Unit -2

What is Information Security?

Information Security is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electronic one. Information can be anything like Your details or we can say your profile on social media, your data in mobile phone, your biometrics etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc.
During First World War, Multi-tier Classification System was developed keeping in mind sensitivity of information. With the beginning of Second World War formal alignment of Classification System was done. Alan Turing was the one who successfully decrypted Enigma Machine which was used by Germans to encrypt warfare data.

Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

1. **Confidentiality –** means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.
2. **Integrity –** means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.
3. **Availability –** means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management.
   Denial of service attack is one of the factor that can hamper the availability of information.

Apart from this there is one more principle that governs information security programs. This is Non repudiation.

- **Non repudiation –** means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. For example in cryptography it is sufficient to show that message matches the digital signature signed with sender's private key and that sender could have a sent a message and nobody else could have altered it in transit. Data Integrity and Authenticity are pre-requisites for Non repudiation.
- **Authenticity –** means verifying that users are who they say they are and that each input arriving at destination is from a trusted source. This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission. For example if take above example sender sends the message along with digital signature which was generated using the hash value of message and private key. Now at the receiver side this digital signature is decrypted using the public key generating a hash value and message is again hashed to generate the hash value. If the 2 value matches then it is known as valid transmission with the authentic or we say genuine message received at the recepient side
- **Accountability –** means that it should be possible to trace actions of an entity uniquely to that entity. For example as we discussed in Integrity section Not every employee should be allowed to do changes in other employees data. For this there is a separate department in an organization that is responsible for making such changes and when they receive request for a change then that letter must be signed by higher authority for example Director of college and person that is allotted that change will be able to do change after verifying his bio metrics,

thus timestamp with the user(doing changes) details get recorded. Thus we can say if a change goes like this then it will be possible to trace the actions uniquely to an entity.

At the core of Information Security is Information Assurance, which means the act of maintaining CIA of information, ensuring that information is not compromised in any way when critical issues arise. These issues are not limited to natural disasters, computer/server malfunctions etc.

Thus, the field of information security has grown and evolved significantly in recent years. It offers many areas for specialization, including securing networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning etc.

What is a Malicious program

The words "Malicious Software" coin the word "Malware" and the meaning remains the same. Malicious Software refers to any malicious program that causes harm to a computer system or network. Malicious Malware Software attacks a computer or network in the form of viruses, worms, trojans, spyware, adware or rootkits.

Their mission is often targeted at accomplishing unlawful tasks such as robbing protected data, deleting confidential documents or add software without the user consent.

Different Types of Malicious Software

Computer Virus

A computer virus is a malicious software which self-replicates and attaches itself to other files/programs. It is capable of executing secretly when the host program/file is activated. The different types of Computer virus are Memory-Resident Virus, Program File Virus, Boot Sector Virus, Stealth Virus, Macro Virus, and Email Virus.

Worms

A worm is a malicious software which similar to that of a computer virus is a self-replicating program, however, in the case of worms, it automatically executes itself. Worms spread over a network and are capable of launching a cumbersome and destructive attack within a short period.

Trojan Horses

Unlike a computer virus or a worm – the trojan horse is a non-replicating program that appears legitimate. After gaining the trust, it secretly performs malicious and illicit activities when executed. Hackers make use of trojan horses to steal a user's password information, destroy data or programs on the hard disk. It is hard to detect!

Spyware/Adware

Spyware secretly records information about a user and forwards it to third parties. The information gathered may cover files accessed on the computer, a user's online activities or even user's keystrokes.

Adware as the name interprets displays advertising banners while a program is running. Adware can also work like spyware, it is deployed to gather confidential information. Basically, to spy on and gather information from a victim's computer.

Rootkit

A rootkit is a malicious software that alters the regular functionality of an OS on a computer in a stealthy manner. The altering helps the hacker to take full control of the system and the hacker acts as the system administrator on the victim's system. Almost all the rootkits are designed to hide their existence.

Malicious Software History

Even before the internet became widespread, malicious software (virus) was infected on personal computers with the executable boot sectors of floppy disks. Initially, the computer viruses were written for the Apple II and Macintosh devices. After the IBM PC and MS-DOS system became more widespread they were also targeted in the similar fashion.

The first worms originated on multitasking Unix systems, they were the first network-borne infectious programs too. SunOS and VAX BSD systems were infected by the first well-known worm of the time called the Internet Worm of 1988. Ever since the advent of Microsoft Windows platform in the 1990s, the infectious codes were written in the macro language of Microsoft Word and similar programs.

Methods of protection against malicious software

Malicious Software is definitely a security threat for corporate users and individuals, thereby detecting and fighting malware remains on top of the agenda for many firms. Since the time BYOD culture started to flourish, Endpoint Security and Endpoint Protection have become the topics of discussion in many IT conference rooms. Many corporates today try to implement the best Endpoint Security or Endpoint Protection software to steer clear of the dangers.

Remember, if it is an individual system, it is essential to have an antivirus installed and if you already have one in place see to that it is updated at regular intervals. This approach will help you to remain safe during new breakouts. Comodo's Free Antivirus, Endpoint Security, Endpoint Protection Solutions are your best option for detecting and fighting malicious software.

What is a Malicious program?

Malicious programs can be divided into the following groups: worms, viruses, trojans, hacker utilities and other malware. All of these are designed to damage the infected machine or other networked machines.

Network Worms

This category includes programs that propagate via LANs or the Internet with the following objectives:

- Penetrating remote machines.
- Launching copies on victim machines.
- Spreading further to new machines.

Worms use different networking systems to propagate: email, instant messaging, file-sharing (P2P), IRC channels, LANs, WANs and so forth.
Most existing worms spread as files in one form or another: e-mail attachments, in ICQ or IRC messages, links to files stored on infected websites or FTP servers, files accessible via P2P networks and so on.
There are a small number of so-called fileless or packet worms; these spread as network packets and directly penetrate the RAM of the victim machine, where the code is then executed.

Worms use a variety of methods for penetrating victim machines and subsequently executing code, including:

- Social engineering; emails that encourage recipients to open the attachment.
- Poorly configured networks; networks that leave local machines open to access from outside the network.
- Vulnerabilities in operating systems and applications.

Today's malware is often a composite creation: worms now often include Trojan functions or are able to infect exe files on the victim machine. They are no longer pure worms, but blended threats.

Classic Viruses

A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the owner. A virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer.
Viruses spread copies of themselves in order to:

- Launch and/or execute code once a user fulfills a designated action.
- Penetrate other resources within the victim's machine.

Unlike worms, viruses do not use network resources to penetrate other machines. Copies of viruses can penetrate other machines only if an infected object is accessed and the code is launched by a user on an uninfected machine. This can happen in the following ways:

- The virus infects files on a network resource that other users can access.
- The virus infects removable storage media which are then attached to a clean machine.
- The user attaches an infected file to an email and sends it to a 'healthy' recipient.

Viruses are sometimes carried by worms as additional payloads or they can themselves include backdoor or Trojan functionality which destroy data on an infected machine.

Trojan Programs

This class of malware includes a wide variety of programs that perform actions without the user's knowledge or consent: collecting data and sending it to a cyber criminal, destroying or altering data with malicious intent, causing the computer to malfunction, or using a machine's capabilities for malicious or criminal purposes, such as sending spam.
A subset of Trojans damage remote machines or networks without compromising infected machines; these are Trojans that utilize victim machines to participate in a Denial of Service "DoS" attack on a designated web site.

Hacker Utilities and other malicious programs

This diverse class includes:

- Utilities such as constructors that can be used to create viruses, worms and Trojans.
- Program libraries specially developed to be used in creating malware.
- Hacker utilities that encrypt infected files to hide them from antivirus software.

- Jokes that interfere with normal computer function.
- Programs that deliberately misinform users about their actions in the system.
- Other programs that are designed to directly or indirectly damage local or networked machines.

Cryptography and its Types

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".
In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography:
In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.
Features Of Cryptography are as follows:

1. **Confidentiality:**
   Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:**
   Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:**
   The creator/sender of information cannot deny his or her intention to send information at later stage.
4. **Authentication:**
   The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:
In general there are three types Of cryptography:

1. **Symmetric Key Cryptography:**
   It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).
2. **Hash Functions:**
   There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:**
   Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

Three types of cryptographic techniques used in general.

1. Symmetric-key cryptography

2. Hash functions.

3. Public-key cryptography

Symmetric-key Cryptography: Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

Public-Key Cryptography: This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

Hash Functions: No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

Digital Signatures

Introduction

A digital signature is exactly what it sounds like a modern alternative to signing documents with paper and pen.

It uses an advanced mathematical technique to check the authenticity and integrity of digital messages and documents. It guarantees that the contents of a message are not altered in transit and helps us overcome the problem of impersonation and tampering in digital communications.

Digital signatures also provide additional information such as the origin of the message, status, and consent by the signer.

The role of digital signatures

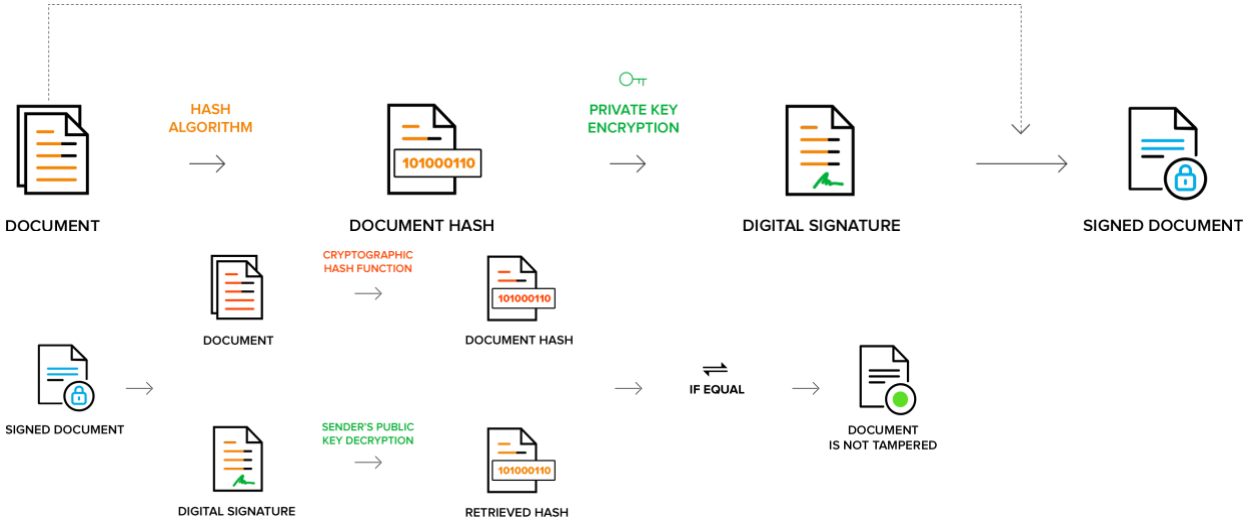
In many regions, including parts of North America, the European Union, and APAC, digital signatures are considered legally binding and hold the same value as traditional document signatures.
In addition to digital document signing, they are also used for financial transactions, email service providers, and software distribution, areas where the authenticity and integrity of digital communications are crucial.
Industry-standard technology called public key infrastructure ensures a digital signature's data authenticity and integrity.

How do digital signatures work?

Using a mathematical algorithm, digital signing solution providers such as Zoho Sign will generate two keys: a public key and a private key. When a signer digitally signs a document, a cryptographic hash is generated for the document.
That cryptographic hash is then encrypted using the sender's private key, which is stored in a secure HSM box. It is then appended to the document and sent to the recipients along with the sender's public key.

The recipient can decrypt the encrypted hash with the sender's public key certificate. A cryptographic hash is again generated on the recipient's end.

Both cryptographic hashes are compared to check its authenticity. If they match, the document hasn't been tampered with and is considered valid.



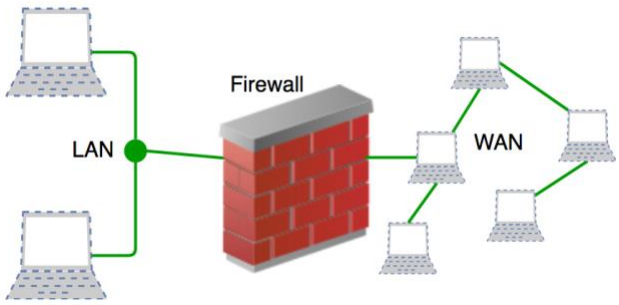
Introduction of Firewall in Computer Network

Last Updated: 21-11-2019

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic
Reject : block the traffic but reply with an "unreachable error"
Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



History and Need for Firewall

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to

specific IP address.
But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.

Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

How Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.
Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.
Default policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop).
Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to *accept*, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as *drop* (or reject) is always a good practice.

Generation of Firewall

Firewalls can be categorized based on its generation.

1. **First Generation- Packet Filtering Firewall :** Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers).
   Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers.

   Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be Filtered according to

following rules:

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.

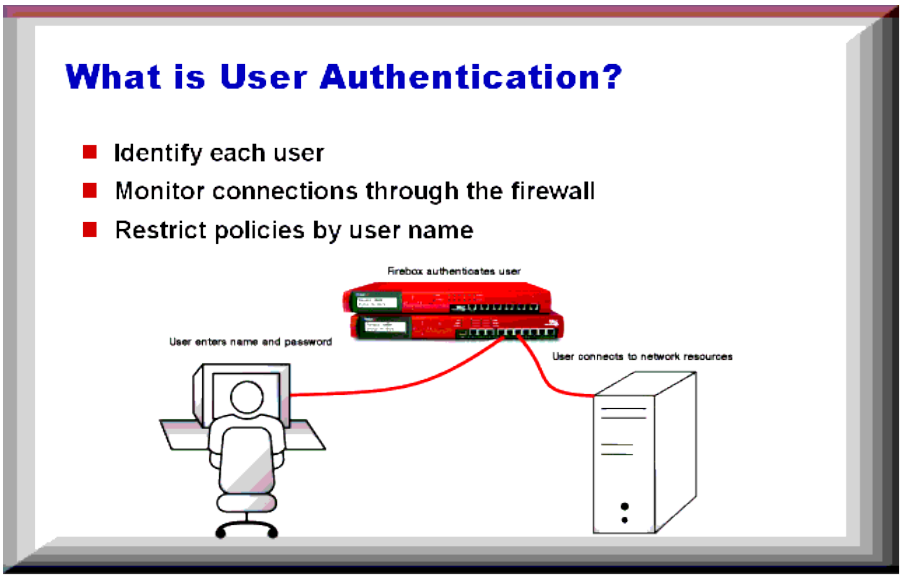
2. **Second Generation- Stateful Inspection Firewall :** Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.
3. **Third Generation- Application Layer Firewall :** Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.
   In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.
   Note: Application layer firewalls can also be used as Network Address Translator(NAT).
4. **Next Generation Firewalls (NGFW) :** Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

Types of Firewall

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

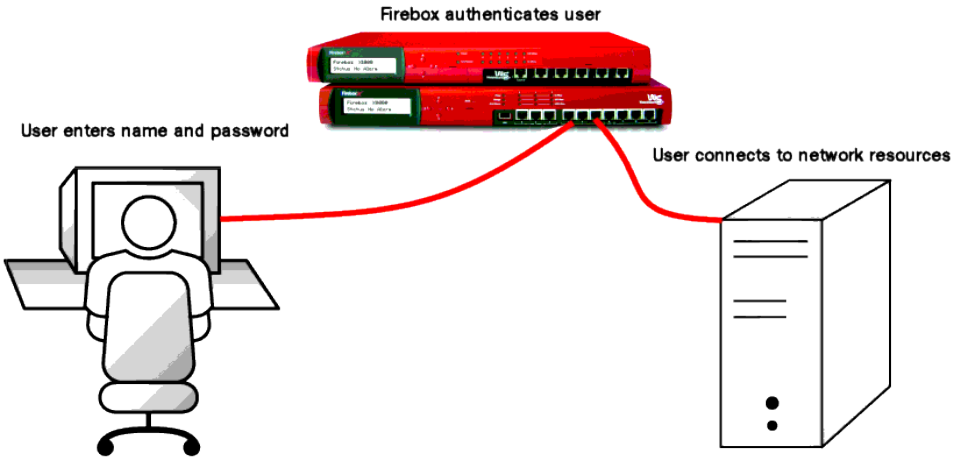
What is User Authentication?



User authentication is a process that allows a device to verify the identity of someone who connects to a network resource. There are many technologies currently available to a network administrator to authenticate users. Fireware operates with frequently used applications, including RADIUS, Windows Active Directory, LDAP, and token-based SecurID. The Firebox also has its own authentication server. You can use the Firebox authentication features to monitor and control connections through the Firebox.

Authentication is very important when you use dynamic IP addressing (DHCP) for computers on the trusted or optional network. It is also important if you must identify your users before you let them connect to resources on the external network. Because the Firebox® associates a user name to an IP address, we do not recommend that you use authentication features in a network with multi-user computers such as Unix servers, terminal servers or Citrix servers. The Firebox authenticates one user per computer.

With WatchGuard® System Manager, you can configure authentication on a per policy basis. For example, you can force some users to authenticate before they connect to an FTP server although they can browse the Internet without authentication.



To get access to services such as HTTP or FTP the user types a domain along with their login name and password. For the duration of authentication, the user name is associated with connections coming from the IP address from which the user authenticated. This makes it possible to monitor not only the computers from which connections originate, but also the users who start

the connection. While the user is authenticated, all the connections that the user starts from the IP address include the session name.

User identification and authentication are essential parts of information security. Users must authenticate as they access their computer systems at work or at home every day. Yet do users understand how and why they are actually being authenticated, the security level of the authentication mechanism that they are using, and the potential impacts of selecting one authentication mechanism or another? Introducing key concepts, Mechanics of User Identification and Authentication: Fundamentals of Identity Management outlines the process of controlled access to resources through authentication, authorization, and accounting in an in-depth, yet accessible manner. It examines today's security landscape and the specific threats to user authentication. The book then outlines the process of controlled access to resources and discusses the types of user credentials that can be presented as proof of identity prior to accessing a computer system. It also contains an overview on cryptography that includes the essential approaches and terms required for understanding how user authentication works. This book provides specific information on the user authentication process for both UNIX and Windows. Addressing more advanced applications and services, the author presents common security models such as GSSAPI and discusses authentication architecture. Each method is illustrated with a specific authentication scenario.

A Guide to Understanding Identification and Authentication in Trusted Systems provides a set of good practices related to identification and authentication (I & A).We have written this guideline to help the vendor and evaluator community under-stand the requirements for I & A, as well as the level of detail required of I & A at all classes, as described in the Department of Defense Trusted Computer Systems Evaluation Criteria. In an effort to provide guidance, we make recommendations in this technical guideline that are not requirements in the Criteria.

The I & A Guide is the latest in a series of technical guidelines published by the National Computer Security Center. These publications provide insight to the Trusted Computer Systems Evaluation Criteria requirements for the computer security vendor and technical evaluator. The goal of the Technical Guideline Program is to discuss each feature of the Criteria in detail and to provide the proper interpretations with specific guidance.

The National Computer Security Center has established an aggressive program to study and implement computer security technology. Our goal is to encourage the widespread availability of trusted computer products for use by any organization desiring better protection of its important data. One of the ways we do this is by the Trusted Product Evaluation Program. This program focuses on the security features of commercially produced and supported computer systems. We evaluate the protection capabilities against the established criteria presented in the Trusted Computer System Evaluation Criteria. This program, and an open and cooperative business relationship with the computer and telecommunications industries, will result in the fulfillment of our country's information systems security requirements. We resolve to meet the challenge of identifying trusted computer products suitable for use in processing delicate information. I invite your suggestions for revising this technical guideline. We will review this document as the need arises.
Explain the difference between identification and authentication (identity proofing).

Identification and authentication are commonly used as a two-step process, but they are distinct activities. Identification is the claiming of an identity. This only needs to occur once per authentication or access process. Any one of the three common authentication factors can be employed for identification. Once identification has been performed, the authentication process must take place. Authentication is the act of verifying or proving the claimed identity. The issue is both checking that such identity actually exists within the known accounts of the secured

Information Security Awareness Policy

Purpose

The purpose of this policy is to raise the awareness of information security, and to inform and highlight the responsibilities faculty, staff, and certain student workers, third party contractors and volunteers have regarding their information security obligations. Formal information security awareness will aid in the protection of data, personal, intellectual property, financial, or restricted and sensitive information, networked systems, and applications entrusted to and utilized by the University, by providing a broad understanding of information security threats, risks and best practices.

Scope

Faculty, Staff and Student Workers:

This policy applies to all faculty, staff and student workers as they may access, store, process, transmit or manage University data, systems, or applications. As members of the Villanova University community faculty, staff and student workers are accountable, and have an obligation to demonstrate an understanding of their unique role and responsibility, as the best defense to ensure the protection of the University's information, data, and reputation.

Third Party Contractors (defined as vendors, consultants – non-Villanova employees) and Volunteers:

Third Party Contractors and volunteers who have access to University Data or systems in the course of their employment or volunteer activities are also covered by this policy. Except under narrow circumstances described in Section IV. Policy Statement below, volunteers may not have access to University Data or systems. When working or providing services on behalf of Villanova, Third Party Contractors and volunteers are accountable and have an obligation to demonstrate an understanding of their unique role and responsibility as the best defense to ensure the protection of the University's information, data, and reputation.

Definitions

1. **University Data:** University Data is any data or information that is created, owned, received, stored, or managed by Villanova University.

2. **Third Party Contractors**: defined as vendors or consultant(s), and not University employees.

Policy Statement

The University Information Security Office is responsible for the information security awareness program, training, education, and awareness communication for the University. The program will include an enhanced understanding and appreciation of information risks; services that the University Information Security Office provides; information about the threats, techniques, and consequences to the University; information on reporting incidents; guidance and resources to protect information and devices at work and at home.

Faculty, Staff and Student Workers:

Formal participation and review of the security awareness program is mandatory for all full time and part time faculty and staff, every three years. Newly hired faculty and staff are required to complete the training within thirty days of their hire date. The requirement for a review every three years shall be superseded by an incident or information indicating a need for immediate intervention and training by a specific department, or the entire University. Additional topic specific training may be required, based on role, information type access/use (e.g. PCI-DSS, Research, HIPAA, etc.), or identified increased risk. Student workers who may have access to, or the ability to store, process, transmit or manage University Data are also required to complete this

training within thirty days of their hire date. It is the responsibility of the student worker's supervisor to ensure that the student worker completes this requirement.

The University Information Security Office will coordinate, monitor, and track the completion of the required Security Awareness program. University Vice Presidents and Deans are required to ensure adherence to the policy, and completion of the required program. Program content will be updated yearly, in order to reflect current security trends, threats, techniques, and the evolving environment of information security.

Failure to comply with this policy may result in denial or removal of access privileges to the University's electronic systems (e-mail, eLearning, wireless, and Villanova network).

Third Party Contractors and Volunteers:

Formal participation and review of the security awareness program for Third Party Contractors who have access to University Data or systems in the course of their academic, employment, or service activities is mandatory as a condition of Third Party Contractor engagement. This program will be delivered through University created videos within thirty days after access is permitted. Volunteers may not have access to University Data or systems except in those instances in which it is strictly necessary in the performance of their volunteer or service activities. Any such access must be requested by the University administrator, faculty or staff who is overseeing the volunteers and authorized by UnIT before such access is granted.

University Vice Presidents and Deans overseeing Third Party Contractors and volunteers with access to University Data are required to ensure adherence to the policy, and completion of the required program. Program content will be updated yearly, in order to reflect current security trends, threats, techniques, and the evolving environment of information security.

Failure to comply with this policy may result in denial or removal of access privileges to the University's electronic systems (e-mail, eLearning, wireless, and Villanova network).

The best security technology in the world can't help you unless employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources. This will involve putting practices and policies in place that promote security and training employees to be able to identify and avoid risks.
A firm's security strategy will only work if employees are properly trained on it. Therefore, the importance of providing information security awareness training cannot be understated. The goal of an awareness program is not merely to educate employees on potential security threats and what they can do to prevent them. A larger goal should be to change the culture of your organization to focus on the importance of security and get buy-in from end users to serve as an added layer of defense against security threats.

Once you have buy-in from employees, your focus can turn to ensuring they get the necessary information they need to secure your business. An effective security awareness program should include education on specific threat types, including but not limited to:

- Malware
- Trojans
- Viruses
- Social engineering
- Phishing

Another important area to address is **the importance of password construction and security**. Seems minor? It's not. Believe it or not, password cracking is remarkably easy, particularly for

advanced hackers. And this 'minor' step that users take every day could make a significant difference in protecting your firm's sensitive information.

Talk to Your Employees About

- **Keeping a clean machine:** Your company should have clear rules for what employees can install and keep on their work computers. Make sure they understand and abide by these rules. Unknown outside programs can open security vulnerabilities in your network.
- **Following good password practices:** Making passwords long and strong, with a mix of uppercase and lowercase letters, numbers and symbols, along with changing them routinely and keeping them private are the easiest and most effective steps your employees can take to protect your data.
- **When in doubt, throw it out:** Employees should know not to open suspicious links in email, tweets, posts, online ads, messages or attachments – even if they know the source. Employees should also be instructed about your company's spam filters and how to use them to prevent unwanted, harmful email.
- **Backing up their work:** Whether you set your employees' computers to backup automatically or ask that they do it themselves, employees should be instructed on their role in protecting their work.
- **Staying watchful and speaking up:** Your employees should be encouraged to keep an eye out and say something if they notice strange happenings on their computer.

Information Security Awareness Program

A good Information Security Awareness Program highlights the importance of information security and introduces the Information Security Policies and Procedures in a simple yet effective way so that employees are able to understand the policies and are aware of the procedures.

Listed below are some of the methods used to communicate the importance of Information Security Policies and Procedures to the employees.

1. Information Classification, Handling and Disposal

All information must be labeled according to how sensitive it is and who is the target audience. Information must be labeled as "Secret", "Confidential", "Internal Use Only" or "Public". Documents that are labeled "Secret" or "Confidential" must be locked away at the end of the workday. Electronic information (Secret or Confidential) should be encrypted or password protected. When the information is no longer required, documents should be shredded while files should be electronically shredded.

2. System Access

No sharing of UserID and password is allowed and staff are made aware of their responsibility on safeguarding their user account and password. Staff are also provided with some useful Password Tips on how to select a good password.

3. Virus

All computers must have anti virus software installed and it is the responsibility of all staff to scan their computer regularly. All software and incoming files should be scanned and staff are advised to scan new data files and software before they are opened or executed. Staff are educated on the importance of scanning and how a virus can crash a hard drive and bring down the office network.

4. Backup

Staff are advised that they are responsible for their own personal computer backup and they should backup at least once a week.

5. Software Licenses

Software piracy is against the law and staff are advised not to install any software without a proper license.

6. Internet Use

Staff are advised that Internet use is monitored. Staff should not visit inappropriate websites such as hacker sites, pornographic sites and gambling sites. No software or hacker tools should be downloaded as well.

7. Email Use

Staff should not use the email system for the following reasons

- Chain letters
- Non company sponsored charitable solicitations
- Political campaign materials
- Religious work, harassment
- And any other non-business use.

Staff are allowed to use the email for personal use but within reason.

8. Physical security of notebooks

All notebooks should be secured after business hours in a cabinet, in a docking station or with a cable lock.

9. Internal Network Protection

All workstations should have a password protected screen saver to prevent unauthorized access into the network. For those using, Windows 7, they should lock their workstation. To prevent staff from downloading screen savers from the Internet, you can restrict the screen savers to the default ones which come with Windows 7.

10. Release of Information to Third Parties

Confidential information should not be released to third parties unless there is a need to know and a Non Disclosure Agreement has been signed. It is the responsibility of all staff to safeguard the company's information.

Training materials should also review corporate policies and clearly detail consequences for any suspicious or malicious behavior amongst employees.

For your convenience, we've compiled a variety of information on various security policies, including:

- Acceptable Use
- Social Media
- Bring Your Own Device
- Security Incident Management

Dos and Don'ts

A Dos and Don'ts checklist is given to all new staff upon joining company. As it may be sometime before they attend the actual security training, the checklist would be a good and easy way for them to learn about what they should and should not do. The information in the checklist is listed below.

Don'ts

- Do not share your password with anyone including staff

- Do not write your password on any paper, whiteboard or post it pad
- Do not use easy to remember words as passwords e.g. Aug2001
- Do not use personal information or any word in any language spelled forwards or backwards in any dictionary
- Do not visit inappropriate web sites e.g. pornographic or hacker web sites
- Do not download unlawful or unlicensed software from the Internet
- Do not install unlicensed software onto your computer

Dos

- Do change your password regularly for every system.
- Do use a combination of letters, symbols and number for passwords
- Do use difficult passwords which are at least 6 characters long
- Do enable your Screen Saver Password or lock your workstation
- Do scan your computer regularly for viruses and any diskettes as well before you use them on your computer
- Do check that your virus software patches have been updated when you receive the regular update emails from Desktop Support
- Do backup your data at least once a week. It is your responsibility to do so.
- Do lock away all confidential documents, files and diskettes at the end of each work day

Training Your Employees

Training employees is a critical element of security. They need to understand the value of protecting customer and colleague information and their role in keeping it safe. They also need a basic grounding in other risks and how to make good judgments online.

Most importantly, they need to know the policies and practices you expect them to follow in the workplace regarding Internet safety.

Top 10 Security Awareness Training Topics for Your Employees

An organization's employees are one of the biggest risks to its cybersecurity. In fact, human error is considered the leading cause of data breaches.

However, an organization's employees can also be a huge asset for an organization's cybersecurity. If employees are provided with the knowledge they require to identify cyberthreats — through an effective and engaging security training program — they can act as another line of defense for an organization.

We made simulated phishing training easy

Get a first-hand look at the training content, phishing simulations and integrations that make Infosec IQ an industry leader.

When designing a cybersecurity training program, it's important to ensure that it covers the cyberthreats that an organization is most likely to face. This article outlines the ten most important security awareness topics to be included in a security awareness program

1. Email scams

Phishing attacks are the most common method that cybercriminals use to gain access to an organization's network. They take advantage of human nature to trick their target into falling for the scam by offering some incentive (free stuff, a business opportunity and so on) or creating a sense of urgency.

Phishing awareness should be a component of any organization's security training program. This should include examples of common and relevant phishing emails and tips for identifying attempted attacks, including:

- Do not trust unsolicited emails
- Do not send any funds to people who request them by email, especially not before checking with leadership
- Always filter spam
- Configure your email client properly
- Install antivirus and firewall program and keep them up to date
- Do not click on unknown links in email messages
- Beware of email attachments. Verify any unsolicited attachments with the alleged sender (via phone or other medium) before opening it
- Remember that phishing attacks can occur over any medium (including email, SMS, enterprise collaboration platforms and so on)

2. Malware

Malware is malicious software that cybercriminals use to steal sensitive data (user credentials, financial information and so on) or cause damage to an organization's systems (e.g., ransomware and wiper malware). It can be delivered to an organization in a number of different ways, including phishing emails, drive-by downloads and malicious removable media.

Employee security awareness training on malware should cover common delivery methods, threats and impacts to the organization. Important tips include:

- Be suspicious of files in emails, websites and other places
- Don't install unauthorized software
- Keep antivirus running and up to date
- Contact IT/security team if you may have a malware infection

3. Password security

Passwords are the most common and easiest-to-use authentication system in existence. Most employees have dozens of online accounts that are accessed by providing a username (often their email address) and a password.

Poor password security is one of the biggest threats to modern enterprise security. Some important password security tips to include in training content:

- Always use a unique password for each online account
- Passwords should be randomly generated
- Passwords should contain a mix of letters, numbers and symbols

- Use a password manager to generate and store strong passwords for each account
- Use multi-factor authentication (MFA) when available to reduce the impact of a compromised password

4. Removable media

Removable media (such as USBs, CDs and so on) are a useful tool for cybercriminals since they enable malware to bypass an organization's network-based security defenses. Malware can be installed on the media and configured to execute automatically with Autorun or have an enticing filename to trick employees into clicking. Malicious removable media can steal data, install ransomware or even destroy the computer they're inserted into.

Malicious removable media can be distributed by being dropped in parking lots and common areas or being handed out at conferences and other public events. Employees should be trained to properly manage untrusted removable media:

- Never plug untrusted removable media into a computer
- Bring all untrusted removable media to IT/security for scanning
- Disable autorun on all computers

5. Safe internet habits

Almost every worker, especially in tech, has access to the internet. For this reason, the secure usage of the internet is of paramount importance for companies.

Security training programs should incorporate safe internet habits that prevent attackers from penetrating your corporate network. Some important content to include in training:

- The ability to recognize suspicious and spoofed domains (like yahooo.com instead of yahoo.com)
- The differences between HTTP and HTTPS and how to identify an insecure connection
- The dangers of downloading untrusted or suspicious software off the internet
- The risks of entering credentials or login information into untrusted or risks websites (including spoofed and phishing pages)
- Watering hole attacks, drive-by downloads and other threats of browsing suspicious sites

6. Social networking dangers

Enterprises use social networking as a powerful tool to build a brand (either locally or globally) and generate online sales. Unfortunately, cybercriminals also use social media for attacks that put an organization's systems and reputation at risk.

To prevent the loss of critical data, the enterprise must have a viable social networking training program that should limit the use of social networking and inform employees of the threats of social media:

- Phishing attacks can occur on social media as well as over email
- Cybercriminals impersonating trusted brands can steal data or push malware
- Information published on social media can be used to craft spearphishing emails

7. Physical security and environmental controls

Security awareness isn't just about what resides in your company's computers or handheld devices. Employees should be aware of potential security risks in physical aspects of the workplace, such as:

- Visitors or new hires watching as employees type in passwords (known as "shoulder surfing")
- Letting in visitors claiming to be inspectors, exterminators or other uncommon guests who might be looking to get into the system (called "impersonation")
- Allowing someone to follow you through a door into a restricted area (called "tailgating")
- Leaving passwords on pieces of paper on one's desk
- Leaving one's computer on and not password-protected when leaving work for the night
- Leaving an office-issued phone or device out in plain sight
- Physical security controls (doors, locks and so on) malfunctioning

8. Clean desk policy

Sensitive information on a desk such as sticky notes, papers and printouts can easily be taken by thieving hands and seen by prying eyes. A clean desk policy should state that information visible on a desk should be limited to what is currently necessary. Before leaving the workspace for any reason, all sensitive and confidential information should be securely stored.

9. Data management and privacy

Most organizations collect, store and process a great deal of sensitive information. This includes customer data, employee records, business strategies and other data important to the proper operation of the business. If any of this data is publicly exposed or accessible to a competitor or cybercriminal, then the organization may face significant regulatory penalties, damage to consumer relationships and a loss of competitive advantage.

Employees within an organization need to be trained on how to properly manage the businesses' sensitive data to protect data security and customer privacy. Important training content includes:

- The business's data classification strategy and how to identify and protect data at each level
- Regulatory requirements that could impact an employee's day-to-day operations
- Approved storage locations for sensitive data on the enterprise network
- Use a strong password and MFA for accounts with access to sensitive data

10. Bring-your-own-device (BYOD) policy

BYOD policies enable employees to use their personal devices in the workplace. While this can improve efficiency — by enabling employees to use the devices that they are most comfortable with — it also creates potential security risks.

BYOD policies and employee security awareness training should include the following tips:

- All devices used in the workplace should be secured with a strong password to protect against theft
- Enable full-disk encryption for BYOD devices
- Use a VPN on devices when working from untrusted Wi-Fi
- BYOD-approved devices should be running a company-approved antivirus

- Only download applications from major app stores or directly from the manufacturer's website

Conclusion

Employees play a crucial role in running a successful business. An untrained and negligent workforce can put your enterprise in danger of multiple data breaches. Therefore, organizations must adopt a viable security training program that should encompass the essential guidelines needed to thwart imminent cyber-incidents.

Your organization should also set monthly training meetings, provide frequent reminders, train all new personnel on new policies as they arrive, make training material available and implement creative incentives to reward employees for being proactive in ensuring the security of the organization.

Application security

Application security describes security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked. It encompasses the security considerations that happen during application development and design, but it also involves systems and approaches to protect apps after they get deployed.

Application security may include hardware, software, and procedures that identify or minimize security vulnerabilities. A router that prevents anyone from viewing a computer's IP address from the Internet is a form of hardware application security. But security measures at the application level are also typically built into the software, such as an application firewall that strictly defines what activities are allowed and prohibited. Procedures can entail things like an application security routine that includes protocols such as regular testing.

Application security definition

Application security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.

Buying and selling products and services through mobile devices are the new trend. A housewife can purchase her kitchen appliances from the comfort of her living room, a busy person can order lunch from office, one can use mobile platforms to sell goods and services − all with a few clicks.

Why application security is important

Application security is important because today's applications are often available over various networks and connected to the cloud, increasing vulnerabilities to security threats and breaches. There is increasing pressure and incentive to not only ensure security at the network level but also within applications themselves. One reason for this is because hackers are going after apps with their attacks more today than in the past. Application security testing can reveal weaknesses at the application level, helping to prevent these attacks.

Types of application security

Different types of application security features include authentication, authorization, encryption, logging, and application security testing. Developers can also code applications to reduce security vulnerabilities.

- **Authentication**: When software developers build procedures into an application to ensure that only authorized users gain access to it. Authentication procedures ensure that a user is who they say they are. This can be accomplished by requiring the user to provide a user name and password when logging in to an application. Multi-factor authentication requires more than one form of authentication—the factors might include something you know (a password), something you have (a mobile device), and something you are (a thumb print or facial recognition).

- **Authorization**: After a user has been authenticated, the user may be authorized to access and use the application. The system can validate that a user has permission to access the application by comparing the user's identity with a list of authorized users. Authentication must happen before authorization so that the application matches only validated user credentials to the authorized user list.
- **Encryption**: After a user has been authenticated and is using the application, other security measures can protect sensitive data from being seen or even used by a cybercriminal. In cloud-based applications, where traffic containing sensitive data travels between the end user and the cloud, that traffic can be encrypted to keep the data safe.
- **Logging**: If there is a security breach in an application, logging can help identify who got access to the data and how. Application log files provide a time-stamped record of which aspects of the application were accessed and by whom.
- **Application security testing**: A necessary process to ensure that all of these security controls work properly.

Application security in the cloud
Application security in the cloud poses some extra challenges. Because cloud environments provide shared resources, special care must be taken to ensure that users only have access to the data they are authorized to view in their cloud-based applications. Sensitive data is also more vulnerable in cloud-based applications because that data is transmitted across the Internet from the user to the application and back.

Mobile application security
Mobile devices also transmit and receive information across the Internet, as opposed to a private network, making them vulnerable to attack. Enterprises can use virtual private networks (VPNs) to add a layer of mobile application security for employees who log in to applications remotely. IT departments may also decide to vet mobile apps and make sure they conform to company security policies before allowing employees to use them on mobile devices that connect to the corporate network.

Web application security
Web application security applies to web applications—apps or services that users access through a browser interface over the Internet. Because web applications live on remote servers, not locally on user machines, information must be transmitted to and from the user over the Internet. Web application security is of special concern to businesses that host web applications or provide web services. These businesses often choose to protect their network from intrusion with a web application firewall. A web application firewall works by inspecting and, if necessary, blocking data packets that are considered harmful.

What are application security controls?
Application security controls are techniques to enhance the security of an application at the coding level, making it less vulnerable to threats. Many of these controls deal with how the application responds to unexpected inputs that a cybercriminal might use to exploit a weakness. A programmer can write code for an application in such a way that the programmer has more control over the outcome of these unexpected inputs. Fuzzing is a type of application security testing where developers test the results of unexpected values or inputs to discover which ones cause the application to act in an unexpected way that might open a security hole.

M-Commerce

What is M-Commerce?

Mobile commerce or simply M-Commerce means engaging users in a buy or sell process via a mobile device. For instance, when someone buys an Android app or an iPhone app, that person

is engaged in m-commerce. There are a number of content assets that can be bought and sold via a mobile device such as games, applications, ringtones, subscriptions etc.

How does M-Commerce Work?

Let's look at some of the points that you need to remember as a business, while engaging in m-commerce −

Decide Where to Sell

Before you sell your products or services via m-commerce, you need to decide what type of outlets or stores suit your business best. Let us suppose you have created ringtones − you can sell them either at specific third-party outlets or to independent aggregators who charge you a commission for the service.

You can also sell your ringtones on mobile stores or app stores such as Android marketplace or App store (Apple). These stores are frequently visited by many buyers and hence ideal for making sales easily and efficiently. Finally, you can also sell via your own mobile store by creating a mobile website specifically for sales or as by setting-up an m-commerce page on your main website.

Set up Mobile Billing

Once you have decided where to sell, the next step is to set up your merchant account. For instance, you can use third-party services such as PayPal. This is ideal for small businesses or also large companies. A third-party application makes it really easy for you as well as your customers to make the payments, but then they do charge commission on the transaction.

You can also set-up your own billing and payment gateway, but make sure that you make it really easy for users. Mobile users do not use keyboards or a mouse so make sure that the design of your m-commerce site is intuitive, with easy navigation tools and the right display sizes. Basically, make your m-commerce site optimized for Smartphone users.

Benefits of M-Commerce

The major benefit of engaging in m-commerce is the sheer size of potential sales. The probability of your potential customers owning a Smartphone is very high, so you can safely assume that you will get much more positive response from mobile devices than your website. M-commerce is recommended for every business irrespective of its type, scale, and size.

Mobile devices help users to navigate the world. Customers use mobile devices for all aspects of their needs. They act on the information they see. So advertisers need to extend online advertising and should strive to be seen on mobiles.

Mobile commerce definition

Mobile commerce, also called mCommerce, refers to any transaction completed with a mobile device – be it a smartphone, tablet, or even a wearable device (see the trend for wearable payments, for example).

Experts consider mobile commerce as the next phase of eCommerce, as it allows consumers to buy goods or services online – but from anywhere and at any time.

But mobile commerce is so much more than that. In fact, mCommerce triggered the emergence of brand-new industries and services or helped the existing ones to grow in new directions. Examples of such innovations include:

- tickets and boarding passes,
- mobile banking,
- money transfers, contactless payments, and in-app payments,
- digital content purchases,
- location-based services,
- mobile marketing, including coupons and loyalty cards.

What are the key mobile commerce advantages?

Now that you know what mobile commerce is all about, you might be wondering why so many businesses are investing in it today. The truth is that a mCommerce application offers numerous advantages to companies and customers who use them.

Here are three good reasons why your business needs a mobile commerce application.

1. Better customer experience

We all know what happened when eCommerce became popular. It made shopping so much more convenient and fun for customers. They could browse through a wide range of products, benefit from more competitive pricing, and complete their purchases without having to step away from their computers.

It's safe to say that we all got used to purchasing products and services online. With mobile commerce, we retain all the benefits of eCommerce – but now we don't even have to use our laptops or desktop computers anymore. As long as consumers have a mobile device, they can shop whenever they want and from wherever.

Mobile commerce allows companies to interact with customers easily because they're using apps and services their target audiences already know and like to use.

To amplify the user experience in their mobile commerce applications, companies use cutting-edge solutions such an augmented reality (AR) or chatbots. For example, IKEA is among the top retailers that take advantage of AR apps to boost their mobile commerce business.

2. Omnichannel

This is a unique strength of mobile commerce applications. An omnichannel experience is an experience of customers who purchase from stores that sell through multiple online and offline channels. Examples of such touch points include brick-and-mortar stores, an online store, online marketplaces like Amazon, social media apps like Facebook or Instagram, and dedicated mobile apps.

To get ahead of their competition, businesses are striving to list their products wherever they know potential consumers are already spending their time.

This type of contextual commerce offers companies an opportunity to help their customers buy what they need from platforms and services they use every day. Moreover, mCommerce also makes it easier to plan and execute multi-channel marketing and sales strategies.

3. Great variety of payment options

New mobile payment solutions emerge every year. Businesses can now offer their customers a broad and diverse range of payment options to make the process of buying products and services even smoother.

All of that doesn't mean we're moving our credit cards or cash behind. However, mobile commerce takes advantage of solutions that don't force users to manually enter their details every single time they make a purchase. Examples of such modern mobile payment solutions are PayPal One Touch, Amazon Pay, and Apple Pay.

Types of mobile commerce applications

mCommerce applications cover a broad range of transaction options. However, it's possible to divide them into one of the following types:

- Mobile shopping – this type of mCommerce implementation is most similar to eCommerce, only accessible through a mobile device. We're talking about dedicated apps, optimized websites, or even social media platforms like Facebook or Instagram that allow in-app purchases or linking to online stores.
- Mobile banking – mobile banking is quite similar to online banking. However, you will find that some transactions might be restricted or limited on mobile devices. Mobile banking is a type of implementation that usually involves a dedicated application – though some financial services companies are now experimenting with chatbots or messaging apps to deliver customer service.
- Mobile payments – this type of mobile commerce focuses on the progressive innovation in payment options realized with mobile devices. Today consumers can take advantage of many diverse mobile payment options that go way beyond mobile wallets.

Technology of M – Commerce

1.Location-Based Marketing

In 2016, Entrepreneur reported that 75% of marketers believed that location-based marketing was an important element to their business strategy. While location-based marketing is not a new tactic, there is still a lot of untapped potential, when done right.

The benefits of location-based marketing for businesses are clear: more opportunities to deliver personalized, relevant mobile shopping experiences and interesting ways to connect with shoppers in real-time.

- **Geo-targeting** allows you to detect and determine the geolocation of a user and deliver customized content such as an ad or a push notification to that visitor based on his or her current location.
- **Geo-Fencing** utilizes GPS technology and at its core is similar to Geo-targeting, with the difference being that you can define a geographic boundary or "virtual fence" in which text messages, email alerts or app notifications are triggered whenever a user's mobile phone enters (or exits) that defined space.1-800-Flowers presents one of the more interesting uses

of geo-fencing by targeting mobile phone owners with ads once they are within a certain radius of a store.

- **Beaconing**: Beacons are inexpensive devices that can be placed in physical stores or locations. They transmit Bluetooth Low Energy (BLE) messages to send information to smartphones within about 300 feet–as long as the phone is bluetooth-enabled. You can send targeted offers to shoppers and pull mobile-wielding pedestrians in off the street to drive in-store traffic.

2 Mobile Retargeting

Have you ever seen an ad with an offer that you've viewed recently or received a notification or an email reminding you that you haven't completed a purchase? Consider yourself *remarketed*.

While it can sometimes feel strange to get an advertisement from an online store you just visited, retargeting is a powerful tool that marketers will only improve on in 2017.

Google's mobile path to purchase report revealed that consumers spend 15+ hours a week researching products on their smartphones and that mobile influences their purchase decisions. According to a report from Juniper Research, over two billion mobile phone or tablet users will have made some form of mobile commerce transaction by the end of 2017.
As you see, there is a huge audience to fight for.

Mobile Retargeting is a way to get the attention of these mobile shoppers. It comes down to two different approaches:

- **List-based retargeting** works like this: upload your list of email addresses or phone numbers to your retargeting platform (such as Facebook or Twitter). It will identify the users you wish to serve retargeting ads to. This can work well if you have a large mailing list or subscription service.
- **Pixel-based retargeting** is a more common. Whenever a mobile user visits your site, an unobtrusive retargeting pixel (cookie) is placed in their browser. As they continue to browse the web that cookie communicates with your retargeting platform to serve personalized ads based on the pages on your site that they have viewed.

3 Virtual and Augmented Reality on Mobile

Virtual and Augmented reality is showing up in all of its various forms to provide an immersive and guided shopping experience to mobile users everywhere. It has emerged as one of the top trends to watch.
By integrating VR / AR into the mobile shopping journey, you can provide for an immersive and unique product experience that allows consumers to engage with your brand emotionally.

- **Virtual Reality** creates a digital environment that replaces reality. Users can download an app and connect their mobile devices to a headset or glasses to be able to walk through virtual representation of a store, pick up objects and explore them in 3D. Are you searching for a new car? Volvo introduced a ground-breaking new strategy: you can virtually tour a vehicle with your mobile device. The fashion industry dipped into VR this past summer too.

What is the Scope of Mobile Commerce in India?

In India, the majority of the people, irrespective of their ages, are using a smartphone. Especially during the coronavirus pandemic, the few people who didn't use a smartphone probably started using one. From children in their nappies to grannies in their chairs are using a smartphone for multiple reasons. On average, the age group between 25 and 34 are using these smartphones to shop online. The m-commerce niche is to be completely explored and utilized in its full potential and India is actively working in that regard. Following are a few initiatives taken by the Government of India in order to encourage m-commerce:

1. Unified Payment Interface
2. GST Implementation
3. Mobile Wallets
4. The Digital India Makeover
5. Startup India
6. Skill India

Apart from the above-mentioned initiatives, the Prime Minister of the country has quite supported and encouraged digital transactions with the use of mobile banking and e-banking for cashless transactions. One instance for this initiative is the launch of the BHIM app that facilitates digital transactions directly through the banks using UPI.
When we say m-commerce, here we refer to the transaction of goods and services using mobile devices. There have been evidently great impacts in the m-commerce market with the ever-increasing sales of smartphones, not only in India but across the world. In the past few decades, the development of mobile applications has turned out to become a boon for the m-commerce industry.

If we compare the time spent by an individual on a web browser to the time spent on mobile phones, there is a huge difference and that clearly signifies the dominance of mobile apps in the mobile commerce industry. Researches state that mobile apps can boost sales by over 50% for a regular ecommerce business. Moreover, nearly 49.2% are done via mobile devices. With such whooping usage of mobile apps for ecommerce, India can be foreseen to compete with the developing nations in terms of mobile commerce.

Digital Marketing

What Is Digital Marketing?

Digital marketing is the use of the Internet, mobile devices, social media, search engines, and other channels to reach consumers. Some marketing experts consider digital marketing to be an entirely new endeavor that requires a new way of approaching customers and new ways of understanding how customers behave compared to traditional marketing.

KEY TAKEAWAYS

- Digital marketing is the use of the Internet to reach consumers.
- Digital marketing is a broad field, including attracting customers via email, content marketing, search platforms, social media, and more.

Understanding Digital Marketing

Digital marketing targets a specific segment of the customer base and is interactive. Digital marketing is on the rise and includes search result ads, email ads, and promoted tweets – anything that incorporates marketing with customer feedback or a two-way interaction between the company and customer.

Internet marketing differs from digital marketing. Internet marketing is advertising that is solely on the Internet, whereas digital marketing can take place through mobile devices, on a subway platform, in a video game, or via a smartphone app.

In the parlance of digital marketing, advertisers are commonly referred to as sources, while members of the targeted ads are commonly called receivers. Sources frequently target highly specific, well-defined receivers. For example, after extending the late-night hours of many of its locations, McDonald's needed to get the word out. It targeted shift workers and travelers with digital ads because the company knew that these people made up a large segment of its late-night business. McDonald's encouraged them to download a new Restaurant Finder app, targeting them with ads placed at ATMs and gas stations, as well as on websites that it knew its customers frequented at night.

Digital Marketing Channels

Website Marketing

A website is the centerpiece of all digital marketing activities. Alone, it is a very powerful channel, but it’s also the medium needed to execute a variety of online marketing campaigns. A website should represent a brand, product, and service in a clear and memorable way. It should be fast, mobile-friendly, and easy to use.

Pay-Per-Click (PPC) Advertising

PPC advertising enables marketers to reach Internet users on a number of digital platforms through paid ads. Marketers can set up PPC campaigns on Google, Bing, LinkedIn, Twitter, Pinterest, or Facebook and show their ads to people searching for terms related to the products or services. PPC campaigns can segment users based on their demographic characteristics (such as by age or gender), or even target their particular interests or location. The most popular PPC platforms are Google Ads and Facebook Ads.

Content Marketing

The goal of content marketing is to reach potential customers through the use of content. Content is usually published on a website and then promoted through social media, email marketing, SEO, or even PPC campaigns. The tools of content marketing include blogs, e-books, online courses, info graphics, podcasts, and webinars.

Email Marketing

Email marketing is still one of the most effective digital marketing channels. Many people confuse email marketing with spam email messages, but that’s not what email marketing is all about. Email marketing is the medium to get in touch with your potential customers or the people interested in your brand. Many digital marketers use all other digital marketing channels to add leads to their email lists and then, through email marketing, they create customer acquisition funnels to turn those leads into customers.

Social Media Marketing

The primary goal of a social media marketing campaign is brand awareness and establishing social trust. As you go deeper into social media marketing, you can use it to get leads or even as a direct sales channel.

Affiliate Marketing

Affiliate marketing is one of the oldest forms of marketing, and the Internet has brought new life to this old standby. With affiliate marketing, influencers promote other people's products and get a commission every time a sale is made or a lead is introduced. Many well-known companies like Amazon have affiliate programs that pay out millions of dollars per month to websites that sell their products.

Video Marketing

YouTube has become the second most popular search engine and a lot of users are turning to YouTube before they make a buying decision, to learn something, read a review, or just to relax. There are several video marketing platforms, including Facebook Videos, Instagram, or even Tik-Tok to use to run a video marketing campaign. Companies find the most success with video by integrating it with SEO, content marketing, and broader social media marketing campaigns.

SMS Messaging

Companies and nonprofit organizations also use SMS or text messages to send information about their latest promotions or giving opportunities to willing customers. Political candidates running for office also use SMS message campaigns to spread positive information about their own platforms. As technology has advanced, many text-to-give campaigns also allow customers to directly pay or give via a simple text message.

Digital Marketing Challenges

Digital marketing poses special challenges for its purveyors. Digital channels are proliferating rapidly, and digital marketers have to keep up with how these channels work, how they're used by receivers, and how to use these channels to effectively market their products or services. In addition, it's becoming more difficult to capture receivers' attention, because receivers are increasingly inundated with competing ads. Digital marketers also find it challenging to analyze the vast troves of data they capture and then exploit this information in new marketing efforts.

The challenge of capturing and using data effectively highlights that digital marketing requires an approach to marketing based on a deep understanding of consumer behavior. For example, it may require a company to analyze new forms of consumer behavior, such as using website heatmaps to learn more about the customer journey.