Episteme: an online interdisciplinary, multidisciplinary & multi-cultural journal

Bharat College of Arts and Commerce, Badlapur, MMR, India

Volume 8, Issue 4 December 2019

# *A STUDY OF E-BANKING: ONLINE PAYMENTS SYSTEM*

By Vishakha Torane

**Abstract:**

Electronic banking is also known by names like e banking, virtual banking, online banking, or internet banking. It is the use of electronic and telecommunications network for delivering various banking products and services. Through e-banking, a customer can access his account and conduct many transactions using his computer or mobile phone. Banks around the world provide their banking services online though electronic channels, one of the most widely used is the internet channel. Many people avail internet banking services which is convenient in this day and age. On-line banking platforms allow consumers to manage their accounts globally and at their convenience. The internet banking services should be be at top level of security and risk free in order to be trusted by customers. In this study the attack models have been explained and the top risks factors that the internet banking services come to face and applications have been discussed. This study deals with experimental models that can be applied to curb cybercrime attacks and make the internet banking applications more secure to the consumer strata.

**Keywords:** Internet banking, internet banking risks, internet banking services

## Introduction

Online banking allows customers to make financial transactions on a secure website operated through their bank. On-line banking solutions have many features and capabilities in common, but traditionally also have specific applications. Almost all the banks in the world are providing the online facility that ranges from day to day transactions to account opening, issuing credit cards, paying and getting the loans and debts and providing customers facilities to shop online. Some banks are also providing the facilities to draw cash from their bank accounts online and they can pay their bill online.

The term “Internet Banking” or “e-banking” refers to the use of the Internet as a remote delivery channel for banking services. In other words and according to some resources, internet banking is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting bank branches.

With the use of online banking, the user feels secure and can do it from their home/office and no need to go to bank time to time in physical. Just log in to the website of concern bank and enter your account number and make the payments. One can get access to all the services provided by the banks to perform the desire task. The services offered by the online bank are the same for a customer who is provided in physically interactions and on many occasions banks offer more in the online. Online banking feature seems best for performing their monetary action that they require. So the online service solves the customer's problems and save time for the customers. More people are using their services through the online banking because it is easy to access and save time for not waiting in queues to receive service. In fact, the customer can make transactions by simply clicking on the buttons of his computer.

The idea of paying for goods and services electronically is not a new concept. All around evidence of transactions taking place where at least part of the process is carried on electronically. Variety of schemes has been proposed to allow payment to be effected.

## Literature Review

Internet is bringing so much changing in peoples life that they can get whatever they think by sitting at home and without making any efforts. This is the benefit of using internet. We can see everything from home accessories to services, consultants, gaming to online selling are done through internet. You only need to type the key word which you require and get the results at glance. The same case is with banking. All the international banks and local banks have the online websites that provides services for their customers to get their banks from their homes. The customer can get online forms and you have to fill the form and submit all required information to open new account in the bank. The online service solves customer's problems and he does not have to go the branch of the bank. The banks offer many services for customers as pay services bills as water and electricity. These features are useful for both the customer and the companies because it save a lot of time and reduce the number of the required employee to complete these transactions.

The bank has great benefits from the online banking; the bank can reduce the number of employees and the number of opened branches to offer services to customers. The customer use the online banking to request service from the bank and the bank employee receive and process the customer's requests

## E-banking in India

In India, since 1997, when the ICICI Bank first offered internet banking services, today, most new-generation banks offer the same to their customers. In fact, all major banks provide e-banking services to their customers.

Popular services under e-banking in India

- ATMs (*Automated Teller Machines*)
- Telephone Banking
- Electronic Clearing Cards
- Smart Cards
- EFT (*Electronic Funds Transfer*) System
- ECS (*Electronic Clearing Services*)
- Mobile Banking
- Internet Banking
- Telebanking
- Door-step Banking

Keeping money in electronic wallet can be used whenever required for making payments for various reasons or send money to anyone. E-payments empowers organizations, governments, businesses, individual to avoid hard cash and make cashless payments for various services Food & Beverages; Tickets for events, movies, rail, bus, air, etc.; Local Public Transport (Uber, Ola, Taxi, Rickshaw, etc.); Goods (Apparels, electronics).

Various payment platforms like:

**PayTM**

India's largest payments platform is currently handling millions of transactions. This platform which makes instant payments was founded in 2010. It is a platform which provides a digital wallet to store money. PayTM wallet can also be used to make bill payments, transfer money and avail services from travel, entertainment and retail industry. Payment links, reporting links, payment methods, are the rich solution feature of PayTM. PayTM has the largest saved cards repository.

**MobiKwik**

It is an independent mobile payment network that supposedly connects 25 million users with 50,000 retailers and more. It was founded in 2009 Guru gram. It provides a digital wallet and mobile based payment services. MobiKwik allows its users to use cards, net banking and even cash on delivery service for the purpose of paying bills, recharge and shop in the market. Recently MobiKwik has tied up with grocery, restaurants and other offline merchants which are large and small time.

There are total 10,000,000+ numbers of installs of MobiKwik

**PAYPAL**

An American company is operative in a global online payments system that supports online money handovers and serves as an electronic alternative to traditional payments methods. EBay is the parent company of PAYPAL. *PayPal* is the faster, safer way to send money, make an online payment, receive money or set up a merchant account. PAYPAL operates as a payment processor for online vendors, auction sites, etc.

**PayUMoney**

It is a Gurgaon based company which provides online payments solutions and enables the users to store cash and make payment for various transactions, goods and services. In order to differentiate themselves from other players, they provide wide range of benefits that include one-touch check out and discounts / cash back offers on every transaction made.

PayUMoney also ensures the right purchase and customer satisfaction by providing instant refunds on cancellation of an order also by protecting buyer's right. There are total 100,000+ numbers of installs of Pay Money.

**BHIM**

It is a mobile app, developed by the National Payments Corporation of India. It is based on the Unified Payment

Interface (UPI), where the bank details or even internet is not required to make payments. Simply using mobile number, aadhar card number, name or any banks UPI ID anyone can send or receive money in any preferred language.

**Objectives**

a) To understand the f platforms available for epayments.

b) To examine the effect of epayments contribution towards the sustainability of the business growth.

**What are the Benefits of Online Banks?**

The benefits of online banking are its relative convenience. An individual can access their balances, transfer funds and set up monthly payments from their computers without moving to anywhere. Additionally, the majority of online banks offer mobile applications for your smartphone, although these are also offered by many retail banks as well.

Another popular advantage is is the ability to deposit checks through an app. Many online banks will allow you to do this, including Ally e Check Deposit and CIT Bank's mobile app. Although this was previously limited to more tech-savvy banks, it has also been adopted by many retail banks in recent years.

Rewards programs are another feature that we don't typically see offered by retail banks outside of credit cards. Discover's Cash back Checking account allows customers to earn cash rewards on qualifying debit card transactions.

online banks are almost always open. While most retail banks will be closed on weekends or holidays, online banks allow you to access your account 24/7 and have customer service representatives available around the clock.. You do not have to stand in a queue to pay off your bills. Also you do not have to keep receipts of all of your bills, as you can now easily view your transactions.

**Disadvantages of online banking**

- Understanding the usage of internet banking might be difficult at the first. That said, there are some sites which offer a demo on how to access online accounts (not all banks offer this). So, a person who is new to technology might face some difficulty.
- Security of transactions is a big issue. Your account information might get hacked by unauthorized people over the internet. If the bank's server is down, then you cannot access your accounts.
- Password security is a must. After receiving your password, change it and memorize it. Otherwise, your account may be misused.

**Internet Banking Attacker Modelling**

Internet banking applications can be attacked with different intensity, skill and persistence and these elements are usually correlated with the profile of the human behind the attack. The bank should decide which types of attacker it expects to be more likely than others and focus on defending against these types. Attempting to defend against all categories of attackers may well lead to unnecessary expenditure.

- **Opportunistic attacker/malware:** This type of attack agent attempts to carry out preprogrammed attacks and is limited by the level of intelligence that can be implemented into software at the present date. It is thorough, quick and precise, but can't cope often with unfamiliar circumstances and does not apply intuition or ingenuity to the attack. It targets an entire population of online targets and swiftly moves from one target to the next should the attacks not succeed. It will typically focus on stealing credentials and credit card numbers; and will often try to hijack a system into joining a botnet, putting its network bandwidth and computing power in the service of the botnet controller.

- **Organized crime:** Distinguished mainly by their motivation, these attackers are knowledgeable in security and adaptive to the point of creating custom tools for their attacks (including targeted malware). Security researchers may be motivated by the challenge of overcoming obstacles or by the desire to blow the whistle, while criminal elements are motivated by financial gain and supporting real-life criminal activities (organized crime). Their targets are typically singled out among their peers and the attackers persist in attacking them beyond any initial difficulties.

- **Insiders/disgruntled employees:** While they may not be highly skilled technically, this class of attackers has the advantage that they start "from the inside", with a certain level of privileges and prior knowledge. Their motivation is usually either greed or retaliation for perceived injustices.

- **State-level attackers:** With considerable resources and skills at their disposal and applying a planned, thorough and systemic approach with patience, this type of attacker is the most difficult to defend against. The attacks will blend as necessary offline components such as bribes, infiltration of the target organization, interrogation and military action. The actors carrying out the attacks usually benefit from political and legal protection.

- **Denial of service:** The Denial of Service (DoS) attack is focused on bringing down application, service or website for the purpose it was designed. There are many ways to make a service unavailable for legitimate users by manipulating network packets, programming, logical, or resources handling vulnerabilities, among others. If a service receives a very large number of requests, it may stop providing service to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited, or the way the service handles resources are used. Sometimes the attacker can inject and execute arbitrary code while performing a DoS attack in order to access critical information or execute commands on the server. Denial-of-service attacks significantly degrade service quality experienced by legitimate users. It introduces large response delays, excessive losses and service interruptions, resulting in direct impact on availability. For the internet baking, this model of attacks is being used widely in an organized crime way. This type of attacks model can be generated easily and internet banking applications exposed for such attack. Hence, such model of attack needs to be detected and resisted in a dynamic way

- **Phishing**

  Phishing remains one of the most common attack vectors. With this type of threat, attackers send out bogus emails that resemble secure messages from legitimate banks. The email usually includes a link to a spoof website that looks more or less indistinguishable from the real deal. When you enter your login details on the site, you're inadvertently sending your most confidential login credentials directly into the hands of the bad guys. Alternatively, the email may include an attachment that appears to be an important document. When opened, the attachment installs malicious software on your system.

- **Man-in-the-middle attacks**

  Man-in-the-middle" (aka MITM) means that the communication between two partners has been intercepted. This makes it possible for cybercriminals who can successfully impersonate each endpoint (in this case, you and your bank) to not only eavesdrop on your communications but also manipulate the conversation for their own nefarious purposes. For instance, you might think that you're communicating directly with your bank over a private connection, but the messages are actually being sent and received by the attacker. In the case of "man in the browser" attacks, the attack is performed directly in your browser. In this scenario, SSL encryption, which is designed to protect you from conventional "man in the middle" attacks, is ineffective.

- **Malware**

  Malware designed to steal banking credentials, such as bankers and in stealers, usually inject themselves into running browser processes and thus gains full control. This means that banking malware not only knows which websites you open and exactly what you are doing on these sites – including all user details and passwords that you type in – but is also able to manipulate the website displayed, without your knowledge.

**Finding & Suggestions**

**1. Be wary of your emails**

Phishing is such an effective attack vector because it exploits natural human weaknesses. Combat phishing by staying hyper-vigilant when checking your emails. Be wary of any links included in your emails, avoid opening attachments unless absolutely necessary, and remember that a legitimate bank will never ask for your complete password, TAN, PIN or other credentials.

**2. Use two-factor authentication (2FA)**

2FA provides an extra layer of security by requiring you to input a unique code in addition to your regular username and password. Many banks these days offer 2FA in the form of a small device, which generates a new code that you need to enter every time you log in. Be aware that text messaging 2FA is not a foolproof solution and can be hijacked relatively easily.

**3. Keep your software up to date**

Many attacks rely on exploiting security flaws in a piece of software. To fix these vulnerabilities, developers release updates that bolster the security of their application. Minimise the risk of becoming a victim of a banking attack by always keeping your software up to date and enabling automatic updates where possible.

**4. Don't enter sensitive information while on public Wi-Fi**

Public Wi-Fi has become increasingly accessible in recent years, but that doesn't mean it should be trusted. Many public Wi-Fi networks are unencrypted and unsecured, and those who connect to them are easy prey for man-in-the-middle attacks. In addition, there's little way of knowing if you're actually connecting to a rogue hotspot (a free public network established by an attacker to gain access to your personal information). Never input your banking credentials on public Wi-Fi; instead, wait until you get home to your private network, use your cellular data network, or invest in a VPN service.

### 5. Enable account notifications

Many banks give you the option to enable notifications that will alert you when certain activities take place on your account. For instance, you could set this up to receive a text if a certain amount of money is withdrawn or the funds in your account reach a specified threshold. Account notifications won't actively prevent banking attacks, but they can help you quickly detect suspicious activity and give you a head start on stopping the attack.

### 6. Choose a good password

Attackers don't always steal your banking password – sometimes they guess it. You can reduce the risk of brute force attacks, dictionary attacks, and simple guess attacks by choosing a long, unique and random password. Check out our previous blog post for more information on creating and storing good passwords.

### 7. Be mindful of mobile attacks

It's important to remember that mobile devices are not immune to malware and other types of banking attacks. With this in mind, always use your bank's mobile app, as apps tend to be more secure than mobile browsers. Mobile devices are also more susceptible to theft than PCs, so be sure to secure your device with a password, PIN or fingerprint to make it more difficult for thieves to access your data. For the ultimate layer of security, consider investing in proven mobile security software.

## Conclusion

The online banking helps every one for better services on the cost of security. The system allows customers to transfer money, account inquiry and get the balance sheet and many other services. Besides, the idea to get the cash money is also possible. In that case a portable ATM services which will help handicapped, VIP customer and those who are living in remote areas. They do not have access to branch of the bank can be facilitated by providing services. In contrast if customers hire specialized companies to transfer amount to beneficiaries, is not safe. Places are far from banking services; where bank cannot cover remote population but through the mobile services and ATM, which permit customer cash withdrawals, etc. The digital evolution has triggered the way people are communicating, purchasing products, paying their utility bills online, exchange of information or performing business. The technology has altogether changed the consumer behaviour pattern towards purchasing and utilizing the products or services. They try to take advantage of the various digital platforms to expand their business and for sustainable development growth. The organisations through digital are able to share the experience by giving the consumers various options like variety, discounts, product/service comparison, payment preferences, etc. This has in fact exposed consumers towards the habitual use of browsing products, using different online payments that in turn develop trust and usually loyalty towards the products and/or payment platforms. At the same time companies get the necessary development in their businesses, as the advancement of technology has given them liberty for tracking the consumer's preferences, feedbacks, attitude towards the product, their search patterns, etc.

The organisations are trying their level best to attract the consumers towards using their ecommerce and payment platforms to increase their business, but there have been always a hitch in consumers mind regarding the security and privacy. For sustainable growth it is important for the organisations to consider various technologies to overcome the consumer' s concerns. Technologies like block chains are replacing the expensive, unproductive accounting and payment systems of the financial industry; it can also be used to improve efficiency of regulatory compliance procedures and save on the back-office costs, etc. Biometric it is an advancement of epayment technologies, many consumers usually forget the password or get scared to share the pin number, so biometric along with Internet of Things (IoT) and Artificial Intelligence(AI) will help consumer authenticate the purchase or bill payments through the finger print or a retina scan and also detect online fraud. This will help the consumers to build up the confidence and also improve user interface experience. These are few technologies that can be used to enhance the consumer's online epayment experience. WhatsApp using Unified Payments Interface (UPI) implementation where the user just select the WhatsApp contact, enter the amount followed by the four-digit UPI pin and the funds will be transferred. Many organizations' tie-up with already existing payment gateways that have already built trust for example in merchants like Book-MyShow, redBus, Yatra, etc.; their customers can use Amazon Pay as well.

## Recommendations

In future, services to customer are going to be more enhance. This will be possible by making it easier and using smart phone. It's not only the reason that the use of smart phone is easier, but it keeps up with the new trends and technology. Also, the futuristic expectations are to develop more banking service to help community living in remote area, where the access to bank is not possible or the customer is old enough to reach their physically.

## References

- Asli, Y., 2011. Customer's perspectives and risk issues on e-banking. J. Internet Bank. Commer.
- Internet Banking: A Survey of Current and Future Development. Financial Services Group
- https://bizfluent.com/info-8188352-advantages-disadvantages-epayment.html
- Karamjeet Kaur, D. A. (2015, February). E-Payment System on E-Commerce in India. *Int. Journal of Engineering Research and Applications*. Retrieved from http://www.ijera.com/papers/Vol5_issue2/Part%20-%201/M502017987.pdf
- Mukul, P. (2018, February). E-payment: To tap into India's $200-billion market, WhatsApp bets on improvement. *Social*. Retrieved
- from http://indianexpress.com/article/technology/social/e-payment-to-tap-into-indias-200-billion-market-whatsapp-bets-onimprovement/

## Bio

Vishahka Torane is working as an Assistant Professor at Bharat College of Arts & Commerce. The author can be reached at Vishutorne@gmail.com