IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Security Issues in E-Banking

Srinivasa. R,

Assistant Professor of Commerce

Government First Grade College, Bangarpet

INTRODUCTION

Online banking, also known as internet banking, e-banking or virtual banking, is an electronic payment system that enables customers of a bank or other Banks to conduct a range of financial transactions through the Banks's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking, which was the traditional way customers accessed banking services.

To access a bank's online banking facility, a customer with internet access would need to register with the institution for the service and set up a password and other credentials for customer verification. The credentials for online banking are normally not the same as those for telephone or mobile banking. Banks now routinely allocate customer numbers, whether or not customers have indicated an intention to access their online banking facility. Customer numbers are normally not the same as account numbers, because a number of customer accounts can be linked to one customer number. Technically, the customer number can be linked to any account with the bank that the customer controls, though the bank may limit the range of accounts that may be accessed to, say, check savings, loan, credit card and similar accounts.

The customer visits the bank's secure website, and enters the online banking facility using the customer number and credentials previously set up. The types of financial transactions that a customer may transact through online banking are determined by the Banks, but usually include obtaining account balances, a list of recent transactions, electronic bill payments, and fund transfers between a customer's or another's accounts. Most banks also enable a customer to download copies of bank statements, which can be printed at the customer's premises (some banks charge a fee for mailing hard copies of bank statements). Some banks also enable customers to download transactions directly into the customer's accounting software. The facility may also enable the customer to order a cheque book, statements, report loss of credit cards, stop payment on a cheque, advise a change of address, and take other routine actions.

Electronic Banking

Electronic banking is the automated delivery of new and traditional banking products and services directly to customers through electronic interactive communication channels. Electronic banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the internet. It should be noted that electronic banking is a bigger platform than just banking via the internet. Electronic banking can also be defined as a variety of platforms such as Internet banking (Online banking), Telephone banking, TV-based banking, Mobile phone banking, and PC banking (Offline banking), whereby customers access these services using an intelligent electronic device, like a Personal Computer (PC). As many as 7% of account holders in the country are using the Internet for banking transactions.

OBJECTIVES OF THE STUDY

To identify the Security issues in relation to e-banking or Online Banking
To Suggest precautionary measures available for safe Banking.

SECURITY ISSUES IN E-BANKING

1. Viruses and Trojans:

Viruses and Trojans are harmful programs that are loaded onto your computer without your knowledge. The goal of these programs may be to obtain or damage information, hinder the performance of your computer, or flood you with advertising. Viruses spread by infecting computers and then replicating. Trojans appear as genuine applications and then embed themselves into a computer to monitor activity and collect information. Using a firewall and maintaining current virus protection software can help minimise your chances of getting viruses and inadvertently downloading Trojans.

2. Card skimming:

Card skimming is the illegal copying and capture of magnetic stripe and PIN data on credit and debit cards. Skimming can occur at any bank ATM or via a compromised EFTPOS machine. Captured card and PIN details are encoded onto a counterfeit card and used to make fraudulent account withdrawals and transactions.

ATM Skimming

Fraudsters can attach false casings and PIN pad overlay devices onto genuine existing ATMs, or they can attach a camouflaged skimming device onto a card reader entry used in tandem with a concealed camera to capture and record PIN entry details

1. EFTPOS (Electronic funds transfer at point of sale) skimming

A foreign device is implanted into an EFTPOS machine that is capable of copying and capturing card and PIN details processed through the machine.

2. Reusing Passwords, Especially Leaked Ones

Many people — maybe even most people — reuse passwords for different accounts. Some people may even use the same password for every account they use. This is extremely insecure. Many websites — even big, well-known ones like LinkedIn and eHarmony — have had their password databases leaked over the past few years. Databases of leaked passwords along with usernames and email addresses are readily accessible online. Attackers can try these email address, username, and passwords combinations on other websites and gain access to many accounts.

Reusing a password for your email account puts you even more at risk, as your email account could be used to reset all your other passwords if an attacker gained access to it.

However good you are at securing your passwords, you can't control how well the services you use secure your passwords. If you reuse passwords and one company slips up, all your accounts will be at risk. You should use different passwords everywhere — a password manager can help with this.

3. Key loggers

Key loggers are malicious pieces of software that can run in the background, logging every key stroke you make. They're often used to capture sensitive data like credit card numbers, online banking passwords, and other account credentials. They then send this data to an attacker over the Internet.

Such malware can arrive via exploits — for example, if you're using an outdated version of Java, as most computers on the Internet are, you can be compromised through a Java applet on a web page. However, they can also arrive disguised in other software. For example, you may download a third-party tool for an online game. The tool may be malicious, capturing your game password and sending it to the attacker over the Internet.

4. Social Engineering

Attackers also commonly use social engineering tricks to access your accounts. Phishing is a commonly known form of social engineering — essentially, the attacker impersonates someone and asks for your password. Some users hand their passwords over readily. Here are some examples of social engineering:

- You receive an email that claims to be from your bank, directing you to a fake bank website and asking you to fill in your password.
- You receive a message on Facebook or any other social website from a user that claims to be an official Facebook account, asking you to send your password to authenticate yourself.
- You visit a website that promises to give you something valuable, such as free games on Steam or free gold in World of Warcraft. To get this fake reward, the website requires your username and password for the service.

Be careful about who you give your password to — don't click links in emails and go to your bank's website, don't give away your password to anyone who contacts you and requests it, and don't give your account credentials to untrustworthy websites, especially ones that appear too good to be true.

Precautions to be taken for safe online banking

- **Keep your computer up-to-date** with antivirus software, operating system patches, firewalls etc and ensure your browser is set to the highest level of security.
- **Beware of unsolicited emails or phone calls** asking you for PINs or passwords – your bank or the police would never ask for these in full.
- **Always type your bank's address into your web browser** – never follow a link in an email and then enter personal details.
- **A locked padlock or unbroken key symbol** should always appear in your browser window when banking online.
- **The 'http'** at the beginning of the website address will change to 'https' when a secure connection is made.
- **When making a payment**, always double check that you have entered the correct account number and sort code.
- **Never leave your computer unattended** when logged in and log off as soon as you're finished, especially on any public computer.
- **Check your statements regularly** – if you notice anything strange, contact your bank immediately.
- **Beware of any unexpected or suspicious looking 'pop-up'** windows that appear during your online banking session.
- **Stop and think about the process** you normally go through to make a payment to someone – be suspicious if it differs from the last time you used it.
- **Fraudsters** sometimes try to trick people into making a real payment by claiming "it's just a test".
- **Create a strong password** - If your bank requires a user-generated password in order to access online accounts make sure you choose one that is strong. The best way to achieve this is by making it long and a mix of upper and lower case letters, numbers, and specialcharacters.

Always avoid using any common words or phrases and never create a password that contains your name, initials, or your date of birth. If your bank allows it, change your password every few months.

CONCLUSION : Over the last few decades information technology has affected the banking industry highly and has provided a way for the banks to differentiate their products and services. After demonetization, e-banking is gaining more importance and thus cannot ignore e-banking on the grounds of the security problems. At the same time banks should focus on using the Internet's unique characteristics and capabilities to make their web sites more reliable.

References :

1. How to geek.com
2. IBA Website, "Online Tax Accounting System", Accessed January 20, 2015, http://www.iba.org.in/oltas.asp
3. Wikipedia
4. http://www.actionfraud.police.uk/tips-for-safe-and-secure-online-banking-jun13