this webpage researcher provide a demo for encryption and decryption. Encryption is nothing but conversion of user plain text into cipher text and decryption is reverse process of encryption to convert cipher text to again user original plain text. When customer click on encryption button, then the connection string is encrypted again when click on the decryption button then, it will be decrypted. Means when customer login to the bank website if these two strings are encrypted, then it is very difficult for the hacker to hack the user transaction. The researcher tries to keep the system database security.
1.4.8.1 Connection string encryption.

For the most part sensitive information stored in ‘web.config’ file can be the connection string. The customer does not want to reveal the information interrelated to their database to every one of the users where the application is deployed. Every time it is not possible to have a personal machine for customer sites, they may necessitate deploying the site in the shared host surroundings. To encrypt the connection string in the above situation is worthwhile. Hence researcher software provides a facility to encrypt or decrypt the connection string, when customer click on ‘Encryption’ button then the connection string is encrypted.

Screenshot no: - 1.4.8.1 Demo of connection string encryption

![Connection String Encrypted. Please check cipher Connection string at Web.config file](image1)

Screenshot no: - 1.4.8.2 Output of connection string encryption. In `web.config` file connection string is encrypted.
Screenshot no: - 1.4.8.3 Output of connection string decryption

Screenshot no: - 1.4.8.4 Output of connection string decryption. Inweb.config file connection string is decrypted.
1.4.8.5 Query string encryption

Query string encryption is the part of a Uniform Resource Locator (URL) that contains data to be passed to web applications such as CGI programs. The query string is used to transfer small pieces of data between web pages. When readable text data transferred in the query string, the end user might be changing the value in the query string to play around with the application and it leads to compromise the security and data integrity of the system. When a Web page is requested via the Hypertext Transfer Protocol, the server locates a file in its file system based on the requested URL. Through this web page, researcher is encrypting the key-value pairs which are transferred to the next web page. So by using this it is difficult for a hacker to know the actual URL.

Screenshot no: - 1.4.8.5 Demo of Query string encryption
1.4.9 **Password strength checking:** - To do secure transaction, the customer needs to use secure password means tries to make a complicated password. Complicated password is not easily hacked by the hacker. Use of a strong password and change it to regularly make it harder for the hacker to access the information on a customer computer and his online accounts. The password is not fully indestructible and safe and sound measure, but it can assist to construct less vulnerable and deter unauthorized people. This webpage helps the customer to make complicated password and check password strength in percentage.

Screenshot no: - 1.4.9 Password strength checking
1.4.10 Backup of bank transaction through Email: - whenever an Internet banking transaction is performed by the customer in this web page helps to keep a backup of banking transactions. Customers just add an email-id and attach backup transaction details. Then this software sends the transaction files to the specific email-id of the customer.
4.11 Internet Banking transaction

This software provides an Internet banking transaction facility to a customer in which the customer just selects the name of the bank than direct customer logs on to that specific bank site. Hence phishing is controlled. The problem of fake URL, fake sites are always controlled through this process.

Screenshot no: -1.4.11 connecting to the bank website for doing Internet banking transaction
1.4.12 Removal of Session and cookies:

Session, cookies are used to maintain integrity of your Internet banking sessions. It passes each page those customers visit back and forth between server and browser. Default files on a computer, sometimes called 'cache' files, can retain images of data sent or received over the Internet, making them a potential target for a system intruder. Therefore, using this software, customer click on ‘clean’ button, then stored cookies and sessions are deleted from customer computer.

Screenshot no: -1.4.12 Removal of sessions and cookies from a user’s computer.
1.5 CONCLUSION

“Internet banking security software” is the way of securely doing Internet banking transactions. When a customer uses this software’s, then he understands precautions require during an Internet banking transactions. It will help the customer to prevent Internet banking hacking to a certain degree level. This proposed model is one of the demonstrations for bank user and bank organization to make an atmosphere through which security risk, psychological risk, and somewhat Money transfer risk is taken out from the customer mind’s and they involve a step forward to confidently use the Internet banking technology.

1.6 LIMITATIONS

• This software does not offer a facility to automatically bring up-to-date essential application and system software’s
• Through this software’s customer directly connect to the bank site, but no any control over when doing banking transaction

1.7 FUTURE ENHANCEMENTS

• In future researcher develop software which offers a facility to automatically update required application and system software’s
• In future, this software’s provide a facility through which a customer directly connects to the bank site, and provide control over when doing banking transaction.

1.8 REFERENCES

• Black. *ASP.NET 4.0 Projects*. dreamtech.
• https://www.codeproject.com (Accessed on 20/05/2014 at 2:11 pm)
• https://www.w3schools.com (Accessed on 22/05/2014 at 5:44 pm)
• https://www.microsoft.com (Accessed on 24/05/2014 at 8:13 pm)
• https://www.4guysfromrolla.com (Accessed on 21/05/2014 at 3:14 pm)
• https://www.dotnetcurry.com (Accessed on 28/05/2014 at 1:22 pm)
• https://www.forums.asp.net (Accessed on 28/05/2014 at 1:31 pm)
• https://www.c-sharpcorner.com (Accessed on 30/05/2014 at 4:12 pm)