E-Banking

Group Members

Olabode Ezekiel Ayodele	IFT/18/6015
Ausi John Oluwatosin	IFT/18/5992
Ajayi John	IFT/18/5984
Falohun Precious Temitope	IFT/18/6000
Adegoke Oluwadamilare Temitope	IFT/18/5976
Osadugba Oreoluwa Mercy	IFT/18/6023
Abimbola Adebusola Denis	IFT/18/5968
Jacob Ayodeji Pelumi	IFT/18/6007
Adedeji Oluwatelemi	IFT/19/2952

Supervised by Dr. Mrs. Boyinbode & Dr. Adebayo

Content

What is E-Banking?

What is banking? Banking is defined as the business activity of accepting and safeguarding money owned by other individuals and entities, and then lending out this money in order to conduct economic activities such as making profit or simply covering operating expenses.

E-Banking refers to electronic banking. It’s like e-business in the banking industry. Electronic banking is also known as “Virtual Banking” or “Online Banking”. Electronic banking is based on banking based on information technology. Under this I.T system, banking services are delivered through a computer-controlled system. This system involves a direct interface with customers. Customers do not have to visit the bank’s facilities.

It is defined as the use of electronic and telecommunications networks for delivering various banking products and services.

History of E-Banking

Electronic banking, or e-banking, is the term that describes all transactions that take place among companies, organizations, and individuals and their banking institutions. First conceptualized in the mid-1970s, some banks offered customers electronic banking in 1985. However, the lack of Internet users, and costs associated with using online banking, stunted growth. The Internet explosion in the late-1990s made people more comfortable with making transactions over the web. Despite the dot-com crash, e-banking grew alongside the Internet.

While financial institutions took steps to implement e-banking services in the mid-1990s, many consumers were hesitant to conduct monetary transactions over the web. It took widespread adoption of electronic commerce, based on trailblazing companies such as America Online, Amazon.com and eBay, to make the idea of paying for items online widespread. By 2000, 80 percent of the US. banks offered e-banking. Customer use grew slowly. At Bank of America, for example, it took 10 years to acquire 2 million e-banking customers. However, a significant cultural change took place after the Y2K scare ended. In 2001, Bank of America became the first bank to top 3 million online banking customers, more than 20 percent of its customer base. In comparison, larger national institutions, such as Citigroup claimed 2.2 million online relationships globally, while J.P. Morgan Chase estimated it had more than 750,000 online banking customers. Wells Fargo had 2.5 million online banking customers, including small businesses. Online customers proved more loyal and profitable than regular customers. In October 2001, Bank of America customers executed a record 3.1 million electronic bill payments, totaling more than $1 billion. In 2009, a report by Gartner Group estimated that 47 percent of U.S. adults and 30 percent in the United Kingdom bank online.

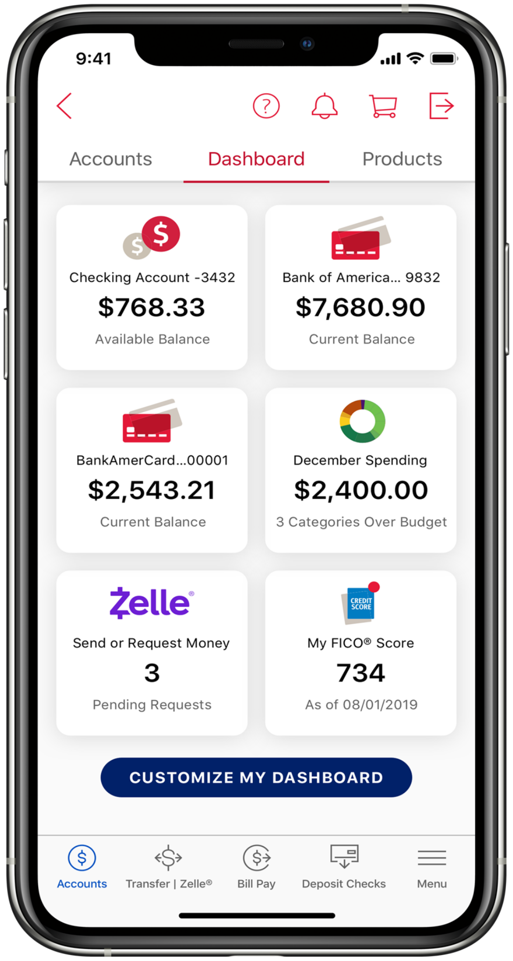
E-Banking Approaches

Since E-banking can be defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels, the e-banking approach can be called the ways by which e-banking is being accomplished .

This are the different approach to E-Banking:

1. **Dial-in Approach:** Requires users to have separate finance software, so that they can do all the process offline and connect to the bank just for transactions. An example of dial in approach is the ussd code which bank users use for offline transactions.

2. **Internet Approach:** Users directly log on to their bank website and complete all their work online. Examples of Internet approach are the mobile apps which we use for our daily transactions.



Checking Account -3432
$768.33
Available Balance

Bank of America... 9832
$7,680.90
Current Balance

BankAmerCard...00001
$2,543.21
Current Balance

December Spending
$2,400.00
3 Categories Over Budget

Zelle®
Send or Request Money
3
Pending Requests

My FICO® Score
734
As of 08/01/2019

Popular Services Provided By E-Banking

Popular services covered under E-banking include: ATMs, Credit cards, Debit Cards, Smart Cards, Electronic Funds Transfer System (EFT), Check the truncation payment system, Mobile Banking, Internet Banking, Telephone Banking, etc.

1. Automated Teller Machines

An ATM is a computerized Teel-communication device which provides the customers the access to financial transactions in public places without human inter-mention. It enables the customers to perform several banking operations such as withdrawals of cash, request of mini-statement etc.

The advantages of ATM are:

ATM provides 24 hours service: ATMs provide service round the clock. The customer can withdraw cash up to a certain limit during any time of the day or night.

ATM gives convenience to bank's customers: ATMs provide convenience to the customers. Now-a-days, ATMs are located at convenient places, such as at the air ports, railway stations, etc. and not necessarily at the Bank's premises.

ATM reduces the workload of bank's staff: ATMs reduce the work pressure on bank's staff and avoids queues in bank premises.

ATM provide service without any error: ATMs provide service without error. The customer can obtain an exact amount. There is no human error as far as ATMs are concerned.

ATM is very beneficial for travelers: ATMs are of great help to travelers. They need not carry large amounts of cash with them.

ATM may give customers new currency notes: The customer also gets brand new currency notes from ATMs. In other words, customers do not get soiled notes from ATMs.

ATM provides privacy in banking transactions: Most of all, ATMs provide privacy in banking transactions of the customer.

2. Electronic Transfer of Funds

This is an electronic debit or credit of a customer's account. Bank customers can buy goods and services without carrying cash by using credit or debit cards. Their cards are issued to the customers by the bankers. This system works on a pin (personal identification number).

The Customer swipes the card by using the card reader device to make the transactions. The development of electronic banking and internet banking helped the customers to utilize their services.

According to the United States Electronic Fund Transfer Act of 1978 it is "a funds transfer initiated through an electronic terminal, telephone, computer (including on-line banking) or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account".

EFT transactions are known by a number of names across countries and different payment systems. For example, in the United States, they may be referred to as "electronic checks" or "e-checks". In the United Kingdom, the term "bank transfer" and "bank payment" are used, while in several other European countries "giro transfer" is the common term.

3. Tele-Banking

Tele-Banking also known as Telephone Banking is a service provided by a bank or other financial institution, that enables customers to perform over the telephone a range of financial transactions which do not involve cash or Financial instruments (such as cheques), without the need to visit a bank branch or ATM.

It is increasingly used these days. It is a delivery channel for marketing, banking services. A customer can do non-cash business related banking over the phone anywhere and at any time. Automatic voice recorders are used for rendering tale-banking services.

To use a financial institution's telephone banking facility, a customer must first register with the institution for the service. They would be assigned a customer number (which is not the same as the account number) and they may be given or set up their own password (under various names) for customer verification.

Customers would call the special phone number set up by the bank and would authenticate their identity through the customer number and a numeric or verbal password or security questions asked by a live representative. The service can be provided using an automated system, using voice recognition capability, DTMF technology or by live customer service representatives.

In India, a variation of telephone banking utilizing missed call numbers, assigned to specific tasks (such as checking balances or performing money transfers), is offered by major banks.

4. Mobile Banking

Mobile Banking is another important service provided by the banks recently, it’s a service provided by a bank or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smartphone or tablet. Unlike the related internet banking it uses software, usually called an app, provided by the financial institution for the purpose. The bank will install particular software and provide a password to enable a customer to utilize this service.

Mobile banking is usually available on a 24-hour basis. Some financial institutions have restrictions on which accounts may be accessed through mobile banking, as well as a limit on the amount that can be transacted. Mobile banking is dependent on the availability of an internet or data connection to the mobile device.

5. **Home Banking**

It is another important innovation that took place in Indian banking sector. The customers can perform a no. of transactions from their home or office. They can check the balance and transfer the funds with the help of a telephone. But it is not that popularly utilized in our country.

6. **Dematerialization Banking**

It is nothing but de-materialization. This is a recent extant in the Indian banking sector. The customer who wants to invest in the stock market or in share and stock needs to maintain this account with the commercial banks. The customer needs to pay certain annual charges to the banks for maintaining this type of account.

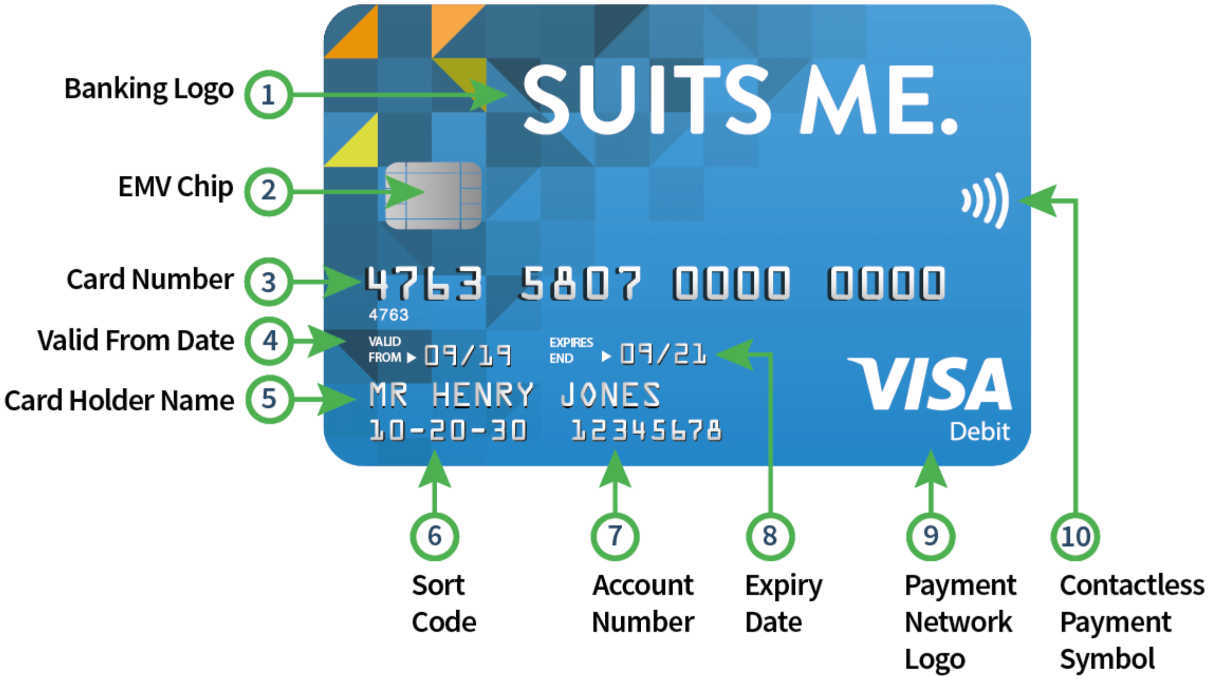
7. **Credit Cards**

A credit card is a small plastic card issued to users as a system of payment. It allows its holder to buy goods and services based on the holder's promise to pay for these goods and services. The issuer of the card creates a revolving account and grants a line of credit to the consumer (or the user) from which the user can borrow money for payment to a merchant or as a cash advance to the user.

A credit card is different from a charge card: a charge card requires the balance to be paid in full each month. In contrast, credit cards allow the consumers a continuing balance of debt, subject to interest being charged. A credit card also differs from a cash card, which can be used like currency by the owner of the card. Most credit cards are issued by banks or credit unions.

Credit cards have a printed or embossed bank card number complying with the ISO/IEC 7812 numbering standard. The card number's prefix, called the Bank Identification Number (known in the industry as a BIN) is the sequence of digits at the beginning of the number that determine the bank to which a credit card number belongs. This is the first six digits for MasterCard and Visa cards. The next nine digits are the individual account number, and the final digit is a validity check code.

Both of these standards are maintained and further developed by ISO/IEC JTC 1/SC 17/WG 1. Credit cards have a magnetic stripe conforming to the ISO/IEC 7813. Most modern credit cards use smart card technology: they have a computer chip embedded in them as a security feature. In addition, complex smart cards, including peripherals such as a keypad, a display or a fingerprint sensor are increasingly used for credit cards.



8. Debit Card

A debit card (also known as a bank card or check card) is a plastic card that provides the cardholder electronic access to his or her bank account/s at a financial institution. Some cards have a stored value against which a payment is made, while most relay a message to the card-holder's bank to withdraw funds from a designated account in favour of the payee's designated bank account. The card can be used as an alternative payment method to cash when making purchases. In some-cases, the cards are designed exclusively for use on the Internet, and so there are no physical cards. In many countries the use of debit cards has become so widespread that their volume of use has overtaken or entirely replaced the check and, in some instances, cash transactions. Like credit cards, debit cards are used widely for telephone and Internet purchases. However, unlike credit cards, the funds paid using a debit card are transferred immediately from the bearer's bank account, instead of having the bearer pay back the money at a later date.

In many countries, such as most of Spain, the use of debit cards has become so widespread they have overtaken cheques in volume, or entirely replaced them, and in some instances, also largely replaced cash transactions. The development of debit cards, unlike credit cards and charge cards, has generally been country-specific, resulting in a number of different systems around the world, which were often incompatible. Since the mid-2000s, a number of initiatives have allowed debit cards issued in one country to be used in other countries and allowed their use for internet and phone purchases.

Debit cards usually also allow instant withdrawal of cash, acting as an ATM card for this purpose. Merchants may also offer cashback facilities to customers, so that a customer can withdraw cash along with their purchase. There are usually daily limits on the amount of cash that can be withdrawn.

9. **Cheques Truncation Payment system (CTPS)**

   Truncation is the process of stopping the flow of the physical cheque issued by a drawer to the drawee branch. The physical instrument will be truncated at some point enroute to the drawee branch and an electronic image of the cheque would be sent to the drawee branch along with the relevant information like the MICR fields, date of presentation, presenting banks etc. Thus with the implementation of cheque truncation, the need to move the physical instruments across branches would not be required, except in exceptional circumstances. This would effectively reduce the time required for payment of cheques, the associated cost of transit and delay in processing, etc., thus speeding up the process of collection or realization of the cheques.

Advantages and Disadvantages of E-banking

E-Banking now-a-days is a common trend here in our country. Everyone should be aware of all the positive and negative sides of technology. Everything has its pros and cons and e-banking isn’t an exception. Let us look at the advantages and disadvantages of e-banking:

Benefits/advantages of electronic banking are:

All the advantages of e-banking are closely related to each other; from convenience to efficiency

1. **Notifications and Alerts:**

   Customers are instantly alerted or notified about new changes in the system. From changes in the policy to logins from new devices, customers get instant notifications and alerts. However, if you’re associated with a real bank, you would probably get a text alert or a customer service agent will call you to notify you about major changes. Chances are, you’re missing out on a lot of changes.

   Banks also endorse new products, services and schemes like new investment options, changes in the loan policies, etc. to online customers first.

2. **Faster Transactions:**

   You don’t have to wait for your turn to transfer funds – you can do that with a single tap of your finger or a single click of your mouse. Funds from one account will be transferred to another in a matter of a few seconds. Anything that requires quick payments can be done with the help of e-banking. For instance, you are required to immediately pay your child’s school fees. You can do it via the bank’s app or website or you can physically go to the bank to withdraw cash and then going to the school to deposit the fees.You’ll probably end up wasting half the day to perform this transaction which with the app’s help could’ve been performed in a matter of minutes.

3. **Offers convenience to customers since they are not required to go to the bank’s facilities:**

   You can conveniently handle your account transactions without all the hassle of being in the queue on a sultry afternoon.

   E-banking is extremely convenient if you have a decent internet connection (wifi or 3G/4G data). You can access the website from anywhere without actually having to visit the bank. If your banking needs don’t involve the assistance of any staff member or a manager, online banking is the best option for you.

4. **Security**

With internet banking, you can always monitor your account activities.This not only serves as a history of all the transactions but also helps you identify threats and suspicious activities before any severe damage can be done to your account.

Online accounts are protected with encryption software that ensures complete safety to the user. Alerts related to passwords and digital signatures are sent periodically to maintain the security of the account.

5. **Easy Access**

Customers can enjoy easy access with online accounts by simply typing in the log-in credentials. In addition to that, customers can also handle several accounts at a time.

Since the internet remains the medium of connection, users can also access different accounts in different banks from a single device.

6. **It is fast and efficient**

In a hurry to apply for an educational loan? Or quickly need to pay bills? Or perform any banking transaction without having to waste half your day? Do it via the internet.

There’s no waiting nor do you have to rush through anything – you can take your time and perform all banking transactions with patience and it will be done in nearly 1/10th the time spent on actually driving down to the bank and getting it done.

7. **It has lesser limitation**

Traditional banks have several constraints like operating hours, the physical location of the bank branch, holidays, etc.

You don’t have to wonder if it’s a holiday with online banking, or what time it is to perform a transaction. Be it Sunday or the middle of the night and you will still be able to do everything (and even more) through their app or website as it's available twenty-four hours a day, throughout the year.

8. **It provides Better Customer Service**

   Banking websites and apps that come with customized web pages to solve customer queries and often have a dedicated 'Frequently Asked Question' (FAQs) section that helps in answering common customer queries.

   You can chat with a customer service agent or call them if you need more help. This not only saves the time of the customers but also that of the bank employees who can shift their focus to more important things.

Disadvantages/Shortcomings of Electronic-banking are

"Every bean has its black"Everyone and everything has some shortcomings. Similarly, there are some limitations of net banking; from security to technology issues

1. **Difficult for people without technical knowledge technical or beginners:**

   Newbies often face difficulty in trying to get the hang of E-banking. Initially, customers are scared of losing their money and are often hesitant to explore all the options and features that are available on the website or on the app.

   New users often give up and stick to traditional banking if timely assistance isn't provided.

2. **Trust and Responsibility**

   Fake websites and phishing sites are common in this age of technology. Can you really trust all websites? Is it wise to trust an online site with all your money? What if the website folds up and all your money is gone? This wouldn't happen in a real bank.

There is trust between the bank and their customers – you know your money is safe with the bank – because they take responsibility for your money. Real banks are permanent and reliable while some websites are not.

While you can easily pay bills and transfer funds, you can’t perform complex transactions online.

3. **Inability to handle complex transaction**

When a large sum of money is involved, it is advisable to visit a real bank and sort it out in-person rather than doing it online.

Some financial transactions also need a document verification (like buying a house) so it is better to submit them physically than digitally.

4. **Financial jargon**

Financial jargon can often get between you and your money. Knowledge is power-or, in this case, knowledge is money.

Though financial literacy can’t be achieved overnight, it can be helped along by a grasp of the basic terms that are commonly used by advisors, analysts, economists, and commentators.

5. **Security issues**

Sure, most banks are well-reputed and established, there are times when you face security issues.There’s always a risk of actual and/or identity theft. It’s also possible to get unauthorized access to your account via a stolen or hacked log-in credential.

6. **Technology issues**

If you don’t have a decent connection or there are bugs in the software, or say, there is a power cut or maybe the servers have gone down – websites are bound to crash and you will undoubtedly face a lot of technological issues.

Wireless or Mobile Banking

Wireless banking is a delivery channel that can extend the reach and enhance the convenience of internet banking products and services.Wireless banking occurs when customers access a financial institution's network(s) using handheld devices such as cellular phones,pagers and personal digital assistants(or similar devices)through telecommunication companies' wireless networks.Wireless banking services in the United States typically supplement a financial institution's e-banking products and services.

Wireless devices have limitations that increase the security risks of wireless- based transactions and that may adversely affect customer acceptance rates.Device limitations include reduced processing speeds,limited battery life,smaller screen sizes,different data entry formats,and limited capabilities to transfer stored records.These limitations combine to make the most recognized Internet language,Hyper-text Markup Language (HTML),ineffective for delivering content to wireless devices.

Wireless Markup Language (WML) has emerged as one of a few common language standards for developing wireless device content.Wireless Application Protocol (WAP) has emerged as a data transmission standard to deliver WML content.

Manufacturers of wireless devices are working to improve device usability and to take advantage of enhanced "third generation" (3G) services.Device improvements are anticipated to include bigger screens,color displays,voice recognition applications,location identification technology (e.g.Federal Communications Commission (FCC)Enhanced 911),and increased battery capacity.These improvements are geared towards increasing customer acceptance and usage.Increased communication speeds and improvements in devices during the next few years should lead to continued increases in wireless subscriptions.

Risk Implications of Wireless Banking

Wireless banking service can significantly increase a financial institution's level of transaction/operations and strategic risks.

Transaction/Operations risk - Wireless services create a heightened level of potential operations risk due to limitations in wireless technology.Security solutions that work.I'm word networks must be modified for applications in a wireless environment.The transfer of information from a wire to a wireless environment can create additional risks to the integrity and confidentiality of the information exchanged.

Strategic risk: Financial institutions considering wireless services should carefully evaluate the significant strategic risk posed by this service delivery channel.Standards for wireless communication are still evolving,creating considerable uncertainty regarding the scalability of existing wireless products.Financial institutions should exercise extra diligence in preparing and evaluating the cost-effectiveness of investments in wireless technology PR in decisions committing the institution to a particular wireless solution,vendor or third-party service provider.

Risk Management of Wireless Banking

Risk management of wireless-based technology solutions, although similar to other electronic delivery channels, may involve unique challenges created by the current state of wireless services and wireless devices.Some of these special considerations are discussed below.

Message Encryption in Wireless Banking

Encryption of wireless banking activities is essential because wireless communications can be recorded and replayed to obtain information.Encryption of wireless communications can occur in the banking application,as part of the data transmission process, or both.

Transactions encrypted in the banking application(e.g.bank-developed for a PDA) remain encrypted until decrypted at the institution. This level of encryption is unaffected by the data transmission encryption process.However, banking-application level encryption typically requires customers to load the banking application and its encryption/decryption protocols on the wireless devices.Since not all wireless devices provide application-loading capabilities,requiring application level encryption may limit the number of customers who can use wireless services.

Wireless encryption that occurs as part of the data transmission process is based upon the device's operating system.A key-risk management control point in wireless banking occurs at the wireless gateway-server where a transaction is converted from a wireless standard to a secure socket layer (SSL) encryption standard and vice versa.

Wireless network security reviews should focus on how institutions establish,maintain and test the security of systems throughout the transmission process,from the wireless device to the institutions' systems and back again.For example,a known wireless security vulnerability exists when the Wireless Application Protocol (WAP) transmission encryption process is used.

WAP transmissions deliver content to the wireless gateway-server where the data is decrypted from WAP encryption and re-encrypted for Internet delivery.This is often called the "Gap-in-WAP" (e.g.,wireless transport layer security (TLS) to Internet-based TLS).The brief instant of decryption increases risk and becomes an important control point,as the transaction may be viewable in plain text (unless encryption also occurred in the application layer). The WAP Forum,a group that oversees WAP protocols and standards,is discussing ways to reduce or eliminate the gap-in-WAP security risk.

Institutions must ensure effective controls are in place to reduce security vulnerabilities and protect data being transmitted and stored.Under the GLBA guidelines,institutions considering implementing wireless services are required to ensure that their information security program adequately safeguards customer information.

Password Security in Wireless

Wireless banking increases the potential for unauthorized use due to the limited availability of authentication control on wireless devices and higher likelihood that the device may be lost or stolen.Authentication solutions for wireless devices are currently limited to username and password combinations that may be entered and stored in clear text view (i.e.,not viewed in asterisks "****").This creates the risk that authentication credentials can be easily observed or recalled from a device's stored memory for unauthorized use.

Cellular phones also have more challenging methods to enter alphanumeric passwords.Customers need to depress telephone keys multiple times to have the right character displayed.This process is complicated if a phone does asterisk password entries,as the user may not be certain that the correct password is enters.This challenge may result in users selecting passwords and personal identification numbers that are simple to enter and easy to guess.

Standards and Interoperability in Wireless Banking

The wireless device manufacturers and content and application providers are working on common standards so that device and operating systems function seamlessly.Standards can play an integral role in providing a uniform entry point to legacy transaction systems. A standard interface would allow institutions to add and configure interfaces,such as wireless delivery, without having to modify or re-write core systems. Interoperability is a critical component of mobile wireless because there are multiple device formats and communication standards that can vary the user's experience.

Wireless Vendors in Wireless Banking

Institutions typically rely on third-party providers to develop and deliver wireless banking applications.Reliance on third-parties is often necessary to gain wireless expertise and to keep up with technology advancements evolving standards.Third-party providers of wireless banking applications include existing Internet application providers and as well as new service providers specializing in wireless communications.

These companies facilitate the transmission of data from the devices to the Internet banking application.Outsourced services may also include managing product and service delivery to multiple communication standards.Institutions that rely on service providers to provide wireless delivery systems should ensure that they employ effective risk management practices.

Products And Service Availability in Wireless

Wireless communication "dead zone"- geographic locations where users cannot access wireless systems - expose institutions and service providers to reliability and availability potables in some parts of the world.For some areas,the communication dead zones may make wireless banking an unreliable delivery system.Consequently,some customers may view the institution as responsible for unreliable wireless banking services provided by third-parties.

A financial institution's role in delivering wireless banking includes developing ways to receive and process wireless device requests.Institutions may find it beneficial to inform wireless banking customers that they may encounter telecommunication difficulties that will not allow them to use the wireless banking products and services.

Disclosure And Message Limitations

The screen size of wireless devices and slow communication speeds may limit a financial institution's ability to deliver meaningful disclosure to customers.However,use of a wireless delivery system does not absolve a financial institution from disclosure requirements.Moreover,limitations on the ability of wireless devices to store documents may affect the institution's consumer compliance disclosure obligations.

Additionally, any institution that opts to rely upon voice recognition technology as a means to overcome the difficulty of entering data through small wireless devices should be aware of the certain status of voice recognition under the E-SIGN Act.

Wireless banking may expose institutions to liability under the Electronic Fund Transfer Act (Regulation E) for unauthorized activities if devices are lost or stolen.The risk exposure is a function of the products,services and capabilities the institution provides through wireless device to its customers.For example,the loss of a wireless device with a stored access code gpr conducting electronic fund transfer would be similar to losing an ATM or debit card with a personal identification number written on it.

However,the risk to the institution may be greater depending on the types of wireless banking services offered (e.g.,bill pay,person-to-person payments) and to the authentication process used to access wireless banking services.

Security Features

Encryption

Bank-level encryption is the highest level of encryption. This provides financial institutions with a high level of protection of customer data and assets. Bank-level encryption helps protect the client's transmitted information from intruders.

Bank-level encryption has the following features:

- protects against unauthorized reading;
- protects against deliberate violation of the integrity or nullification of customer data;
- protects against unwanted copying;
- protects against falsification.

Banks use 128-bit encryption and 256-bit AES, it encrypts the data, turning it to unreadable, when the data reach the right place, it turns to readable. 256-bit encryption is a powerful combination that provides extensive data protection compositions. That is, banks encode money data through this encryption. If a hacker wants to crack 256-bit encrypted data, he will need 2256 different combinations. Even the fastest computer cannot withstand such a load.

Bank encryption uses symmetric encryption which involves only one cryptographic key. Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both the encryption of plain-text and the decryption of cipher-text. The keys may be identical, or there may be a simple transformation to go between the two keys. By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it. Each time you begin an online banking session, your computer and Online Banking systems agree on a random number that serves as the key for the rest of the conversation. What that random number could be depends largely on the strength of encryption your browser utilities.

You know that your data has been encrypted on a given Web page by looking for the following icons in the lower portion of your browser.

Browsers

Netscape Communicator 4.0

Microsoft Internet Explorer (any version) .

Netscape Communicator 4.0 and Microsoft Explorer do not display an icon that distinguishes between 40-bit and 128-bit encryption. However, with Netscape Communicator 4.0, you can click on the icon to determine what level of encryption is being used for a particular Web page.

All Online Banking approved browsers provide detailed information on security levels in the "Preferences" or "Internet Options" section located in the browser's menu bar. See your browser's help or documentation for more information.

If for any reason your secure session ends, your Online Banking session terminates.

Authentication

In banking security, authentication is the process of verifying whether someone (or something) is, in fact, who (or what) it is declared to be. Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. In a normal banking authentication we have the username and password as a form authenticating users but that's a weak form of security because it’s susceptible to attacks e.g. brute force.

Some of the new authentication method used in banks

- PIN: Is a personal identification number. It is commonly assigned to bank customers to use for transactions of ATM

- Virtual Keyboard: It's a keyboard shown on the screen. The user needs to enter his password by clicking on the proper characters
- Partial Password: Authenticating by requesting some random characters from the user's password instead of the full password
- Secret Image: The user would have to select one memorable image from a group of random images to verify his identity
- Smart Card: It has an inbuilt memory with the user's credentials and only requires a password to gain access
- USB token: It is similar to a smart card. USB token is a secure way to provide authentication by providing credentials
- Security Questions: Security questions are used to authenticate users when they forgot or lost their passwords
- Bookmark authentication: Bookmark authentication depends on a bookmark the user creates during the registration process. It's often sent to the new customer via emails, so he/she can add it easily.

Using one-time passwords that are valid for one time use only could solve this problem and reduce the risk. One Time password is valid for one time use and a new password is generated for the next authentication process

- OTP manual: which is randomly generated and sent to your registered mobile number and registered email address for validation of your transaction? This is to provide an enhanced level of security on card transactions.
- OTP automatic: With Auto OTP, after you log into your bank Mobile app, your one-time PIN (OTP) will be encrypted, sent directly to your app and verified in the background, saving you the trouble of keying in an OTP provided to you via SMS or your physical token. Auto OTP is quicker, more convenient and secure.
- OTP synchronous: A synchronized OTP is usually related to a piece of hardware called a security token (e.g., each user is given a personal token that generates a one-time password). It might look like a small calculator or a key-chain charm, with an LCD that

shows a number that changes occasionally. Inside the token is an accurate clock that has been synchronized with the clock on the proprietary authentication server. On these OTP systems, time is an important part of the password algorithm, since the generation of new passwords is based on the current time rather than, or in addition to, the previous password or a secret key

- OTP a-synchronous: When the OTP is generated only after a challenge code is first input into the token, this is called an "asynchronous token" because the OTP is not being generated on any regular basis. It is only generated when the user enters the challenge code.

The problem with password is that users tend to use short and common combinations to avoid memorizing

The three algorithms of OTP:

A special algorithm is used to generate a dynamic password on the fly. There are three different algorithm options:

- Time-based
- Event-based
- Challenge-response

Time-based

With this method, the security token (client) and server create synchronized passwords using the same algorithm. This type of time-based one-time password (TOTP) is therefore known on the user side and the server side and is valid for a precisely defined time interval, usually 1 to 15 minutes.

Event-based

Event-based one-time passwords are generated by performing a specific action, for example by pressing a button on the security token. As with the time-based method, the same algorithm is used on the server side and the user side. The password is calculated based on the previous password so it can be validated by the server.

Challenge-response based

In this method, the server specifies a request (challenge), which the client must answer (response). The client receives a certain value from the server and uses it to calculate the one-time password. Since the server knows the algorithm and the specified value, it can check the generated password.

Advantages	Disadvantages
Difficult to crack during replay attacks	Additional technology needed
No danger that a stolen password can be used for multiple sites or services	Security tokens can fail or break
Greater security for users	Process of OTP password generation can be cumbersome

Multi Factor Authentication

Multi Factor authentication (MFA) is a security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction. MFA is based on this major factors:

- Something the user has: Some physical object in the possession of the user, such as a security token (USB stick), a bank card, a key, etc.
- Something the user knows: Certain knowledge only known to the user, such as a password, PIN, TAN, etc.

- Something the user is: Some physical characteristic of the user (biometric), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.
- Somewhere the user is: Some connection to a specific computing network or using a GPS signal to identify the location.

Advantages of MFA:

- No additional tokens are necessary because it uses mobile devices that are (usually) carried all the time.
- As they are constantly changed, dynamically generated pass-codes are safer to use than fixed (static) log-in information.
- Depending on the solution, passcodes that have been used are automatically replaced in order to ensure that a valid code is always available, transmission/reception problems do not therefore prevent logins.

Disadvantages of MFA:

- Users may still be susceptible to phishing attacks. An attacker can send a text message that links to a spoofed website that looks identical to the actual website. The attacker can then get the authentication code, user name and password.
- A mobile phone is not always available—they can be lost, stolen, have a dead battery, or otherwise not work.
- Mobile phone reception is not always available—large areas, particularly outside of towns, lack coverage.
- SIM cloning gives hackers access to mobile phone connections. Social-engineering attacks against mobile-operator companies have resulted in the handing over of duplicate SIM cards to criminals.
- Text messages to mobile phones using SMS are insecure and can be intercepted by IMSI-catchers Thus third parties can steal and use the token.
- Account recovery typically bypasses mobile-phone two-factor authentication.

- Modern smartphones are used both for receiving email and SMS. So if the phone is lost or stolen and is not protected by a password or biometric, all accounts for which the email is the key can be hacked as the phone can receive the second factor.
- Mobile carriers may charge the user for messaging fees.

Serious Account Management

Although much of the banking world is rapidly moving online, many bank account management processes still need to be completed manually. However, banks can facilitate the process with advanced security, automatic elimination of irregular payments, and closer relationships between front office, back office and the client. E-banking sees a lot of positive developments in this process. Having a close relationship with the client and having a high quality process internally can make life a lot easier for both parties. According to the World bank, three steps are important in this client-bank relationship and the services provided.

Step One – Customer Due Diligence

Bank accounts reveal all financial activity and they come under the close scrutiny of regulations such as Sarbanes-Oxley in the US, or the Tabaksblat code in Holland, CBN in Nigeria. To comply with these regulations, corporations are required to go through a process of due diligence with their bank before opening an account.

Within the financial institution (FI), this process is known as Know Your Customer (KYC). FIs have an obligation to know who their clients are, what they do and if their business is legal. The customer due diligence (CDD) process is twofold: it includes checking the client and also checking the client's payment transactions.

Documents that the bank needs to obtain include authorized signatures and passport details from the company's board members, Chamber of Commerce papers and also the company's holding structure. Banks take a proactive role in this process. A checklist of required documentation is provided and the bank stays in close contact with corporate to lower this paper-burden as much as possible.

How can banks make this process easier?

Once the initial CDD process has been completed and the customer has opened its account with the bank, the bank needs to update this information periodically. Chris Sunderman, sales manager for Rabobank Financial Logistics, says: “The challenge for banks is to obtain this information from the client without excessive disruption.”

There are ways of reducing the burden on the corporate and banks can facilitate the CDD process by filling out forms on the corporate’s behalf. Sunderman adds that: “Having a close relationship with both front and back office makes it easier for the bank to communicate with the client and reduce the paperwork.”

In turn, companies also need to look at their relationships with suppliers and buyers, and this process is comparable to the CDD conducted by banks on prospective customers. Part of this process involves establishing credit limits for buyers in order to control their risks.

Step Two – Implementation

Implementation is the second step. The client has accepted the bank account offer and the CDD is completed. A team has to be put in place to manage the bank account implementation, which includes the bank’s implementation manager, a back office coordinator and a representative from the corporate, for example the treasurer or someone from administration.

Corporate bank account requirements

The bank account requirements of each corporate need to be assessed and summarized in a service agreement. The corporate’s criteria for this agreement will include particulars of tariffs, fees, speed of service and cut off times of payments.

According to Eelco Kaan, head of corporate operations at Rabobank, sensitivity to the client’s needs is very important. He says: “The bank account organization will vary depending on the company's structure and its activities – for example importing, exporting or domestic activities. It also depends on a centralized or a decentralized treasury structure."

For example, a corporation in the food and agricultural industry trades in products that have a limited life span and the payment needs to be made so that the goods are shipped the same day. Therefore the bank has to ensure that those payments are a priority.

Step Three – Ongoing Security and User Identification

Security and user identification play an important role in the payment process for large corporations, even more so compared with small corporate or retail payments. Large payments mean high risks, so there are severe auditing restrictions. In large companies there can be many people involved in payments, so authorization may require several levels and can be complex. For example, a holding company can have several hundred accounts with a number of officers authorized to make payments on each account. Banks are obliged to check that the authorized corporate employees are making the payments.

On the wholesale side, token and signature verification are the two most recent developments in payment security. Tokens that generate unique one-off passwords and numbers can help to prevent fraudulent payments. On the retail side, banks are starting to use mobile phones for identification.

In western Europe, most payments are highly automated and cheque are in decline. However, some payment contracts, such as bulk payment orders, are still authorized with a physical signature, and this could pose some security problems for the bank. Physical signatures are high maintenance because they need to be updated and verified regularly. Sunderman says: "It's the obligation of the bank to go back to its client on a regular basis and check that the authorized signatures are still valid."

The risk of fraud for large corporate payments is hard to quantify; the likelihood is small but the impact is huge. The impact of payment fraud for smaller corporations, for example those in the retail sector, is lower because the volume and value of their payments is relatively low.

Spotting irregular payments

With regards to client transactions, regulations such as OFAC in the US and the European, CBN in Nigeria sanctions list help banks with checking the client’s payments. OFAC and the sanction laws state that irregular payments have to be reported to the regulators. This does not normally affect the corporate and the payment is not usually interrupted.

Most irregular transactions can be picked up automatically. However, many large corporate have irregular payment patterns, so it is a challenge to spot payments that are genuinely irregular. A close client-bank relationship, both on the sales and on the administrative side, is very helpful in this process.

Who is liable for fraudulent payments?

If an employee or ex-employee does successfully execute a fraudulent payment, it is unclear whether the liability for this payment will fall on the bank or the corporate. It depends on what action the company took to prevent the bank executing that payment. For example, the company needs to keep its files up-to-date and it needs to inform the bank when an employee who had authorization to execute payments leaves the company. The bank must also take responsibility and be pro-active in this process of keeping all files updated.

Segregation of functions

Segregation of functions within the bank is important in order to prevent fraud – good practice states that no single employee is responsible for two different steps in the process. Although having one group of people dealing with the customer means the most efficient communication, the mitigation of operational risk means that segregation of duty is necessary. Functions that would be segregated include the verification of manual payments and the subsequent execution of that payment. Kaan says: “It is important that every bank employee involved in processing payments and documents understands the customer’s needs and good communication within the process is vital.”

Opening and managing a corporate account should be a straightforward process, but this depends on the corporate needs and the structure of the accounts they require. The process involves many security measures – maybe more so now than ever before, given the strict regulations on banking and corporate governance, and compliance with anti-money laundering and financial crime prevention legislation.

These regulations provide a lot of chances and opportunities as well. Good communication between the corporate and the bank's front and back offices, as well as user identification tools, such as signature verification and tokens that generate unique passwords, are helping to make the bank account management process as smooth as possible for corporate. The strengthened client-bank relationship will improve this process even more; a beneficial

Session Timeout

According to OWASP(The Open Web Application Security Project) Session timeout represents the event occurring when a user does not perform any action on a web site during an interval (defined by a web server). The event, on the server side, changes the status of the user session to 'invalid' (I.e "not used anymore") and instructs the web server to destroy it (deleting all data contained in it).

Impact of the session timeout on security and best practices:

The Session timeout defines an action window time for a user, this window represents the time in which an attacker can try to steal and use an existing user session…

For this, it's best practices to :

- Set session timeout to the minimal value possible depending on the context of the application.
- Avoid "infinite" session timeout.
- Prefer declarative definition of the session timeout in order to apply a global timeout for all application sessions.

- Trace session creation/destruction in order to analyse the creation trend and try to detect a normal number of session creations (application profiling phase in an attack).

All applications should implement an idle or inactivity timeout for sessions. Session idle timeout should be set to 15 to 60 minutes for most applications. In addition, session timeout must be enforced server-side. If the session timeout is implemented at the client-side, attackers can continue using the session to interact with the server directly.

Another important timeout that seems to be neglected by a lot of applications is the session lifespan timeout or absolute timeout, which means when the lifespan timeout is reached, the system will terminate the session regardless of whether the session is active or idle. In other words, users will have to re-login to the application. This also means the session idle timeout can be extended up to the end of the lifespan timeout. Setting the lifespan timeout to 12 to 24 hours seems to be reasonable for most applications. However, you should follow your company’s policies and standards for these two timeout values.

Digital Certificate

A Digital Certificate is an electronic "password" that allows a person, organization to exchange data securely over the Internet using the public key infrastructure (PKI). Digital Certificate is also known as a public key certificate or identity certificate.

It is true that it is easy to explain what a digital signature is and what its applications are since the term leads to thinking about documents and bureaucratic or administrative procedures. However, talking about digital certificates (which digital signatures are based on) inevitably involves doing so with cryptography and algorithms, a field unknown to many.

Multiple organizations, including financial institutions and banks, use Digital Certificates. Perhaps the most obvious of all is the Secure Socket Layer (SSL), which appears on web pages to ensure the protection of user data by encryption. We can see it next to the navigation bar, in the form of a padlock, to indicate that the website we are visiting is safe and that it can be trusted.

We know how valuable trust is for every organization, especially for financial institutions. However, why are digital certificates so important?

Digital certificates are computer files that are used to provide a digital identity to a person, organization or electronic device. They are issued by recognized certification authorities (CA) and are based on asymmetric cryptography; therefore, they contain a public key and a private key. The first is available to everyone, while the second is only known by the certificate holder. Thus, the privacy of the information exchanged between two users is guaranteed.

A digital certificate contains a series of data associated with the user it identifies, such as its name, the expiration date of the certificate, a copy of the public key and the digital signature of the CA. With all these elements a digital identity is generated, which will be associated, as previously stated, with a person or a device.

The digital certificates are applied to digital signature, thus securing the identity of the signatory and protecting the information contained in the document. In addition, they can carry out authentication operations and encryption (emails, transactions, etc.).

By using digital certificates, the risk of fraud and identity theft is significantly reduced, threats that can pose a severe risk to the reputation of an organization, with significant economic losses. Repudiation is also avoided.

SSL(Socket Socket Layer)

SSL (Secure Sockets Layer) is a security technology that is commonly used to secure server to browser transactions. This generally includes the securing of any information passed by a browser (such as a customer's credit card number or password) to a web-server (such as an online store or online banking application).

What is an Extended Validation SSL Certificate?

Extended Validation Secure Sockets Layer (SSL) Certificates are special SSL Certificates that work with high security Web browsers to clearly identify a Web site's organizational identity. Extended Validation (EV) helps you make sure a Web site is genuine and verified.

Why Are (EV) SSL Certificates Being Implemented?

Malicious and suspicious online activity, phishing attacks have dramatically increased in recent years, creating a heightened need for improved visibility of security.

Before you share your confidential data online, you require proof of identification from a trusted source. The Extended Validation SSL Standard raises the bar on verification of SSL Certificates and enables visual displays in high security browsers. (EV) SSL Certificates empower you to protect yourself online.

The public key and the private key also work together to encrypt or "seal" your information so that it is more difficult to intercept. In other words, digital certificates don't just work to authenticate the identity of the sender, but also of the recipient. For instance, an email sent on a digital certificate network is encrypted from the moment you click Send to the moment the intended recipient opens the message. If the recipient does not have the private key information indicated on your digital certificate, they will not be able to open the message.

Advantages of Digital Certificate:

The biggest advantages of digital certificate-based authentication are privacy-based. By encrypting your communications — emails, logins or online banking transactions — digital certificates protect your private data and prevent the information from being seen by unintended eyes. Digital certificate systems are also user-friendly, usually working automatically and requiring minimal action or involvement from either senders or recipients. Microsoft states that certificate servers are cheaper and easier to manage than other certificate authorities or systems used for encryption.

- Communication Security

Billions of emails are being transmitted over the Web. For important communication between different entities, a Digital Certificate is used as an attachment to an electronic mail message for security purposes and to verify the authenticity of the senders.

- Online Banking

Online banking would not be possible or acceptable by millions of customers without Digital Certificates provided by specialized third-party companies or reputable Certificate Authorities (CAs) such as VeriSign, DigiCert, Thawte and GeoTrust. These certificates ensure the important variables of trust and integrity and facilitate additional levels of protection for sensitive data exchange, information access and transactions.

- Facilitating E-commerce

Millions of Americans are shopping online and need to be sure that Websites, portals and e-retailer sites are secure and reliable. A Certificate Authority's secured seal sign or a Secure Socket Layer (SSL) certificate enables encryption of sensitive information on e-commerce sites and reassures customers about the safety and trustworthiness of shopping, divulging credit card information or doing business online.

- Thwart Online Threats

Regular log-ins or sign-ins on Websites, portals, social media sites, processing sensitive information such as licenses, addresses and birth dates are integral daily online activities of millions of Internet users. To negate the increasing perils and threats of online fraud and identity theft, the third party certification authority provided in the form of Digital Certificates can be reassuring for millions of Internet users and casual surfers.

Other Advantages

Certificate Authorities have extended the standard electronic authentication features of Digital Certificates and leveraged their advantages beyond PCs to include mobile phones, smart cards and other handheld devices.

Disadvantages of Digital Certificate:

While the idea of digital certificates is to block outsiders from intercepting your messages, the system is not an infallible one. In 2011, for example, a Dutch digital certificate authority called DigiNotar was compromised by hackers. Since certificate authorities are the ones in charge of issuing digital certificates (think of them as the digital version of a passport office), hackers often target these authorities in order to manipulate certificate information. As a result, when a certificate authority is compromised, hackers can create websites or send emails that look genuine and pass certification tests, but are actually fraudulent.

Digital certificate authorities constantly update their software to make sure that security threats like this are kept to a minimum, but security threats are still a concern. In 2013, Forbes noted that digital certificates had become a prime target for hackers and other cyber-criminals, given that the information they protect is so valuable. The software requires constant vigilance to protect users from cybercrime.

Virtual Keyboard

When entering private data (for example, your login and password for an online banking account) from a regular keyboard, there is always a risk of data interception by some spyware. Such programs record the keys pressed on the keyboard and therefore capture the data entered from the regular keyboard to pass it to the malefactor.

Advantages

The Virtual Keyboard is designed to protect your password from malicious “Spyware” and “Trojan Programs”. Use of Virtual keyboard will reduce the risk of password theft. One benefit of a physical keyboard is the ability to feel the keys pushing down.

Safety Measures

1. **Never Click On Suspicious Links**

   Have you ever received an email with a link that didn’t look right? Or a weird looking text message? When you looked at it you thought, something doesn’t feel right here. When that happens, trust your instincts. If you ever receive a text message or email containing a link you don’t recognize, DO NOT click on it. Why? Because it may be a link to a malicious website trying to impersonate your bank. If you enter your banking info into that site, you’ve just given it to cyber criminals who could log into your online banking. For example, you might receive an email saying your banking password needs to be reset with a link for you to click. If you click that link and enter your password, you've just given it to thieves. Only enter your online banking information into your bank's official website or app. This will keep you from leaking security information to the wrong people. If you ever receive a request via email or text to send your password information, you can be sure it is a scam. Don't do it. Additionally, as a best practice, you shouldn't send online banking information over email or text for security purposes.

2. Only Bank On Secure WiFi Networks

Generally speaking, public WiFi networks like the ones you'll find at your local coffee shop or library aren't very secure. After all, they have to accommodate as many people as possible. The low level of security makes them prime targets for hackers who can quickly break down their defenses. Whenever possible, don't do your online banking over a public WiFi network. Rather, only do transactions over a secure network like the password protected one at home. If you absolutely need to access your bank while you're out and about, turn off the WiFi and bank over your cellular network.

3. Only Use Official Banking Apps

You should only use your bank or credit union's official smartphone app for online banking. These online apps are rigorously tested to ensure all your data is secure and encrypted. These apps also tend to be much more secure than text messaging, making them the absolute safest way to bank online. Never use a financial application created by someone other than where you bank. The developers could very well be stealing your private information for devious purposes. If you have any doubts about the origin of the app, don't use it. When in doubt, call your bank or credit union to verify that an app is legitimate. Thieves are smart and will do whatever they can to steal your info, including creating a fake app that looks eerily close to the authentic one.

4. Don’t Overshare Online

When a hacker is trying to steal your information, one of the first places they’ll look is your social media profiles. Why? They know that most people use common information such as the names of their children as passwords and they know they can find that online. They’ll gather as much information about you as they can on these social media sites and then begin trying to use it as your password. Thus, when sharing information on social media you should be very careful about your privacy settings as well as the amount of information you share.

5. Create Banking Notifications

Many banks and credit unions allow customers to get text and email alerts about certain transactions in their accounts. For example, you can receive text messages whenever a transaction over a certain dollar amount occurs or when your balance dips below a certain amount. Getting these notifications allows you to be alerted the moment something suspicious begins happening in your bank account. If you see a transaction you didn’t initiate, immediately call your bank and have them put a stop on it.

6. Log Out When Your Session Is Finished

Whenever you’re done with your online banking session, immediately logout. This minimizes the chances of someone stealing your information. It’s extremely important to logout if you are banking in a public space where you could accidentally leave your phone or tablet. Having someone snatch your phone from a coffee table while a banking session is still active could be disastrous. Thankfully, most online banking applications automatically log you out after a set time. However, it’s still best practice to log out immediately after finishing your session.

7. Keep Your Software Up To Date

Many people find it annoying when they discover an update is available for their phone software. They have to download the new software, install it, and restart their phone, all of which seems annoying. However, it's essential to keep your phone software up-to-date for security reasons. Every time a new version of your phone's operating system releases, security holes are patched. If you choose not to update your phone, a hacker could steal your information through one of those security holes. Think of it kind of like your front door. If you realized that your front door had a hole in it, making it easy for criminals to unlock your door, you would fix that hole. Every time you download the latest version of an operating system, you are fixing a hole.

8. Create An Uncrackable Password

Unfortunately, many people select simple passwords that are easy to remember but also easy for cybercriminals to crack. They choose something like their birthday, phone number, Social Security number, dog, child, favorite sports team, or favorite season. While these types of passwords certainly make things easier to remember, they're actually dangerous. A hacker can use a variety of software programs to guess at your password until it gets it right, opening the digital vault. Your password should contain a variety of uppercase and lowercase letters, numbers, and special characters. If you're worried about forgetting your password, you can use a secure password saving device such as LastPass or 1Password. These require a master password and securely encrypt all your information.

Note security should be based on these three things which are:

- **Confidentiality:**
  The information within the message or transaction is kept confidential. It may only be read and understood by the intended sender and receiver.
- **Integrity:**
  The information within the message or transaction is not tampered accidentally or deliberately with en route without all parties involved being aware of the tampering.

- **Access Control:**
  Access to the protected information is only realized by the intended person or entity.

Conclusion

E-Banking or Electronic Banking is a major innovation in the field of Banking that has brought about easy and direct banking. This innovation keeps improving and various steps are being taken by researchers to ensure the stability and improvement of the innovations. Although there are some drawbacks including security concerns.