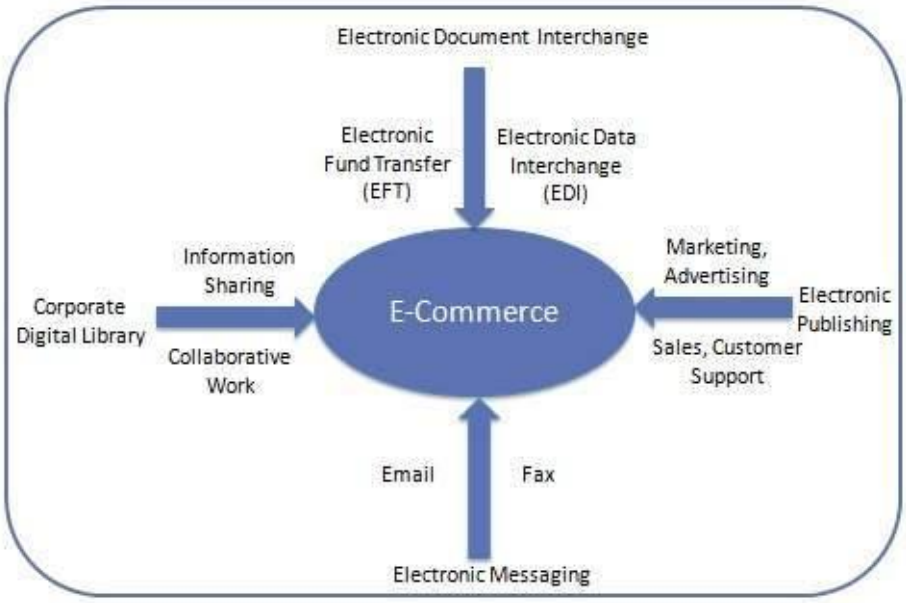
DEFINITION OF E-COMMERCE

E-Commerce or Electronics Commerce is a methodology of modern business, which addresses the need of business organizations, vendors and customers to reduce cost and improve the quality of goods and services while increasing the speed of delivery. Ecommerce refers to the paperless exchange of business information using the following ways −

- Electronic Data Interchange (EDI)
- Electronic Mail (e-mail)
- Electronic Bulletin Boards
- Electronic Fund Transfer (EFT)
- Other Network-based technologies



Features

E-Commerce provides the following features −

Non-Cash Payment − E-Commerce enables the use of credit cards, debit cards, smart cards, electronic fund transfer via bank's website, and other modes of electronics payment.

24x7 Service availability − E-commerce automates the business of enterprises and the way they provide services to their customers. It is available anytime, anywhere.

Advertising / Marketing − E-commerce increases the reach of advertising of products and services of businesses. It helps in better marketing management of products/services.

Improved Sales − Using e-commerce, orders for the products can be generated anytime, anywhere without any human intervention. It gives a big boost to existing sales volumes.

Support − E-commerce provides various ways to provide pre-sales and post-sales assistance to provide better services to customers.

Inventory Management − E-commerce automates inventory management. Reports get generated instantly when required. Product inventory management becomes very efficient and easy to maintain.

Communication improvement − E-commerce provides ways for faster, efficient, reliable communication with customers and partners.

Traditional Commerce v/s E-Commerce

Sr. No.	Traditional Commerce	E-Commerce
1	Heavy dependency on information exchange from person to person.	Information sharing is made easy via electronic communication channels making little dependency on person to person information exchange.
2	Communication/ transaction are done in synchronous way. Manual intervention is required for each communication or transaction.	Communication or transaction can be done in asynchronous way. Electronics system automatically handles when to pass communication to required person or do the transactions.

3	It is difficult to establish and maintain standard practices in traditional commerce.	A uniform strategy can be easily established and maintain in e-commerce.
4	Communications of business depends upon individual skills.	In e-Commerce or Electronic Market, there is no human intervention.
5	Unavailability of a uniform platform as traditional commerce depends heavily on personal communication.	E-Commerce website provides user a platform where al l information is available at one place.

E-Commerce - Advantages

E-Commerce advantages can be broadly classified in three major categories −

- Advantages to Organizations
- Advantages to Consumers
- Advantages to Society

Advantages to Organizations

- ✓ Using e-commerce, organizations can expand their market to national and international markets with minimum capital investment. An organization can easily locate more customers, best suppliers, and suitable business partners across the globe.
- ✓ E-commerce helps organizations to reduce the cost to create process, distribute, retrieve and manage the paper based information by digitizing the information.
- ✓ E-commerce improves the brand image of the company.
- ✓ E-commerce helps organization to provide better customer services.
- ✓ E-commerce helps to simplify the business processes and makes them faster and efficient.
- ✓ E-commerce reduces the paper work.

- ✓ E-commerce increases the productivity of organizations. It supports "pull" type supply management. In "pull" type supply management, a business process starts when a request comes from a customer and it uses just-in-time manufacturing way.

Advantages to Customers

- ✓ It provides 24x7 support. Customers can enquire about a product or service and place orders anytime, anywhere from any location.
- ✓ E-commerce application provides users with more options and quicker delivery of products.
- ✓ E-commerce application provides users with more options to compare and select the cheaper and better options.
- ✓ A customer can put review comments about a product and can see what others are buying, or see the review comments of other customers before making a final purchase.
- ✓ E-commerce provides options of virtual auctions.
- ✓ It provides readily available information. A customer can see the relevant detailed information within seconds, rather than waiting for days or weeks.
- ✓ E-Commerce increases the competition among organizations and as a result, organizations provides substantial discounts to customers.

Advantages to Society

- ✓ Customers need not travel to shop a product, thus less traffic on road and low air pollution.
- ✓ E-commerce helps in reducing the cost of products, so less affluent people can also afford the products.
- ✓ E-commerce has enabled rural areas to access services and products, which are otherwise not available to them.
- ✓ E-commerce helps the government to deliver public services such as healthcare, education, social services at a reduced cost and in an improved manner.

E-Commerce – Disadvantages

The disadvantages of e-commerce can be broadly classified into two major categories −

- Technical disadvantages
- Non-Technical disadvantages

Technical Disadvantages

- ✓ There can be lack of system security, reliability or standards owing to poor implementation of e-commerce.
- ✓ The software development industry is still evolving and keeps changing rapidly.
- ✓ In many countries, network bandwidth might cause an issue.
- ✓ Special types of web servers or other software might be required by the vendor, setting the e-commerce environment apart from network servers.
- ✓ Sometimes, it becomes difficult to integrate an e-commerce software or website with existing applications or databases.
- ✓ There could be software/hardware compatibility issues, as some e-commerce software may be incompatible with some operating system or any other component.

Non-Technical Disadvantages

- ✓ **Initial cost** − The cost of creating/building an e-commerce application in-house may be very high. There could be delays in launching an e-Commerce application due to mistakes, and lack of experience.
- ✓ **User resistance** − Users may not trust the site being an unknown faceless seller. Such mistrust makes it difficult to convince traditional users to switch from physical stores to online/virtual stores.
- ✓ **Security/ Privacy** − It is difficult to ensure the security or privacy on online transactions.
- ✓ Lack of touch or feel of products during online shopping is a drawback.
- ✓ E-commerce applications are still evolving and changing rapidly.

- ✓ Internet access is still not cheaper and is inconvenient to use for many potential customers, for example, those living in remote villages.

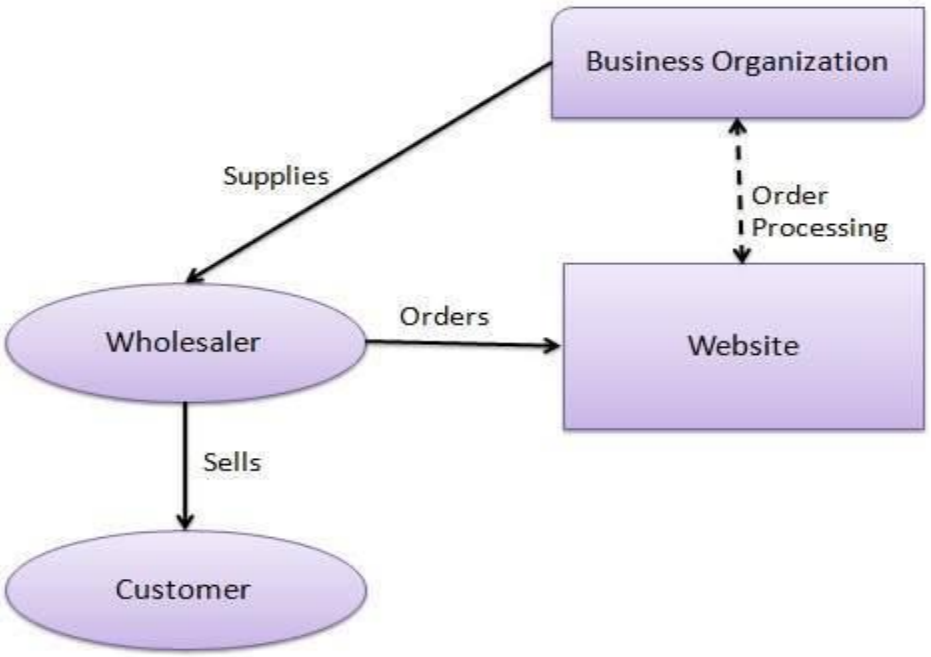
E-Commerce - Business Models

E-commerce business models can generally be categorized into the following categories.

- Business - to - Business (B2B)
- Business - to - Consumer (B2C)
- Consumer - to - Consumer (C2C)
- Consumer - to - Business (C2B)
- Business - to - Government (B2G)
- Government - to - Business (G2B)
- Government - to - Citizen (G2C)

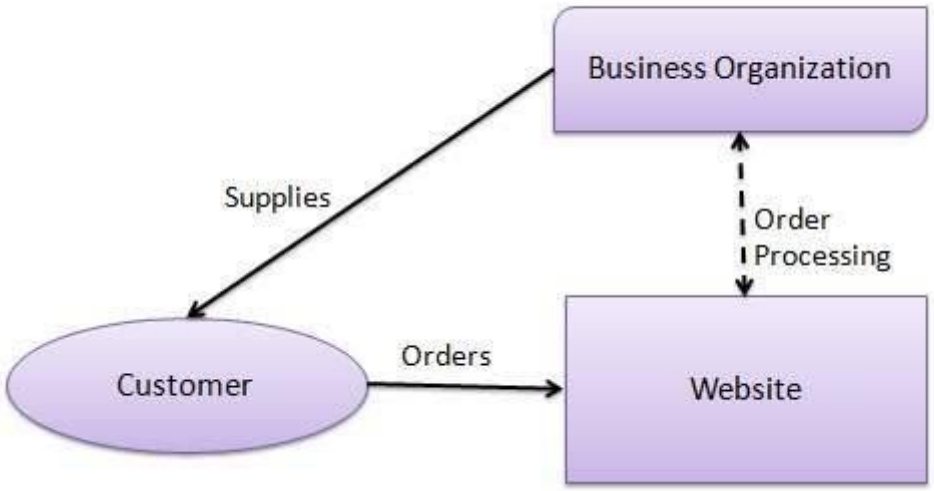
Business - to - Business

A website following the B2B business model sells its products to an intermediate buyer who then sells the product to the final customer. As an example, a wholesaler places an order from a company's website and after receiving the consignment, sells the end product to the final customer who comes to buy the product at one of its retail outlets.



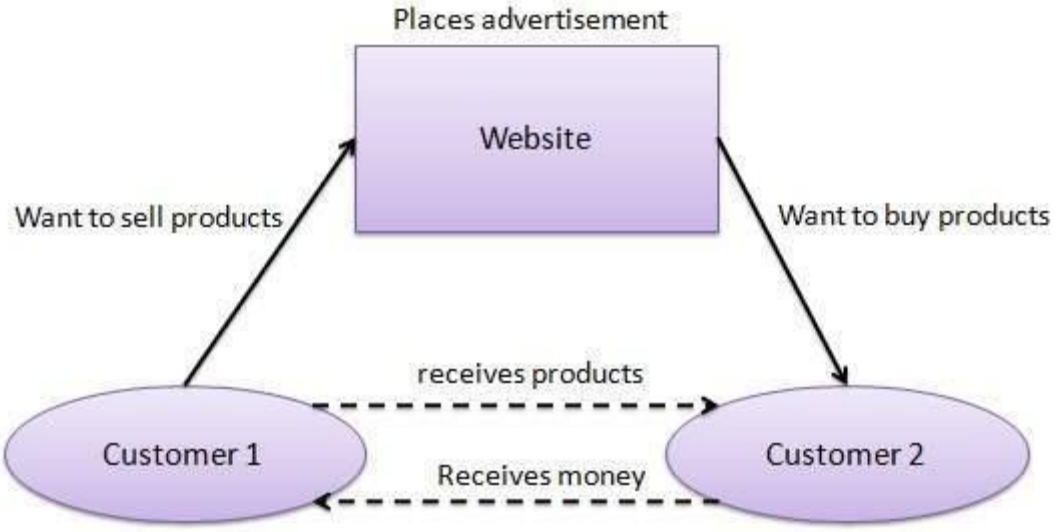
Business - to - Consumer

A website following the B2C business model sells its products directly to a customer. A customer can view the products shown on the website. The customer can choose a product and order the same. The website will then send a notification to the business organization via email and the organization will dispatch the product/goods to the customer.



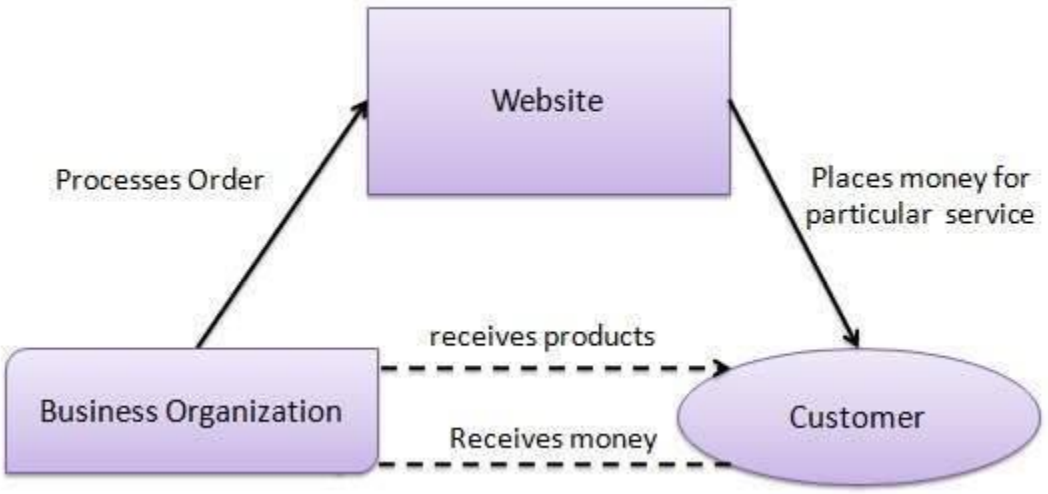
Consumer - to - Consumer

A website following the C2C business model helps consumers to sell their assets like residential property, cars, motorcycles, etc., or rent a room by publishing their information on the website. Website may or may not charge the consumer for its services. Another consumer may opt to buy the product of the first customer by viewing the post/advertisement on the website.



Consumer - to - Business

In this model, a consumer approaches a website showing multiple business organizations for a particular service. The consumer places an estimate of amount he/she wants to spend for a particular service. For example, the comparison of interest rates of personal loan/car loan provided by various banks via websites. A business organization who fulfills the consumer's requirement within the specified budget, approaches the customer and provides its services.

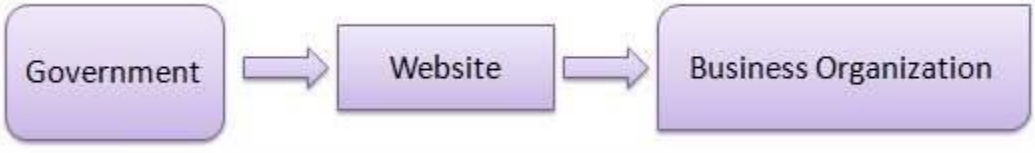


Business - to - Government

B2G model is a variant of B2B model. Such websites are used by governments to trade and exchange information with various business organizations. Such websites are accredited by the government and provide a medium to businesses to submit application forms to the government.

Government - to - Business

Governments use B2G model websites to approach business organizations. Such websites support auctions, tenders, and application submission functionalities.



Government - to - Citizen

Governments use G2C model websites to approach citizen in general. Such websites support auctions of vehicles, machinery, or any other material. Such website also provides services like registration for birth, marriage or death certificates. The main objective of G2C websites is to reduce the average time for fulfilling citizen's requests for various government services.

ELEMENTS OF E-COMMERCE SECURITY

When you look into the ecommerce world, everything is a transmission of data between two or more parties online. However, on the other hand, the internet is nowadays undergoing security threats and cyber-attacks.

An ecommerce website must protect its assets from unauthorized access, use, alteration, or destruction. It requires a reliable infrastructure and framework to enable a secure and successful ecommerce business. The most common security breach for the ecommerce website is concerned with ***Integrity, Availability, Confidentiality, Non-repudiation, Authenticity,*** *and* ***Privacy****.*

Six Dimensions of Ecommerce Security

1. Integrity

We all have the one common question, whether we have received the same data that the sender has sent. Now it is the duty for integrity for the correctness of the information that has been transmitted or received or displayed on a website over the internet.

Integrity can ensure that information on the internet has not been altered in any way by an unauthorized party. It maintains the consistency, accuracy, and trustworthiness of the information over its entire life cycle.

Customer perspective on integrity: Is the information I have transmitted or received is altered?

Merchant perspective on integrity: Is the information present on the website is altered without an authorization? Is the information received from the customer is valid or not?

Example: *The most common threat will be "would any unauthorized person will intercept and redirect payment into a different account" since ecommerce sites prefer online transfer mostly.*

Let us consider a subscription model, where you will give credit card details for a bill payment to the merchant. If someone added extra cost on

your credit card bill without both yours or merchant's knowledge, then you need to pay extra money for something you haven't purchased.

2. Non-repudiation

Good business depends on both buyers and sellers. They must not deny any facts or rules once they accept that there should not be any repudiation.

Non-repudiation confirms whether the information sent between the two parties was received or not. It ensures that the purchase cannot be denied by the person who completed the transaction. In other words, it's an **assurance that anyone cannot deny** the validity of transaction.

Mostly non-repudiation uses a digital signature for online transactions because no one can deny the authenticity of their signature on a document.

Customer perspective: Can a party take action on me if I have denied the action?

Merchant perspective: It's possible for a customer to deny a product after ordering it.

Example: *When a merchant doesn't have enough proof of customers who have ordered with them during a credit card payment transaction, it will not be processed further to the merchant.*

Sometimes customers claim that they haven't ordered the product from a particular merchant if they disliked the product later.

3. Authenticity

In ecommerce, since both the customer and seller need to trust each other, they must remain as who they are in real. Both the seller and buyer must provide proof of their original identity so that the **ecommerce transaction can happen securely between them.**

Every ecommerce site uses authenticity as a tool to ensure the identity of the person over the internet. In ecommerce, fraudulent identity and authentication are also possible, which makes identity a difficult process.

Some common ways to ensure a person's identity are customer log in using a password.

Customer perspective: Who am I dealing with? Who can I assure the person I am dealing with is who they claim to be?

Merchant perspective: Is the customer that I am communicating are a real person? If not, what could be their identity?

Example: *Some users can use a fake email address to access any of the ecommerce services.*

4. Confidentiality

Confidentiality refers to protecting information from being accessed by an unauthorized person on the internet. In other words, only the people who are authorized can gain access to view or modify or use the sensitive data of any customer or merchants.

According to Juniper Research, nearly 146 billion records will be exposed by criminal data breaches between 2018 and 2023.

One confidentiality breach will be sniffing. It's a program that steals all the important files of the company, individual identity or **email message or personal report** of the internet user.

Customer perspective: Can someone other than the intended recipient or a person read my message?

Merchant perspective: Whether information on my site can be accessed by the unauthorized person without knowledge?

Example: *Ecommerce uses a user name and password to login to their account. Let's consider this case for resetting the password, where an ecommerce site sends a one-time password to their customer in email or phone number if someone else reads it.*

5. Privacy

Where confidentiality is a concern about the information present during communication, privacy is concerned with personal details. In general,

privacy is used to control the usage of information by the customers that they have given to the merchant.

According to Fortune, 1.16 billion email address and passwords are exposed in 2019 through security breaches.

Privacy is a major threat to any online transaction or internet user since **personal information has been revealed** and there is no way back to disclose them.

Customer perspective: Can I control the usage of information about myself that I have transmitted to the ecommerce site?

Merchant perspective: What if anyone else uses personal data collected as part of the ecommerce transaction?
Is there any unauthorized person to access a customer's personal data?

Example: *If a hacker breaks into the ecommerce site, they can gain access to the customer credit card details or any other customer information. This also violates information confidentiality and personal privacy.*

6. Availability

Continuous availability of the data is the key to provide a better customer experience in ecommerce. The continuous availability of the ecommerce website increases online visibility, search engine rankings, and site traffic. Data which is present on the website must be secured and available 24x7x 365 for the customer without downtime. If it is not, it will be difficult to gain a competitive edge and survive in the digital world.

Customer perspective: Can I access the site at anytime from anywhere?

Merchant perspective: Whether my site is operating without any downtime?

Example: *An ecommerce website can be flooded with useless traffic that causes to shut down your site, making impossible for the user to access the site.*

E-COMMERCE THREATS

E-Commerce refers to the activity of buying and selling things over the internet. Simply, it refers to the commercial transactions which are conducted online. E-commerce can be drawn on many technologies such as mobile commerce, Internet marketing, online transaction processing, electronic funds transfer, supply chain management, electronic data interchange (EDI), inventory management systems, and automated data collection systems.

E-commerce threat is occurring by using the internet for unfair means with the intention of stealing, fraud and security breach. There are various types of e-commerce threats. Some are accidental, some are purposeful, and some of them are due to human error. The most common security threats are an electronic payments system, e-cash, data misuse, credit/debit card frauds, etc.

Electronic payments system:

With the rapid development of the computer, mobile, and network technology, e-commerce has become a routine part of human life. In e-commerce, the customer can order products at home and save time for doing other things. There is no need of visiting a store or a shop. The customer can select different stores on the Internet in a very short time and compare the products with different characteristics such as price, color, and quality.

The electronic payment systems have a very important role in e-commerce. E-commerce organizations use electronic payment systems that refer to paperless monetary transactions. It revolutionized the business processing by reducing paperwork, transaction costs, and labor cost. E-commerce processing is user-friendly and less time consuming than manual processing. Electronic commerce helps a business organization expand its market reach expansion. There is a certain risk with the electronic payments system.

Some of them are:

The Risk of Fraud

An electronic payment system has a huge risk of fraud. The computing devices use an identity of the person for authorizing a payment such as passwords and security questions. These authentications are not full proof in determining the identity of a person. If the password and the answers to the security questions are matched, the system doesn't care who is on the other side. If someone has access to our password or the answers to our security question, he will gain access to our money and can steal it from us.

The Risk of Tax Evasion

The Internal Revenue Service law requires that every business declare their financial transactions and provide paper records so that tax compliance can be verified. The problem with electronic systems is that they don't provide cleanly into this paradigm. It makes the process of tax collection very frustrating for the Internal Revenue Service. It is at the business's choice to disclose payments received or made via electronic payment systems. The IRS has no way to know that it is telling the truth or not that makes it easy to evade taxation.

The Risk of Payment Conflicts

In electronic payment systems, the payments are handled by an automated electronic system, not by humans. The system is prone to errors when it handles large amounts of payments on a frequent basis with more than one recipients involved. It is essential to continually check our pay slip after every pay period ends in order to ensure everything makes sense. If it is a failure to do this, may result in conflicts of payment caused by technical glitches and anomalies.

E-cash

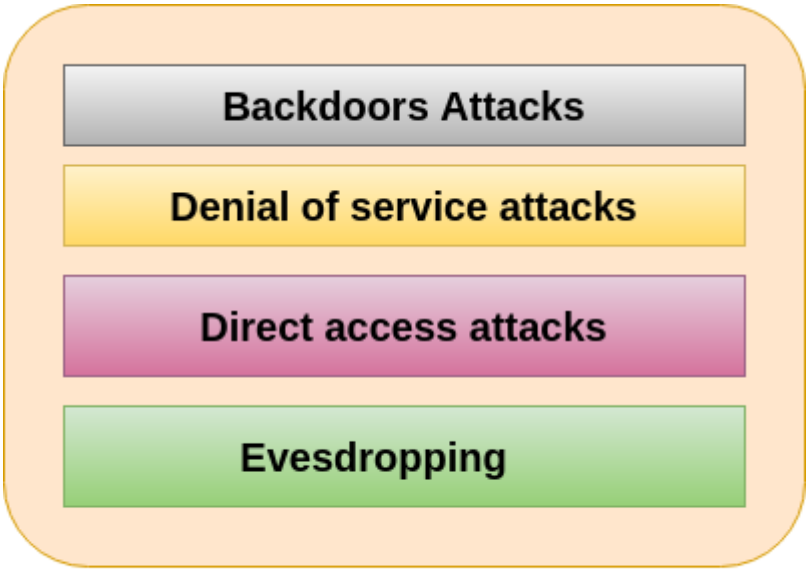
E-cash is a paperless cash system which facilitates the transfer of funds anonymously. E-cash is free to the user while the sellers have paid a fee for this. The e-cash fund can be either stored on a card itself or in an account which is

associated with the card. The most common examples of e-cash system are transit card, PayPal, GooglePay, Paytm, etc.

E-cash has four major components-

- **Issuers** - They can be banks or a non-bank institution.
- **Customers** - They are the users who spend the e-cash.
- **Merchants or Traders** - They are the vendors who receive e-cash.
- **Regulators** - They are related to authorities or state tax agencies.

In e-cash, we stored financial information on the computer, electronic device or on the internet which is vulnerable to the hackers. Some of the major threats related to e-cash system are-



E-cash Threats

Backdoors Attacks

It is a type of attacks which gives an attacker to unauthorized access to a system by bypasses the normal authentication mechanisms. It works in the background and hides itself from the user that makes it difficult to detect and remove.

Denial of service attacks

A denial-of-service attack (DoS attack) is a security attack in which the attacker takes action that prevents the legitimate (correct) users from accessing the

electronic devices. It makes a network resource unavailable to its intended users by temporarily disrupting services of a host connected to the Internet.

Direct Access Attacks

Direct access attack is an attack in which an intruder gains physical access to the computer to perform an unauthorized activity and installing various types of software to compromise security. These types of software loaded with worms and download a huge amount of sensitive data from the target victims.

Eavesdropping

This is an unauthorized way of listening to private communication over the network. It does not interfere with the normal operations of the targeting system so that the sender and the recipient of the messages are not aware that their conversation is tracking.

Credit/Debit card fraud

A credit card allows us to borrow money from a recipient bank to make purchases. The issuer of the credit card has the condition that the cardholder will pay back the borrowed money with an additional agreed-upon charge.

A debit card is of a plastic card which issued by the financial organization to account holder who has a savings deposit account that can be used instead of cash to make purchases. The debit card can be used only when the fund is available in the account.

Some of the important threats associated with the debit/credit card are-

ATM (Automated Teller Machine)

It is the favorite place of the fraudster from there they can steal our card details. Some of the important techniques which the criminals opt for getting hold of our card information is:

Skimming

It is the process of attaching a data-skimming device in the card reader of the ATM. When the customer swipes their card in the ATM card reader, the information is copied from the magnetic strip to the device. By doing this, the

criminals get to know the details of the Card number, name, CVV number, expiry date of the card and other details.

Unwanted Presence

It is a rule that not more than one user should use the ATM at a time. If we find more than one people lurking around together, the intention behind this is to overlook our card details while we were making our transaction.

Vishing/Phishing

Phishing is an activity in which an intruder obtained the sensitive information of a user such as password, usernames, and credit card details, often for malicious reasons, etc.

Vishing is an activity in which an intruder obtained the sensitive information of a user via sending SMS on mobiles. These SMS and Call appears to be from a reliable source, but in real they are fake. The main objective of vishing and phishing is to get the customer's PIN, account details, and passwords.

Online Transaction

Online transaction can be made by the customer to do shopping and pay their bills over the internet. It is as easy as for the customer, also easy for the customer to hack into our system and steal our sensitive information. Some important ways to steal our confidential information during an online transaction are-

- By downloading software which scans our keystroke and steals our password and card details.
- By redirecting a customer to a fake website which looks like original and steals our sensitive information.
- By using public Wi-Fi

POS Theft

It is commonly done at merchant stores at the time of POS transaction. In this, the salesperson takes the customer card for processing payment and illegally copies the card details for later use.

E-COMMERCE SECURITY BEST PRACTICES

10 E-Commerce Security Tips to Protect Your Business

There are countless ways to improve ecommerce security. Some of them are beyond what the average B2B or B2C business needs to invest their time and money into. Here are 10 key tips to help your ecommerce site protect your consumers and your business.

1. Suggest Strong Passwords

The most basic security measure both customers and employees can take is to create strong passwords. A strong password uses numbers, special characters, and sometimes both lowercase and uppercase letters.

Another factor to consider when creating strong passwords is for individuals to create unique passwords across all of their logins. According to a Google survey, 52% of people use the same password for multiple websites.

A password manager is a great tool to encourage your employees to create strong passwords for each tool or platform they use. With each unique password stored in a secure place, it alleviates the frustration of trying to remember a large set of complex passwords and eliminates the risk of reusing passwords on other sites.

2. Implement Multilayer Security

Make user data protection a top priority by implementing a multilayer security plan. Without layered security measures in place, breaches are inevitable.

It's crucial to ensure that only company employees dealing directly with a transaction have access to personal information. The cost of data breaches can be catastrophic to your business's reputation if there is an information leak. For both of these reasons, investing in additional security measures (beyond requiring strong passwords) is important.

What is Multilayer Security?

Most of us are familiar with multifactor authentication by now. One example is when logging onto a website. Users are contacted via text or email with a code which they enter into a field to verify their identity.

Another example is for users to download the website's mobile app and login to the app in order to confirm they are the user who is trying to access the site. The goal is to set up additional security walls to prevent data breaches.

A content delivery network (CDN) is another useful multilayer security tool. This approach stores data across a distributed network of servers and protects against distributed denial of service (DDoS) attacks. A DDoS attack uses several sources at one time to flood a website with traffic to make it unavailable to users and gain access to data.

Why is Multilayer Security Important?

Using a multilayer security system provides added layers of protection for businesses both internally and externally. Each measure makes it more difficult for hackers with stolen passwords to login. Implementing multilayer security is a smart recommendation for employees as well as customers. This extra measure improves brand reputation.

3. Use a Firewall

Firewalls monitor all traffic coming and going from a site to block suspicious traffic. Firewalls are unique to each company and are built using a set of predetermined rules to pick out untrustworthy traffic sources.

The type of attacks that firewalls can prevent include DDoS attacks and Structured Query Language (SQL) injection. SQL injection is a common cyber attack tactic that "injects" harmful code into a website's makeup to breach data or destroy the database.

4. Use a Payment Provider

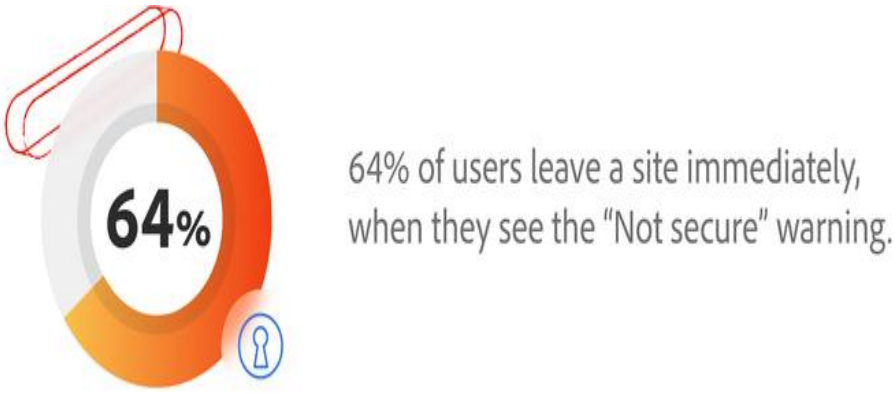
There are a number of tools available that can process all of your customers' financial information and keep their credit card data safe. Do not store any customer financial data on company servers. Payment providers encrypt customer payment data as an extra measure to protect against cybersecurity attacks.

5. Install a Secure Socket Layer (SSL) Certificate for HTTPS Security

An SSL encrypts and protects a customer's financial data as it travels between their device and the payment processor.

If you've ever visited a site and noticed "Not secure" displayed in the address bar, it's because they're not using an SSL. When a website uses SSL, HTTP becomes HTTPS, which is the standard for internet security and is safer for users.

Not using an SSL is not only poor security, but it may dissuade users from visiting your site. Some browsers even have a pop up warning page that the page isn't secure. In fact, a study by John Cabot found that 64% of users leave a site immediately when they see the "Not secure" warning.



SSL and HTTPS are the standard for ecommerce security and should always be used going forward. As a bonus HTTPS improves your site's SEO because Google ranks secure pages higher.

6. Update Your Software and Hardware

It's easy to get behind on software updates, especially when they are suggested to us frequently and on multiple devices. Ignoring these updates decreases site security and must be prioritized.

Software updates aren't released just for new front end features. Tools are often updated to patch vulnerabilities and improve security. Look for a platform that keeps code up-to-date by distributing patch releases often.

Additionally, consider giving employees a scheduled hour weekly or monthly to devote to downloading new updates so they don't feel like it's cutting into their work hours.

7. Follow Payment Card Industry Data Security Standard (PCI-DSS) Requirements

PCI-DSS is a set of requirements that guides any business that collects, processes, and stores credit card information.

Most of these ecommerce security tips are part of PCI-DSS compliance. For example, firewalls, strong passwords, cardholder data protection, and antivirus software are all components of PCI-DSS. If you implement all of the tips on this list, there's a good chance your business is close to PCI compliant.

Check out the *Adobe PCI Compliance Checklist For Ecommerce Businesses* to see where you stand:

Early Years

A PCI compliance checklist was needed in the early years of ecommerce because there were no set standards for web site architecture design or configuration—let alone measures to protect sensitive data such as credit card numbers and data tracking. With the increasing instances of unauthorized transactions reported by consumers, Visa launched its own requirements and standards platform to be followed by any retailer conducting business on the Internet and accepting Visa as a tender.

There were other credit card brands working on similar projects at the time, but Visa had the strongest requirements. Eventually the brands came together and helped form the *Payment Card Industry Data Security Standard* (PCI DSS) council to create a formal set of requirements and standards that covered all brands. The standards help to not only protect the card brands, but also retailers and consumers.

Definition of a PCI Compliance Checklist and Why It's So Important

PCI DSS is so important because it provides a set of baseline requirements and standards on how to protect consumer credit card data, which is referred to as cardholder data or CHD. The standards help guide companies on how to initially build an internal Information Security program, and design it to meet their own business needs. The requirements and standards also help to identify where and how CHD is coming from, moving through, and ultimately being stored. Mapping how the data moves throughout a company's network is one of the first steps to knowing how to protect it.

Why Your Business Will Be Better with a Comprehensive PCI Compliance Checklist

A PCI compliance program is just one piece of a company's overall Information Security program. There is a symbiotic relationship between the programs. Having one helps to strengthen the other. The PCI compliance program helps to identify a basic set of standards that, when implemented correctly for the business, help to strengthen the company's overall Information Security program.

Risks of Being Non-Compliant

The risks range from monetary fines imposed by the card issuers to loss of consumer trust in the businesses who are found to be non-compliant. Trust is built over years and can be as valuable as any product sold. Beware of violating that trust by not protecting consumer card data as the effects of that can have a lasting impact on your business.

What You Need to Do to Protect Your Business

The latest update to the standard, PCI DSS v3, has six main requirements that are broken out into twelve sub-requirements that contain more than three hundred specific standards that have to be met. These standards have one main goal in mind: protecting cardholder data. That is the golden nugget that every person with malicious intent is trying to get to. Once they have cardholder data, it can be used for their own profit at the expense of the consumer, partner, business, and the card issuers.

If You Were Writing a PCI Compliance Checklist, What Would You Include?

The PCI DSS provides a general set of standards that can be implemented across any business model. Over the years the council has improved on the language, definitions, and applicability of the requirements and the changes have incrementally helped to improve PCI DSS compliance as a whole. Your PCI compliance checklist should include the following:

- Use a firewall between the payment card data and the public network, and keep the firewall updated.
- Don’t use vendor-supplied default passwords that come with network equipment or devices used in payment processing.
- Do not store cardholder data. If you have a business need to keep cardholder data, make sure you use strong encryption. You can use Magento’s BrainTree extension to shift the storage of cardholder data off of your system.
- Use encryption to protect all transmission of cardholder data over any public network.
- Use antivirus software on all machines in the cardholder data environment and ensure that the software is regularly updated.
- Check that your card processing systems have vendor-supplied security patches installed.
- Limit access to cardholder data to as few people as possible.
- Assign a unique ID number to each user so that everyone is accountable for his own actions.
- Restrict physical access to the cardholder data environment.
- Monitor all access to the network and cardholder data environment.
- Regularly test your security systems and network environment.
- Maintain a security policy and ensure that all personnel are aware of it.

How Does Magento Help Businesses Remain Compliant?

Magento offers a payment application/bridge that meets a specific version of the PCI DSS, the PA DSS or *Payment Application Data Security Standard*. This standard is a stand-alone certification process offered by the council. Magento’s payment application/bridge has undergone the process to become PA DSS certified. While Magento provides a PA-DSS compliant application/payment bridge, it does not make you PCI compliant automatically due to the number of PCI controls that lie outside the Magento platform.

For more information about completing your PCI compliance checklist or recommendations for a qualified security assessor, contact Magento online.

How to Measure Compliance?

Patch management reports are a tool for measuring compliance. They provide routine updates on how your ecommerce platform stacks up against PCI compliance regulations. You should also regularly assess hardware, software, servers, and user accounts for vulnerabilities.

Another strategy for measuring compliance is penetration testing. Penetration testing is attempting to hack your own system — either from the inside or outside. It's a great way to expose vulnerabilities and keep your system secure.

8. Back up Data

All data should be routinely backed up so that it can be restored in the event of a breach or system crash. While most security tips aim to prevent cyberattacks, you need to have a plan in place to recover data if other security methods fail.

9. Establish Best Practices

Ecommerce security tips are only as valuable as your internal team and customers make them. Educate your employees and customers about online security — including how to create strong passwords and how to implement multifactor authentication.

Be sure to share the steps you've taken to protect customer data with your users. This transparency helps make them smarter online consumers.

10. Choose the Right Hosting Provider

A good hosting provider improves your ecommerce security strategy by:

1. Monitoring threats
2. Providing upgrades to continually improve security
3. Fixing technical issues in a timely manner
4. Including robust built-in security features

INTRODUCTION TO DIGITAL PAYMENTS

How to define digital payments?

A digital payment, sometimes called an electronic payment, is the transfer of value from one payment account to another using a digital device such as a mobile phone, POS (Point of Sales) or computer, a digital channel communications such as mobile wireless data or SWIFT (Society for the Worldwide Interbank Financial Telecommunication). This definition includes payments made with bank transfers, mobile money, and payment cards including credit, debit and prepaid cards.

There is no single, universally accepted definition of digital payments because digital payments can be partially digital, primarily digital, or fully digital. For example, a partially digital payment is one in which both payer and payee use cash via third party agents, with providers making digital bank transfers in the backend. A primarily digital payment might be one in which the payer initiates the payment digitally to an agent who receives it digitally but the payee receives the payment in cash from that agent.

So, the definition must be fit-for-purpose. One definition emphasizes the payer-payee interface as the defining element. Another defines digital payments based on the payment instrument, or some other variable. These definitional choices become particularly relevant when the objective is to estimate the number or share of digital payments in a specific use-case, organization, company, country, or region. The definition of digital payments determines how they are measured. For more details about definition and measurement Box 1 further down.

Benefits of Digital Payments

Regardless of the definition, some things we know for sure: Digital payments offer significant benefits to individuals, companies, governments, or international development organizations. The benefits of going digital include:

Cost savings through greater efficiency and speed. For example, a recent report by the Better than Cash Alliance and the Inter-American Development Bank shows that the Government of Peru could save US$96 million by shifting all government payments to more efficient digital options currently available in the market.

Transparency and security by enhancing traceability and accountability, reducing corruption and theft as a result. For example, a recent report analyzes risks incurred by individual purchasing clerks in cocoa value chains (including assault), due to the prevalence of cash. As of March 2019, the Government of India

has saved almost $14 billion in social protection payments through electronic Debit Benefits Transfers.

Financial inclusion by increasing access to a range of financial services, including savings accounts, credit and insurance products. The Committee on Payments and Market Infrastructure and the World Bank published the flagship report 'Payment Aspects of Financial Inclusion (PAFI)', outlining how digital payments help advance financial inclusion.

Women's economic participation by giving women more control over their financial lives and providing them greater economic opportunities. A G20 GPFI report highlights how digital payments contribute to women's economic participation.

Inclusive growth Cumulatively, the benefits outlined above help unlock economic opportunity for the financially excluded, and enable a more efficient flow of resources in the economy. There is robust academic evidence about the impact of the widespread adoption of digital payments on poverty reduction (see Jack and Suri, 2016) and on SDG progress.

Not all digital payments are equal

To realize the benefits of digital payments, they must be done responsibly and in ways that protect and promote the well-being of the end-user. The Better Than Cash Alliance's Responsible Digital Payment Guidelines (RDPG) help define responsible digital payments. The Guidelines identify eight good practices for engaging with clients who are sending or receiving digital payments and who have previously been financially excluded or underserved.

These eight guidelines specifically address the challenges of shifting from cash to digital. Digital payments can raise security and privacy concerns, therefore, the guidelines recommend measures to ensure the confidentiality and security of client data.

The resilience or reliability of the digital payment system and infrastructure is equally crucial. System outages might unreasonably prevent users from accessing their funds, therefore, it is imperative that providers keeping funds safe – that robust steps are taken to ensure network reliability and system capacity, as well as a payments channel secure from fraud, hacking, and any other form of unauthorized use.

Furthermore, costs and other ongoing fees for payees need to be transparent. Ultimately, affordability is key for sustainability and long-term usage – and the solutions need to remain so over time. It is also important for products and services to be gender intentional, by designing solutions that take into account the needs of women and to ensure that women are not excluded due to lack of digital access or confidence.

Finally, the recourse mechanism needs to be clear and be designed with a "client-centric" approach in order to raise trust amongst users.

Digital innovations will continue to improve and grow the payments sector

The pace of digital innovation in payments is driving a reduction in costs projected double compound annual growth rate. It is resulting in new business models and a more competitive environment as new players emerge. These are some of the innovations:

Contactless payments – a secure payment method using a debit, credit or smartcard enabled by Radiofrequency Identification (RFID) or near-field communication (NFC). This digital payment method is growing in popularity due to its speed and seamless experience.

Open Application Programming Interfaces (API) - a publicly available API that provides developers with programmatic access to a proprietary software application or web service. Open APIs allow new providers to build services on top of existing infrastructure. The relevance of these approaches is that it lowers barriers to entry for new financial technology players, encouraging innovation and enabling the rise of seamless digital payment services for the end-user.

Distributed ledger technology (DLT) - A database that is consensually shared and synchronized across multiple sites, institutions or geographies. This database architecture solves the problem of trust among multiple stakeholders and the so-called "double spend", which refers to the dilemma of ensuring a digital asset is not spent twice. Since all members of the network hold a copy of the ledger at all times, DLT allows for decentralized digital payment systems that do not rely on a

single central authority, such as a bank or a public institution (see our full series on DLT and digital payments here).

QR codes - a two-dimensional Quick Response bar code or square-shaped code that contains data. It has become popular as it is a quick and easy way to exchange information and has the potential of substantially reducing payment acceptance costs. All that is needed for the payment to take place is a digital device with a camera linked to an account.

Biometric Payments – Biometric digital payments use Biometric ID as a means of verification and authorization of payments. Biometric ID is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures.

Central Bank Digital Currencies (CBDC) - Globally, emerging market economies are moving from conceptual research to intensive practical development. Central banks representing a fifth of the world's population say they are likely to issue the first CBDCs in the next few years.

Common types of digital payments

CONTACTLESS PAYMENTS

CREDIT AND DEBIT CARDS

ONLINE PAYMENTS

MOBILE MONEY

CHIP-AND-PIN

E-WALLET

WATCH

ONLINE BANKING SECURITY

Whether it is bill payments, funds transfer or creation of a fixed deposit, internet banking allows you to do it in a fast and convenient way. Instead of going to the bank and waiting in an unending queue, internet banking has made all banking functions accessible through a few clicks. However, this facility needs to be used very carefully due to the risk of phishing – fraudulent means of attaining your confidential banking information.
Listed below are seven smart tips for internet banking.

Change your password regularly

For the first time you login to your internet banking account, you will need to use the password provided by the bank. However, you need to change this password in order to keep your account safe. In addition, keep changing your password at regular intervals. More importantly, keep the password confidential at all times.

Do not use public computers to login

Avoid logging in to your bank account at common computers in cyber cafes or libraries. These are crowded places, and there are more chances of your password being traced or seen by others. If you have to login from such places, make sure you clear the cache and browsing history, and delete all the temporary files from the computer. Also, never allow the browser to remember your ID and password.

Do not share your details with anyone

Your bank will never ask for your confidential information via phone or email. So whether you get an apparent phone call from the bank or an email requesting your details, do not give out your login information. Use your login ID and password only on the official login page of the bank, which should be a secure website. Look for 'https://' in the URL when logging in; it means that the website is secure.

Keep checking your savings account regularly

Check your account after making any transaction online. Verify whether the right amount has been deducted from your account. If you see any discrepancies in the amount, inform the bank immediately.

Always use licensed anti-virus software

To protect your computer from new viruses, ensure that you always use licensed anti-virus software. Pirated versions of anti-virus software's may be available for free, but they may fail to protect your computer from new viruses prevalent in the online world. In addition, you will get notifications for updates in the software periodically. Make sure that you keep your anti-virus updated, so that your confidential information is always protected.

Disconnect the internet connection when not in use

Most broadband users do not disconnect the internet connection on their computer when they are not using it. Malicious hackers can access your computer via an internet connection and steal your confidential banking information. To keep your data protected, ensure that you disconnect from the internet when you do not require it.

Type your internet banking URL

It is a safer to type your bank URL in the address bar of the browser than clicking on links given in an email. There are instances of fraudsters sending emails with fraudulent websites links that are designed exactly like the bank's original website. Once you enter your login details on such a website, they may be used to access your account and steal your money. While logging on, check for 'https://' in the URL and ensure that it is your bank's authentic website.

MOBILE BANKING SECURITY

Like most people, you probably use a mobile banking application…
Because, if you're like me you're always on the run.

Mobile banking is a fast and convenient way to effectively manage your money – i.e. check your balance, transfer money, pay bills online, and more.

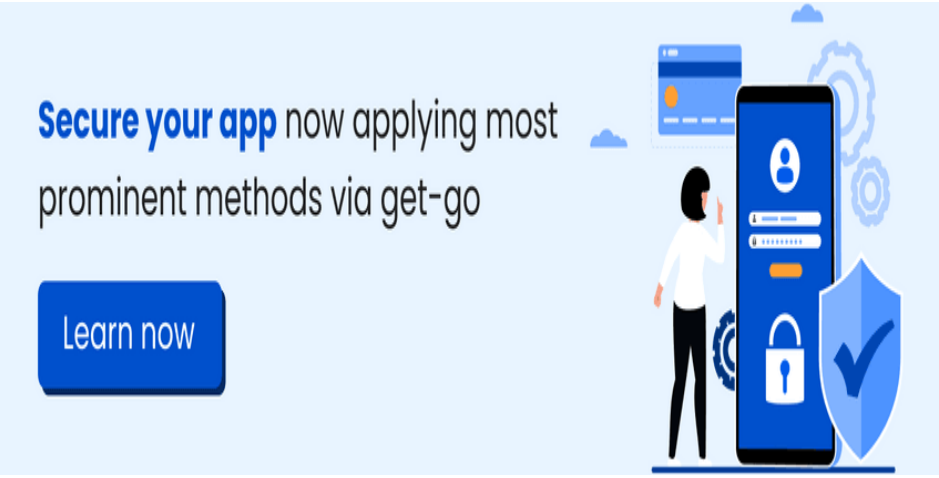
However, only about two-thirds of bank customers with a cellular device currently enjoy the benefits of mobile banking.

Why has the adoption rate not yet reached its highest potential? One of the reasons is a lack of trust from the consumers.

Especially seen in older generations, individuals do not fully trust technology. The thought of having all their banking information right on a mobile app – and at the palm of their hand – simply scares them, rather than intrigues them.

But, with fraud, IP infringement and malware so prevalent in our technology-driven world, how do you convince the remaining percentage of bank customers to take advantage of the ease of mobile banking?
I'll tell you how…

Make it safer – overwhelm them with the amount of security that accompanies your mobile banking application.



Why are Banking Apps Vulnerable?

The architecture of mobile banking apps is usually prone to some serious mobile banking vulnerabilities that may lead to financial security breaches.

Basically, a mobile-based online banking app is a type of software that is directly connected to the bank's backend system via Application Programming Interfaces (APIs).

Generally, these APIs are based on open source code, which is quite supportive of the app developers. However, sometimes these APIs may create vulnerable security loopholes for mobile banking applications.

Here, the irony is that web app firewalls or a source code protection may not reduce or solve these loopholes.

Online and mobile banking system attackers can take advantage of machine-to-machine interactions by creating shadow APIs on their own. Ironically, these shadow APIs do not resurface as compromised endpoints.

Here are some high-risk vulnerabilities that can dampen your mobile banking app's performance:

Lack of a united app ownership

App ownership becomes one of the most dangerous vulnerabilities when it comes to securing mobile banking solutions. Usually, there are two owners in this case: one is the external owner, and another who works for the bank.

In the banking sector, the line of business managers has ownership of mobile banking apps. Another owner of the app is the IT department at the bank. Apart from this, there is an external entity that is involved in the mobile banking app development and the management of its APIs.

Such type of ownership creates serious security concerns as the above mentioned three owners are sharing the responsibility. Because of this, there is a strong possibility that something may go wrong at any time.

Insecure data storage

iOS and Android are official app stores that offer a unique level of security through a wide range of features, such as permission systems or TouchID. If you do not use them properly, you may face privacy based online threats, opening your crucial personal data to hackers.

Faulty communication

Mobile apps need to communicate with external data sources like NFC, Bluetooth devices, servers, different authorization mechanisms, and authentication tokens.

You cannot avoid this communication; otherwise, the app could not perform to its potential. But, this activity can definitely create a mobile security threat for you by leaking your data.

So here are the different security vulnerabilities faced by the credit unions, financial institutions and banking institutions. Let us now move forward towards some important banking fraud cases.

Critical mobile banking fraud cases

Fake bank

Mobile banking security researchers are constantly detecting and preventing latest app based banking Trojans, Malware, fake banking apps, phishing attacks and brute force attacks that impact mobile banking apps.

Fake Bank is one such spyware that monitors the verification messages that are sent by the bank to the customers. When mobile banking app users get a verification code, the spyware copies the same and sends it to hackers or cybercriminals.

Duplicate Flash Player

Duplicate Flash Player is a video application which is either installed via an infected SMS or predatory E-Mail that contains some malicious download link. Once the mobile device users install the app over a smartphone, it requests the mobile phone administrator rights via permission prompt.

After this, the malware of the app creates a dummy login screen that gets visible when the user opens it next time. Once the user enters the user credentials or bank login credentials, the malware copies it and sends the data into the database of the malicious users that it can use later on.

Svpeng

Roman Unuchek, Kaspersky Lab's senior malware analyst has found a new modification of mobile banking trojan Svpeng. It is one of the most dangerous mobile banking malware.

For example, the Trojan can draw itself over other apps and unofficial sources, give itself permissions to send and receive SMS, carry out financial transactions, make calls, and read contacts and grant itself device administrator rights and block any attempt to cancel this action.

What can financial institutions do for app security?

1. Add a multi-factor authentication feature

Simply requiring the submission of a single password before granting access to your customer's bank account is a defense system which can be beaten.

By adding a multi-factor authentication or a two-factor authentication feature – such as generated one-time passwords or biometric authentication methods such as fingerprints – you add an additional layer of security which cannot easily be deceived.

2. Encourage the use of NFC-embedded SIM cards

While you can't force this security option on your consumers, you can highly suggest it. An NFC-embedded SIM card is a SIM card that allows consumers to securely download their credit card information into the Near Field Communication (NFC) SIM card.

This mobile banking security tip is more of a means to protect the information of their financial accounts – by not carrying their actual card, and not swiping it, they lessen the risks that their credit card information could be compromised, potentially giving access to their mobile bank application.

3. End-to-end encryption

Many entities like payment cards, merchants, card brands, and issuing banks play a significant role in an online transactions. The exchange of loads of sensitive data worth billions of dollars takes place in a year. Due to this, it has become a hotspot for hackers.

End-to-End encryption is a solution to this massive threat as it ensures that data is safe and sound. It conducts security audits and penetration tests which takes the security measures to an extra mile.

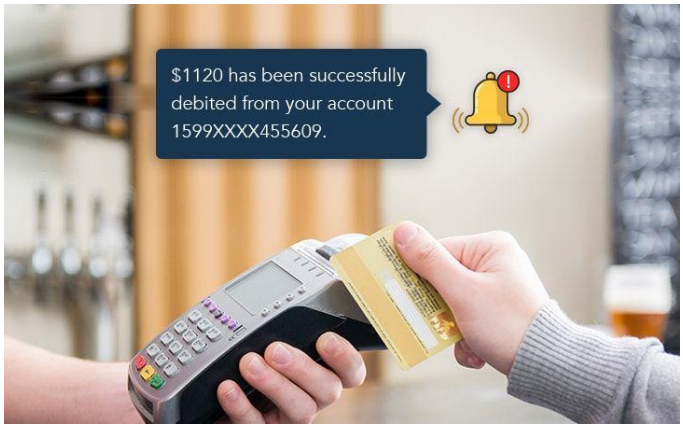
4. Fingerprinting device

Introduction of Fingerprinting devices adds an extra layer in banking mobile apps. It obtains various sets of signals such as IP address, location, remote server, time of the day, device type, location, PIN code, public wi-fi details, screen seize, mobile-enabled internet browser, etc.

You can hire mobile application development teams or skilled mobile app developers to build an app which has fingerprinting feature or which are compatible with some fingerprinting devices or cell phones.

5. Offer real-time text and email alerts

It is safe to assume someone using mobile banking on their mobile browsers has direct access to their email and/or text messages.



By sending a quick, real-time email or text alert to notify a customer of account activity, they could easily prevent fraud, social engineering or an identity theft issue.

For example, some mobile bank applications allow you to be notified on your mobile devices if more than a customer-specified amount of money is spent.

This type of security feature could easily let someone know if the sensitive user information has been compromised, as they would likely be aware of such a large amount of money being spent from their account.

6. The power of paperless banking

The advents of IT technology and Mobile apps have had a massive impact on all sectors. Banking services and the financial sector are no exceptions; digitalization has transformed most of its processes.

With digitalization the banks can go completely paperless with most of its process, including something as basic as opening a bank account, account activation process, imparting accurate account activation instructions, money transfer confirmations and handling the online transaction.

Using digital or online platforms assist in increasing efficiency and transparency as all the file is in digital forms and their access becomes quick and convenient. To implement all these banking institutions would require a mobile app solution provider which can provide them with an enterprise mobility solution.

7. Utilize behavior analysis

There is specialized software on the market that will monitor and analyze the banking login location, and online accounts activity of consumers.

Thanks to this technology, your mobile banking app could flag, several business logic errors, abnormal behavior or unauthorized access for further investigation.

Further investigation could be an email or text alert to the customer advising of suspicious activity, or a call from the bank further investigating the suspicious activity.

8. Safe digitalized documentation

Another way by which you can increase security of mobile banking app is through Safe Digitalized Documentation. Setting up an electronic signature can help in several verticals like ecommerce, call centers, retail branches, etc.

This method helps in bringing a huge portion of documentation on mobile which enables financial organizations to provide mobile banking customers with various benefits. And most importantly it avoids cases of fraud and thus increases the security.

9. Use secure access

By using a secure internet connection and positive technologies like HTTPS, customer account information can be better secured between the mobile web browser and the website they are connected to.

This technology will further protect customers against data theft and fraudulent logins.

Financial institutions often find themselves between a rock and a hard place – most customers want an acceptable level of convenience for mobile banking transactions.

But with mobile banking comes an increased security risk of critical vulnerabilities both for the bank and the mobile banking users.

Of course, the challenge is staying ahead of cyber criminals and continuously working to improve the security level of mobile banking applications and to make mobile banking safe.

By incorporating new technologies and agile development processes, financial institutions can continue to improve the risk score and security of their mobile apps and ward off the unwanted visitors – such as hackers.

Furthermore, these technologies will provide a strong authentication for mobile banking solution and wireless carriers of banking.

However, this is also a two-way street. In improving mobile bank application security, customers must also take their own precautions.

The financial institution that offer mobile banking applications should continue to educate customers and encourage them regarding Internet security and things that could put them at an increased risk of fraudulent activity.

PSD2 regulations

The chief aim of PSD2 regulations is to combat banking security flaws such as reverse engineering, theft of funds,. Along with this, PSD2 regulations also provide a strong defence mechanism against fraudulent activities and intends to increase digital security and enhance the usage of digital documents.

Moreover, it also supports the idea of open banking mobile technologies and improved online security.

PSD2 allows the financial companies, FinTech businesses, banks, big corporate firms and clients to work with banks via close co-ordination. Besides this, the law focuses on providing much improved online security to consumers in terms of online payments and customer experience overall.

Educate your customer

Your work doesn't get finished by managing the financial security. You also have to make your customers aware of financial fraud too. In addition to this, clients should have to take precautions against financial fraud as well.

Apart from this, there are some critical authorization flaws or vulnerabilities in business logic can damage the mobile banking experience for the customers. Besides this, any banking transaction that took place via public wi-fi hotspots is also harmful.

This is why banks and financial institutions that are offering mobile applications need to educate mobile users about financial security. Banks need to guide customers on the latest mobile technologies to prevent frauds and steps to secure their finances.

SECURITY OF DEBIT AND CREDIT CARD

Precautions for use of Debit / Credit Card:

- ✓ Do sign your card on the backside, immediately on receipt from the bank.
- ✓ Always erase the 3-digit CVV number on the backside of the card. Memorize it for your use.
- ✓ Do not share your Credit / Debit Card numbers, PIN number with anyone, not even with the bank officials.
- ✓ Do not write down your PIN number anywhere. Memorize it.
- ✓ Do not share your OTP (One Time Password) with anyone over phone or mail.
- ✓ Do not carry out financial transactions while using public networks, i.e., Internet café, free Wi-Fi, etc.,
- ✓ While using ATMs, make sure that you shield keypad of ATM with your hand while entering your PIN.
- ✓ Ensure that merchants swipe your card in your presence in their Point of Sale (POS) terminals. Shield the POS PIN pad while entering your PIN.
- ✓ Avoid using ATMs located in isolated or dimly lit places without security.
- ✓ Do not crumple and throw away the ATM transaction slips. The information printed in the slip can be misused. Always destroy the transaction slips into small pieces and then throw them into the trash.
- ✓ Do not use ATM where the card reader appears to be tampered with, i.e., broken, scratched, damaged, sticky with glue, has extra wiring or loose parts around the slot, difficulty in inserting the card, etc., Look for any camera / blinking light in the close vicinity.
- ✓ Do not delay to report a lost Debit / Credit Card as the consequences can be adverse.
- ✓ Do change your PIN numbers as often as convenient.

- ✓ Register for SMS and E-mail alerts, whenever your account is accessed or debited.
- ✓ Verify the transactions in your bank statement regularly to identify suspicious transactions.
- ✓ Beware of unsolicited calls, texts or emails asking for sensitive financial information like Debit card/Credit card/ ATM pin/CVV/Expiry date or Password.

Best Practices to secure Debit/ Credit Cards:

- ✓ Download our mobile app CCB Mobile from Playstore to **Block your Rupay Debit card** to avoid fraudulent transactions and **Unblock the card only while using it**.
- ✓ While making online transactions with credit/debit card, **user must only use card at established and reputed sites** as there are less chances of card fraud on a reliable website.
- ✓ Always ensure that the **address of the website** where transactions to be done, **starts with"https://" and not "http://"**
- ✓ Always perform online financial transactions from a **secure computer system updated with latest security updates/patches**, anti-virus and anti-spyware software and personal firewall.
- ✓ **Change** your card **PIN** (Personal Identification Number) **periodically.**
- ✓ **Do not disclose any personal information online** like your date of birth, billing address, etc., on the Internet because that can be misused to unlock your account password.
- ✓ **Never share card details over the phone** or with anyone in person as it is easier way for others to get access to your credit card confidential information and make the online transactions.
- ✓ **Do not send card and account details through e-mail** to prevent from malicious use by others
- ✓ **Regularly check account statement related to the card** and notify the card company in caseof any discrepancy.

- ✓ **Ensure whether your card is enabled/disabled for International use**, disable if it is not necessary. Check with your bank for any additional options such as restricting the usage of cards on different payment channels viz., PoS/ATM/E-Commerce or Domestic/International usage time-to time through bank's own interface/app.

- ✓ **Never leave your card unattended.**

- ✓ **Keep card help line** phone numbers with you **for any kind of assistance.**

- ✓ Download our mobile app CCB mobile from Playstore to **Block your Rupay Debit Card** to avoid fraudulent transactions and **Unblock the card only while using it**.

Best Practices for users:

- ✓ **Ensure that you have your strong passwords** for all accounts. Use of non-dictionary words is also advised. Do not share your password with others.

- ✓ **Shop with companies/websites you know**. If the company is unfamiliar, investigate their authenticity and credibility. Conduct an internet search for the company/website name.

- ✓ Websites having click and wrap agreements, privacy policies, **by reading these policies one knows about the uses of information by websites**. Websites do sell this information. Some major social networking sites use or sell information (not personal data) about you to display advertising or other information they believe might be useful to you. Therefore, it is advised that one should read the privacy policies of websites before getting into it.

- ✓ **Minimum amount of information should only be disclosed** such as screen name should not givea clue to the identity of the user.

- ✓ **Avoid posting personal information** such as your address, phone numbers, e-mail address, license number, Aadhar No, birth date, birth place, location for any given day, school's name of kids, and family details.

- ✓ While posting photos, **avoid providing details** of where you live, work or go to college. Also, do not post photos depicting negative or inappropriate behaviors, remember you are writing your own history and it will continue to exist in the cyber world.

- ✓ **Look for encryption**, before making any sort of digital payment, look for signs that show whether the website is encrypted or not. To do this, look for two things: the trusted security lock symbols and the extra “s” at the end of http in the URL or web address bar.
- ✓ **Avoid connecting with strangers** since you don't know that your information could be used in away you didn't intend.
- ✓ **Verify emails and links in emails** you supposedly get from your social networking site. These are often designed to gain access to your user name, password, and ultimately your personal information. These mails could be phishing emails too. Do not click on any links without identifying the genuineness. In case the link seems to be a genuine website, do not click, copy andpaste in the address bar
- ✓ Keep your **anti-virus and software updated**.
- ✓ **Own your online identity** - Check privacy and security settings and set it to your comfort level for information sharing
- ✓ **Secure your login** - Use strongest authentication tools wherever available and applicable, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are always not enough to protect key accounts like email, banking and e-wallets.