

Cyber Security  
(MCA 207, Credits: 4, Contact  
Hours: L-3 T-0 P-2)

# UNIT 1

# 1. What is Cyber Security???

- Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security.
- Cyber security can be described as the collective methods, technologies, and processes to help protect the confidentiality, integrity, and availability of computer systems, networks and data, against cyber-attacks or unauthorized access. The main purpose of cyber security is to protect all organizational assets from both external and internal threats as well as disruptions caused due to natural disasters.
- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- Mobile Security
- Mobile security refers to protecting both organizational and personal information stored on mobile devices like cell phones, laptops, tablets, etc. from various threats such as unauthorized access, device loss or theft, malware, etc.

- **Identity Management and Data Security:** Identity management includes frameworks, processes, and activities that enables authentication and authorization of **legitimate individuals** to information systems within an organization. Data security involves implementing strong information storage mechanisms that ensure security of data at rest and in transit.
- **Information security** protects the **integrity and privacy of data**, both in storage and in transit.
- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- **End-user education** addresses the **most unpredictable cyber-security factor: people**. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

## 2. SECURITY GOALS

- Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.
- **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.
- **Integrity** – means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example, a hacker may intercept data and modify it before sending it on to the intended recipient. Another example of a failure of integrity is when you try to connect to a website and a malicious attacker between you and the website redirects your traffic to a different website. In this case, the site you are directed to is not genuine.
- **Availability** – means information must be available when needed. Denial of service attack is one of the factor that can hamper the availability of information.

- Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.
- The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security.
- In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

# • Confidentiality

- Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people while making sure that authorized people can access it. It is common for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.
- Sometimes safeguarding data confidentiality involves special training for those privy to sensitive documents. Such training would typically include security risks that could threaten this information. Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training may include strong passwords and password-related best practices and information about social engineering methods, to prevent users from bending data-handling rules with good intentions and potentially disastrous results.
- Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm. Other options include biometric verification and security tokens. In addition, users can take precautions to minimize the number of places where the information appears and the number of times it is actually transmitted to complete a required transaction. Extra measures might be taken in the case of extremely sensitive documents, such as storing only on air gapped computers, disconnected storage devices or, for highly sensitive information, in hard copy form only.
- Some measures to keep your information confidential are:
  - ✓ Encryption
  - ✓ Password
  - ✓ Two-factor authentication
  - ✓ Bio-metric

# • Integrity

- Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.
- Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version control may be used to prevent erroneous changes or accidental deletion by authorized users from becoming a problem. In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash.
- Some data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state.
- Integrity, in the world of information security means maintaining the accuracy, and completeness of data. It is about protecting data from being modified or misused by an unauthorized party. Integrity involves maintaining the consistency and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and precautionary steps must be taken to ensure that data cannot be altered by unauthorized people.
- For example, in a breach of integrity, a hacker may seize data and modify it before sending it on to the intended recipient.
- Measures to maintain the integrity of information include:
  - ✓ Encryption
  - ✓ User Access Controls
  - ✓ Version Control
  - ✓ Backups

- **Availability** is one of the three basic functions of security management that are present in all systems. Availability is the assertion that a computer system is available or accessible by an authorized user whenever it is needed. Systems have high order of availability to ensure that the system operates as expected when needed. Availability provides building of fault tolerance system in the products. There are mainly two threats to availability of the system which are as follows:

- 1. Denial of Service 2. Loss of Data Processing Capabilities
- The above two facets of availability are explained as following below:

#### 1. Denial of Service:

Denial of Service specifies to actions that lock up computing services in a way that the authorized users is unable to use the system whenever needed.

- In computing, a **denial-of-service attack (DoS attack)** is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

#### 2. Loss of Data Processing Capabilities:

The loss of data processing capabilities are generally caused by the natural disasters or human actions is perhaps more common.

- Contingency planning is the measure to counter such type of losses, which helps in minimizing the time for that a data processing capability remains unavailable. Contingency planning provides an alternative means of processing which involves business resumption planning, alternative site processing or simply disaster recovery planning thereby ensures data availability.

- Your information is more **vulnerable to availability threats** than the other two components in the CIA model. Making regular off-site backups can limit the damage caused to the hard drives by natural disasters. **Information only has value if the right people can access it at the right times.**
- Measures to mitigate threats to availability include:
  - ✓ Off-site backups (**Off-site backup** is a method of **backing up data to a remote server** or to media that is transported **off site**. The two most common forms of **off-site backup** are cloud **backup** and tape **backup**. During cloud **backup**, also referred to as online **backup**, a copy of the data is sent over a network to an **off-site** server.)
  - ✓ Disaster recovery
  - ✓ Redundancy
  - ✓ Proper monitoring
  - ✓ Environmental controls
  - ✓ Virtualization (**Virtualization** is the process of **creating a software-based, or virtual, representation of something**, such as virtual applications, servers, storage and networks. It is the single most effective way to reduce IT expenses while boosting efficiency and agility for all size businesses.)
  - ✓ Server clustering (**Server clustering** refers to a **group of servers working together on one system to provide users with higher availability**. These clusters are used to reduce downtime and outages by allowing another server to take over in the event of an outage. )
  - ✓ Continuity of operations planning

# 3. Security Services

- **Authentication:** assures recipient that the **message is from the source that it claims to be from.**
- **Access Control:** controls who can have **access to resource under what condition**
- **Availability:** available to authorized entities for 24/7.
- **Confidentiality:** information is not made available to unauthorized individual
- **Integrity:** assurance that the message is unaltered
- **Non-Repudiation:** protection against denial of sending or receiving in the communication



## AUTHENTICATION

- The assurance that the communicating entity is the one that it claims to be.

### Peer Entity Authentication

- Used in association with a logical connection to provide confidence in the identity of the entities connected.

### Data Origin Authentication

- In a connectionless transfer, provides assurance that the source of received data is as claimed.

## ACCESS CONTROL

- The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

## DATA CONFIDENTIALITY

- The protection of data from unauthorized disclosure.

### Connection Confidentiality

- The protection of all user data on a connection.

### Connectionless Confidentiality

- The protection of all user data in a single data block

### Selective-Field Confidentiality

- The confidentiality of selected fields within the user data on a connection or in a single data block.

### Traffic Flow Confidentiality

- The protection of the information that might be derived from observation of traffic flows.

## DATA INTEGRITY

- The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

### **Connection Integrity with Recovery**

- Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

### **Connection Integrity without Recovery**

- As above, but provides only detection without recovery.

### **Selective-Field Connection Integrity**

- Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

### **Connectionless Integrity**

- Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

### **Selective-Field Connectionless Integrity**

- Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

## NONREPUDIATION

- Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

### Nonrepudiation, Origin

- Proof that the message was sent by the specified party.

### Nonrepudiation, Destination

- Proof that the message was received by the specified party.

- **Confidentiality** means that data, objects and resources are protected from unauthorized viewing and other access.
- **Integrity** means that data is protected from unauthorized changes to ensure that it is reliable and correct.
- **Availability** means that authorized users have access to the systems and the resources they need.

- 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 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. Three categories in which someone may be authenticated are: something the user knows, something the user is, and something the user has.

**Accountability** – means that it should be possible to trace actions of an entity uniquely to that entity. For example : 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.

# Vulnerabilities in Information Security

**Vulnerabilities** are weaknesses in a system that gives threats the opportunity to compromise assets. All systems have vulnerabilities. Even though the technologies are improving but the number of vulnerabilities are increasing such as tens of millions of lines of code, many developers, human weaknesses, etc. Vulnerabilities mostly happened because of **Hardware, Software, Network** and **Procedural vulnerabilities**.

## 1. Hardware Vulnerability:

A hardware vulnerability is a weakness which can be used to attack the system hardware through physically or remotely.

For examples:

- Old version of systems or devices
- Unprotected storage
- Unencrypted devices, etc.

## 2. Software Vulnerability:

A software error happen in development or configuration such as the execution of it can violate the security policy. For examples:

- Lack of input validation
- Unverified uploads
- Cross-site scripting
- Unencrypted data, etc.

## 3. Network Vulnerability:

A weakness happen in network which can be hardware or software.

For examples:

- Unprotected communication
- Malware or malicious software (e.g.:Viruses, Keyloggers, Worms, etc)
- Social engineering attacks
- Misconfigured firewalls

## 4. Procedural Vulnerability:

A weakness happen in an organization operational methods.

For examples:

- Password procedure – Password should follow the standard password policy.
- Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

- How cybersecurity vulnerability is different from a cybersecurity threat?
- Vulnerabilities differ from cyber threats in that they are **not introduced on a system, they are there from the beginning.**
- Very rarely are cyber vulnerabilities created as a result of actions taken by cybercriminals, instead, they are usually caused by operating system flaws or network misconfigurations.
- Conversely, **cyber** threats are introduced as a result of an outside event such as an employee downloading a virus or a **social engineering attack.**

- **Common types of cybersecurity vulnerabilities**

- When building a vulnerability management program, there are several key cybersecurity vulnerabilities that you must be aware of. Below are six of the most common types of cybersecurity vulnerabilities:

- **1. System misconfigurations**

- System misconfigurations occur as a result of network assets having vulnerable settings or disparate security controls.

- A common tactic cybercriminals use is to probe networks for system misconfigurations and gaps that can be exploited.

- **2. Out of date or unpatched software**

- Unpatched vulnerabilities can be exploited by cybercriminals to carry out attacks and steal valuable data.

- Similar to system misconfigurations, cyber adversaries will probe networks looking for unpatched systems they can compromise.

- To limit this risk, It is important to establish a **patch management schedule** so that all new system patches are implemented as soon as they are released.

- **3. Missing or weak authorization credentials**

- A common tactic attackers employ is to brute force their way into a network by guessing employee credentials.

- It is important to educate employees on cybersecurity best practices so that their login information cannot be easily exploited to gain access to a network.

- **4. Malicious insider threats**
- Whether unknowingly or with malicious intent, employees who have access to critical systems can share information that allows cybercriminals to breach a network.
- **Insider threats** can be difficult to track since all actions taken by employees will appear legitimate and therefore raise little to no red flags.
- To help combat these threats, consider investing in network access control solutions, and segment your network based on employee seniority and expertise.
- **5. Missing or poor data encryption**
- Networks with missing or poor encryption allow attackers to intercept communication between systems, leading to a breach.
- When poorly or unencrypted information is interrupted, cyber adversaries are able to extract critical information and inject false information onto a server.
- **6. Zero-day vulnerabilities**
- Zero-day threats are specific software vulnerabilities that are known to the attacker but have not yet been identified by an organization.
- This means that there is no available fix since the vulnerability has not yet been reported to the system vendor.
- These are extremely dangerous as there is no way to defend against them until after the attack has been carried out.
- It is important to remain diligent and **continuously monitor** your systems for vulnerabilities in order to limit the likelihood of a zero-day attack.

# 5. Sources of Security Threats

- Primary sources of threats are employees/insiders, malicious hackers, natural disasters, foreign adversaries, and hostile attacks.
- In several cases, the areas for sources of threats may overlap. For example, hostile attacks may be performed by foreign adversaries or a disgruntled employee

- When you identify a cyber threat, it's important to understand who is the threat actor, as well as their **tactics, techniques and procedures (TTP)** (behaviors, methods, tools and strategies that cyber attackers used to plan and execute cyber attacks on networks). Common sources of cyber threats include:
  - **State-sponsored**—cyberattacks by countries can disrupt communications, military activities, or other services that citizens use daily.
  - **Terrorists**—terrorists may attack government or military targets, but at times may also target civilian websites to disrupt and cause lasting damage.
  - **Industrial spies**—organized crime and international corporate spies carry out industrial espionage and monetary theft. Their primary motive is financial.
  - **Organized crime groups**—criminal groups infiltrate systems for monetary gain. Organized crime groups use phishing, spam, and malware to carry out identity theft and online fraud.
  - **Hackers**—there is a large global population of hackers, ranging from beginner “script kiddies” or those leveraging ready made threat toolkits, to sophisticated operators who can develop new types of threats and avoid organizational defenses.
  - **Hacktivists**—hacktivists are hackers who penetrate or disrupt systems for political or ideological reasons rather than financial gain.
- **Malicious insider**—insiders represent a very serious threat, as they have existing access to corporate systems and knowledge of target systems and sensitive data. Insider threats can be devastating and very difficult to detect.
- **Cyber espionage**—is a form of cyberattack that steals classified, or sensitive intellectual data to gain an advantage over a competitive company or government entity.

# 6. Target assets

- Attack Target refers to the victim of Cyber attack incident at which cyber threat actors aim to achieve a specific objective which involves an intelligent planning.
- 
- **Industrial Applications:** An Industry as a greatest sector plays an important role in the economic development of a nation as it provides employment to the people. Industries present a different type of value which includes services and products as deliverables. Some examples of Industrial Applications are Education, Healthcare, Finance, Energy, Insurance, Petroleum, Media, Automotive, Service, Production and so on.

- **Operating System Applications:** An Operating System is a primary software that controls and coordinates the Hardware resources and handles the other programs to run effectively. Some commonly used Operating System Applications are Microsoft's Windows, Mac OS, Linux etc.
- 
- **Mobile Operating System Applications:** Mobile Operating System is a software that is specifically crafted (slimmed down version) to run on smartphones, tablet PCs and other mobile devices. The platform allows other applications to run over it. Some popular Mobile Operating System Applications are Google's Android OS, Apple's iOS, Symbian, Windows etc.
- 
- **Web Browser Applications:** Web Browser is a Software application which allows display and access to the websites. A variety of Web browsers are available at present with different features and crafted to run on different Operating System. Some popular web browsers used for exploring the World Wide Web are Google Chrome, Mozilla Firefox, Internet Explorer, Apple Safari, Opera etc.

- **Social Network Applications:** Social Network refers to a virtual community, where on the online platform people make connections with others based on common interests. People use it to build relationships for social and business purposes where they can talk, share ideas and make new connections. Being a largest and most influential component in the online world people connect to each other through some popular platforms such as Facebook, Twitter, Instagram, YouTube, LinkedIn, MySpace etc.
- 
- **Network Applications:** A Network consists of set of interconnected devices aiming resource sharing, files exchange and communication. Network applications follow Client-Server architecture where client such as a portable device runs a Web Client program like Safari or Google Chrome and Server such as data center runs a Web Server program such as Apache, Google, nginx information server. Network applications can be of two kinds one which offers service and stores information while another one only offers service.

# 7. Insider threats

- An insider threat is a security risk that originates within the targeted organization.
- This doesn't mean that the actor must be a current employee or officer in the organization.
- They could be a consultant, former employee, business partner, or board member.
- Anyone who has insider knowledge and/or access to the organization's confidential data, IT, or network resources is a potential insider threat.

# Types of Insider Threats

- The two main types of insider threats are turncloaks and pawns, which are malicious insiders and unwilling participants, respectively.

## Turncloaks

- A turncloak is an **insider who is maliciously stealing data**. In most cases, it's an employee or contractor – someone who is supposed to be on the network and **has legitimate credentials but is abusing their access for fun or profit**. We've seen all sorts of motives that drive this type of behavior: some as sinister as selling secrets to foreign governments, others as simple as taking a few documents to a competitor upon resignation.

## Pawns

- A pawn is just a **normal employee** – a **do-gooder who makes a mistake that is exploited by a bad actor or otherwise leads to data loss or compromise**. Whether it's a lost laptop, mistakenly emailing a sensitive document to the wrong person, or executing a malicious Word macro, the pawn is an **unintentional participant in a security incident**

- How to Detect an Insider Threat

## Insider Threat Indicators

### Digital

- Obtaining **large amounts of data**
- Sharing data with **outsiders**
- Seeking or saving **sensitive data**
- Requests for access to **sensitive data** not related with their job function
- Acting outside of their unique **behavioral profile**
- Make use of **unauthorized storage** devices

### Behavioral

- Attempting to **bypass security**
- Frequently in the office during **off-hours**
- Displaying **disgruntled behavior**
- Violating any **corporate policies**, even those unrelated to security
- Discussing **resignation** or looking for new career opportunities
- Acting **withdrawn** or unusual

## Insider Threat Examples

- Here are a few recent examples of insider threats from the news.
- Tesla: A malicious insider sabotaged systems and sent proprietary data to third parties.
- Facebook: A security engineer abused his access to stalk women.
- Coca-Cola: A malicious insider stole a hard drive full of personnel data.
- Suntrust Bank: A malicious insider stole personal data, including account information, for 1.5 million customers to provide to a criminal organization.

- Fighting Insider Threats

## Insider Threat Defense Plan



- Monitor activity, files and emails on your core data sources
- Identify and discover where your sensitive files live
- Determine who has access to that data and who should
- Maintain a least privilege model through your infrastructure
- Apply security analytics to alert on abnormal behaviors
- Train your employees to adopt a data security mindset

**VARONIS**

# 8. Intruders and Hackers

- The hacker is a ‘computer criminal’ to hack or theft or steals the organization information. The hacker is someone who is mastermind in art of programming to point that he or she simply sit down and hack in a program that works.
- But the intruders are basically who violate networks and information systems. The intruders are aware of weakness in system and networks through their continuously network scanning programs

- **What Hackers means and their motives:**
- The most common usage of "hacker" is to breakdown computer security without authorization or indeed, usually through a computer network or the internet for terrorism, vandalism, credit card fraud, identity theft, intellectual property theft, and many other forms of crime. This can mean taking control of a remote computer through a network, or software cracking. These hackers are called **cracker** or **black-hat hacker** or simply **"criminal"**. But the one who help the government or organization to trace the intrusions of black-hat hacker and break the network or information by criminals called as **"Ethical Hacker"**.
- The modern day hackers have enormously more power available through the internet access, and they are easily breaking the network access by using user-friendly hacking tools. The hacker motives are classified in three broad categories as:
  - **Recreation:** Those who hacks in to network for **'just fun'** or to prove their technical powers.
  - **Remuneration:** The people who hack the network for **personal gain** like attempt to transfer funds in their own bank accounts, **'hackers for hire'** as to break the network on paid by others basis.
  - **Revenge:** Dissatisfied customers, disgruntled former employees, angry competitors comes in this category

- **What intruder's means and their motives:**
- A network intruder are gaining access through unauthorised access to networking devices through physical, system and remote attempts. The intruder uses some outdated exploits that are ineffective against upto-date patched hosts. The intruders are of two types. One is external intruder is an unauthorized user of the system or network, and the internal intruder is an authorized user who has access to certain areas of the internal system or network.
- The intruders are basically three forms one 'masquerade user' who is authorized user to use computer, second 'misfeasor' legitimate user who misuse his/her privileges and third 'clandestine user' who seizes his supervisory control of the system and uses it to suppress audit information.
- The intruder's main motives are
- ✓ To perform network scanning to find out vulnerable hosts in the network.
- ✓ To install an FTP server for distributing illegal content on network (ex. pirated software or movies)
- ✓ To use the host as a spam relay to continuous flood in the network
- ✓ To establish a web server (non-privileged port) to be used for some phishing scam.

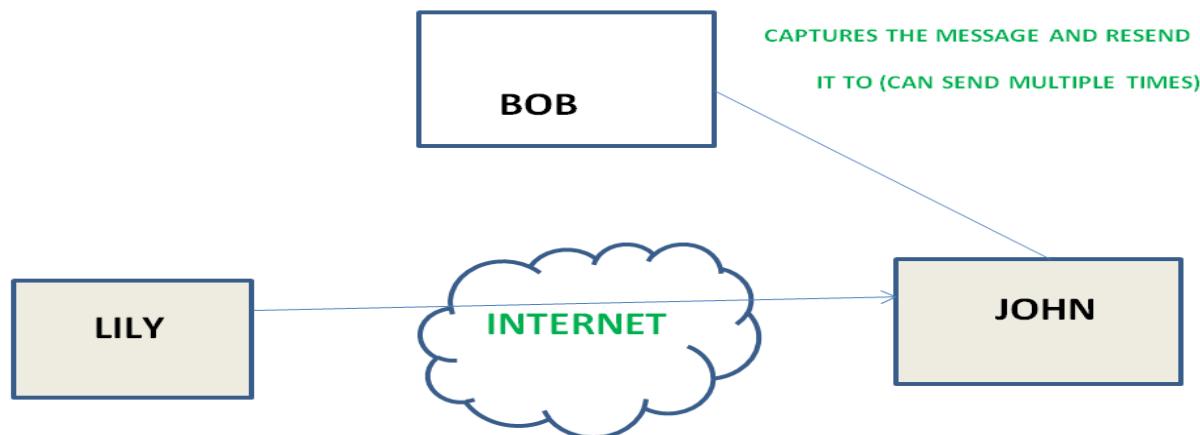
- **Tools used by Hackers & Intruders:** There are several common tools used by computer criminals to penetrate network as:
  - x Trojan horse- These are malicious programs or legitimate software is to be used set up a back door in a computer system so that the criminal can gain access.
  - x Virus- A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents.
  - x Worm - The worm is like a virus and also a self replicating program. The difference between a virus and a worm is that a worm does not attach itself to other code.
  - x Vulnerability scanner – This tool is used by hackers & intruders for quickly check computers on a network for known weaknesses. Hackers also use port scanners. This check to see which ports on a specified computer are "open" or available to access the computer.
  - x Sniffer – This is an application that captures password and other data in transit either within the computer or over the network.
  - x Exploit – This is an application to takes advantage of a known weakness.
  - x Social engineering – Through this to obtain some form of information.
  - x Root kit - This tool is for hiding the fact that a computer's security has been compromised

# 9. Active and Passive attacks

- **Active attacks:** An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following:
  - **Masquerade**  
Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks.
  - **Modification of messages**  
It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.

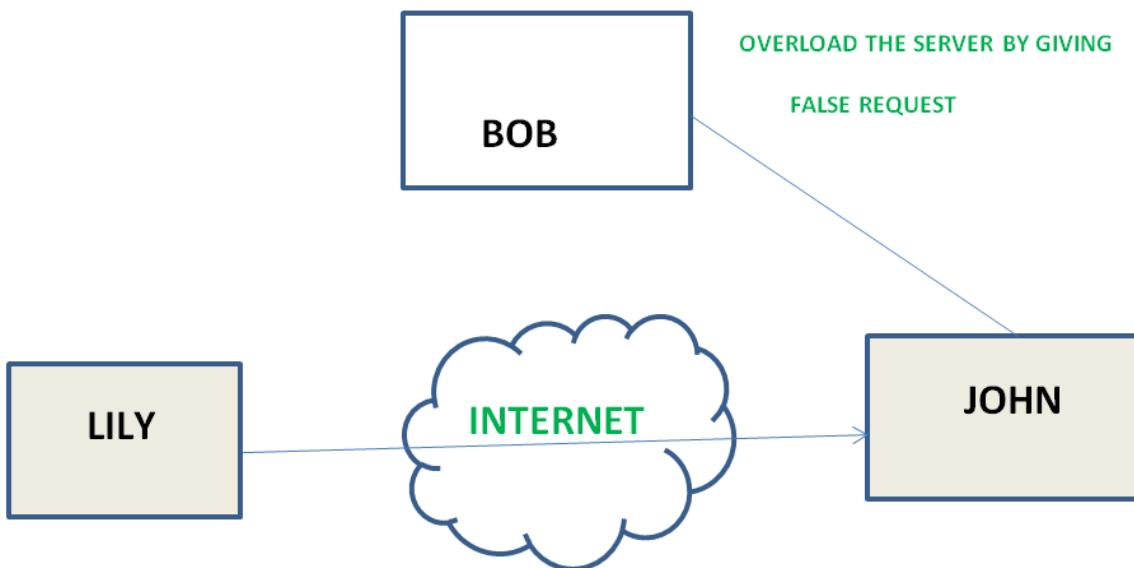


- **Repudiation –**  
This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. For example, customer ask his Bank “To transfer an amount to someone” and later on the sender(customer) deny that he had made such a request. This is repudiation.
- **Replay –**  
It involves the passive capture of a message and its subsequent transmission to produce an authorized effect.

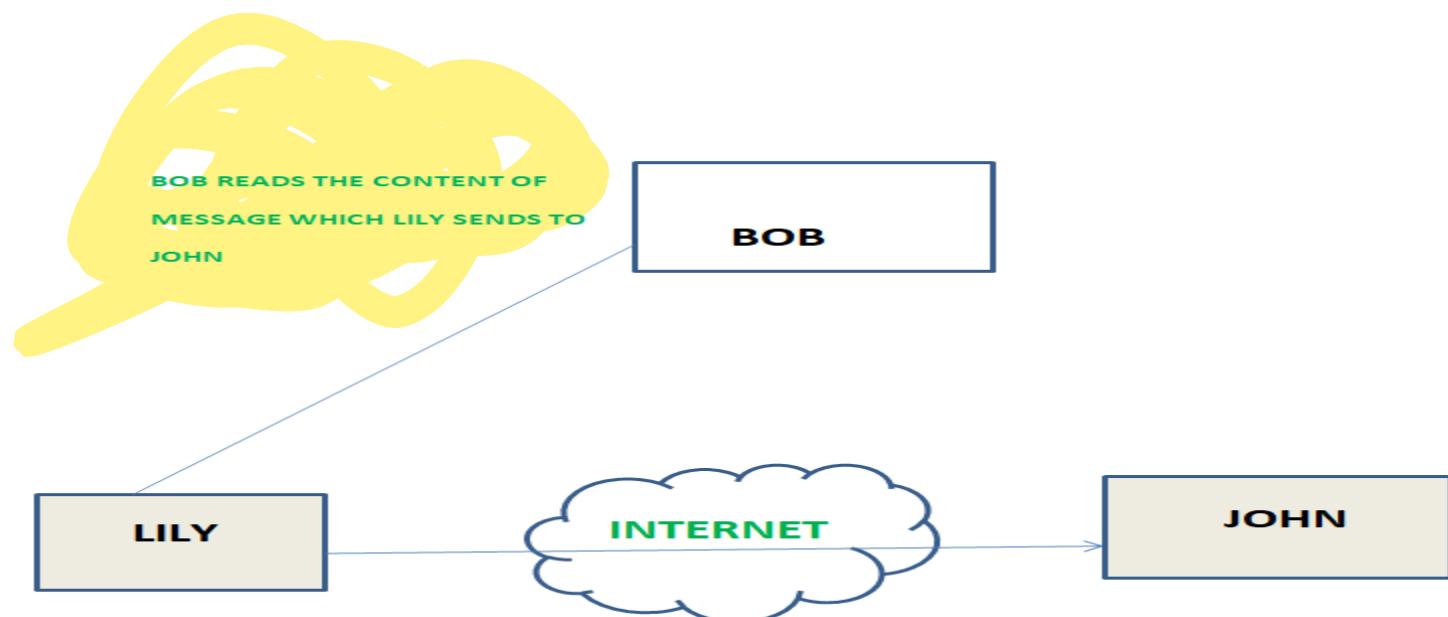


- **Denial of Service** –

It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it by messages so as to degrade performance.



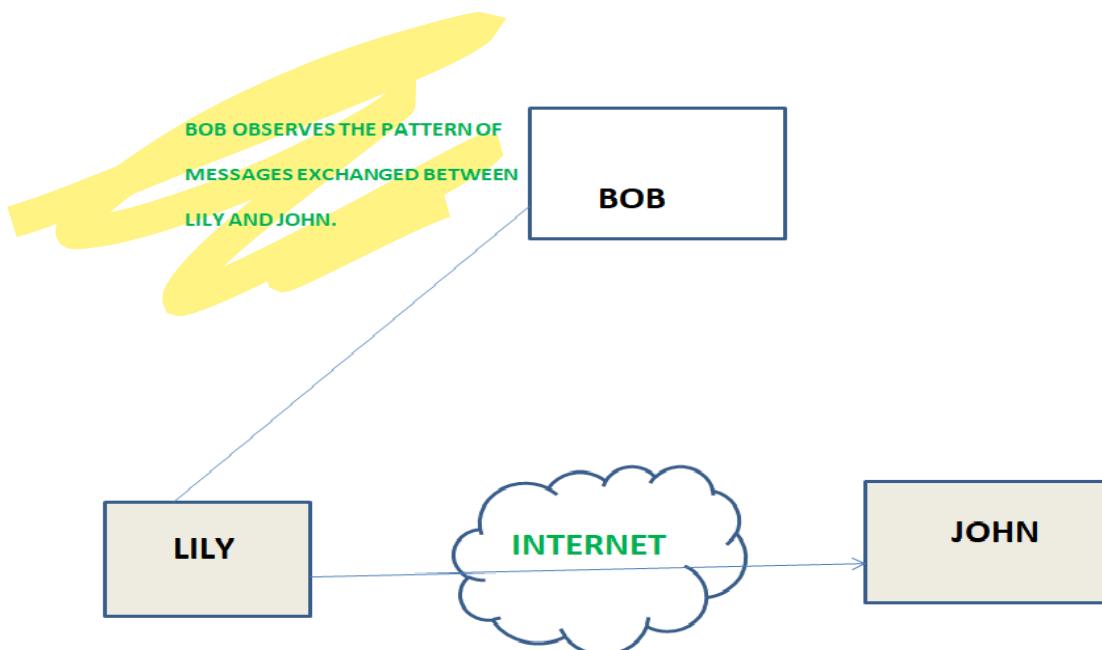
- **Passive attacks:** A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:
- **The release of message content –** Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



- **Traffic analysis –**

Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.

The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.



# 10. Malware/Malicious Software

- The term **malware** is a contraction of *malicious software*. Put simply, malware is any piece of software that was written with the intent of damaging devices, stealing data, and generally causing a mess. Viruses, Trojans, spyware, and ransomware are among the **different kinds of malware**.
- Malware is often created by teams of hackers: usually, they're just looking to make money, either by spreading the malware themselves or selling it to the highest bidder on the Dark Web (the portion of the Internet that is intentionally hidden from search engines, uses masked IP addresses, and is accessible only with a special web browser).
- However, there can be other reasons for creating malware too — it can be used as a tool for protest, a way to test security, or even as weapons of war between governments.
- Malware is the collective name for a number of malicious software variants, including viruses, ransomware and spyware. Shorthand for malicious software, malware typically consists of code developed by cyberattackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network.
- Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware.
- Though varied in type and capabilities, malware usually has one of the following objectives:
  - ❖ Provide remote control for an attacker to use an infected machine.
  - ❖ Send spam from the infected machine to unsuspecting targets.
  - ❖ Investigate the infected user's local network.
  - ❖ Steal sensitive data.

- **How to protect against malware**
- When it comes to malware, prevention is better than a cure. Fortunately, there are some common sense, easy behaviors that minimize your chances of running into any nasty software.
- **Don't trust strangers online!** “Social engineering”, which can include strange emails, abrupt alerts, fake profiles, and curiosity-tickling offers, are the #1 method of delivering malware. If you don’t know exactly what it is, don’t click on it.
- **Double-check your downloads!** From pirating sites to official storefronts, malware is often lurking just around the corner. So before downloading, always double-check that the provider is trustworthy by carefully reading reviews and comments.
- **Get an ad-blocker!** Malvertising – where hackers use infected banners or pop-up ads to infect your device – is on the rise. You can’t know which ads are bad: so it’s safer to just block them all with a reliable ad-blocker.
- **Careful where you browse!** Malware can be found anywhere, but it’s most common in websites with poor backend security, like small, local websites. If you stick to large, reputable sites, you severely reduce your risk of encountering malware.

# 11. VIRUS

- Programs that copy themselves throughout a computer or network.
- Viruses piggyback on existing programs and can only be activated when a user opens the program.
- At their worst, viruses can corrupt or delete data, use the user's email to spread, or erase everything on a hard disk.

- a computer virus is “malware attached to another program (such as a document), which can replicate and spread after an initial execution on a target system where human interaction is required. Many viruses are harmful and can destroy data, slow down system resources, and log keystrokes.”
- Most computer viruses target systems running Microsoft Windows. Macs, on the other hand, enjoy a reputation as virus-proof super machines.
- In reality, Macs are not inherently safer. There are more Windows users in the world than Mac users and cybercriminals simply choose to write viruses for the operating system (OS) with the largest amount of potential victims.

- The easiest way to differentiate computer viruses from other forms of malware is to think about viruses in biological terms.
- Take the flu virus, for example. The flu requires some kind of interaction between two people—like a hand shake, a kiss, or touching something an infected person touched. Once the flu virus gets inside a person's system it attaches to healthy human cells, using those cells to create more viral cells.

A computer virus works in much the same way:

- A computer virus requires a host program.
- A computer virus requires user action to transmit from one system to another.
- A computer virus attaches bits of its own malicious code to other files or replaces files outright with copies of itself.
- It's that second virus trait that tends to confuse people. Viruses can't spread without some sort of action from a user, like opening up an infected Word document. Worms, on the other hand, are able to spread across systems and networks on their own, making them much more prevalent and dangerous

## **How does a computer virus find me?**

Even if you're careful, you can pick up computer viruses through normal Web activities like:

- Sharing music, files, or photos with other users
- Visiting an infected website
- Opening [spam email](#) or an email attachment
- Downloading free games, toolbars, media players and other system utilities
- Installing mainstream software applications without thoroughly reading license agreements

## **What does a computer virus do?**

- Some computer viruses are programmed to harm your computer by damaging programs, deleting files, or reformatting the hard drive.
- Others simply replicate themselves or flood a network with traffic, making it impossible to perform any internet activity.
- Even less harmful computer viruses can significantly disrupt your system's performance, sapping computer memory and causing frequent computer crashes.

## **What are the symptoms of a computer virus?**

Your computer may be infected if you recognize any of these [malware symptoms](#):

- Slow computer performance
- Erratic computer behavior
- Unexplained data loss
- Frequent computer crashes

## How to protect against computer viruses

Take these steps to safeguard your PC with the best computer virus protection:

- ✓ Use antivirus protection and a firewall
- ✓ Get antispyware software
- ✓ Always keep your antivirus protection and antispyware software up-to-date
- ✓ Update your operating system regularly
- ✓ Increase your browser security settings
- ✓ Avoid questionable Web sites
- ✓ Only download software from sites you trust.
- ✓ Carefully evaluate free software and file-sharing applications before downloading them.
- ✓ Don't open messages from unknown senders
- ✓ Immediately delete messages you suspect to be spam

# 12. Worms

- **Worms** are a self-replicating type of malware (and a type of virus) that enter networks by exploiting vulnerabilities, moving quickly from one computer to another.
- Because of this, worms can propagate themselves and spread very quickly – not only locally, but have the potential to disrupt systems worldwide.
- Unlike a typical virus, worms don't attach to a file or program.
- Instead, they slither and enter computers through a vulnerability in the network, self-replicating and spreading before you're able to remove the worm.
- But by then, they'll already have consumed all the bandwidth of the network, interrupting and arresting large network and web servers.

- Definition: A computer **worm** is a malicious, self-replicating software program (popularly termed as 'malware') which affects the functions of software and hardware programs.

Description: It fits the description of a computer virus in many ways. For example, it can also self-replicate itself and spread across networks. That is why worms are often referred to as viruses also.

- But computer worms are different from computer viruses in certain aspects.
- First, unlike viruses which need to cling on to files (host files) before they can diffuse themselves inside a computer, **worms exist as separate entities or standalone software.**
- **They do not need host files or programs.**
- Secondly, unlike viruses, **worms do not alter files but reside in active memory and duplicate themselves.**
- Worms use parts of the operating system that are automatic and usually invisible to the user.
- Their existence in the system becomes apparent only when their uncontrolled replication consumes system resources, slowing or halting other tasks in the process.
- In order to spread, **worms either exploit the vulnerability of the target system or use some kind of social engineering method to trick users into executing them.**
- Once they enter a system, they take advantage of file-transport or information-transport features in the system that allows them to travel unaided.
- A computer worm called '**Stuxnet worm**' turned heads the world over recently when it attacked the **nuclear facilities of Iran**. This worm reportedly destroyed roughly a fifth of Iran's nuclear centrifuges by causing them to spin out of control by increasing the pressure on the spinning centrifuges, while displaying that everything was under control. It managed this feat by replaying the plant's protection system values in the control room while the attack was happening.

## What damage can computer worms cause?

- It depends on the type of computer worm and the desires of its creator. Some worms are used to spread other types of malware for cybercrime like corporate espionage and others are used to highlight particular security vulnerabilities but do no real damage (minus network congestion).
- Many of the first computer worms were proofs of concept designed to do nothing more than infect computers and reproduce themselves in the background. Often the only way to identify an infection was when a worm made too many copies of itself and caused the system to slow.
- But with time, worms are becoming a means to an end, often carrying a payload that aims to steal sensitive data or cause a data breach.
- It's common to use the worm to gain initial access to a system and then use privilege escalation to gain further access to a system.

# How do computer worms spread?

## 1. Email

One of the most common ways for computer worms to spread is via email spam. In years gone by, worms could hide in the main text of an email, but as modern email clients caught on and began blocking direct embedding circa 2010, the risk for this type of attack is fairly low.

While embedded worms may be things of the past, email attachments remain popular hiding spots for worms. What may appear to be a benign work document or personal photo can, in fact, be hiding malicious code, waiting to be released when you click a link or open said attachment. Once a machine has been infected, the worm may replicate itself by emailing itself to everyone in your address book or automatically replying to emails in your inbox.

## 2. Operating system vulnerabilities

Every operating system has its vulnerabilities (yes, [even macOS](#)) and some worms are specifically coded to take advantage of these weak points. Perhaps the most infamous example is [Conficker](#), a worm first identified in 2008 which exploited a vulnerability in a network service present in many versions of Windows, including Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 Beta and Windows 7 Beta. At its peak, Conficker infected as many as 15 million computers.

## 3. Instant messaging

Worms can take on similarly deceptive forms in instant messaging software and take advantage of users who are probably not on high alert when using such services.

In the past, instant messaging software such as mIRC, MSN Messenger, Yahoo IM and ICQ proved to be exceptionally fertile breeding grounds for worms. In today's digital landscape, modern chat systems are just as vulnerable, with Facebook Messenger a common infection point for worms such as Dorkbot, which spreads via an executable file disguised as a JPG image.

- **4. Smartphones**
- Globally, there were about 2.8 billion active smartphones being used at the end of 2016, [according to data](#) collated by market intelligence firm Newzoo. With these figures in mind, it should come as little surprise that worm creators are increasingly turning their attention to mobile devices.

# 13. Trojans

- A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.
- A Trojan acts like a bona fide application or file to trick you. It seeks to deceive you into loading and executing the malware on your device. Once installed, a Trojan can perform the action it was designed for.
- A Trojan is sometimes called a Trojan virus or a Trojan horse virus, but that's a misnomer. Viruses can execute and replicate themselves. A Trojan cannot. A user has to execute Trojans. Even so, Trojan malware and Trojan virus are often used interchangeably.
- It is a type of computer software that is camouflaged in the form of regular software such as utilities, games and sometimes even antivirus programs. Once it runs on the computer, it causes problems like killing background system processes, deleting hard drive data and corrupting file allocation systems.
- A Trojan Horse or Trojan is a malware type which covertly attaches itself to a benign application to perform atrocious actions after activation such as spying on you, gathering data, creating backdoor access, disrupting performance etc. For sending the gathered information Trojan connects themselves to the remote server also known as Command and Control server.
- Trojans spread themselves through user interaction. No self replication and no self reproduction by infecting files are the properties of Trojan.
- Trojans gain entry to the system through malicious email attachments, social engineering, and execution of malicious files and so on.
- Trojans can take form of a backdoor which creates a channel to the remote server.

## Some of the common actions that Trojans take are:

- **Creating backdoors:** Trojans typically make changes to your security system so that other malware or even a hacker can get in. This is usually the first step in creating a botnet.
- **Spying:** Some Trojans are essentially spyware designed to wait until you access your online accounts or enter your credit card details, and then send your passwords and other data back to their master.
- **Turning your computer into a zombie:** Sometimes, a hacker isn't interested in you, but just wants to use your computer as a slave in a network under their control.
- **Sending costly SMS messages:** Even smartphones get Trojans, and a common way for criminals to make money is by making your phone send costly SMS messages to premium numbers.

## What does a Trojan look like?

- Well, that's just it: Trojans can look like just about anything. The computer game you downloaded from a strange website. The "free" MP3 by that band you secretly like. Even an advertisement might try to install something on your computer.
- Some Trojans are specifically designed to trick you into using them. They can use misleading language or try to convince you they are a legitimate app. This is why it's so important to watch out for unsafe websites and never download things carelessly.

# 14. Ransomware

- **Ransomware** is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again. This class of malware is a criminal moneymaking scheme that can be installed through deceptive links in an email message, instant message or website.
- There are a number of vectors ransomware can take to access a computer. One of the most common delivery systems is phishing spam — attachments that come to the victim in an email, masquerading as a file they should trust. Once they're downloaded and opened, they can take over the victim's computer, especially if they have built-in social engineering tools that trick users into allowing administrative access.
- There are several things the malware might do once it's taken over the victim's computer, but by far the most common action is to encrypt some or all of the user's files. If you want the technical details, the Infosec Institute has a great in-depth look at how several flavors of ransomware encrypt files.
- But the most important thing to know is that at the end of the process, the files cannot be decrypted without a mathematical key known only by the attacker. The user is presented with a message explaining that their files are now inaccessible and will only be decrypted if the victim sends an untraceable Bitcoin payment (Digital money that's instant, private, and free from bank fees OR **Bitcoin** is a digital or virtual currency created in 2009 that uses peer-to-peer technology to facilitate instant payments.) to the attacker.

# • Types of ransomware

- Ransomware attacks can be deployed in different forms. Some variants may be more harmful than others, but they all have one thing in common: a ransom. Here are seven common types of ransomware.
- **Cryptomalware**. This form of ransomware can cause a lot of damage because it encrypts things like your files, folders, and hard-drives. One of the most familiar examples is the destructive 2017 WannaCry ransomware attack. It targeted thousands of computer systems around the world that were running Windows OS and spread itself within corporate networks globally. Victims were asked to pay ransom in Bitcoin to retrieve their data.
- **Lockers**. Locker-ransomware is known for infecting your operating system to completely lock you out of your computer or devices, making it impossible to access any of your files or applications. This type of ransomware is most often Android-based.
- **Scareware**. Scareware is fake software that acts like an antivirus or a cleaning tool. Scareware often claims to have found issues on your computer, demanding money to resolve the problems. Some types of scareware lock your computer. Others flood your screen with annoying alerts and pop-up messages.
- **Doxware**. Commonly referred to as leakware or extortionware, doxware threatens to publish your stolen information online if you don't pay the ransom. As more people store sensitive files and personal photos on their computers, it's understandable that some people panic and pay the ransom when their files have been hijacked.
- **Mac ransomware**. Mac operating systems were infiltrated by their first ransomware in 2016. Known as KeRanger, this malicious software infected Apple user systems through an app called Transmission, which was able to encrypt its victims' files after being launched.
- **Ransomware on mobile devices**. Ransomware began infiltrating mobile devices on a larger scale in 2014. What happens? Mobile ransomware often is delivered via a malicious app, which leaves a message on your device that says it has been locked due to illegal activity.

## • Who are the targets of ransomware attacks?

- Ransomware can spread across the Internet without specific targets. But the nature of this file-encrypting malware means that cybercriminals also are able to choose their targets. This targeting ability enables cybercriminals to go after those who can — and are more likely to — pay larger ransoms.
- Here are four target groups and how each may be impacted.
- **Groups that are perceived as having smaller security teams.** Universities fall into this category because they often have less security along with a high level of file-sharing.
- **Organizations that can and will pay quickly.** Government agencies, banks, medical facilities, and similar groups constitute this group, because they need immediate access to their files — and may be willing to pay quickly to get them.
- **Firms that hold sensitive data.** Law firms and similar organizations may be targeted, because cybercriminals bank on the legal controversies that could ensue if the data being held for ransom is leaked.
- **Businesses in the Western markets.** Cybercriminals go for the bigger payouts, which means targeting corporate entities. Part of this involves focusing on the United Kingdom, the United States, and Canada due to greater wealth and personal-computer use.

## Dos and don'ts of ransomware

- Ransomware is a profitable market for cybercriminals and can be difficult to stop. Prevention is the most important aspect of protecting your personal data. To deter cybercriminals and help protect yourself from a ransomware attack, keep in mind these eight dos and don'ts.
- 1. **Do use security software.** To help protect your data, install and use a trusted security suite that offers more than just antivirus features. For instance, [Norton 360 With LifeLock Select](#) can help detect and protect against threats to your identity and your devices, including your mobile phones.
- 2. **Do keep your security software up to date.** New ransomware variants continue to appear, so having up-to-date internet security software will help protect you against cyberattacks.
- 3. **Do update your operating system and other software.** Software updates frequently include patches for newly discovered security vulnerabilities that could be exploited by ransomware attackers.
- 4. **Don't automatically open email attachments.** Email is one of the main methods for delivering ransomware. Avoid opening emails and attachments from unfamiliar or untrusted sources. Phishing spam in particular can fool you into clicking on a legitimate-looking link in an email that actually contains malicious code. The malware then prevents you from accessing your data, holds that data hostage, and demands ransom.
- 5. **Do be wary of any email attachment that advises you to enable macros to view its content.** Once enabled, macro malware can infect multiple files. Unless you are absolutely sure the email is genuine and from a trusted source, delete the email.
- 6. **Do back up important data to an external hard drive.** Attackers can gain leverage over their victims by encrypting valuable files and making them inaccessible. If the victim has backup copies, the cybercriminal loses some advantage. Backup files allow victims to restore their files once the infection has been cleaned up. Ensure that backups are protected or stored offline so that attackers can't access them.
- 7. **Do use cloud services.** This can help mitigate a ransomware infection, since many cloud services retain previous versions of files, allowing you to "roll back" to the unencrypted form.
- 8. **Don't pay the ransom.** Keep in mind, you may not get your files back even if you pay a ransom. A cybercriminal could ask you to pay again and again, extorting money from you but never releasing your data.

# 15. Spywares

- Spyware is a type of malicious software -- or [malware](#) -- that is installed on a computing device without the end user's knowledge. It invades the device, steals sensitive information and internet usage data, and relays it to advertisers, data firms or external users. Any software can be classified as spyware if it is downloaded without the user's authorization. Spyware is controversial because, even when it is installed for relatively innocuous reasons, it can violate the end user's privacy and has the potential to be abused.
- Spyware is one of the most common threats to internet users. Once installed, it monitors internet activity, tracks login credentials and spies on sensitive information. The primary goal of spyware is usually to obtain credit card numbers, banking information and passwords.
- Spyware can be difficult to detect; often, the first indication a user has that a computing device has been infected with spyware is a noticeable reduction in processor or network connection speeds and -- in the case of mobile devices -- data usage and battery life. [Antispyware](#) tools can be used to prevent or remove spyware. Antispyware tools can either provide real-time protection by scanning network data and blocking malicious data, or they can detect and remove spyware already on a system by executing scans.

# How spyware works

- Spyware can affect any personal computer (PC) or Mac, as well as iOS or Android devices. While the Windows operating system ([OS](#)) is more likely to fall prey to an infiltration, [hackers](#) are getting better at finding ways into Apple's OS as well. Some of the most common ways for computers to become infected include the following:
- pirating media, including games, videos and music;
- downloading materials from unreliable or unknown sources;
- accepting a [pop-up advertisement](#) or prompt without reading the content; and
- accepting and opening email attachments from unrecognized senders.

- In its least damaging form, spyware exists as an application that starts up as soon as the device is turned on and continues to run in the background. Its presence will steal random access memory (RAM) and processor power and could generate infinite pop-up ads, effectively slowing down the web browser until it becomes unusable.
- Spyware may also reset the browser's homepage to open to an ad every time or redirect web searches and control the provided results, making the search engine useless. Additionally, spyware can change the computer's dynamically link libraries (DLLs) -- which are used to connect to the internet -- resulting in connectivity failures that can be hard to diagnose.
- At its most damaging, spyware will track web browsing history and record words, passwords and other private information, such as credit card numbers or banking records. All of this information can be gathered and used for identity theft.
- Spyware can also secretly make changes to a device's firewall settings, reconfiguring the security settings to allow in even more malware. Some forms of spyware can even identify when the device is trying to remove it from the Windows registry and will intercept all attempts to do so.

# Types of spyware



## ADWARE

Any software application that displays advertisements while the program is running. Examples: banners, pop-up windows



## KEYBOARD LOGGERS

A type of surveillance technology used to monitor and record keystrokes. Cyber-criminals can use these to steal sensitive information such as authorization credentials, enterprise data and computer activity.



## TROJANS

A software application that appears harmless but can inflict damage or data loss to a system.



## MOBILE SPYWARE

A type of spyware that can infect mobile devices that typically enters via SMS or MMS communication channels.

- **Adware.** Malicious [adware](#) is often bundled in with free software, shareware programs and utilities downloaded from the internet or surreptitiously installed onto a user's device when the user visits an infected website. Many internet users were first introduced to spyware in 1999 when a popular freeware game called *Elf Bowling* came bundled with tracking software. Adware is often flagged by antimalware programs as whether the program in question is malicious or not.
- **Cookies** that track and record users' personally identifiable information (PII) and internet browsing habits are one of the most [common types of adware](#). An advertiser might use cookies to track what webpages a user visits in order to target advertising in a contextual marketing campaign. For example, an advertiser could track a user's browser history and downloads with the intent to display pop-up or banner advertisements to lure the user to make a purchase. Because data collected by spyware is often sold to third parties, regulations such as the General Data Protection Regulation ([GDPR](#)) have been enacted to protect the PII of website visitors.
- **Keyboard loggers.** [Keyloggers](#) are a type of system monitor that are often used by cybercriminals to steal PII, login credentials and sensitive enterprise data. Keyloggers may also be used by employers to observe employees' computer activities; parents to supervise their children's internet usage; device owners to track possible unauthorized activity on their devices; or law enforcement agencies to analyze incidents involving computer use.
- Hardware keyloggers resemble a Universal Serial Bus (USB) flash drive and serve as a physical connector between the computer keyboard and the computer, while software keylogging programs do not require physical access to the user's computer for installation. Software keyloggers can be downloaded on purpose by someone who wants to monitor activity on a particular computer, or they can be downloaded unwittingly and executed as part of a [rootkit](#) or remote access Trojan ([RAT](#)).
- **Trojans.** [Trojans](#) are typically malicious software programs that are disguised as legitimate programs. A victim of a Trojan could unknowingly install a file posing as an official program, allowing the Trojan to have access to the computer. The Trojan can then delete files, encrypt files for ransom or allow others to have access to the user's information.
- **Mobile spyware.** Mobile spyware is dangerous because it can be transferred through Short Message Service (SMS) or Multimedia Messaging Service (MMS) text messages and typically does not require user interaction to execute commands. When a smartphone or tablet gets infected with mobile spyware that is sideloaded with a third-party app, the phone's camera and microphone can be used to spy on nearby activity, record phone calls, and log browsing activity and keystrokes. The device owner's location can also be monitored through the Global Positioning System ([GPS](#)) or the mobile computing device's [accelerometer](#).

## **How to prevent spyware**

- Maintaining strict cybersecurity practices is the best way to prevent spyware. Some best practices include the following:
  - only downloading software from trusted sources;
  - reading all disclosures when installing software;
  - avoiding interaction with pop-up ads; and
  - staying current with updates and patches for browser, OS and application software.
- In addition, users should install antispyware tools, use extensive and reputable [antivirus software](#), avoid opening emails from unrecognized senders and enable two-factor authentication ([2FA](#)) whenever possible.
- iPhone users can activate 2FA at no additional cost, enabling them to protect all the data on their smartphone and prevent mobile spyware attacks. Two-factor authentication can also be used in a variety of other common services, including PayPal, Google, Dropbox and Microsoft Office 365, as well as in social networking sites, such as Instagram, Snapchat, Facebook and Twitter. Most major banks have also started implementing 2FA in their websites and mobile apps. Some services have even increased their authentication process to three- and four-factor authentication -- [3FA](#) and [4FA](#), respectively.
- To further reduce the probability of infection, network administrators should practice the principle of least privilege ([POLP](#)) and require remote workers to access network resources over a virtual private network ([VPN](#)) that runs a security scan before granting access privileges.

## **Antispyware tools**

- When choosing an antispyware tool, it is important to know that some only perform when the scan is manually started, while others are continuously running and monitoring computer activity to ensure spyware can't record the user's information. Furthermore, users should apply caution when downloading antispyware tools. Reviews can be read to determine which tools are safest, and it is recommended that the user only download tools from reputable sites.

- Some antispyware tools include the following:
- **Malwarebytes** is an antimalware/spyware tool that can remove spyware from Windows, macOS, Android and iOS. [Malwarebytes](#) can scan through registry files, running programs, hard drives and individual files. Once a spyware program is detected, a user can quarantine and delete it. However, users can't set up automatic scanning schedules.
- **Trend Micro HouseCall** is another antispyware tool that doesn't require user installation. Because it doesn't require installation, HouseCall uses minimal processor and memory resources, as well as disk space. However, like Malwarebytes, users cannot set automatic scans.
- **Windows Defender** is an antimalware Microsoft product included in the Windows 10 OS under Windows Defender Security Center. The software is a lightweight antimalware tool that protects against threats such as spyware, adware and viruses. [Windows Defender](#) includes multiple features, such as Application Guard, Exploit Guard, Advanced Threat Protection and Analytics. Windows Defender users can set automatic Quick and Full scans, as well as set alerts for low, medium, high and severe priority items.

- **How to remove spyware**
- In order to remove spyware, device users **must first identify that the spyware exists in their system**. There are several symptoms to look for that can signify the presence of an attack. They include the following:
  - The device runs at a much slower speed than normal.
  - The device consistently crashes unexpectedly.
  - Pop-up ads appear whether the user is online or offline.
  - The device starts running out of hard drive space.
- If it is determined that spyware has infected the system, then the user should perform the following steps:
  - Disconnect the internet connection.
  - Check the device's programs list to see if the unwanted software is listed. If it is, choose to remove it from the device. After uninstalling the program, reboot the entire system.
  - If the above step does not work, then run a scan of the system using reputable antivirus. The scan will find suspicious programs and ask the user to either clean, quarantine or delete the software.
  - The user can also download a virus removal tool or antispyware tool and allow it to run through the system.
  - If none of the above steps work, then the user will have to access the device's hard drive in safe mode. However, this requires a tool that will enable the user to access the spyware folders and manually delete them. While this sounds complicated, the process should only take a few minutes.

# 16. Rootkit

- Rootkits are a type of malware that are designed so that they can remain hidden on your computer. But while you might not notice them, they are active. Rootkits give cybercriminals the ability to remotely control your computer.
- Rootkits can contain a number of tools, ranging from programs that allow hackers to steal your passwords to modules that make it easy for them to steal your credit card or online banking information. Rootkits can also give hackers the ability to subvert or disable security software and track the keys you tap on your keyword, making it easy for criminals to steal your personal information.
- Because rootkits can hijack or subvert security software, they are especially hard to detect, making it likely that this type of malware could live on your computer for a long time causing significant damage. Sometimes the only way to completely eliminate a well-hidden rootkit is to erase your computer's operating system and rebuild from scratch.
- How do rootkits get on your computer? You might open an email and download a file that looks safe but is actually a virus. You might also accidentally download a rootkit through an infected mobile app.

- Types of rootkits
- Here are five types of rootkits.
- 1. **Hardware or firmware rootkit**
- The name of this type of rootkit comes from where it is installed on your computer. This type of malware could infect your computer's hard drive or its system BIOS, the software that is installed on a small memory chip in your computer's motherboard. It can even infect your router. Hackers can use these rootkits to intercept data written on the disk.
- 2. **Bootloader rootkit**
- Your computer's bootloader is an important tool. It loads your computer's operating system when you turn the machine on. A bootloader toolkit, then, attacks this system, replacing your computer's legitimate bootloader with a hacked one. This means that this rootkit is activated even before your computer's operating system turns on.
- 3. **Memory rootkit**
- This type of rootkit hides in your computer's RAM, or Random Access Memory. These rootkits will carry out harmful activities in the background. The good news? These rootkits have a short lifespan. They only live in your computer's RAM and will disappear once you reboot your system — though sometimes further work is required to get rid of them.
- 4. **Application rootkit**
- Application rootkits replace standard files in your computer with rootkit files. They might also change the way standard applications work. These rootkits might infect programs such as Word, Paint, or Notepad. Every time you run these programs, you will give hackers access to your computer. The challenge here is that the infected programs will still run normally, making it difficult for users to detect the rootkit.
- 5. **Kernel mode rootkits**
- These rootkits target the core of your computer's operating system. Cybercriminals can use these to change how your operating system functions. They just need to add their own code to it. This can give them easy access to your computer and make it easy for them to steal your personal information.

# • How to defend against rootkits

- Because rootkits are so dangerous, and so difficult to detect, it's important to exercise caution when surfing the internet or downloading programs. There is no way to magically protect yourself from all rootkits.
- Fortunately, you can increase your odds of avoiding these attacks by following the same common-sense strategies you take to avoid all computer viruses, including these.

## **Don't ignore updates**

- Updates to your computer's applications and operating system can be annoying, especially when it seems as if there's a new update for you to approve every time you turn on your machine. But don't ignore these updates. Keeping your operating systems, antivirus software, and other applications updated is the best way to protect yourself from rootkits.

## **Watch out for phishing emails**

- Phishing emails are sent by scammers who want to trick you into providing them your financial information or downloading malicious software, such as rootkits, onto your computer. Often, these emails will look like they come from a legitimate bank or credit card provider. These messages may state that your account is about to be frozen or that you need to verify your identity. The messages will also ask that you click on a link.
- If you do, you'll be taken to a fake website. Once there, you might accidentally download a rootkit to your computer.
- The lesson? Never click on any links supposedly sent from a financial services company. If the message is supposedly coming from a company with which you have no accounts, delete them. If the message comes from a company you do business with, log into your online account or call the company. If there's really a problem, it should show up on your online account or a customer-service representative will confirm it.

## **Be careful of drive-by downloads**

- Drive-by downloads can be especially troublesome. These happen when you visit a website and it automatically installs malware on your computer. You don't have to click on anything or download anything from the site for this to happen. And it's not just suspicious websites that can cause this. Hackers can embed malicious code in legitimate sites to cause these automatic downloads.
- The best way to help protect yourself? Approve updates to your computer's software quickly. Set your operating system, browsers, and all applications to install updates automatically so that your computer systems will always have the most up-to-date protections in place.

## **Don't download files sent by people you don't know**

- Be careful, too, when opening attachments. Don't open attachments sent to you by people you don't know. Doing so could cause a rootkit to be installed in your computer.
- If you receive a suspicious attachment? Delete the email message immediately

# 17. Adware

- **Adware definition**
- Adware, also known as **advertisement-supported software**, generates revenue for its developers by automatically generating adverts on your screen, usually within a web browser. Adware is typically created for computers but can also be found on mobile devices. Some forms of adware are highly manipulative and create an open door for malicious programs.
- **What is adware?**
- Adware is software that **displays unwanted (and sometimes irritating) pop-up adverts which can appear on your computer or mobile device**. Adware typically ends up on a user's device through one of two ways:
- You **might install a free computer program or app without necessarily realizing that it contains additional software** that contains adware. This allows the app developer to make money but means you could download adware onto your systems without necessarily consenting.
- Alternatively, there may be a vulnerability in your software or operating system which hackers exploit to insert **malware**, including some types of adware, into your system.

- **How do you get adware?**
- Adware normally comes in software/programmes that you download from the internet – usually freeware or [shareware](#) – and it secretly installs itself onto your device without your knowledge.
- Free software which contains some ads may be annoying but is not illegal. However, if a third-party programme adds malicious ad software onto your device without your consent, then it is illegal.
- **How does adware work?**
- Adware works by installing itself quietly onto your devices, hoping you'll – accidentally or otherwise – click on an advert that it displays to you.
- This is because, ultimately, adware exists to make money.
- Adware creators and distributing vendors make money from third parties via either:
  - Pay-per-click (PPC) — they get paid each time you open an ad.
  - Pay-per-view (PPV) — they get paid each time an ad is shown to you.
  - Pay-per-install (PPI) — they get paid each time bundled software is installed on a device.
- Adware can also track your search and browsing history to display ads that are more relevant to you. Once the developer has your location and browser history, they can make additional income by selling that information to third parties.
- At the less harmful end of the spectrum, adware is simply a nuisance. At the more harmful end, it can be a damaging malware threat to your cybersecurity.

- **How to tell if you have an adware infection**
- Signs that you may be infected with unwanted adware include:
  - **Computer adware infection signs**
  - An unexpected change in your web browser home page
  - Web pages that you visit not displaying correctly
  - Being overwhelmed with pop-up ads — sometimes even if not browsing the internet
  - Slow device performance
  - Device crashing
  - Reduced internet speeds
  - Redirected internet searches
  - Random appearance of a new toolbar or browser add-on
  - **Mobile adware infection signs**
  - On your phone, signs are similar:
    - Your phone is slow
    - Apps take longer to load
    - Your battery drains quickly
    - Your phone has apps you don't remember downloading
    - There is unexplained data usage and higher than expected phone bills
    - There are numerous ad pop-ups

- **Android adware removal**
- If you are wondering how to get rid of adware on your phone, here are some Android-specific tips:
  - Step 1: Start your phone in Safe Mode
  - Step 2: Remove malicious device admin apps
  - Step 3: Uninstall the malicious apps from your Android phone
  - Step 4: Use antivirus software for Android to remove viruses, adware, and other malware
  - Step 5: Remove redirects and pop-up ads from your browser

# 18. Backdoor

- A backdoor is any method that allows somebody — hackers, governments, IT people, etc. — to remotely access your device without your permission or knowledge.
- Hackers can install a backdoor onto your device by using malware, by exploiting your software vulnerabilities, or even by directly installing a backdoor in your device's hardware/firmware.
- Once hackers log into your machine without your knowledge, they can use backdoors for a variety of reasons, such as:
  - **Surveillance.**
  - **Data theft.**
  - **Cryptojacking.**
  - **Sabotage.**
  - **Malware attack.**
- Nobody is immune to backdoor hacking, and hackers are constantly inventing new methods and malware files to gain access to user devices.

- In cybersecurity, a backdoor is anything that can allow an outside user into your device without your knowledge or permission. Backdoors can be installed in two different parts of your system:
- **Hardware/firmware.** Physical alterations that provide remote access to your device.
- **Software.** Malware files that hide their tracks so your operating system doesn't know that another user is accessing your device.
- A backdoor can be installed by software and hardware developers for remote tech support purposes, but in most cases, backdoors are installed either by cybercriminals or intrusive governments to help them gain access to a device, a network, or a software application.
- **Any malware that provides hackers access to your device can be considered a backdoor** — this includes rootkits, trojans, spyware, cryptojackers, keyloggers, worms, and even ransomware.
- **How Do Backdoor Attacks Work?**
- In order for cybercriminals to successfully install a backdoor on your device, they first need to gain access to your device, either through physical access, a malware attack, or by exploiting a system vulnerability — here are some of the more common vulnerabilities that hackers target:
  - **Open ports.**
  - **Weak passwords.**
  - **Out-of-date software.**
  - **Weak firewalls.**

- Here are a few examples of the different kinds of backdoors that are frequently used:
- **Trojans.** Trojans are malware files that pretend to be legitimate files to gain access to your device. Once you click on the “allow *insert-program-here* to make changes on your device?” button on your PC, the Trojan is then able to install itself on your device. Trojan backdoors can allow users to access your files and programs, or install more serious malware files on your device.
- **Rootkits.** Rootkits are advanced malware threats that are able to hide their activities from an operating system so that the operating system gives security privileges (root access) to the rootkit. Rootkits can allow a hacker to remotely access your device, alter your files, observe your activity, and sabotage your system. Rootkits can take the form of either software or even physically altered computer chips — you can read more about rootkits [here](#).
- **Hardware backdoors.** Hardware backdoors are modified computer chips or other firmware/hardware that provide non-users access to a device. This can include phones, IoT devices like thermostats and home security systems, routers, and computers. Hardware backdoors can communicate user data, provide remote access, or be used for surveillance. Hardware backdoors can be shipped with products (either by a rogue manufacturer or for some benign purpose), but they can also be physically installed in the event that a device is stolen.
- **Cryptographic backdoors.** Cryptographic backdoors are essentially a “master key” that can unlock every piece of encrypted data that uses a specific encryption protocol. Encryption standards like AES use end-to-end encryption so that only the parties that have exchanged a randomly generated cryptographic key are able to decrypt the information being shared. Backdoors are a way of breaking this secure conversation, manipulating the complex mathematics of a specific cryptographic protocol to give an outside user access to all of the encrypted data being shared between parties.

# 19. Bots

- An Internet bot is a software application that runs automated tasks over the internet. Tasks run by bots are typically simple and performed at a much higher rate compared to human Internet activity.
- Some bots are legitimate—for example, Googlebot is an application used by Google to crawl the Internet and index it for search. Other bots are malicious—for example, bots used to automatically scan websites for software vulnerabilities and execute simple attack patterns.

- What Is a Botnet
- There are many types of malware that infect end-user devices, with the objective of enlisting them into a botnet. Any device that becomes infected starts communicating with a Command and Control (C&C) center and can perform automated activities under the attacker's central control.
- Many threat actors are actively engaged in building massive botnets, with the biggest ones spanning millions of computers. Often, the botnet can grow itself, for example by using infected devices to send out spam emails, which can infect more machines.
- Botnet owners use them for large-scale malicious activity, commonly Distributed Denial of Service (DDoS) attacks. Botnets can also be used for any other malicious bot activity, such as spam bots or social bots (described below), albeit on a much larger scale.

## • **Types of Bots**

- There are many types of bots active on the Internet, both legitimate and malicious. Below are several common examples.

### **Spider Bots**

- Spider bots, also known as web spiders or crawlers, browse the web by following hyperlinks, with the objective of retrieving and indexing web content. Spiders download HTML and other resources, such as CSS, JavaScript, and images, and use them to process site content.
- If you have a large number of web pages, you can place a robots.txt file in the root of your web server, and provide instructions to bots, specifying which parts of your site they can crawl, and how frequently.

### **Scraper Bots**

- Scrapers are bots that read data from websites with the objective of saving them offline and enabling their reuse. This may take the form of scraping the entire content of web pages or scraping web content to obtain specific data points, such as names and prices of products on eCommerce sites.
- Web scraping is a gray area -in some cases, scraping is legitimate and may be permitted by website owners. In other cases, bot operators may be violating website terms of use, or worse—leveraging scraping to steal sensitive or copyrighted content.

### **Spam Bots**

- A spambot is an Internet application designed to gather email addresses for spam mailing lists. A spam bot can gather emails from websites, social media websites, businesses and organizations, leveraging the distinctive format of email addresses.
- After attackers have amassed a large list of email addresses, they can use them not only to send spam email, but also for other nefarious purposes:
- **Credential cracking**—pairing emails with common passwords to gain unauthorized access to accounts.
- **Form spam**—automatically inserting spam, such as ads or malware links, into forms on popular websites, typically comment or feedback forms.
- Apart from the direct damage caused to end-users and organizations affected by spam campaigns, spam bots can also choke server bandwidth and increase costs for Internet Service Providers (ISPs).

- **Social Media Bots**
  - Bots are operated on social media networks, and used to automatically generate messages, advocate ideas, act as a follower of users, and as fake accounts to gain followers themselves. It is estimated that 9-15% of Twitter accounts are social bots.
  - Social bots can be used to infiltrate groups of people and used to propagate specific ideas. Since there is no strict regulation governing their activity, social bots play a major role in online public opinion.
  - Social bots can create fake accounts (although this is becoming more difficult as social networks become more sophisticated), amplify the bot operator's message, and generate fake followers/likes. It is difficult to identify and mitigate social bots, because they can exhibit very similar behavior to that of real users.
- **Download Bots**
  - Download bots are automated programs that can be used to automatically download software or mobile apps. They can be used to influence download statistics, for example to gain more downloads on popular app stores and help new apps get to the top of the charts. They can also be used to attack download sites, creating fake downloads as part of an application-layer Denial of Service (DoS) attack.
- **Ticketing Bots**
  - Ticketing Bots are an automated way to purchase tickets to popular events, with the aim of reselling those tickets for a profit. This activity is illegal in many countries, and even if not prohibited by law, it is an annoyance to event organizers, ticket sellers and consumers.
  - Ticketing bots tend to be very sophisticated, emulating the same behaviors as human ticket buyers. In many ticketing domains, the proportion of tickets purchased by automated bots ranges between 40-95%.

## How To Detect Bot Traffic in Web Analytics?

- Following are a few parameters you can use in a manual check of your web analytics, to detect bot traffic hitting a website:
- **Traffic trends**—abnormal spikes in traffic might indicate bots hitting the site. This is particularly true if the traffic occurs during odd hours.
- **Bounce rate**—abnormal highs or lows may be a sign of bad bots. For example, bots that hit a specific page on the site and then switch IP will appear to have 100% bounce.
- **Traffic sources**—during a malicious attack, the primary channel sending traffic is “direct” traffic and the traffic will consist of new users and sessions.
- **Server performance**—a slowdown in server performance may be a sign of bots.
- **Suspicious IPs/geo-locations**—an increase in activity to an unknown IP range or a region you don’t do business in.  
Suspicious hits from single IPs—a big number of hits from a single IP. Humans typically request a few pages and not others, whereas bots will often request all pages.
- **Language sources**—seeing hits from other languages your customers do not typically use.

# 20. Social Engg.

- Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
- Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack.
- Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.
- What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems.
- Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

## How Does Social Engineering Happen?

- Social engineering happens because of the human instinct of trust. Cybercriminals have learned that a carefully worded email, voicemail, or text message can convince people to transfer money, provide confidential information, or download a file that installs malware on the company network.  
Consider this example of spear phishing that convinced an employee to transfer \$500,000 to a foreign investor:
- Thanks to careful spear phishing research, the cybercriminal knows the company CEO is traveling.
- An email is sent to a company employee that looks like it came from the CEO. There is a slight discrepancy in the email address – but the spelling of the CEO's name is correct.
- In the email, the employee is asked to help the CEO out by transferring \$500,000 to a new foreign investor. The email uses urgent yet friendly language, convincing the employee that he will be helping both the CEO and the company.
- The email stresses that the CEO would do this transfer herself but since she is travelling, she can't make the fund transfer in time to secure the foreign investment partnership.
- Without verifying the details, the employee decides to act. He truly believes that he is helping the CEO, the company, and his colleagues by complying with the email request.
- A few days later, the victimized employee, CEO, and company colleagues realize they have been a victim of a social engineering attack and have lost \$500,000.

## **• Examples of Social Engineering Attacks**

- Savvy cybercriminals know that social engineering works best when focussing on human emotion and risk. Taking advantage of human emotion is much easier than hacking a network or looking for security vulnerabilities.
- These examples of social engineering emphasize how emotion is used to commit cyber attacks:

### **Fear**

- You receive a voicemail that says you're under investigation for tax fraud and that you must call immediately to prevent arrest and criminal investigation. This social engineering attack happens during tax season when people are already stressed about their taxes. Cybercriminals prey on the stress and anxiety that comes with filing taxes and use these fear emotions to trick people into complying with the voicemail.

### **Greed**

- Imagine if you could simply transfer \$10 to an investor and see this grow into \$10,000 without any effort on your behalf? Cybercriminals use the basic human emotions of trust and greed to convince victims that they really can get something for nothing. A carefully worded baiting email tells victims to provide their bank account information and the funds will be transferred the same day.

### **Curiosity**

- Cybercriminals pay attention to events capturing a lot of news coverage and then take advantage of human curiosity to trick social engineering victims into acting. For example, after the second Boeing MAX8 plane crash, cybercriminals sent emails with attachments that claimed to include leaked data about the crash. In reality, the attachment installed a version of the Hworm RAT on the victim's computer.

### **Helpfulness**

- Humans want to trust and help one another. After doing research into a company, cybercriminals target two or three employees in the company with an email that looks like it comes from the targeted individuals' manager. The email asks them to send the manager the password for the accounting database – stressing that the manager needs it to make sure everyone gets paid on time. The email tone is urgent, tricking the victims into believing that they are helping out their manager by acting quickly.

### **Urgency**

- You receive an email from customer support at an online shopping website that you frequently buy from telling you that they need to confirm your credit card information to protect your account. The email language urges you to respond quickly to ensure that your credit card information isn't stolen by criminals. Without thinking twice and because you trust the online store, you send not only your credit card information but also your mailing address and phone number. A few days later, you receive a call from your credit card company telling you that your credit card has been stolen and used for thousands of dollars of fraudulent purchases.

# Social engineering attack techniques

- Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are the five most common forms of digital social engineering assaults.
- **Baiting**
  - As its name implies, baiting attacks use a **false promise to pique a victim's greed or curiosity**. They lure users into a trap that steals their personal information or inflicts their systems with malware.
  - The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait—typically malware-infected flash drives—in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look to it, such as a label presenting it as the company's payroll list.
  - Victims pick up the bait out of curiosity and insert it into a work or home computer, resulting in automatic malware installation on the system.
  - Baiting scams don't necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application.
- **Scareware**
  - Scareware involves victims being **bombarded with false alarms and fictitious threats**. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.
  - A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, "Your computer may be infected with harmful spyware programs." It either **offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected**.
  - Scareware is also distributed via spam email that doles out bogus warnings, or makes offers for users to buy worthless/harmful services.

- **Pretexting**
- Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.
- The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data.
- All sorts of pertinent information and records is gathered using this scam, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

### **Phishing**

- As one of the most popular social engineering attack types, [phishing](#) scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.
- An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker.
- Given that identical, or near-identical, messages are sent to all users in phishing campaigns, detecting and blocking them are much easier for mail servers having access to threat sharing platforms.

### **Spear phishing**

- This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. [Spear phishing](#) requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skillfully.
- A spear phishing scenario might involve an attacker who, in impersonating an organization's IT consultant, sends an email to one or more employees. It's worded and signed exactly as the consultant normally does, thereby deceiving recipients into thinking it's an authentic message. The message prompts recipients to change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials.

## Social engineering prevention

- Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps. Therefore, be wary whenever you feel alarmed by an email, attracted to an offer displayed on a website, or when you come across stray digital media lying about. Being alert can help you protect yourself against most social engineering attacks taking place in the digital realm.

Moreover, the following tips can help improve your vigilance in relation to social engineering hacks.

- Don't open emails and attachments from suspicious sources – If you don't know the sender in question, you don't need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider's site. Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.
- Use multifactor authentication – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise. (Multi-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence.)
- Be wary of tempting offers – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.
- Keep your antivirus/antimalware software updated – Make sure automatic updates are engaged, or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied, and scan your system for possible infections.

# 21. Phishing

- Phishing is a type of [social engineering attack](#) often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a [malicious](#) link, which can lead to the installation of malware, the freezing of the system as part of a [ransomware attack](#) or the revealing of [sensitive information](#).
- An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.
- Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an [advanced persistent threat](#) (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.
- An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

- **Phishing attack examples**

- The following illustrates a common phishing scam attempt:
- A spoofed email ostensibly from myuniversity.edu is mass-distributed to as many faculty members as possible.
- The email claims that the user's password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.
- Several things can occur by clicking the link. For example:
- The user is redirected to myuniversity.edurenwal.com, a bogus page appearing exactly like the real renewal page, where both new and existing passwords are requested. The attacker, monitoring the page, hijacks the original password to gain access to secured areas on the university network.
- The user is sent to the actual password renewal page. However, while being redirected, a malicious script activates in the background to hijack the user's session cookie. This results in a reflected XSS attack, giving the perpetrator privileged access to the university network.

The screenshot shows a Gmail inbox with the following details:

- Google** search bar and navigation icons.
- Gmail** button with a dropdown arrow.
- Important: Your Password will expire in 1 day(s)** notification.
- Inbox** button with a 'x' icon.
- Compose** and **Print** buttons.
- From:** MyUniversity (with a person icon) to me.
- Date:** 12:18 PM (50 minutes ago).
- Subject:** (empty)
- Message Preview:**

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.

Please follow the link below to update your password

[myuniversity.edu/renewal](http://myuniversity.edu/renewal)



Thank you  
MyUniversity Network Security Staff

- # Phishing techniques
- ## Email phishing scams

- Email phishing is a numbers game. An attacker sending out thousands of fraudulent messages can net significant information and sums of money, even if only a small percentage of recipients fall for the scam. As seen above, there are some techniques attackers use to increase their success rates.
- For one, they will go to great lengths in designing phishing messages to mimic actual emails from a spoofed organization. Using the same phrasing, typefaces, logos, and signatures makes the messages appear legitimate.
- In addition, attackers will usually try to push users into action by creating a sense of urgency. For example, as previously shown, an email could threaten account expiration and place the recipient on a timer. Applying such pressure causes the user to be less diligent and more prone to error.
- Lastly, links inside messages resemble their legitimate counterparts, but typically have a misspelled domain name or extra subdomains. In the above example, the myuniversity.edu/renewal URL was changed to myuniversity.edurenwal.com. Similarities between the two addresses offer the impression of a secure link, making the recipient less aware that an attack is taking place.



- **Spear phishing**
- Spear phishing targets a specific person or enterprise, as opposed to random application users. It's a more in-depth version of phishing that requires special knowledge about an organization, including its power structure.
- An attack might play out as follows:
- A perpetrator researches names of employees within an organization's marketing department and gains access to the latest project invoices.
- Posing as the marketing director, the attacker emails a departmental project manager (PM) using a subject line that reads, Updated invoice for Q3 campaigns. The text, style, and included logo duplicate the organization's standard email template.
- A link in the email redirects to a password-protected internal document, which is in actuality a spoofed version of a stolen invoice.
- The PM is requested to log in to view the document. The attacker steals his credentials, gaining full access to sensitive areas within the organization's network.
- By providing an attacker with valid login credentials, spear phishing is an effective method for executing the first stage of an APT.

- ## How to prevent phishing

- Phishing attack protection requires steps be taken by both users and enterprises.
- For users, vigilance is key. A spoofed message often contains subtle mistakes that expose its true identity. These can include spelling mistakes or changes to domain names, as seen in the earlier URL example. Users should also stop and think about why they're even receiving such an email.
- For enterprises, a number of steps can be taken to mitigate both phishing and spear phishing attacks:
  - [Two-factor authentication \(2FA\)](#) is the most effective method for countering phishing attacks, as it adds an extra verification layer when logging in to sensitive applications. 2FA relies on users having two things: something they know, such as a password and user name, and something they have, such as their smartphones. Even when employees are compromised, 2FA prevents the use of their compromised credentials, since these alone are insufficient to gain entry.
  - In addition to using 2FA, organizations should enforce strict password management policies. For example, employees should be required to frequently change their passwords and to not be allowed to reuse a password for multiple applications.
  - Educational campaigns can also help diminish the threat of phishing attacks by enforcing secure practices, such as not clicking on external email links.

# 22. Key Logging

- Keyloggers are built for the **act of keystroke logging** — creating **records of everything you type on a computer or mobile keyboard**. These are used to **quietly monitor your computer activity while you use your devices as normal**. Keyloggers are used for legitimate purposes like feedback for software development but can be misused by criminals to steal your data.

## **Keystroke Logging Definition**

- The concept of a keylogger breaks down into two definitions:

- **Keystroke logging:** Record-keeping for every key pressed on your keyboard.

- **Keylogger tools:** Devices or programs used to log your keystrokes.

- You'll find use of keyloggers in everything from Microsoft products to your own employer's computers and servers. In some cases, your spouse may have put a keylogger on your phone or laptop to confirm their suspicions of infidelity. Worse cases have shown criminals to implant legitimate websites, apps, and even USB drives with keylogger malware.

- Whether for malicious intent or for legitimate uses, you should be aware how keyloggers are affecting you. First, we'll further define keystroke logging before diving into how keyloggers work. Then you'll be able to better understand how to [secure yourself](#) from unwanted eyes.

## **How Keystroke Logging Works**

- Keystroke logging is an act of **tracking and recording every keystroke entry made on a computer, often without the permission or knowledge of the user**. A "keystroke" is just any interaction you make with a button on your keyboard.

- Keystrokes are how you "speak" to your computers. **Each keystroke transmits a signal that tells your computer programs what you want them to do.**

- These commands may include:

- **Length of the keypress**

- **Time of keypress**

- **Velocity of keypress**

- **Name of the key used**

- When logged, all this information is like listening to a private conversation. You believe you're only "talking" with your device, but another person listened and wrote down everything you said. With our increasingly digital lives, we share a lot of highly sensitive information on our devices.

- User behaviors and private data can easily be assembled from logged keystrokes. Everything from online banking access to social security numbers is entered into computers. Social media, email, websites visited, and even text messages sent can all be highly revealing.

- **What does a Keylogger Do?**
- **Keylogger tools** can either be **hardware or software** meant to automate the process of keystroke logging. These tools record the data sent by every keystroke into a text file to be retrieved at a later time. Some tools can record everything on your copy-cut-paste clipboard, calls, GPS data, and even microphone or camera footage.
- Keyloggers are a **surveillance tool** with legitimate uses for personal or professional IT monitoring. Some of these uses enter an ethically questionable grey area. However, other keylogger uses are explicitly criminal.
- Regardless of the use, keyloggers are often used without the user's fully aware consent and keyloggers are used under the assumption that users should behave as normal.
- **Types of Keyloggers**
- Keylogger tools are mostly constructed for the same purpose. But they've got important distinctions in terms of the methods they use and their form factor.
- Here are the two forms of keyloggers
- **Software keyloggers**
- **Hardware keyloggers**

## Why Keystroke Logging is a Threat?

- Threats of keyloggers can come from many issues around the collection of sensitive data.
- When you are unaware that everything you type onto your computer keyboard is being recorded, you may inadvertently expose your:
  - Passwords.
  - Credit card numbers.
  - Communications.
  - Financial account numbers.
- Sensitive information like this is highly valuable to third-parties, including advertisers and criminals. Once collected and stored, this data then becomes an easy target for theft.
- **Data breaches** can expose saved keystroke logs, even in legitimate use cases. This data can easily be leaked inadvertently via an unsecured or unsupervised device or through a [phishing attack](#). More common leaks can occur by a direct criminal attack with malware or other means. Organizations collecting mass keylogging data can be prime targets for a breach.
- **Criminal use of keyloggers** can collect and exploit your information just as easily. Once they've infected you with malware via [drive by download](#) or other means, time is of the essence. They can access your accounts before you even know that your sensitive data has been compromised.

# 23. Mail Bombs

- A mail bomb is the sending of a massive amount of e-mail to a specific person or system. A huge amount of mail may simply fill up the recipient's disk space on the server or, in some cases, may be too much for a server to handle and may cause the server to stop functioning.
- Mail bombs not only inconvenience the intended target but they are also likely to inconvenience everybody using the server.

- On Internet usage, an **email bomb** is a form of net abuse that sends large volumes of email to an address to overflow the mailbox, overwhelm the server where the email address is hosted in a denial-of-service attack (DoS attack) or as a smoke screen to distract the attention from important email messages indicating a security breach.

# 24. Cyber Pornography

- Cyber Pornography means *the publishing, distributing or designing pornography by using cyberspace*. The technology has its pros and cons and cyber pornography is the result of the advancement of technology. With the easy availability of the Internet, people can now view thousands of porn on their mobile or laptops, they even have access to upload pornographic content online.
- Obscenity and Pornography
- Obscenity and Pornography are often used synonymously. But it should be noted that obscenity is a wider concept than pornography. Obscenity means anything which is immoral and against the sentiments of people, whereas pornography refers to the act of causing sexual excitement through films, pictures or books. Thus, pornography is just a part of obscenity.

- **Porn Content**
- 30% of Internet content is porn. One can get abundant access to pornographic content on the dark web. Dark web even contains the child pornographic contents. It is worthy to note that only 10% of the total content is available on the surface web, the rest of the content is available on the dark work and the deep web.
- In the year 2005, there were more than 2 billion searches for porn.
- Almost 20% of the mobile phone searches are for porn.
- 28,258 users watch porn every second.
- 90% of boys and 60% of girls watch porn by the time they turn 18.
- Porn Revenue
- The pornography industry is the fastest growing industry. It is estimated to be worth approximately \$60 billion in the year 2007.
- The U.S. is the world leader in the pornography industry. It spends \$12 billion on porn followed by Australia, which generates \$1.5 billion revenue from porn sites.

- **Porn rise**
- Easy access to the Internet has helped the people to view pornographic content without compromising their privacy and without disclosing their identity to anyone.
- It has removed the hurdles of the conventional form of pornography, where people used to buy the pornographic content in printed form, the people nowadays, can view the content without any fear of being caught by someone.
- Easy accessibility to sites that offer porn content for free.
- **Effects of Pornography**
- Many surveys reveal that a person who is **addicted to pornography** has a change in attitude towards himself and his family.
- Pornography which is usually viewed in private often leads to **deception in marriage and which may, later on, affect their family life.**
- It may lead to **adultery, prostitution** and **many unreal expectations** that can result in dangerous promiscuous behaviour.
- Pornography may **lead to addiction, escalation, desensitization and acting out sexually by one person.**

- Cyber pornography is banned in many countries but legalized in some. Cyber Pornography is neither banned nor legalised under the IT Act, 2000. The IT Act prohibits the production and distribution of cyber pornography but does not prohibit the viewing or downloading of pornographic content if it is not child pornography.
- Section 67 of the Information Technology Act, 2000 makes the following acts punishable with imprisonment up to 3 years and a fine up to 5 lakhs:
- **Publication**— It includes uploading of pornographic content on a website, WhatsApp group or any other digital portal where third parties can have access to such pornographic content.
- **Transmission**— It means to send obscene material to any person electronically.
- **Causing to be published or transmitted**— It is a comprehensive terminology which would end up making the intermediary portal liable, using which the offender has published or transmitted such obscene content. The Intermediary Guidelines under the Information Technology Act put an onus on the Intermediary/Service Provider to exercise due diligence to ensure that their portal is not being misused.
- Section 67A of the Information Technology Act makes publication, transmission and causing to be transmitted and published any material containing sexually explicit act or conduct punishable with imprisonment up to 5 years and a fine up to ₹10 lakhs.
- Following conclusions can be made by understanding the above provisions:
- Viewing Cyber pornography is legal in India. Merely downloading and viewing such content does not amount to an offence.
- Publication of pornographic content online is illegal.
- Storing Cyber pornographic content is not an offence.
- Transmitting cyber pornography via instant messaging, emails or any other mode of digital transmission is an offence.

- **Exceptions**
- The section 67A of the IT Act does not prohibit books, pamphlets, magazines or pictures which are created for educational purposes or which is kept for religious purposes. Thus, the section does not prohibit the preserving of sculptures that are of historical importance.
- Child Pornography
- Section 67B of the IT Act, 2000 makes it publishing, transmitting, viewing or downloading child pornography illegal. The fact that the internet has made child pornography more accessible to the distributors, as well as the collectors, cannot be denied.
- According to Section 67B, any person who has not attained the age of 18 years is a child. It further states that child pornography can be committed in the following five ways:
- By publishing or transmitting or causing to publish or transmit any material electronically that depicts the children engaged in a sexually explicit act or conduct.
- By depicting children in an obscene or sexually explicit manner.
- By inducing children to online relationship with one or more children for and on a sexually explicit act, or in a manner that may offend a reasonable adult on the computer resource.
- By facilitating child abuse online.
- By recording own abuse or that of others pertaining to sexually explicit act with others.

## **POCSO (The Protection of Children from Sexual Offences) Act, 2012**

- The POCSO Act, 2012 was specifically enacted to prevent children from sexual offences. The act protects children from sexual assault, sexual harassment, and pornography. The act aims to protect the interests and well-being of the children. For the purpose of the act, any person who has not attained the age of 18 years is a child. The Act is gender-neutral.
- The provisions relating to Cyber Pornography under the POCSO Act are discussed below:
- Section 13 of the POCSO Act, 2012, defines the offence of child pornography, it states that whosoever, uses a child in any form of media for the sexual gratification shall be guilty of the offence of child pornography.
- Section 14 of the POCSO Act, 2012, provides the punishment for using a child for pornographic purposes.

## Why is Cyber Pornography difficult to regulate?

- It isn't as easy as it seems to regulate Cyber Pornography. It is really difficult to regulate Cyber Pornography. Some of the reasons for the same are:
- The Internet is a global network, connecting various computers. It is highly decentralized i.e. no single entity has control over the content published on the Internet.
- People can use proxy servers to access pornographic content on the Internet. Thus, they can even access banned websites by using proxy servers.
- There are a large number of servers on the Internet that contains pornographic content. It is highly difficult to regulate such a large number of servers.
- Adult websites are not the only way to download porn. There are other communication protocols that the Internet users follow to download the pornographic content, say, for example, if a website is banned, the users may download porn by using Bit-Torrent technology. Similarly, peer-topper networks such as eMule or Bulletin Boards can be used to download and share files, including porn.

# 25. Intellectual Property Theft

- Intellectual property theft (IP theft) refers to the robbing of people or companies of their ideas, inventions, and creative expressions (i.e., their IP).
- There are four main types of IP, including trade secrets, trademarks, copyrights, and patents.
- IP can include everything from proprietary products and parts, to movies, music, web content, business processes, and software.

- IP theft may result in significant losses for organizations and can add up to substantial sums at a country-wide level.
- Also, if a cybersecurity breach allows malicious actors to steal data, an organization can face compliance and legal issues, since that breach may affect other sensitive data of customers, employees, and partners. Thus, businesses that suffer breaches will likely focus less on further development and success due to putting efforts and resources into lawsuits.

## Consequences of IP theft for IP owners

Compliance issues due to improper data security

Lawsuits and other legal issues

Loss of a competitive edge

Bad press and reputational losses

Loss of customer trust

Slowdown in business growth



[www.ekrantsystem.com](http://www.ekrantsystem.com)

# 3 methods of intellectual property theft

1  
Hacking

2  
Privilege abuse

3  
Human errors



## Malware types for IP theft

Keyloggers

01

Cross-site scripting

02

Drive-by downloads

03

Man-in-the-browser

04

## Who can abuse their access rights and steal an organization's intellectual property?



Current employees



Former employees



Privileged users



Third parties

# 26. Session Hijacking

- A session hijacking attack happens when an attacker takes over your internet session — for instance, while you're checking your credit card balance, paying your bills, or shopping at an online store.
- Session hijackers usually target browser or web application sessions.
- A session hijacking attacker can then do anything you could do on the site. In effect, a hijacker fools the website into thinking they are you.
- Just as a hijacker can commandeer an airplane and put the passengers in danger, a session hijacker can take over an internet session and cause big trouble for the user.

# How does session hijacking work?

- There are many different types of session hijacking attacks, and we'll include details and examples of session hijacking attacks below. But first, let's take a quick look at how session hijacking works:
- **Session hijacking Step 1: An unsuspecting internet user logs into an account.** The user may log into a bank account, credit card site, online store, or some other application or site. The application or site installs a temporary "session cookie" in the user's browser. That cookie contains information about the user that allows the site to keep them authenticated and logged in and to track their activity during the session. The session cookie stays in the browser until the user logs out or is automatically logged out.
- **Session hijacking Step 2: A criminal gains access to the internet user's valid session.** Cybercriminals have different methods to steal sessions. Many common types of session hijacking involve grabbing the user's session cookie, locating the session ID within the cookie, and using that information to take over the session. The session ID is also known as a session key. When the criminal gets the session ID, they can take over the session without being detected.
- **Session hijacking Step 3:** The session hijacker gets a payoff for stealing the session. Once the original internet user has gone on their way, the hijacker can use the ongoing session to commit an array of nefarious acts. They can steal money from the user's bank account, purchase items, grab personal data to commit ID theft, or encrypt important data and demand a ransom for its return.
- Here are a few hypothetical examples of session hijacking:
- **Session hijacking example #1:** Cassie is sitting in a coffee shop sipping a latte and checking her money market account balance. A hijacker at the next table uses "session sniffing" to grab the session cookie, take over the session, and access her bank account.
- **Session hijacking example #2:** Justin gets an email about a sale at his favorite online retailer, and he clicks the link and logs in to start shopping. The email was sent by an attacker, who included his own session key in the link. The attacker steals the session, goes on a shopping spree, and pays with Justin's saved credit card.
- Session hijackers know all kinds of tricks for stealing sessions, and it's good to know how they work so you can help stay safe online.

## 5 Methods of Session Hijacking

- Want to know more about how session hijacking works? Here are the main types of session hijacking attacks that hijackers use to take over internet sessions:
- Brute force** – In a brute force attack, the attacker guesses the session ID and uses it to hijack the session. Brute force attacks usually work only when the website has lax security and uses short, easy-to-guess session keys.
- Cross-site scripting** – A cross-site scripting attack takes advantages of security weak spots in a web server. In cross-site scripting, an attacker injects scripts into web pages. These scripts cause your web browser to reveal your session key to the attacker so they can take over the session.
- Malware** – Cybercriminals can trick you into clicking a link that installs malware on your device to allow them to hijack a session. The malware may survey and conduct “session sniffing” to find a session. The malware then grabs the session cookie and sends it to the criminal, who can then get your session ID to take over your session.
- Session side jacking** – In this type of attack, a criminal needs access to a user’s network traffic. They may gain access when the user uses unsecured Wi-Fi or by engaging in man-in-the-middle attacks. In session side jacking, a criminal uses “packet sniffing” to monitor an internet user’s network traffic to search for sessions. In this way, the attacker is able to get ahold of a session cookie and use it to take over the session.
- Session fixation** – In a session fixation attack, the criminal creates a session ID and tricks the user into starting a session with it. One common way to do this is to send an email to the user with a link to a login form for the website the attacker wants to access. The user logs in with the phony session ID, giving the attacker a way in the door.
- These are some of the most common methods of session hijacking.

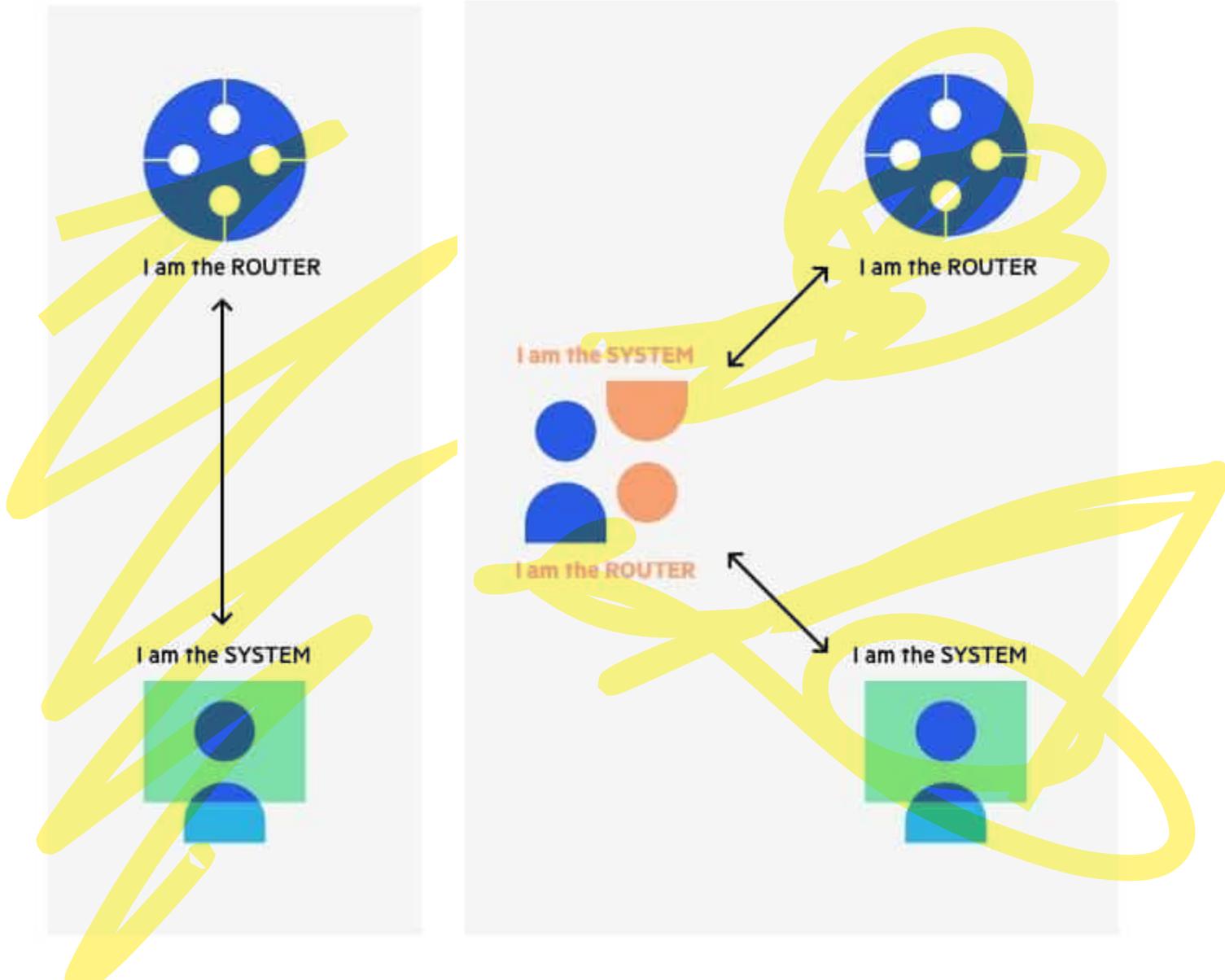
# 27. ARP Spoofing

- **What is the ARP Protocol?**
- Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address, and vice versa. Most commonly, devices use ARP to contact the router or gateway that enables them to connect to the Internet.
- Hosts maintain an ARP cache, a mapping table between IP addresses and MAC addresses, and use it to connect to destinations on the network. If the host doesn't know the MAC address for a certain IP address, it sends out an ARP request packet, asking other machines on the network for the matching MAC address.
- The ARP protocol was not designed for security, so it does not verify that a response to an ARP request really comes from an authorized party. It also lets hosts accept ARP responses even if they never sent out a request. This is a weak point in the ARP protocol, which opens the door to ARP spoofing attacks.

## **What is ARP Spoofing (ARP Poisoning)???**

- An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices. The attack works as follows:
- The attacker must have access to the network. They scan the network to determine the IP addresses of at least two devices—let's say these are a workstation and a router.
- The attacker uses a spoofing tool, such as Arpspoof or Driftnet, to send out forged ARP responses.
- The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker's MAC address. This fools both router and workstation to connect to the attacker's machine, instead of to each other.
- The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with each other.
- The attacker is now secretly in the middle of all communications.

The ARP spoofing attacker pretends to be both sides of a network communication channel



- The ARP spoofing attacker pretends to be both sides of a network communication channel
- Once the attacker succeeds in an ARP spoofing attack, they can:
  - **Continue routing the communications as-is**—the attacker can sniff the packets and steal data, except if it is transferred over an encrypted channel like HTTPS.
  - **Perform session hijacking**—if the attacker obtains a session ID, they can gain access to accounts the user is currently logged into.
  - **Alter communication**—for example pushing a malicious file or website to the workstation.
  - **Distributed Denial of Service (DDoS)**—the attackers can provide the MAC address of a server they wish to attack with DDoS, instead of their own machine. If they do this for a large number of IPs, the target server will be bombarded with traffic.

# 28. DoS Attack

- **What is a denial-of-service attack?**
- A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning.
- DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to additional users.
- A DoS attack is characterized by using a single computer to launch the attack.

## How does a DoS attack work?

- The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests. The multiple attack vectors of DoS attacks can be grouped by their similarities.

DoS attacks typically fall in 2 categories:

- **Buffer overflow attacks**
- An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in denial-of-service.
- **Flood attacks**
- By saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service. In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

# How can you tell if a computer is experiencing a DoS attack?

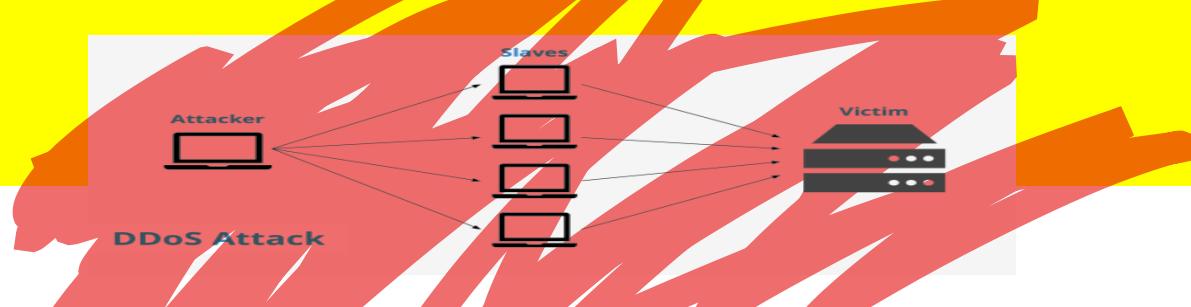
- While it can be difficult to separate an attack from other network connectivity errors or heavy bandwidth consumption, some characteristics may indicate an attack is underway.

## Indicators of a DoS attack include:

- Atypically slow network performance such as long load times for files or websites
- The inability to load a particular website such as your web property
- A sudden loss of connectivity across devices on the same network

## 29. DDOS Attack

- A **distributed denial-of-service (DDoS) attack** is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
- In **2015** and **2016**, a criminal group called the **Armada Collective** repeatedly extorted banks, web host providers, and others in this way.
- in **2016**, **Dyn**, a major domain name system provider — or DNS — was hit with a **massive DDoS attack that took down major websites and services, including AirBnB, CNN, Netflix, PayPal, Spotify, Visa, Amazon, The New York Times, Reddit, and GitHub.**
- The **gaming industry** has also been a target of DDoS attacks, along with software and media companies.
- DDoS attacks are sometimes **done to divert the attention of the target organization**. While the **target organization focuses on the DDoS attack, the cybercriminal may pursue a primary motivation such as installing malicious software or stealing data.**



# 30. Advanced Persistent Threat

- What is an APT
- An advanced persistent threat (APT) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data.
- The targets of these assaults, which are very carefully chosen and researched, typically include large enterprises or governmental networks. The consequences of such intrusions are vast, and include:
  - Intellectual property theft (e.g., trade secrets or patents)
  - Compromised sensitive information (e.g., employee and user private data)
  - The sabotaging of critical organizational infrastructures (e.g., database deletion)
  - Total site takeovers

- **How an APT attack works?**

- Attackers executing APTs typically take the following sequential approach to gain and maintain ongoing access to a target:
- **Gain access:** APT groups gain access to a target by targeting systems through the internet. Normally, through spear phishing emails or via an application vulnerability with the intention of leveraging any access by inserting malicious software into the target.
- **Establish a foothold:** After gaining access to the target, threat actors use their access to do further reconnaissance. They begin exploiting the malware they've installed to create networks of backdoors and tunnels that they can use to move around unnoticed. APTs may use advanced malware techniques such as code rewriting to cover their tracks.
- **Gain even greater access:** Once inside the targeted network, APT actors may use methods such as password cracking to gain administrative rights. This, in order to control more of the system and get even deeper levels of access.
- **Move laterally:** Once threat actors have breached their target systems, including gaining administrator rights, they can then move around the enterprise network at will. Additionally, they can attempt to access other servers, as well as other secure areas of the network.
- **Stage the attack:** At this point, the hackers centralize, encrypt and compress the data so they can exfiltrate it.
- **Take the data:** The attackers harvest the data and transfer it to their own system.
- **Remain until they're detected:** The cybercriminals can repeat this process for long periods of time until they're detected, or they can create a backdoor so they can access the system again at some point.

# 31. Mobile Codes

- **What is Malicious Mobile Code and How Does It Work?**
- Malicious mobile code is becoming a popular way to get malware installed on a computer. Malicious mobile code is malware that is obtained from remote servers, transferred across a network, and then downloaded on to your computer. This type of code can be transmitted through interactive Web applications such as ActiveX controls, Flash animation, or JavaScript.
- **Malicious Mobile Code Focus**
- Malicious mobile code focuses on the security issues that relate to ActiveX controls, Flash animation, JavaScript, and Java Applets. The security issues are concerns related to the ability of these programs to read from and write to files and folders on your computer's hard drive. There are also security concerns with regard to the ability of these programs to run and attach programs, which provides a high risk potential for the distribution of malicious mobile code.
- Although there are security patches that address these concerns, computer users often do not upgrade the service patches due to a number of reasons. They may not be aware of new security patches for download or they may use the default security settings on their browsers which are set to allow these programs to run automatically when a website is visited.
- The developers of malicious mobile code are aware of these types of vulnerabilities that are created by users and organizations that do not employ Internet and Web rules when their workers surf the Internet. As a result, they use malicious mobile code to exploit these vulnerabilities.

- **How Malicious Mobile Code Works**
- Malicious mobile code criminals are not only well-versed in computer programming, they are also knowledgeable in marketing techniques that are based on how Internet surfers think. These are marketing strategies that appeal to the Internet surfer's interests.
- Armed with this knowledge, **malicious mobile code** criminals program codes that install malware into items of interest such as free screensavers, music downloads, games, pornography, and other applications that are accessed on the Internet. All of these applications generally require interactive plug-ins such as ActiveX, JavaScript, or Flash, and they exist on websites that are infected with malware. Once the user clicks on the website and uses these applications, the malware is installed without the user's permission and is usually the initial step to a combined malware attack. The malware is installed on the user's computer and then it generates additional malware such as spyware, keylogging, adware, and other malicious software. This allows the intruder to access personal and financial information, passwords, logins, and other sensitive data.

- **How to Fight Malicious Mobile Code**
- You can help to combat malicious mobile code by keeping your antivirus program updated and changing your browser configuration settings to block interactive applications such as JavaScript from running automatically. Additionally, keep up on the patch updates and try employing a sandbox technology.
-

# 32. Anonymity Networks

- What Does Anonymity Network Mean?
- An anonymity network enables users to access the Web while blocking any tracking or tracing of their identity on the Internet. This type of online anonymity moves Internet traffic through a worldwide network of volunteer servers. Anonymity networks prevent traffic analysis and network surveillance - or at least make it more difficult.
- One open-source anonymity software free to public use is known as Tor. Tor software conceals the user's location and/or usage. Another anonymity network is Freenet, which enables users to anonymously publish "freesites" as well as share files and chat on forums. Still another anonymity network is I2P. I2P identity-sensitive networks are at once distributed and dynamic in nature and they route traffic through other peers.

In order to use Tor, users must run onion routing. This technology encrypts and then rebounds communications onto a network of relays run by volunteers throughout the world. Users who want their Internet searches to remain private use anonymity networking. Within the Tor network, Internet traffic is sent to various routers, one at a time. The Tor node, or exit relay, shows up as the actual communication originator rather than the sender.

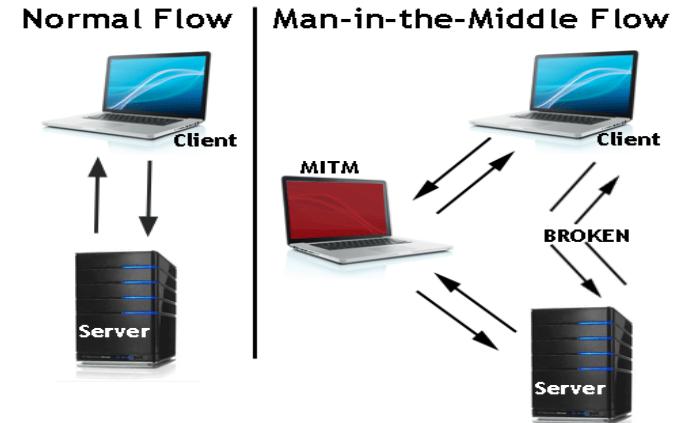
# Man in the Middle attack

- What Is a Man-in-the-Middle Attack?
- A **man-in-the-middle attack** is a type of cyberattack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM.

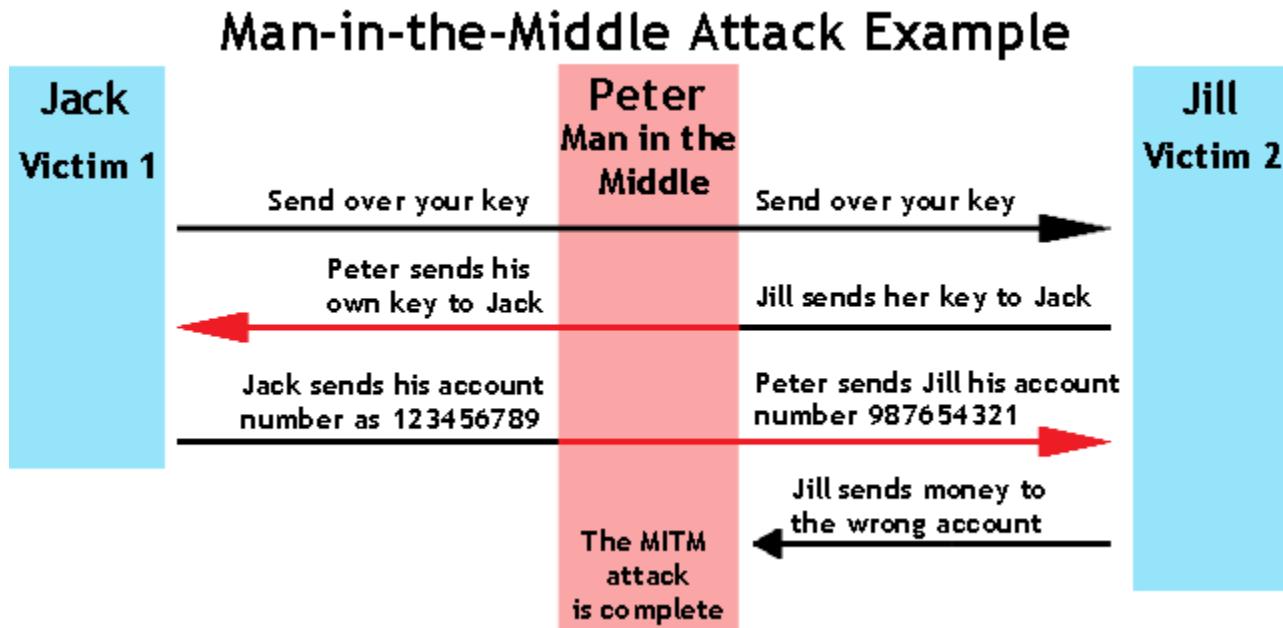
## Key Concepts of a Man-in-the-Middle Attack

- Man-in-the-middle is a type of eavesdropping attack that occurs when a malicious actor inserts himself as a relay/proxy into a communication session between people or systems.
- A MITM attack exploits the real-time processing of transactions, conversations or transfer of other data.
- Man-in-the-middle attacks allow attackers to intercept, send and receive data never meant to be for them without either outside party knowing until it is too late.

- In the image above, you will notice that the attacker inserted him/herself in-between the flow of traffic between client and server. Now that the attacker has intruded into the communication between the two endpoints, he/she can inject false information and intercept the data transferred between them.
- Below is another example of what might happen once the man in the middle has inserted him/herself.



- The hacker is impersonating both sides of the conversation to gain access to funds. This example holds true for a conversation with a client and server as well as person-to-person conversations. In the example above, the attacker intercepts a public key and with that can transpose his own credentials to trick the people on either end into believing they are talking to one another securely.



- **Man in the middle attack prevention**
- Blocking MITM attacks requires several practical steps on the part of users, as well as a combination of encryption and verification methods for applications.
- For users, this means:
  - Avoiding WiFi connections that aren't password protected.
  - Paying attention to browser notifications reporting a website as being unsecured.
  - Immediately logging out of a secure application when it's not in use.
  - Not using public networks (e.g., coffee shops, hotels) when conducting sensitive transactions.
- For website operators, secure communication protocols, including TLS and HTTPS, help mitigate spoofing attacks by robustly encrypting and authenticating transmitted data. Doing so prevents the interception of site traffic and blocks the decryption of sensitive data, such as authentication tokens.
- It is considered best practice for applications to use SSL/TLS to secure every page of their site and not just the pages that require users to log in. Doing so helps decreases the chance of an attacker stealing session cookies from a user browsing on an unsecured section of a website while logged in.'

# Dark Web

## What Is the Dark Web?

- The dark web refers to encrypted online content that is not indexed by conventional search engines. Sometimes, the dark web is also called the dark net. The dark web is a component of the deep web that describes the wider breadth of content that does not appear through regular Internet browsing activities.
- Specific browsers, such as Tor Browser, are required to reach the dark web.
- Using the dark web often provides considerably more privacy than just using Tor to access the web. Many dark web sites simply provide standard web services with more secrecy, which benefits political dissidents and people trying to keep medical conditions private. Unfortunately, online marketplaces for drugs, exchanges for stolen data, and other illegal activities get most of the attention.
- Through the dark web, private computer networks can communicate and conduct business anonymously without divulging identifying information, like location.

- The darknets which constitute the dark web include small, friend-to-friend peer-to-peer networks, as well as large, popular networks such as Tor, Freenet, I2P, and Riffle operated by public organizations and individuals.
- Users of the dark web refer to the regular web as Cleernet due to its unencrypted nature.

## The dark web itself: Illegal or not?

- The simple answer? The dark web itself is not illegal\*. What's illegal is some of the activity that occurs on the dark web. There are sites, for instance, that sell illegal drugs and others that allow you buy firearms illegally. There are also sites that distribute child pornography.
- The dark web itself, though, is not illegal. It offers plenty of sites that, while often objectionable, violate no laws. You can find, for instance, forums, blogs, and social media sites that cover a host of topics such as politics and sports which are not illegal.

## Is it illegal to access and browse the dark web?

- Using Tor to access and browse the dark web is not illegal\*. You will, though, have to be cautious. Surfing the dark web might not be illegal. But visiting certain sites, or making certain purchases, through the dark web is illegal.
- If you use the dark web to purchase illegal drugs or firearms, that's illegal. You won't be committing criminal acts, though, if you use the dark web to participate in forums or to read hidden blog posts anonymously. There are exceptions. You could potentially be participating in illegal behavior if you participate in certain forums, especially if it includes threats, hate speech, or inciting or encouraging criminal behavior.
- The key here is to use common sense. If something is illegal outside of the dark web, it will be illegal in this hidden section of the internet, too.

## Is it safe to access and browse the dark web?

- If you're careful, you can safely access and browse the dark web. First, download the Tor browser, which will give you access to dark web sites and keep you anonymous while searching the sometimes-seedier corners of the internet.
- Tor will allow you to visit websites that have the .onion extension. That's why Tor's full name is The Onion Router.
- You might consider investing in a [VPN](#), or virtual private network, too, when accessing and searching the dark web. A VPN helps keeps you anonymous when searching the internet, whether you are scanning the surface web or the dark web. When using a VPN, most likely only you and your VPN provider will know what sites you have visited. While it is legal to use a VPN in the U.S., it is always the user's responsibility to familiarize themselves with other countries' laws before using a VPN outside the U.S.

- Regular browsers can't access dark web websites. Instead, the dark web uses what's called The Onion Router hidden service protocol. "Tor" servers — derived from "The Onion Router" — are undetectable from search engines and offer users complete anonymity while surfing the web. At the same time, dark web website publishers are also anonymous thanks to special encryptions provided by the protocol.
- When you access the dark web, you're not surfing the interconnected servers you regularly interact with. Instead, everything stays internal on the Tor network, which provides security and privacy to everyone equally.
- Worth noting: Dark web website addresses end with .onion instead of the surface web's .com, .org, or .gov, for example.
- What's on the dark web?
- The dark web operates with a high degree of anonymity. It hosts harmless activities and content, as well as criminal ones.
- For instance, one dark web website might provide complex riddles. Another might be a kind of book club that makes eBooks look more professional. Yet another might offer a forum for people who believe free speech is threatened.
- But the dark web is better known for dark content — meaning, illegal and sometimes disturbing content. For instance, here's a sample of illegal things you can find on the dark web.
- **Stolen information.** When there's been a data breach, there's a chance the accessed information — from Social Security numbers to bank card numbers — will end up for sale on the dark web. You can also buy things like log-in credentials, hacked Netflix accounts, and more.
- **Illicit substances.** Illegal drugs — and prescription drugs — are peddled on the dark web. You might also find toxic chemicals that can cause other types of damage.
- **Disturbing and dangerous items and services.** It can get ugly fast. Things like gore, murderers-for-hire, human trafficking, child pornography, body parts, counterfeit goods, and guns for sale can be found on the dark web.
- In short, you can buy just about anything you can imagine — including things you'd probably be better off not imagining.
- What makes it possible to do business on the dark web? Financial transactions use Bitcoin, the cryptocurrency that helps assure buyers and sellers anonymity.

## Is the dark web safe?

- The dark web may be safe in some cases — think, legitimate content — but not in others.
- Here are a few safety issues to consider.
- **Criminal element.** There's a chance you will find websites run by criminals. Beyond selling illegal goods and services, they may seek to exploit you and steal from you.
- **Breaking the law.** You can be prosecuted for things you do on the dark web. It's important to behave in an appropriate and legal manner.
- **Suspicious links.** If you click on any links, you may be taken to material you might not want to see. It's also possible that clicking a link or downloading a file could infect your device with malware.
- **Law enforcement.** Law enforcement officials operate on the dark web to catch people engaged in criminal activity. Like others on the dark web, law enforcement can do their work under a cloak of anonymity.
- If you decide to venture to the dark web, it's smart to be selective about the websites you access.

## Accessing the dark web with Tor browser

- Getting to the dark web is actually a lot easier than you might think. All you have to do is download a dark web browser, like the Tor browser.
- Once you install a dark web browser on your device, it functions just like a regular browser: type in a URL, and off you go.
- However, finding the material you're looking for on the dark web is more difficult than using a search engine like Google. The dark web doesn't have an index or ranking system to help you find what you need.
- There are such things as dark web search engines. One called the Uncensored Hidden Wiki offers some guidance to content on the dark web, but it may include illegal websites.

- **Advantages of the Dark Web**

- The dark web helps people to maintain privacy and freely express their views. Privacy is essential for many innocent people terrorized by stalkers and other criminals. The increasing tendency of potential employers to track posts on social media can also make it difficult to engage in honest discussions publicly. Finally, the popularity of the dark web with criminals makes it a perfect way for undercover police officers to communicate.

- **Disadvantages of the Dark Web**

- The dark web empowers ordinary people, but some people will inevitably abuse that power. The dark web can make it easier to commit some of the worst crimes. For example, the combination of the dark web and cryptocurrencies theoretically makes it much easier to hire someone to commit a murder. While the dark web promises privacy to its users, it can also be used to violate the privacy of others. Private photos, medical records, and financial information have all been stolen and shared on the dark web.

- Browsing the dark web can be dangerous
- There are people and things on the dark web that you'll want to avoid. Here are a few of them:
- **Viruses.** Some websites could infect your devices with viruses, and there are a lot of [different types](#) of viruses to watch out for. Remember to never download anything from websites you don't trust.
- **Hackers.** You can find hacker forums on the dark web. You can hire computer hackers to do illegal activities. Not surprisingly, a lot of these people would be willing to hack your devices.
- **Webcam hijacking.** A website on the dark web may try to get a remote administration tool — also known as a "RAT" — onto your device. That can lead to someone hijacking your webcam — essentially, letting them see what you're up to through your device's camera lens. It's a smart practice to cover your webcam with a piece of paper or tape if you're not using it.
- Dark web content may be illegal
- Anytime you're in the company of illegal drugs, illegal content, and other sordid online activities, you could risk landing in legal trouble.
- A mistaken keystroke or simple curiosity might not be a reliable defense. Here are two examples of dark web content and activities that would raise legal concerns.
- Sharing pictures and videos of child pornography. In one FBI arrest, the perpetrator traded material on a website with more than 100,000 registered users. The FBI busted him.
- Purchasing illegal goods or services. If you buy illegal drugs or hire a hit man, you can be arrested for committing an illegal act. But browsing a website that offers those two things would not be illegal.

- Dos and don'ts on the dark web
- Law enforcement officials have an interest in stopping illegal activity on the dark web. When they do, there are legal consequences.
- Here are some notable cases where law enforcement took down criminals doing business on the dark web.
- **Silk Road.** This online black market sold illegal drugs. It was launched in 2011. Total revenue was estimated at US\$1.2 billion. Founder Ross Ulbricht was convicted and sentenced to life in prison.
- **AlphaBay.** This was another online black market, launched in 2014. It grew to an estimated 10 times the size of Silk Road. Merchandise ranged from drugs to breached data. Alleged founder Alexandre Cazes was arrested. He was found dead in a Thai jail cell, apparently by suicide, several days later.

**Hansa.** This online black market expanded after AlphaBay was shut down and vendors moved to the platform. But Dutch police had already infiltrated the marketplace and seized information tied to its operation. Police shut down Hansa in 2017.

- Why do the dark web exist?
- The dark web operates on the principle of total anonymity. What you do there is your business. With certain precautions, what you do there can't be tracked or traced to you.
- For some people, privacy is a big concern on the internet. They [might want control over the personal information](#) that standard internet service providers and websites collect on them.
- Freedom of speech also is an issue, and some people would make an argument for privacy and anonymity based on the First Amendment. That's one reason why law-abiding citizens might value the privacy of Tor and other dark web browsers.
- Anonymity can have positive effects — like being able to express views that are unpopular, but not illegal. And the dark web helps make things like that possible.
-

# Virtual Private Network (VPN)

- A **VPN**, or **virtual private network**, is a secure tunnel between your device and the internet. VPNs protect your online traffic from snooping, interference, and censorship.
- A virtual private network (VPN) gives you online privacy and anonymity by **creating a private network from a public internet connection**.
- VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable.
- Most important, VPN services establish **secure and encrypted connections** to provide greater privacy than even a secured Wi-Fi hotspot.

- A VPN (virtual private network) is the easiest and most effective way for people to protect their internet traffic and hide their identities online. As you connect to a secure VPN server, your internet traffic goes through an **encrypted tunnel that nobody can see into**, including hackers, governments, and your internet service provider.
- **Consumers use VPNs** to keep their online activity private and ensure access to sites and services that might otherwise be restricted.
- **Companies use VPNs** to connect far-flung employees as if they were all using the same local network at a central office, but with fewer benefits for individuals than a personal VPN.

## Why do you need a VPN service?

- Surfing the web or transacting on an unsecured Wi-Fi network means you could be exposing your private information and browsing habits. That's why a virtual private network, better known as a VPN, should be a must for anyone concerned about their online security and privacy.
- Think about all the times you've been on the go, reading emails while in line at the coffee shop, or checking your bank account while waiting at the doctor's office. Unless you were logged into a private Wi-Fi network that requires a password, any data transmitted during your online session could be vulnerable to eavesdropping by strangers using the same network.
- The encryption and anonymity that a VPN provides helps protect your online activities: sending emails, shopping online, or paying bills. VPNs also help keep your web browsing anonymous.

- **Benefits and advantages of VPN**
- **Change your location**
- Using a VPN **changes your IP address**, the unique number that identifies you and your location in the world. With a new IP address, you can browse the internet as if you were in the UK, Germany, Canada, Japan, or virtually any country, if the VPN service has servers there.
- **Protect your privacy**
- Changing your IP address with a VPN helps **hide your identity** from websites, apps, and services that want to track you. Good VPNs also **hide your activity** from your internet provider, mobile carrier, and anyone else who may be listening, thanks to a layer of strong encryption.
- **Increase your security**
- Using a VPN **protects you from hacking** in many forms, including packet sniffing, rogue Wi-Fi networks, and man-in-the-middle attacks. Travelers, remote workers, and all kinds of on-the-go individuals use a VPN whenever they're on an untrusted network like free public Wi-Fi.
- **Unblock websites**
- If you're in a part of the world that restricts access to Google, Wikipedia, YouTube, or other sites and services, using a VPN will let you regain access to the free internet. You can also use a VPN to break through firewalls on school or office networks.

- **When should I use a VPN?**
- If privacy is important to you, you should use a VPN **every time you connect to the internet**. A VPN app runs in the background of your device so it won't get in the way while you use other apps, stream content, and browse the internet. And you'll have peace of mind knowing your privacy is always protected.
- But here are some situations in which a VPN is especially useful:
  - **While traveling**
  - Exploring the world doesn't mean you have to change the way you use the internet. A VPN lets you use the internet as if you were still in your home country, [no matter how far you travel](#).
  - **While streaming**
  - Using a VPN lets you watch movies and TV on streaming services like [Netflix](#), [Hulu](#), [Amazon](#), and [HBO](#) with freedom from ISP throttling or blocking by your ISP or local Wi-Fi network.
  - **While on public Wi-Fi**
  - Public Wi-Fi hotspots like those in cafes, airports, and parks are common hunting grounds for cybercriminals. Using a VPN on your devices [stops hackers in their tracks](#).
  - **While gaming**
  - Using a VPN unlocks games, maps, skins, and other add-ons that might be restricted on your network. It also [shields you from DDoS attacks](#) and reduces ping and overall lag.
  - **While torrenting**
  - P2P file sharing usually means that strangers can see your IP address and possibly track your downloads. A VPN hides your IP address, letting you [torrent safely and anonymously](#).
  - **While shopping**
  - Some online stores show different prices to people in different countries. With a VPN, you can [find the best deals in the world](#) no matter where you're shopping from.

## How does a VPN work?

- To understand how a VPN works, it helps to first understand how your internet connection works without one.
- **Without a VPN**
- When you access a website without a VPN, you are being connected to that site through your internet service provider, or ISP. The ISP assigns you a **unique IP address** that can be used to identify you to the website. Because your ISP is handling and directing all your traffic, it can see which websites you visit. And your activity can be linked to you by that unique IP address.
- **With a VPN**
- When you connect to the internet with a VPN, the VPN app on your device (also called a **VPN client**) establishes a secure connection with a **VPN server**. Your traffic still passes through your ISP, but your ISP can no longer read it or see its final destination. The websites you visit can no longer see your original IP address, only the IP address of the VPN server, which is shared by many other users and changes regularly.

Here are several key concepts related to VPN that will help you understand how a VPN works and the benefits it provides:

- **Proxying**
  - The VPN server acts like a **proxy**, or stand-in, for your web activity: Instead of your real IP address and location, websites you visit will only see the IP address and location of the VPN server.
  - This makes you more **anonymous** on the internet.
- **Authentication**
  - Establishing a secure connection is a tricky problem solved by clever mathematics in a process called **authentication**.
  - Once authenticated, the VPN client and VPN server can be sure they are talking to each other and no one else.
- **Tunneling**
  - VPNs also protect the connection between client and server with tunneling and encryption.
  - Tunneling is a process by which each data packet is **encapsulated** inside another data packet. This makes it harder for third parties to read in transit.
- **Encryption**
  - Data inside the tunnel is also **encrypted** in such a way that only the intended recipient can decrypt it. This keeps the contents of your internet traffic completely hidden, even from your internet service provider.

- **VPN protocols**
- VPN protocols are the **methods** by which your device connects to the VPN server. Some protocols are better for **speed**, some are better for **security**, and some simply work better under certain network conditions.
- ExpressVPN automatically chooses the best protocol for your network, but you can also choose one manually.
- Popular VPN protocols in use today include:
- [Lightway](#)
- [OpenVPN](#)
- [IKEv2](#)
- [L2TP / IPsec](#)
- [PPTP](#)
- [WireGuard\\*](#)
- [SSTP\\*\\*](#)

- **Types of VPN**
- **Commercial VPN**
- A commercial VPN, also called a personal VPN or a consumer VPN, is a private service offered directly to individuals, usually for a fee.
- ExpressVPN is such a VPN service because it directly caters to the privacy needs of its customers.
- **Corporate VPN**
- A corporate VPN, also called a business VPN, allows an organization's remote employees to connect securely to the internet as if they were physically present in the office.
- Unlike commercial VPNs, however, corporate VPNs are meant to protect the privacy of the company and not necessarily the individual.
- **Self-setup VPN**
- Some tech experts and DIY hobbyists choose to set up their own VPN using their own equipment.
- Self-setup VPNs, however, do not provide the protection of shared IP addresses, server locations in multiple countries, or many other features enjoyed by commercial VPN users.

- **Alternatives to VPN**
- A VPN isn't the only tool that can increase your privacy, security, and/or freedom online.
- **Tor**
- Tor (short for The Onion Router) is a free network of servers, or “nodes,” that randomly route internet traffic between each other in order to obfuscate the origin of the data.
- Using Tor can significantly increase your anonymity, and [using Tor in conjunction with a VPN](#) creates the best possible protection from surveillance.
- The biggest drawback of Tor, however, is speed. Because your traffic is relayed through several hops, you will probably find it inconvenient to stream, download, or torrent with Tor.
- **Proxy services**
- A proxy server is any intermediary between your device and the internet. Unlike a VPN, however, most “proxy services” you'll find are quite slow and don't offer any privacy or security benefits.
- So-called “free proxy services” are especially dangerous, as many will find other ways to [monetize your data](#), like selling it to third parties.
- Neither Tor nor a proxy service can replace the benefits of a VPN. A trustworthy VPN is still the **best privacy solution for most people**.

# Proxy Server

- What's a Proxy Server?
- A proxy server acts as a gateway between you and the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.
- If you're using a proxy server, internet traffic flows through the proxy server on its way to the address you requested. The request then comes back through that same proxy server (there are exceptions to this rule), and then the proxy server forwards the data received from the website to you.
- If that's all it does, why bother with a proxy server? Why not just go straight from to the website and back?
- Modern proxy servers do much more than forwarding web requests, all in the name of data security and network performance. Proxy servers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests. A good proxy server keeps users and the internal network protected from the bad stuff that lives out in the wild internet. Lastly, proxy servers can provide a high level of privacy.

- How Does a Proxy Server Operate?
- Every computer on the internet needs to have a unique Internet Protocol (IP) Address. Think of this IP address as your computer's street address. Just as the post office knows to deliver your mail to your street address, the internet knows how to send the correct data to the correct computer by the IP address.
- A proxy server is basically a computer on the internet with its own IP address that your computer knows. When you send a web request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the web server, and forwards you the web page data so you can see the page in your browser.
- When the proxy server forwards your web requests, it can make changes to the data you send and still get you the information that you expect to see. A proxy server can change your IP address, so the web server doesn't know exactly where you are in the world. It can encrypt your data, so your data is unreadable in transit. And lastly, a proxy server can block access to certain web pages, based on IP address.

- Why Should You Use a Proxy Server?
  - There are several reasons organizations and individuals use a proxy server.
- **To control internet usage of employees and children:** Organizations and parents set up proxy servers to control and monitor how their employees or kids use the internet. Most organizations don't want you looking at specific websites on company time, and they can configure the proxy server to deny access to specific sites, instead redirecting you with a nice note asking you to refrain from looking at said sites on the company network. They can also monitor and log all web requests, so even though they might not block the site, they know how much time you spend cyberloafing.
- **Bandwidth savings and improved speeds:** Organizations can also get better overall network performance with a good proxy server. Proxy servers can cache (save a copy of the website locally) popular websites – so when you ask for [www.varonis.com](http://www.varonis.com), the proxy server will check to see if it has the most recent copy of the site, and then send you the saved copy. What this means is that when hundreds of people hit www.varonis.com at the same time from the same proxy server, the proxy server only sends one request to varonis.com. This saves bandwidth for the company and improves the network performance.
- **Privacy benefits:** Individuals and organizations alike use proxy servers to browse the internet more privately. Some proxy servers will change the IP address and other identifying information the web request contains. This means the destination server doesn't know who actually made the original request, which helps keeps your personal information and browsing habits more private.
- **Improved security:** Proxy servers provide security benefits on top of the privacy benefits. You can configure your proxy server to encrypt your web requests to keep prying eyes from reading your transactions. You can also prevent known malware sites from any access through the proxy server. Additionally, organizations can couple their proxy server with a Virtual Private Network (VPN), so remote users always access the internet through the company proxy. A VPN is a direct connection to the company network that companies provide to external or remote users. By using a VPN, the company can control and verify that their users have access to the resources (email, internal data) they need, while also providing a secure connection for the user to protect the company data.

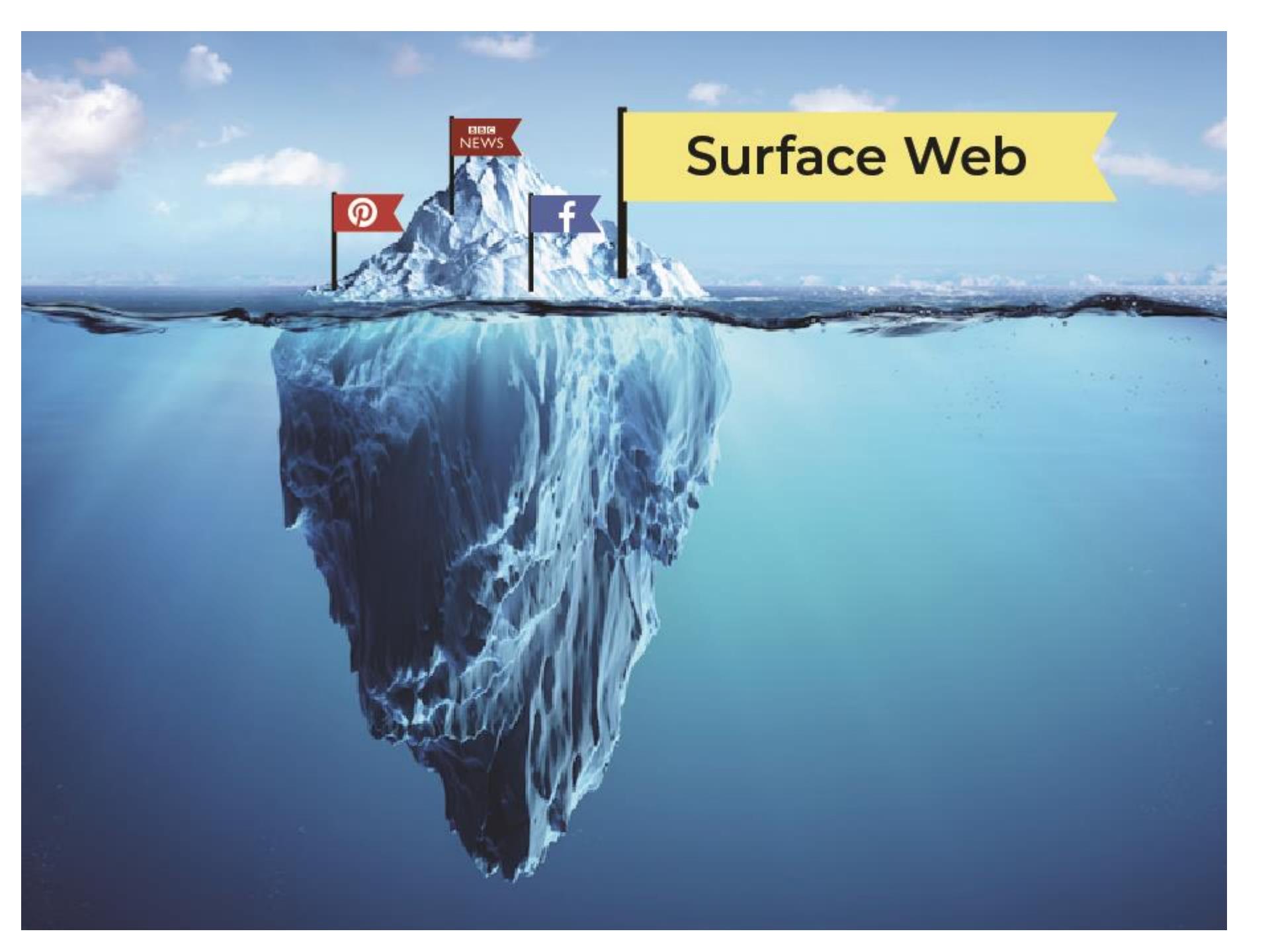
- **Get access to blocked resources:** Proxy servers allow users to circumvent content restrictions imposed by companies or governments. Is the local sportsball team's game blacked out online? Log into a proxy server on the other side of the country and watch from there. The proxy server makes it look like you are in California, but you actually live in North Carolina. Several governments around the world closely monitor and restrict access to the internet, and proxy servers offer their citizens access to an uncensored internet.

- Proxy Server Risks
- You do need to be cautious when you choose a proxy server: a few common risks can negate any of the potential benefits:
- **Free proxy server risks**
  - You know the old saying “you get what you pay for?” Well, using one of the many [free proxy server services](#) can be quite risky, even the services using ad-based revenue models.
  - Free usually means they aren’t investing heavily in backend hardware or encryption. You’ll likely see performance issues and potential data security issues. If you ever find a completely “free” proxy server, tread very carefully. Some of those are just looking to steal your credit card numbers.
- **Browsing history log**
  - The proxy server has your original IP address and web request information possibly unencrypted, saved locally. Make sure to check if your proxy server logs and saves that data – and what kind of retention or law enforcement cooperation policies they follow.
  - If you expect to use a proxy server for privacy, but the vendor is just logging and selling your data you might not be receiving the expected value for the service.
- **No encryption**
  - If you use a proxy server without encryption, you might as well not use a proxy server. No encryption means you are sending your requests as plain text. Anyone who is listening will be able to pull usernames and passwords and account information really easily. Make sure whatever proxy server you use provides full encryption capability.

# • What it is

- To most users, the internet is what they experience through their email client and web browser every day, but there are a number of expansive services that operate in the background and the “web” is just one part of it. Behind that web browser, there are multiple layers that the average user may encounter tangentially or never. The three parts commonly used to divide the web are the Surface Web, the Dark Web, and the Deep Web.
- **The Surface Web** is what users access in their regular day-to-day activity. It is available to the general public using standard search engines and can be accessed using standard web browsers that do not require any special configuration, such as Mozilla Firefox, Microsoft’s Internet Explorer or Edge, and Google Chrome.
- **The Deep Web** is the portion of the web that is not indexed or searchable by ordinary search engines. Users must log in or have the specific URL or IP address to find and access a particular website or service. Some pages are part of the Deep Web because they do not use common top-level domains (TLDs), such as .com, .gov, and .edu, so they are not indexed by search engines, while others explicitly block search engines from identifying them. Many Deep Web sites are data and content stored in databases that support services we use every day, such as social media or banking websites. The information stored in these pages updates frequently and is presented differently based on a user’s permissions.
- **The Dark Web** is a less accessible subset of the Deep Web that relies on connections made between trusted peers and requires specialized software, tools, or equipment to access. Two popular tools for this are Tor and I2P. These tools are commonly known for providing user anonymity. Once logged into Tor or I2P the most direct way to find pages on the Dark Web is to receive a link to the page from someone who already knows about the page. The Dark Web is well known due to media reporting on illicit activity that occurs there. Malicious actors use the Dark Web to communicate about, sell, and/or distribute illegal content or items such as drugs, illegal weapons, malware, and stolen data. However, just like the Surface Web, there are several legitimate activities on the Dark Web as well, including accessing information, sharing information, protecting one’s identity, and communicating with others. Many news organizations operate on the Dark Web to protect confidential sources.

- **How to Access Surface Web?**
- Unlike the deep web and dark web, the surface web is actually accessible to any user on the internet. Also known as “Light Net” or Indexed Web, any user can access the surface web like a cakewalk. It isn’t a no-brainer task unlike the dark web because everything you find on the World Wide Web is the surface web itself.
- It contains pages that are allotted under “indexable” to be readily accessible by any search engine’s result page. As a matter of fact, the surface web percentage is only 4% of the internet! But if these search engines primarily access the surface web through web crawlers or website data then what happens to the rest of 96%?

A photograph of a large iceberg floating in the ocean. The visible portion above the water's surface is small compared to the massive amount submerged below. On top of the visible part, there are four red flags with white icons: Pinterest (P), BBC News, and Facebook (f).

# Surface Web

## Surface Web

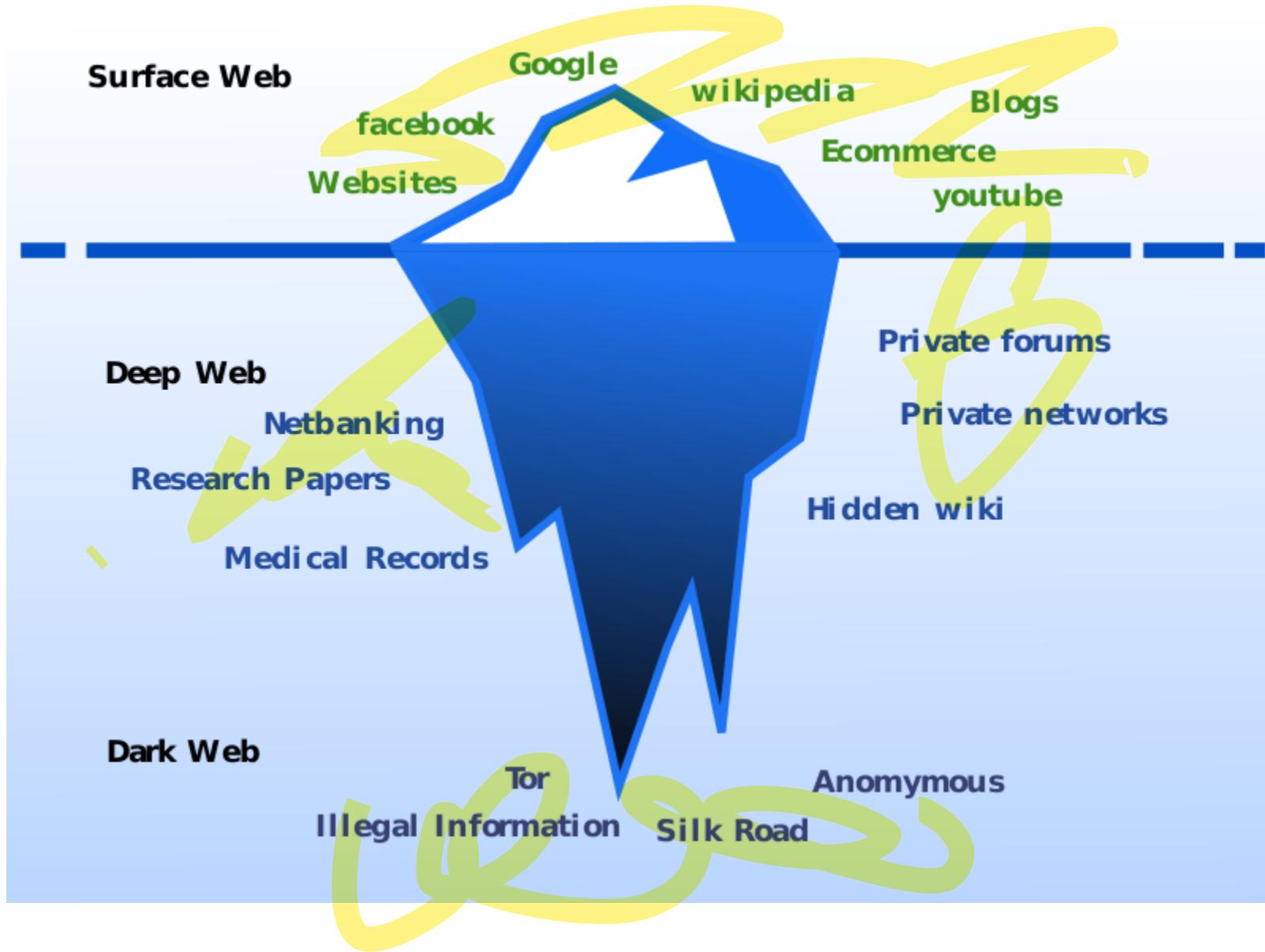
1. The prime and accessible part of the internet.
2. This uses search engines like Google, Bing, Edge, etc.
3. It has publically available websites and web search engines that can crawl and index to find data from websites.
4. Only 4% of pages on the internet are indexed by the search engines here.
5. It contains 19 TB of legal and illegal content on the internet.
6. Comparative to the deep web and dark web, the small scale of illegal activities take place on the surface web.

## Dark Web

1. The hidden part of the internet that requires specific software or tool to gain access.
2. This uses the Tor network and search engines like notEvil, Torch, Ahmia, etc.
3. It has Tor-encrypted websites that cannot be indexed easily to find or read website data.
4. The dark web is 500x times larger than the surface web and comes in 96% of the hidden internet.
5. It contains 7500 TB of illegal content that is restricted from normal users on the internet.
6. Criminals anonymously perform large-scale illegal activities and sell weapons, drugs, including human trafficking and cybercrimes.

- Similarly, in the facts about the surface web, it is ironically home to the deep web. The downsides of the surface web are trolls, stalkers, data exploitation, pornography, identity theft, hacking, the intrusion of privacy, etc. The Internet is the last safe place where no matter what users do, they tend to leave their digital traces. Don't be surprised if you find out that Google is aware of your shoe size.





	<b>Surface Web</b>	<b>Deep Web</b>	<b>Dark Web</b>
<b>Description</b>	Content that search engine can find	Content that search engine cannot find	Content that are hidden intentionally
<b>Known as</b>	Visible web, Indexed web	Invisible web, Hidden web, Deep web	-
<b>Constitutes</b>	Web	Web	Web
<b>Contents</b>	Legal	Legal + Illegal	Illegal
<b>Information found</b>	4%	96%	-
<b>Browsers</b>	Google chrome, Mozilla firefox, opera	-	TOR browser

# • Proxy Server

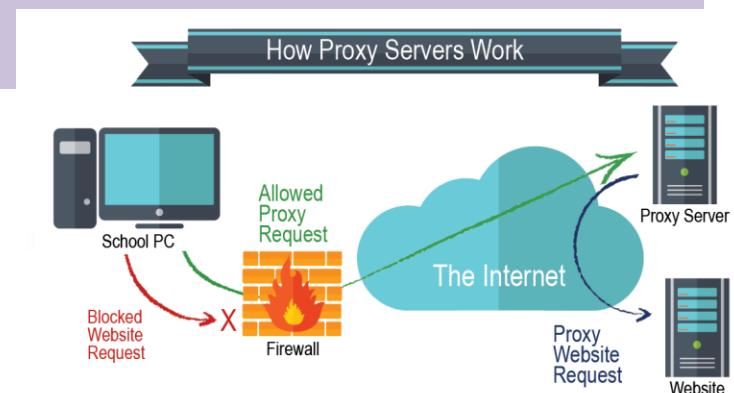
- A proxy server is a computer on the web that redirects your web browsing activity. Here's what that means.
- Normally, when you type in a website name (Amazon.com or any other), your Internet Service Provider (ISP) makes the request for you and connects you with the destination—and reveals your real IP address, as mentioned before.
- When you use a proxy your online requests get rerouted.
- While using a proxy, your Internet request goes from your computer to your ISP as usual, but then gets sent to the proxy server, and then to the website/destination. Along the way, the proxy uses the IP address you chose in your setup, masking your real IP address.

## Why you might want to use a proxy.

- Here why some people turn to using a proxy—and why you might be interested as well.
- A school or local library blocks access to certain websites and a student wants to get around that.
- You want to look at something online that interests you...but you would prefer it couldn't be traced back to your IP address and your location.
- You're traveling abroad and the technology set up in the country you're in prevents you from connecting to a website back home.
- You want to post comments on websites but you do not want your IP address to be identified or your identity tracked down.
- Your employer blocks access to social media or other sites and you'd like to bypass those restrictions.

## Why you might not want to use one

- You should keep in mind that your employer, your ISP and other networks might object to your using a proxy. Just because you can do it, doesn't mean you should. And in some cases, websites will blacklist IP addresses they suspect or know are from a proxy.



# UNIT 2

# Cyber Crime

- **What is Cyber Crime?**
- Cyber crime is broadly defined as any illegal activity that involves a computer, another digital device or a computer network.
- Cyber crime includes common [cyber security threats](#) like social engineering, software vulnerability exploits and network attacks. But it also includes criminal acts like hacktivist protests, harassment and extortion, money laundering, and more.
- Cyber crime targets both individuals and companies.
- Typically, attackers target businesses for direct financial gain or to sabotage or disrupt operations.
- They target individuals as part of large-scale scams, or to compromise their devices and use them as a platform for nefarious activity.

- **COMMON EXAMPLES OF CYBERCRIME**
- **A) Malware**
- A computer virus infects computer systems, corrupts files, and messes with the general functioning of the computer. It also replicates itself to corrupt other devices and systems. A virus is malware that encompasses malicious software, programs, or codes written to damage or corrupt data, steal it, and make money in the bargain. This also includes ransomware that will need you to pay a ransom to decrypt data that has been locked or adware that will spam you with unnecessary ads.
- **B) Phishing**
- Phishing campaigns are ones where spam mails or any other forms of communication crowd inboxes and trick recipients into doing things that will put security at risk. These emails or communications contain infected attachments or links to sites or viruses. They may also ask for confidential information. In spear-phishing, campaigns trick specific targets into putting the individual or organizational security in jeopardy. Spear-phishing campaigns are crafted to look very trustworthy and do not contain any apparent clues to show they are a hoax.

- **C) Identity theft and fraud**
- To commit such crimes , access to personal data serves as the primary fuel. The different types of cybercrimes that help to get access are:
- ● **Phishing:** Fraudulent messages and links are used as baits to lure victims to sites where they have to disclose personal information like usernames and, passwords.
- ● **Pharming:** A more profound step, pharming uses malware to redirect users to fake websites where they pass their details used for malicious activities.
- ● **Keylogging:** It logs all the critical information you type and stores it for cybercriminals to access.
- ● **Sniffing:** If you connect to an unsecured and unencrypted Wi-Fi(for.e.g.-in a public space), hackers can steal data by sniffing through internet traffic with the help of special tools.

- **D) Cyber Bullying**
- It includes all kinds of online harassment like sexual harassment, stalking, doxing, which means exposing personal information with consent and framing (hacking into someone's social media account and creating fake posts).
- **E) Crypto Jacking**
- A tool that hackers use to break into a device and use it to mine cryptocurrency without consent or personal knowledge. JavaScript is used by crypto miners to infect a device after a user visits the infected website. The user will incur huge bills and also performance issues and, in the bargain, inflated profits for cybercriminals.

- **F) Cyber Extortion**
- It is exactly what it sounds like-a a digitized version of money extortion. Ransomware is one of the most common forms to encrypt files and then extort money to unlock them. Blackmailing victims by revealing their personal information, photographs, videos, and threatening business by DDoS attacks (bringing down a system or network) are some other ways of cyber extortion.
- **G) Cyber Espionage**
- As mentioned earlier, cybercriminals are state-sponsored groups that penetrate the complicated matrix of networks of countries and renowned organizations to create war, conflict, differences and other frightening things in the world.

# Cyber Attacks methodology/Process

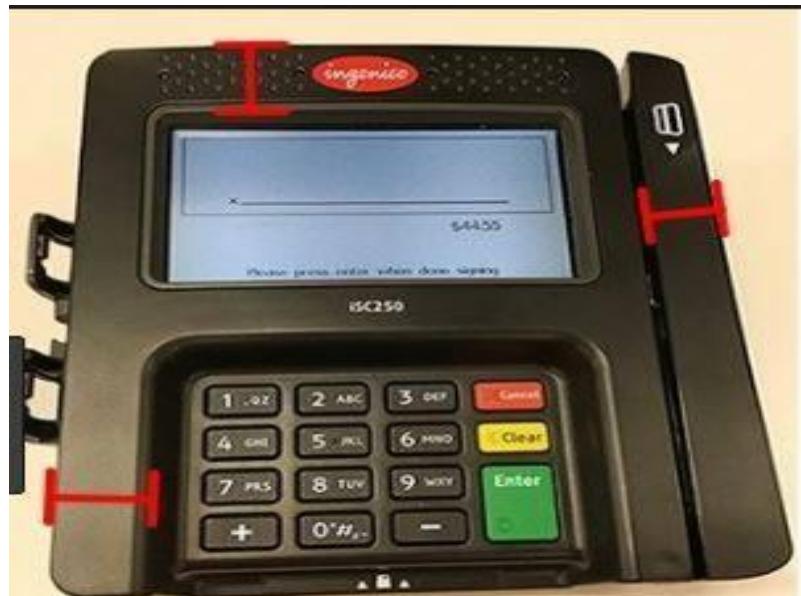
- The Cyber attack process is a management tool required to better conceptualize and understand how the cyber intrusion takes place.
- It provides a clear and systematic way to security professionals to detect and prevent cyber intrusions and continuously improve the network security.
- As we all know that there is a never ending tussle between the security experts and the cybercriminals but we all need to develop a safeguard mechanism so that we can protect ourselves in this dangerous battleground.

- The cyber attack process consists of seven stages which the attacker uses to attack the target. The Cyber attack process is popularly known as Cyber Kill Chain developed by Lockheed-Martin in 2011 . We anatomize cyber attack via a process lens and the seven stages are described as follows:
- **Reconnaissance:** Reconnaissance is the first stage in the cyber attack process in which the attacker selects its target and tries to gather as much information as much he can long before the actual attack. The attacker tries to find out the loopholes and vulnerabilities by analyzing the security defense of the target's network, resources and other technicalities. Some of its examples are: email harvesting, port scanning, vulnerability scanning etc.
- **Weaponization:** Weaponization is the second stage where the attacker with great care crafts a payload or malware meeting the specific requirements of the network to be targeted. The attacker creates the weapon based on the information gathered in the first step as he has already found the loopholes and vulnerabilities in this step. Some of its examples are: couple infected document with a phishing mail, malware distributed via USB drive, couple an exploit with backdoor etc.

- **Delivery:** Delivery is the third stage where the actual transmission of weapon occurs. Using possible intrusion means such as USB drive, mail attachments, websites, exploits etc. the attacker strikes the victim. Some of its examples are: sending the phishing mail, distributing malware via USB stick etc.
- **Exploitation:** Exploitation is the fourth stage where the attacker triggers the actual code locally or remotely to exploit discovered weakness in the environment. The impact of the code execution varies depending on the strength of malware or payload used. The example is: exploiting weakness by triggering code.
- **Installation:** Installation is the fifth stage but it is optional as it depends on the type of malware. If the exploitation is successful then the weapon code installs itself and some additional malice files on the target system. Example: Backdoor installation.
- **Command and Control:** Command and Control is the sixth stage where that attacker after infection gains control on the target system and remotely controls it. The connecting channel between the target system and the remote attacker allows the attacker to perform activities which pleases them. Example: A command channel enables remote control over target system.
- **Actions on Objective:** This is the final stage of cyber attack process where the attacker carries out the actions for which the attack was intended. The goals or objectives are based on attack. Examples: denial of service, information destruction, financial gain etc.

# Credit Card Fraud

- **What Is Credit Card Fraud?**
- Credit card fraud is when someone uses your credit card or credit account to make a purchase you didn't authorize. This activity can happen in different ways:
- If you lose your credit card or have it stolen, it can be used to make purchases or other transactions, either in person or online.
- Fraudsters can also steal your credit card account number, PIN and security code to make unauthorized transactions, without needing your physical credit card. (Unlawful transactions like these are known as card-not-present fraud.)



**SUSPICIOUS**



**SAFE**



## **What Is Identity Theft?**

- [Identity theft](#) involves the use of illegally obtained information about you, like your name, birthday, Social Security number, credit card numbers and more, in order to use existing credit accounts or open new ones in your name. When this happens, criminals capture the spending power of your credit while you get stuck with the bill.

## **What to Do if You're a Victim**

- Because credit card fraud can happen at any time, even when your card is still safely in your wallet, it's important to monitor all your credit card accounts regularly.
- If you discover someone has made unauthorized charges on your credit card account, you should:
- Immediately [contact the credit card company](#). While card issuers are constantly on the lookout for fraud and will investigate if you catch something they don't, most also offer [zero-liability policies](#), meaning you won't be responsible for any fraudulent charges on your accounts. The [Avant Credit Card](#) and Chase Sapphire Preferred® Card, among many others, offer fraud liability coverage for unauthorized purchases. What's more, federal law limits your liability for fraudulent credit card charges. If someone uses your lost or stolen credit card before you report it missing to the card issuer, you can only be held responsible for \$50 of any fraudulent charge. If you report the loss before the card is used, you're not responsible for any charges, nor are you liable if it's just the card number that's stolen and used.

- Change your online passwords and PINs to prevent fraudsters from doing any further damage.
- Closely monitor account activity, and consider contacting Experian to put an [initial security alert](#) on your credit report. This can be especially helpful if you're not sure how your information was compromised. Whichever credit bureau you contact will notify the other two major bureaus of your request.
- Keep an eye on your bank statements, and if you notice signs of fraud, notify your bank immediately.
- Request a copy of your credit report. Often, signs of fraud—such as new accounts you don't recognize—will show up on credit card statements first, soon to follow on your credit reports. When you request a fraud alert, you will also get a copy of your credit report. Did you know you can also get a [free copy of your Experian credit report](#) at any time, too?
- If something you see causes you to believe you're a victim of identity theft (such as someone opening a credit card in your name), follow all the steps above, plus:
  - Add a fraud alert to your credit report by visiting our [fraud center](#).
  - If you find fraudulent accounts or inquiries on your credit report, contact each creditor directly to make them aware of the fraud. If you're a member of [Experian](#), you'll also have access to a dedicated Fraud Resolution Agent, who will work with you to correct fraudulent information with your creditors.
  - Consider reporting the theft by filing a police report and document all contacts you make with credit bureaus, creditors and authorities regarding the crime. You can also [report identity theft to the Federal Trade Commission](#), which separately tracks identity crimes. If your wallet or purse is lost or stolen, immediately notify your bank and credit card companies. You should never carry your Social Security card with you, but in case it's lost or stolen, contact the Social Security Administration and consider placing a [fraud alert](#) on your credit report.

- **Types of Credit Card Fraud**

- Fraudsters are creative people, and they've come up with many ways to pilfer your personal information and destroy your hard-earned good credit, including:
- **Stealing a credit card:** You look away for a moment and your wallet disappears off the store counter where you placed it while making a purchase. Or, you forget to zip up your purse in a crowd and someone slips your wallet from your bag. When your credit card is stolen, you should immediately notify the card issuer.
- **Using a lost or found credit card:** Accidents happen and it's possible a card falls out of your pocket in a parking lot. Someone who finds the card could try to use it. Always [report lost cards to the credit card issuer](#) immediately to reduce the chance of someone doing damage to your balance.
- **Account takeover:** A fraudster can use personal information such as your home address, mother's maiden name, etc., to contact your credit card company or bank, pretend they're you, claim your card has been lost or stolen, or that you've changed addresses, and get the card issuer to send them a new card. Some issuers allow you to have a verbal password when calling them, and this could be a good way to help prevent this type of fraud.

- **Counterfeit cards:** After illegally obtaining your credit card account information with a device called a "[skimmer](#)," fraudsters can create and use a duplicate card. The increased use of chip-and-PIN (aka EMV) technology in the U.S. has reduced this type of fraud.
- **Intercepting mailed cards:** Although credit card companies try to protect cards in transit, a new card can still be stolen from your mailbox.
- **Fraudulent applications:** Using your name, birth date, Social Security number and other personal information, criminals can apply for new credit in your name.
- **Card-not-present:** As point-of-service fraud has decreased because of EMV technology, this type of fraud has increased, payment experts report. Criminals don't need the physical card in order to use it fraudulently. They only need basic info such as the credit card number and cardholder's name to commit mail order or online fraud.

- **How to Identify Credit Card Fraud**
- Fortunately, fraudsters leave signs that you can sometimes detect if you are vigilant. You may be more likely to spot credit card fraud if you:
  - Review your billing statements every month to scan for unfamiliar charges.
  - Watch for bills from unknown sources or calls from collection agencies for accounts you didn't open.
  - Check your credit report regularly and look for unfamiliar inquiries, new accounts you didn't authorize or addresses of locations where you've never lived.
  - Enroll in a [credit monitoring](#) or [identity theft protection](#) service.
  - If you find evidence of fraud on your credit report, visit our [fraud center](#) and dispute any unauthorized or suspicious information.

- **How Will Credit Card Fraud Impact My Credit?**
- Credit card fraud can [negatively affect your credit](#), especially if it takes you a while to notice. The good news is you can minimize the impact by taking the steps noted above. Credit card fraud can affect your credit in following ways:
- Late payments on your credit report: If a fraudster uses your personal information to open a credit card with no intention of ever paying a bill, and that card is reported to the credit bureaus, your credit score could plummet. Payment history is the most [important factor in credit scores](#), accounting for 35% of your FICO® Score<sup>®</sup>, the most commonly used credit scores.
- High credit utilization: If a fraudulent credit card, or one of your own cards, is being used to run up charges you didn't authorize, that can affect your credit utilization. Your [credit utilization ratio](#), which measures the amount of credit you're using relative to your credit limits, is the second most important factor in your credit scores. If fraudulent activity raises your total credit utilization to over 30%, your credit scores could suffer, at least temporarily.

- **Tips for Avoiding Credit Card Fraud:**
- Don't give out your credit card number online unless the site is secure and reputable. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but provides some assurance.
- Don't trust a site just because it claims to be secure.
- Before using the site, check out the security/encryption software it uses.
- Make sure you are purchasing merchandise from a reputable source.
- Do your homework on the individual or company to ensure that they are legitimate.
- Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.
- Consider not purchasing from sellers who won't provide you with this type of information.
- Check with the Better Business Bureau from the seller's area.
- Check out other websites regarding this person/company.
- Don't judge a person or company by their website; flashy websites can be set up quickly.
- Be cautious when responding to special investment offers, especially through unsolicited e-mail.
- Be cautious when dealing with individuals/companies from outside your own country.
- If possible, purchase items online using your credit card. You can often dispute the charges if something goes wrong.
- Make sure the transaction is secure when you electronically send your credit card number.
- Keep a list of all your credit cards and account information along with the card issuer's contact information. If anything looks suspicious or you lose your credit card(s), contact the card issuer immediately.

# Software Piracy and Legal Issues



Software piracy is the act of **stealing software that is legally protected.**

This stealing includes selling, distributing, modifying or copying the software.

- Software piracy has become a worldwide issue with China, the United States and India being the top three offenders. The commercial value of pirated software is \$19 billion in North America and Western Europe and has reached \$27.3 billion in the rest of the world. According to the [2018 Global Software Survey](#), 37% of software installed on personal computers is unlicensed software.
- Software piracy doesn't require a hacker or skilled coder. Any normal person with a computer can become a software pirate if they don't know about the software laws. With such a widespread impact, it's important to understand what software piracy is and the dangers it presents.

- **Software Piracy – Definition**
- Software piracy is the act of stealing software that is legally protected. This stealing includes copying, distributing, modifying or selling the software.
- Copyright laws were originally put into place so that the people who develop software (programmers, writers, graphic artists, etc.) would get the proper credit and compensation for their work. When software piracy occurs, compensation is stolen from these copyright holders.
- **Software Piracy Regulation**
- Computer piracy is illegal and constitutes a federal crime. The monetary penalties for those who break this law can reach up to \$150,000 per instance of copyright violation.
- **End-User License Agreement**
- The End-User License Agreement (EULA) is a license used for most software. It is a contract between the manufacturer and/or author and the end user. This agreement defines rules for software use and not every agreement is the same. One common rule in most EULAs prohibits users from sharing the software with others.

- Software piracy is stealing. If you or your company are caught copying and/or distributing illegal copies of software, you could be held liable under both civil and criminal laws. If the software owner decides to sue you or your company, the owner can seek to stop you from using/distributing its software immediately and can also request monetary damages.
- In addition to legal consequences, users of pirated or counterfeit software could experience:
- Exposure to software viruses, corrupt disk or defective software
- Inadequate or no product documentation
- No warranties
- Lack of technical support
- Ineligibility for software upgrades offered to properly licensed users

- **Types of Software Piracy**
  - There are five main types of software piracy. This variety of pirating techniques explains how some individuals purposely pirate software while others may unknowingly be an accomplice.
  - **Softlifting**
    - Softlifting is when someone purchases one version of the software and downloads it onto multiple computers, even though the software license states it should only be downloaded once. This often occurs in business or school environments and is usually done to save money. Softlifting is the most common type of software piracy.
  - **Client-server overuse**
    - Client-server overuse is when too many people on a network use one main copy of the program at the same time. This often happens when businesses are on a local area network and download the software for all employees to use. This becomes a type of software piracy if the license doesn't entitle you to use it multiple times.
  - **Hard disk loading**
    - Hard disk loading is a type of commercial software piracy in which someone buys a legal version of the software and then reproduces, copies or installs it onto computer hard disks. The person then sells the product. This often happens at PC resale shops and buyers aren't always aware that the additional software they are buying is illegal.
  - **Counterfeiting**
    - Counterfeiting occurs when software programs are illegally duplicated and sold with the appearance of authenticity. Counterfeit software is usually sold at a discounted price in comparison to the legitimate software.
  - **Online Piracy**
    - Online piracy, also known as Internet piracy, is when illegal software is sold, shared or acquired by means of the Internet. This is usually done through a peer-to-peer (P2P) file sharing system, which is usually found in the form of online auction sites and blogs.

## The Dangers of Software Piracy

- Software piracy may have a cheaper price point, but there are many dangers that software pirates should be aware of.
- Consequences of software piracy are:
- Increased chances that the software will malfunction or fail
- Forfeited access to support for the program such as training, upgrades, customer support and bug fixes
- No warranty and the software can't be updated
- Increased risk of infecting your PC with malware, viruses or [adware](#)
- [Slowed down PC](#)
- Legal repercussions due to copyright infringement
- Keep your PC secure by only purchasing software from authorized dealers. Be aware of any software's terms and conditions — make sure you agree and adhere to their guidelines. Protect your device from any further threats with [Panda Security's Free Antivirus](#) for your Mac or Windows devices.

- **LEGAL ISSUES AND CHALLENGES**
- **The Issue of Jurisdiction**
- Since the internet is an intangible space, determination of jurisdiction can be problematic. In the case of online copyright infringement, various countries or regions could be involved. The question then arises as to which jurisdiction would be applicable. It could be decided based on the origin of the matter. It could also be decided based on place of storage, or even in the place where the material is finally used or displayed. It is not necessary that what constitutes illegal copyright infringement in one country, would be illegal copyright infringement in another country too. Sometimes different countries can even have conflicting laws. This makes it difficult to punish an individual. There is also the issue of determining whether or not such infringement has taken place. With the increasing complexity of the cyberspace, it becomes very difficult to determine whether or not an individual is responsible for any infringement. After the establishment of an infringement case, the determination of what jurisdiction is to be applied is added trouble. The problem becomes all the more difficult to sort when there are conflicting laws in different countries regarding the matter. And lastly, the lack of feasibility as well as higher costs makes it rather difficult to punish a person. Therefore, it is important to have clear cut rules about the determination of jurisdiction when it comes to online copyright infringement. It is also difficult to determine the work's place of origin
- **The Issue of Public Vs Private Use**
- Under traditional copyright laws, especially the act of 1957, there is a distinction provided between the reproduction of particular content in public and private domains. This distinction allows a person to reproduce copies of copyrighted content in the public domain, with prior permission from the author or original creator. However, the cyberspace makes such distinction difficult. Since one person can transfer material to several people through the internet, the copyright laws regarding public and private spaces have become difficult.

- **The Issue of Rights of Reproduction**
- The right of reproduction is a huge issue on the internet. Distribution of any material over the internet requires the material to be reproduced. Data through the internet is transferred using a technique wherein there is a breakdown in the entire information into small packets. These small packets are then reconstituted to form the entire matter. This technique is called “packet switching”. Packet Switching therefore means that there is reproduction at every stage of transmission of data through a computer. This makes it difficult to have a clear cut idea about the exact rights of reproduction and can be misused in cases of breach.

- **The Issue of Enforcing Liability**
- The major issue with regards to copyright infringement over the internet is liability. To enforce any form of punishment against an offender, it is important to determine where exactly the liability lies. However, in one issue related to copyright infringement over the internet, several people can be involved. Information could go through several layers and several different computers before being transmitted into the public domain. Several people could be involved in such infringements. Quite often; these people could be based in entirely different places[5]. For example, the question is, in a piracy case, whether the liability would lie on the party receiving the information, the party that transmits such information or the act that has been involved in the process. Section 79 of the IT Act 2000 intermediaries will not be liable for any third-party information". However, it does become difficult to determine whether or not the intermediary is at fault. The section, though meant to protect innocent intermediaries, is often misused by criminals for their gains.[6]
- **Implementing harmonious State IPR Laws in India**
- There is a lack of harmony between the state IPR laws about online copyright infringement on the internet. The varying domestic laws regarding digital piracy and copyright infringement n different states make effective implementation very troublesome. Since online copyright infringement usually has several players and could involve multiple offenders from various states, it becomes necessary to have state laws which are in harmony. For example, some states can compel the ISPs to examine the material. Whereas, several other states do not hold that power. This usually leads to the issues of disharmony and delay.

- **Why is internet piracy such a menace?**
- Internet piracy has become a huge copyright issue, in the past few years. The unhindered growth of technology along with the increase in cybercrimes has made internet piracy issues quite common in today's day and age. Here are a few reasons why internet piracy is becoming such a huge problem
- Easy and wide distribution using the internet
- No limits as to the number of people that a material can be distributed to
- Difficult to distinguish between the original and the fake copies
- Hardly any cost associated with the illegal distributing
- Easy to access copyrighted material without the threat of being raced down.

# M-Commerce

- 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.
- 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.

- **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.
- a. 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 as 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.

- b. 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.
- c. 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.

- **Security threats in m-commerce**
- Every mobile commerce transaction is made of three parts, with each raising its own security issue:
- **the user** (the person making a purchase),
- **the server** (the business that owns the app),
- **the connection** (the technology that brings the two above components together).

- Here are five key threats present in today's landscape:
- **Connection** – this part of an m-commerce application is the easiest one to compromise. Hackers can cause data leakages of sensitive user data or business data that could harm your company. How can you deal with it? Check out the tips listed below in the paragraph “20 best practices for securing mobile commerce”. Hint: combining Transport Layer Security (TLS) with certificate pinning makes accessing the data very hard.
- **Payments** – a lack of security here could have many terrible consequences. For example, a compromised payment gateway could cause the user to pay someone else instead of your store. You will never see the money, and they will never get the product – with your reputation on the line.
- **Keyboard** – if the user downloads a third-party keyboard, the content they type can be intercepted. Prevent users from using keyboards that aren't part of their device's operating systems by disabling this option.
- **Copying content to your application** – here's a common scenario: we store a long password in notes (disclaimer: we definitely don't recommend that!), so once we need to use it, we simply copy it from our notes and then use it to access an app or website. Others might have access to the clipboard and intercept your password. You can notify users when clipboard content is used or send a properly formatted message with a code that is automatically placed in the password field.
- **Files saved in device memory** – if someone gets a chance to use another user's device, and your application saves its files in a public place, it's easy to access this data. Avoid saving sensitive data in unencrypted device memory or the cache.

# Security issues in Mobile wallet

- **1) Using Multiple Software Options**
- Similar to laptops and desktops, mobile phones are also working on various hardware and software systems. There are still some people who are using the old versions of iOS and Android globally. And this can lead to various security issues. The devices are not well supportive of the latest mobile security technologies which attract the hackers and fraudsters for exploiting and attacking.
- Again, if mobile applications are secure, the device may not meet the standards, providing you with the [basics of mobile security](#). The mobile devices also need to be secure enough with advanced features to protect you from any kind of frauds. Some of the examples of a secure mobile device include verification codes to mobiles or emails, face scanners, fingerprint scanner, geofencing, voice recognition, etc.
- Hence, look for a smartphone with advanced features regarding the software and hardware for an end to end protection of your payments and accounts.

- **2) Oops! I lost my phone!**
- Today, smartphones are similar to credit cards. It contains all the necessary details like the contact information, names, personal collection of photographs, social media connections, and whatnot.
- Similarly, it also provides complete access to bank accounts, debit cards, and credit cards through various payment apps, mobile wallets, online banking apps, and much more. But what if you misplace your phone at any store, restaurant, or any other crowded place? All your personal details are sure to get leaked right? And this includes all the banking and mobile payment details, which can lead to frauds.
- Not, every person who would find your phone would return it. Hence, it is better to look for smartphones that come with in-built protection to protect your phone, mobile phone wallets, and other fraud activities.
- Rather than looking for a single authentication method, go for a two-factor authentication process for unlocking the phone through facial recognition, fingerprint and iris scan options along with the PIN.

- **3) Inappropriate using habits**
- Even if you have a highly secure mobile phone, the way you use your mobile phone can be problematic regarding payment security. The fraudsters can use the website version of your mobile phone to make purchases or payments. Many mobile phone users use Google Chrome browsers for making payments through mobiles on Android phones. And browsers like Chrome and Safari are highly risky to use for making payments.
- If you are using [mobile phones for making payments](#), for adding to its security, it is essential to use browser detection, which would protect the users from the frauds carried out through insecure mobile browsers. Instead of such browsers, look for secure and advanced mobile apps that come with an updated version. Lastly, there are mobile users who don't use any kind of PIN locks or other security options on their mobile phones, which allows the fraudsters to make frauds when the devices are lost. So, look for an updated payment app and browser for adding to the security of mobile phones.
- **4) Protect your mobile wallet**
- With the introduction of mobile payment options, several payment apps came into existence. Paytm, Google Pay, Apple Pay, PayPal, and many such payment wallets rapidly gained popularity with amazing offers, cashback, discounts, etc. All such applications work when a debit or credit card is added in the mobile wallet. Details like the card number, VCC number, expiry date of the card, etc. when entered in the application through encryption which is carried out through code. Again, the mobile wallet providers also use a token number generated randomly for making a payment which is not visible to the merchants while transactions are carried out.
- The cybercriminals can misuse your account numbers, but when you add any credit or debit card to the payment apps using any public Wi-Fi, the risks increase to a great extent. The criminals can easily spoof off all the details used for making the transaction used while registering. For protecting yourself from such frauds, use your cards with mobile wallets while you are at home or having a personal network secured with a password. Using Virtual Private Network is also the best way to look for security while using a mobile wallet.

- **5) Beware of App Clones**
- Are you sure you have installed the right application on your mobile phone? Or is it one of the app clones? Surprisingly, there are various app clones designed similar to the original apps that provide secure payment options. When any user uses such app clones and registers their banking details in it, it becomes easier for the criminals to carry out fraud activities through credit cards, debit cards, and other personal information. Such app clones come with ridiculous and poor security options that can be easily accessed by the criminals.
- Both Google and Apple come with required protection while you download it for use. But the cybercriminals still have different ways of installing the clone apps that contain the virus for your device. For the iOS devices, the fraudsters use the jail-broken devices to make a fraud payment. And the best way to keep your cellphone away from such app clones is using an anti-malware tool.
- The systems that contain anti-malware tools or software would protect your phone from the installation of any such app clones. Research is still on the way to find the right solution to such malicious clones. Taking an example of one such successful payment app, [Klarna, Sweden-based payment app](#), has recently raised funding with its 3 powerful strategies.
- There are various measures which can help smartphone users from such frauds or cybercrimes. Do your research, improve the strength of your passwords, use the find my phone app, use your personalized network, avoid making payments with public networks, educate your loved ones with safe mobile payment processes, and much more.
- No doubt, there are some security issues people should be concerned about while using mobile phones, it is still much safer compared to the plastic cards you carry in your pockets. If you use the mobile payment options, being little conscious while using it to make a transaction, there are no chances your financial details would be misused by others. So, think twice and act smart while using mobile phones for making a secure payment.

# Security issues in mobile payment m-banking

- 1. Using a fake mobile banking app
- Some scammers have created fake mobile bank apps to get you to enter your password and other private details. Once they have that information, they can turn around and use it to access your real bank account and take out your money. Always read reviews and make sure you're dealing with the real app for your bank before downloading one or trying to log in. You can also try going to your bank's website and clicking on the link to the download page for its mobile app to make sure you're using the right one.
- 2. Using your mobile banking app on public Wi-Fi
- Public Wi-Fi might enable you to save your monthly cell phone data, but it also makes it much easier for hackers to access your phone and see what you're doing. It is possible for them to hack into your phone when you're using cellular data, too, but that is much harder to do. Always stick to cellular data if you need to access your financial accounts in public, or better yet, wait until you're on a private Wi-Fi network to log into your bank account.

- 3. Not updating your phone's operating system or apps
- Installing updates can be a pain and can keep you from accessing your phone or apps for a while. However, you should always do it anyway. Some of these updates are important security patches that fix flaws in an app that might let hackers more easily access your data. Outdated software is also easier to hack in general. Whenever your phone notifies you about an update, install it as soon as it's feasible, especially if it's for your mobile banking app.
- 4. Storing passwords and PINs on your phone
- You might decide to keep a note on your phone with your bank account password or PIN if you're prone to forgetting it, but this is dangerous, too. If you lose your phone and a would-be thief finds it, they can easily gain access to your financial accounts, and you probably won't even notice until your money is already gone. Try to memorize your passwords, especially your bank account password, so you don't need to store them on your phone or computer.
- 5. Using an easy password
- The days when "Password" was considered a secure password are long behind us -- if they ever existed at all. Fortunately, most online accounts, including mobile banking apps, no longer allow you to use such simplistic passwords. You must choose something that has a mix of capital and lowercase letters with some numbers and symbols thrown in. These types of passwords are more difficult to hack, so using one of them helps keep your account secure.
- You should also use different passwords for all of your online accounts -- or at least use a different password for your mobile banking app -- so that hackers who gain access to one of your online accounts can't break into all of them. Changing your password every couple of months, even if you don't need to, can also keep hackers from accessing your banking information.
- 6. Not password protecting your phone
- Modern smartphones let you enter a passcode or open your phone with a fingerprint scanner so that no one else can access your phone without your permission. This extra layer of security can prevent others from hacking into your mobile banking account or gaining access to other personal information stored on your phone that might help them answer your bank's security questions. Take advantage of these security features to keep your bank account and other personal information protected.

- 7. Not signing up for security alerts
- Security alerts are messages sent to your phone or email that tell you about new or suspicious activity regarding your bank account. It might be a login from a new device or a purchase that seems suspicious.
- These alerts can help you quickly identify when **your identity has been compromised** so you can take action to stop the thief from draining your account. Enroll in these alerts if your bank offers them and check your bank accounts regularly for signs of suspicious activity.
- Mobile banking apps are really useful, and they're not going away anytime soon. But they're also not immune to attack. Avoiding the seven above mistakes is crucial if you want your **bank account** to remain private.

# Identity theft

- What Is Identity Theft?
- Identity theft is the crime of obtaining the personal or financial information of another person for the sole purpose of assuming that person's name or identity to make transactions or purchases.
- Identity theft is committed in many different ways.
- Some identity thieves sift through trash bins looking for bank account and credit card statements; other more high-tech methods involve accessing corporate databases to steal lists of customer information.
- Once they have the information they are looking for, identity thieves can ruin a person's credit rating and the standing of other personal information.

- **Types of identity theft**
- Identity theft is categorized in two ways: true name and account takeover. True-name identity theft means the thief uses personal information to open new accounts. The thief might open a new credit card account, establish cellular phone service or open a new checking account to obtain blank checks.
- Account-takeover identity theft is when the imposter uses personal information to gain access to the person's existing accounts. Typically, the thief will change the mailing address on an account and run up a huge bill before the victim realizes there is a problem. The internet has made it easier for identity thieves to use the information they've stolen since transactions can be made without any personal interaction.
- There are many different examples of identity theft, including:
  - **Financial identity theft.** This is the most common type of identity theft. Financial identity theft seeks economic benefits by using a stolen identity.
  - **Tax-related identity theft.** In this type of exploit, the criminal files a false tax return with the Internal Revenue Service (IRS). Done by using a stolen Social Security number.
  - **Medical identity theft.** Where, the thief steals information like health insurance member numbers, to receive medical services. The victim's health insurance provider may get the fraudulent bills. This will be reflected in the victim's account as services they received.
  - **Criminal identity theft.** In this example, a person under arrest gives stolen identity information to the police. Criminals sometimes back this up with a containing stolen credentials. If this type of exploit is successful, the victim is charged instead of the thief.
  - **Child identity theft.** In this exploit, a child's Social Security number is misused to apply for government benefits, opening bank accounts and other services. Children's information is often sought after by criminals because the damage may go unnoticed for a long time.
  - **Senior identity theft.** This type of exploit targets people over the age of 60. Because senior citizens are often identified as theft targets, it is especially important for seniors to stay on top of the evolving methods thieves use to steal information.
  - **Identity cloning for concealment.** In this type of exploit, a thief impersonates someone else in order to hide from law enforcement or creditors. Because this type isn't explicitly financially motivated, it's harder to track, and there often isn't a paper trail for law enforcement to follow.
  - **Synthetic identity theft.** In this type of exploit, a thief partially or completely fabricates an identity by combining different pieces of PII from different sources. For example, the thief may combine one stolen Social Security number with an unrelated birthdate. Usually, this type of theft is difficult to track because the activities of the thief are recorded files that do not belong to a real person.

- **Identity theft techniques**
- Although an identity thief might hack into a database to obtain personal information, experts say it's more likely the thief will obtain information by using social engineering techniques. These techniques includes the following:
  - **Mail theft.** This is stealing credit card bills and junk mail directly from a victim's mailbox or from public mailboxes on the street.
  - **Dumpster diving.** Retrieving personal paperwork and discarded mail from trash dumpsters is an easy way for an identity thief to get information. Recipients of preapproved credit card applications often discard them without shredding them first, which greatly increases the risk of credit card theft.
  - **Shoulder surfing.** This happens when the thief gleans information as the victim fills out personal information on a form, enter a passcode on a keypad or provide a credit card number over the telephone.
  - **Phishing.** This involves using email to trick people into offering up their personal information. Phishing emails may contain attachments bearing malware designed to steal personal data or links to fraudulent websites where people are prompted to enter their information.

- **Some warning signs of being an identity theft victim include:**
- Victims notice withdrawals from their bank account that weren't made by them.
- An impacted credit score.
- Victims don't receive bills or other important pieces of mail containing sensitive information.
- Victims find false accounts and charges on their credit report.
- Victims are rejected from a health plan because their medical records reflect a condition they don't have.
- Victims receive an IRS notification that another tax return was filed under their name.
- Victims are notified of a data breach at a company that stores their personal information.

- **Other Types of Identity Theft**
- There are less common types of identity theft — and you should know them:
- **Child ID Theft** — Children's IDs are extremely vulnerable. The theft could go undetected for several years. By the time they become adults, the damage already has been done.
- **Tax ID Theft** — Thieves can use your Social Security number to falsely file tax returns with the IRS or state government.
- **Medical ID Theft** — Someone could steal your Medicare ID or health insurance member number to receive medical services. It could also trigger fraudulent billing to your health insurance provider.
- **Senior ID Theft** — Typically, ID theft schemes will target seniors, who are in frequent contact with medical professionals or caregivers who have access to personal information or financial documents.
- **Social ID Theft** — Whatever is on your social media platforms — your name, photos and other personal information — can be used to create a phony account.

- **Impact and prevention**
- In addition to the immediate impact of losing money and running up debt, individual victims of identity theft can incur severe intangible costs. Some costs include damage to reputation and credit report, which can prevent victims from getting credit or even finding a job. Depending on the circumstances, identity theft can take years to recover from.
- To protect yourself from identity theft, experts recommend that individuals regularly check credit reports with major credit bureaus, pay attention to billing cycles and follow up with creditors if bills do not arrive on time.
- Additionally, people should:
  - destroy unsolicited credit applications;
  - watch out for unauthorized transactions on account statements;
  - avoid carrying Social Security cards or numbers around;
  - avoid giving out personal information in response to unsolicited emails; and
  - shred discarded financial documents.

# Password Cracking

- **What is password cracking?**
- Password cracking means recovering passwords from a computer or from data that a computer transmits.
- **Password cracking** is the process of **obtaining the correct password** to an account in an unauthorised way. Every password has vulnerabilities, and this makes it easy to **hack**.
- This doesn't have to be a sophisticated method. A brute-force attack where all possible combinations are checked is also password cracking.
- If the password is stored as plaintext, hacking the database gives the attacker all account information

- **Why people crack passwords**
- There are many reasons why attackers want to crack passwords. First, they try to obtain access to restricted data and systems, get a foothold in companies' networks, or just seize control of an account and use it for their own purposes.
- **How long does it take to crack a password**
- With one minute of computation time, an eight-character alphanumeric lowercase word should take five minutes or less on average to guess correctly from among all possibilities in a brute force attack containing 26 English characters; with ten seconds of computations, that same length word would typically take 20 hours or longer on average using brute force guessing without any type of outside help – such as wordlists.

## Two primary forms of password cracking

- One of the most common **types of password attacks** are:
- **Brute force**
- Brute force attacks involve an attacker submitting many possible passwords to test them with the hope of eventually guessing correctly and cracking this password. Brute force attacks very often use a list of commonly-used passwords.
- **Dictionary attacks**
- A **dictionary attack** is when an attacker uses a list of words pulled from sources such as dictionaries, thesauruses, and newspapers to crack passwords.

## Password guessing vs password cracking

- **Password guessing** is the process of entering a password manually by the user to see if it is correct, whereas **password cracking involves using programs or software** to try several combinations of possible passwords at once.

# Password cracking techniques used by hackers

- A typical password cracking attack looks like this:
- Get the password hashes
- Prepare the hashes for a selected cracking tool
- Choose a cracking methodology
- Run the cracking tool
- Evaluate the results
- If needed, tweak the attack
- Go to Step 2
- Now let's discuss the most popular password cracking techniques. There are many cases when these are combined together for greater effect.

- **1. Phishing**
- Phishing is the **most popular technique** that involves **luring the user into clicking on an email attachment** or a link that contains malware. The methods for doing so usually involve sending some important and official-looking email that warns to take action before it's too late. In the end, password-extracting software is installed automatically or the user enters his account details into a look-alike website.
- There are different types of phishing tailored for a particular situation, so we'll look at the few common ones:
- **Spear phishing** targets a particular individual and tries to gather as much personal information as possible before the attack.
- **Whaling** targets senior executives and uses company-specific content, which can be a customer complaint or a letter from a shareholder.
- **Voice phishing** involves a fake message from a bank or some other institution, asking a user to call the helpline and enter his account data.
- **2. Malware**
- As you've seen, malware is often part of the phishing technique too. However, it can work without the "social engineering" factor if the user is naive enough (he usually is). Two of the most common malware types for stealing passwords are **keyloggers** and **screen scrapers**. As their names imply, the former sends all your keystrokes to the hacker, and the latter uploads the screenshots.
- Other types of malware can also be used for password stealing. A backdoor trojan can grant full access to the user's computer, and this can happen even when installing so-called **grayware**. Also known as potentially unwanted applications, these programs usually install themselves after clicking the wrong "Download" button on some website. While most will display ads or sell your web usage data, some might install much more dangerous software.

- **3. Social engineering**
- This password cracking technique **relies on gullibility** and may or may not employ sophisticated software or hardware – phishing is a type of [social engineering](#) scheme.
- Technology has revolutionized social engineering. In 2019 hackers used AI and voice technology to impersonate a business owner and fooled the CEO to transfer \$243,000. This attack demonstrated that faking voice is no longer the future, and video imitation will become commonplace sooner than you think.
- Usually, the attacker contacts the victim disguised as a representative of some institution, trying to get as much personal info as possible. There's also a chance that by posing as a bank or Google agent, he or she might get the password or credit card info right away. Contrary to the other techniques, **social engineering can happen offline** by calling or even personally meeting the victim.
- **4. Brute force attack**
- If all else fails, password crackers have the brute force attack as a last resort. It basically involves **trying all possible combinations** until you hit the jackpot. However, password cracking tools allow to modify the attack and significantly reduce the time needed to check all variations. The user and his habits are the weak links again here.
- If the attacker was able to brute force a password, he will assume the password has been re-used and try the same combination of login credentials on other online services. This is known as **credential stuffing** and is very popular in the age of data breaches.

- **5. Dictionary attack**
- A dictionary attack is a type of brute force attack and it's often **used together with other brute force attack types**. It automatically checks if the password is not some often-used phrase like "iloveyou" by looking at the dictionary. The attacker might also add passwords from other leaked accounts. In such a scenario, the chance of a successful dictionary attack increases substantially.
- If users were to choose strong passwords that contain not only one word, such attacks would quickly downgrade to a simple brute force attack. In case you use a password manager, then generating a random set of symbols is the best choice. And if you don't, a long phrase made of at least five words is great too. Just don't forget to re-use it for every account.
- **6. Spidering**
- Spidering is a **supplementary password cracking technique** that helps with the above-mentioned brute force and dictionary attacks. It **involves gathering information about the victim**, usually a company, presuming that it uses some of that info for password creation. The **goal is to create a word list** that would help guess the password faster.
- After checking the company's website, social media, and other sources, one can come up with something like this:
  - Founder name – Mark Zuckerberg
  - Founder DOB – 1984 05 14
  - Founder's sister – Randi
  - Founder's other sister – Donna
  - Company name – Facebook
  - Headquarters – Menlo Park
  - Company mission – Give people the power to build community and bring the world closer together
  - Now all you have to do is upload it to a proper password cracking tool and reap the benefits.

- **7. Guessing**
- While guessing is far from the most popular password cracking technique, it relates to business-oriented spidering above. Sometimes the attacker doesn't even have to gather information about the victim because **trying some of the most popular passphrases** is enough. If you recall using one or more of the pathetic passwords in the list below, we strongly recommend changing them now.
- **Some of the most common passwords worldwide:**
  - 123456
  - 123456789
  - qwerty
  - password
  - 12345
  - qwerty123
  - 1q2w3e
  - 12345678
  - 111111
  - 1234567890
- Even though the number of people who use simple or default passwords like "password" "qwerty," or "123456" is diminishing, many still love easy and memorable phrases. Those often include names of pets, lovers, pet-lovers, ex-pets, or something related to the actual service, like its name (lowercase).

- **8. Rainbow table attack**
- As mentioned above, one of the first things to do when password cracking is getting the password in the form of a hash. Then you create a table of common passwords and their hashed versions and check if the one you want to crack matches any entries.  
Experienced hackers usually have a rainbow table that also involves leaked and previously cracked passwords, making it more effective.
- Most often, **rainbow tables have all possible passwords that make them extremely huge**, taking up hundreds of GBs. On the other hand, they make the actual attack faster because most of the data is already there and you only need to compare it with the targeted hash-password. Luckily, most users can protect themselves from such attacks with large salts and key stretching, especially when using both.
- If the salt is large enough, say 128-bit, two users with the same password will have unique hashes. This means that generating tables for all salts will take an astronomical amount of time. As for the key stretching, it increases the hashing time and limits the number of attempts that the attacker can make in given time.

# What Is Spamming?

- Spamming is the sending of an unsolicited email. What this means is that you send an email, generally an ad of some sort, to someone who has not requested to receive that information from you.  
**Electronic spamming** is the use of electronic messaging systems to send an unsolicited message (**spam**), especially advertising, as well as sending messages repeatedly on the same site. While the most widely recognized form of spam is [email spam](#), the term is applied to similar abuses in other media: [instant messaging spam](#), [Usenet newsgroup spam](#), [Web search engine spam](#), [spam in blogs](#), [wiki spam](#), [online classified ads](#) spam, [mobile phone messaging spam](#), [Internet forum spam](#), [junk fax transmissions](#), [social spam](#), spam mobile apps, television [advertising](#) and file sharing spam. It is named after [Spam](#), a luncheon meat, by way of a [Monty Python sketch](#) about a menu that includes Spam in every dish. The food is stereotypically disliked/unwanted, so the word came to be transferred by analogy.
- Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, servers, infrastructures, IP ranges, and domain names, and it is difficult to hold senders accountable for their mass mailings. Because the [barrier to entry](#) is so low, spammers are numerous, and the volume of unsolicited mail has become very high. In the year 2011, the estimated figure for spam messages is around seven trillion. The costs, such as lost productivity and fraud, are borne by the public and by [Internet service providers](#), which have been forced to add extra capacity to cope with the deluge. Spamming has been the subject of legislation in many jurisdictions.
- A person who creates electronic spam is called a *spammer*.

# Spamming In different media

- **Email**
- Email spam, also known as unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. Spam in email started to become a problem when the Internet was opened up to the general public in the mid-1990s. It grew exponentially over the following years, and today composes some 80 to 85 percent of all the e-mail in the World, by a "conservative estimate". Pressure to make email spam illegal has been successful in some jurisdictions, but less so in others. The efforts taken by governing bodies, security systems and email service providers seem to be helping to reduce the onslaught of email spam. According to "2014 Internet Security Threat Report, Volume 19" published by [Symantec Corporation](#), spam volume dropped to 66% of all email traffic. Spammers take advantage of this fact, and frequently outsource parts of their operations to countries where spamming will not get them into legal trouble.
- Increasingly, e-mail spam today is sent via "[zombie](#) networks", networks of [virus](#)- or [worm](#)-infected personal computers in homes and offices around the globe. Many modern worms install a [backdoor](#) that allows the spammer to access the computer and use it for malicious purposes. This complicates attempts to control the spread of spam, as in many cases the spam does not obviously originate from the spammer.
- **Instant messaging**
- Instant messaging spam makes use of [instant messaging](#) systems. Although less ubiquitous than its e-mail counterpart, according to a report from Ferris Research, 500 million spam IMs were sent in 2003, twice the level of 2002. As instant messaging tends to not be blocked by firewalls, it is an especially useful channel for spammers. This is very common on many instant messaging systems such as [Skype](#)

- **Newsgroup and forum**
- Newsgroup spam is a type of spam where the targets are Usenet newsgroups. Spamming of Usenet newsgroups actually pre-dates e-mail spam. Usenet convention defines spamming as excessive multiple posting, that is, the repeated posting of a message (or substantially similar messages). Forum spam is the creation of advertising messages on Internet forums. It is generally done by automated spambots. Most forum spam consists of links to external sites, with the dual goals of increasing search engine visibility in highly competitive areas such as weight loss, pharmaceuticals, gambling, pornography, real estate or loans, and generating more traffic for these commercial websites. Some of these links contain code to track the spambot's identity; if a sale goes through, the spammer behind the spambot works on commission.
- **Mobile phone**
- Mobile phone spam is directed at the [text messaging](#) service of a [mobile phone](#). This can be especially irritating to customers not only for the inconvenience, but also because of the fee they may be charged per text message received in some markets. The term "SpaSMS" was coined at the adnews website Adland in 2000 to describe spam SMS. To comply with CAN-SPAM regulations in the US, SMS messages now must provide options of HELP and STOP, the latter to end communication with the advertiser via SMS altogether.
- Despite the high number of phone users, there has not been so much phone spam, because there is a charge for sending SMS, and installing [trojans](#) into other's phones that send spam (common for e-mail spam) is hard because [applications](#) normally must be downloaded from a central database.
- **Social networking spam**
- Facebook and Twitter are not immune to messages containing spam links. Most insidiously, spammers hack into accounts and send false links under the guise of a user's trusted contacts such as friends and family. As for Twitter, spammers gain credibility by following verified accounts such as that of Lady Gaga; when that account owner follows the spammer back, it legitimizes the spammer and allows him or her to proliferate. Twitter has studied what interest structures allow their users to receive interesting tweets and avoid spam, despite the site using the broadcast model, in which all tweets from a user are broadcast to all followers of the user.
- **Social spam**
- Spreading beyond the centrally managed social networking platforms, user-generated content increasingly appears on business, government, and nonprofit websites worldwide. Fake accounts and comments planted by computers programmed to issue social spam can infiltrate these websites. Well-meaning and malicious human users can break websites' policies by submitting profanity, insults, [hate speech](#), and violent messages.

- **Newsgroup and forum**
- Newsgroup spam is a type of spam where the targets are Usenet newsgroups. Spamming of Usenet newsgroups actually pre-dates e-mail spam. Usenet convention defines spamming as excessive multiple posting, that is, the repeated posting of a message (or substantially similar messages). Forum spam is the creation of advertising messages on Internet forums. It is generally done by automated spambots. Most forum spam consists of links to external sites, with the dual goals of increasing search engine visibility in highly competitive areas such as weight loss, pharmaceuticals, gambling, pornography, real estate or loans, and generating more traffic for these commercial websites. Some of these links contain code to track the spambot's identity; if a sale goes through, the spammer behind the spambot works on commission.
- **Mobile phone**
- Mobile phone spam is directed at the [text messaging](#) service of a [mobile phone](#). This can be especially irritating to customers not only for the inconvenience, but also because of the fee they may be charged per text message received in some markets. The term "SpaSMS" was coined at the adnews website Adland in 2000 to describe spam SMS. To comply with CAN-SPAM regulations in the US, SMS messages now must provide options of HELP and STOP, the latter to end communication with the advertiser via SMS altogether.
- Despite the high number of phone users, there has not been so much phone spam, because there is a charge for sending SMS, and installing [trojans](#) into other's phones that send spam (common for e-mail spam) is hard because [applications](#) normally must be downloaded from a central database.

- **Social networking spam**
- Facebook and Twitter are not immune to messages containing spam links. Most insidiously, spammers hack into accounts and send false links under the guise of a user's trusted contacts such as friends and family. As for Twitter, spammers gain credibility by following verified accounts such as that of Lady Gaga; when that account owner follows the spammer back, it legitimizes the spammer and allows him or her to proliferate. Twitter has studied what interest structures allow their users to receive interesting tweets and avoid spam, despite the site using the broadcast model, in which all tweets from a user are broadcast to all followers of the user.
- **Social spam**
- Spreading beyond the centrally managed social networking platforms, user-generated content increasingly appears on business, government, and nonprofit websites worldwide. Fake accounts and comments planted by computers programmed to issue social spam can infiltrate these websites. Well-meaning and malicious human users can break websites' policies by submitting profanity, insults, [hate speech](#), and violent messages.

# Stalking and Obscenity in Internet

- Cyberstalking is stalking or harassment carried out over the internet. It might target individuals, groups, or even organizations and can take different forms including slander, defamation and threats.
- Motives may be to control or intimidate the victim or to gather information for use in other crimes, like identity theft or offline stalking.
- While blame shouldn't be placed on cyberstalking victims, the current online landscape lends itself to creating "easy targets."
- For example, nowadays, many social media users think nothing of publicly posting personal information, sharing their feelings and desires, publishing family photos and more.

- **What is cyberstalking?**
- As mentioned, cyberstalking can take many different forms, but in the broadest sense, it is stalking or harassment that takes place via online channels such as social media, forums or email. It is typically planned and sustained over a period of time.
- Cases of cyberstalking can often begin as seemingly harmless interactions. Sometimes, especially at the beginning, a few strange or perhaps unpleasant messages may even amuse you. However, if they become systematic, it becomes annoying and even frightening.
- For example, if you've received a few negative comments on Facebook and Instagram, it may upset or annoy you, but this isn't cyberstalking yet. For some people, such as semi-celebrities looking for attention, negative comments are actually welcomed.
- However, once you start receiving unwanted and annoying messages repeatedly and feel harassed, then the line has likely been crossed. Cyberstalkers might terrorize victims by sending unpleasant messages systematically, perhaps even several times a day. It is especially unnerving when such messages come from different accounts managed by the same person. It is probably a good idea to report this to both the website owners and law enforcement agencies.
- Cyberstalking doesn't have to involve direct communication, and some victims may not even realize they are being stalked online. Perpetrators can monitor victims through various methods and use the information gathered for crimes like identity theft. In some cases, the line between cyberspace and real life can become blurred. Attackers can collect your personal data, contact your friends and attempt to harass you offline.

- **Who is behind cyberstalking?**
- Most cyberstalkers are [familiar with their victims](#). For most people, frequent messages from friends or colleagues, although often distracting and sometimes annoying, are welcome. However, being monitored by or receiving intrusive messages from an unfamiliar person or a casual acquaintance can be considered cyberstalking. It can have many motives including revenge, anger, control or even lust.
- Plenty of cyberstalking cases involve someone attempting to get the attention of a former or would-be partner. While some people may see this behavior as acceptable and even romantic, if the communication is unwanted, it can be considered harassment. If this happens to you, you can ask that they stop and take measures such as blocking them from your social media accounts. If it persists through other channels, it may be time to call the police (more on that below).
- Other cases of cyberstalking, particularly those involving celebrities or other high-profile individuals, might involve complete strangers. Some perpetrators suffer from mental health issues and even believe their behavior is welcomed.
- Cyberstalking isn't always conducted by individuals and might involve a group of people. They could be targeting an individual, group or organization for various reasons including opposing beliefs, revenge or financial gain.

- **How to avoid cyberstalking?**
- As with many things in life, it's better to be proactive than reactive when it comes to cyberstalking. Becoming a victim will be far less likely if you follow our five simple tips below. These guidelines will enable you to enjoy all the benefits of online communication while remaining completely safe.
- 1) KEEP A LOW PROFILE
- Keeping a subdued online existence is tough for some people, especially those who need to use online platforms for self-promotion or business-related activities. However, many users could benefit from toning things down a little. You should always avoid posting personal details such as your address and phone number, and think carefully about revealing real-time information such as where you are and who you're with.
- In an ideal world, you would avoid using your real name in online profiles. While this is difficult for anything work-related, it's quite feasible for things like forums, message boards and certain social media accounts. For example, you can use a nickname on Instagram or Twitter.
- If you must maintain your real name and photo, be very wary about who you accept connection requests and messages from. If it's not a friend, relative or colleague, do some checks before moving forward.
- In some cases, it's almost impossible to avoid revealing personal information and connecting with people you don't know, for example, on dating websites. Unfortunately, these are popular with scammers, and you may even end up chatting with a potential cyberstalker. For this reason, it's best to stick with reputable sites, do some research about a suitor before revealing personal information or meeting in person and report any activity that makes you feel uncomfortable to the site's administrators.
- 2) UPDATE YOUR SOFTWARE
- Keeping your software up-to-date may not be the first thing that springs to mind when you think about cyberstalking prevention. However, regular software updates are crucial when it comes to preventing information leaks. Many updates are developed to patch security vulnerabilities and help ensure your information remains safe.
- They are especially important for mobile devices which contain valuable data and track your exact location. There are numerous cases in which cyberstalking begins when an attacker pays someone to hack your email or phone and uses the gathered information against you. A such, protecting yourself from hackers is key to cyberstalking prevention.

### 3) HIDE YOUR IP ADDRESS

- Many applications and services [reveal your IP address](#) to the person with whom you're communicating. This may seem unimportant, but this information is directly related to your personal data. For example, your IP address is linked to the internet bill that is sent to your home and which you pay with your credit card. Cyberstalkers can begin with your IP address and use it to find your credit card data and physical address.
- To mask your IP address you can use a Virtual Private Network (VPN). This hides your real IP address and replaces it with a location of your choice, so you could even appear to be in a different country. It also encrypts all of your internet traffic, keeping it safe from the prying eyes of hackers.
- Another option is to use the [Tor browser](#). This also encrypts your traffic, although it may raise flags for law enforcement agencies as it's commonly used by criminals themselves. For the ultimate in privacy and anonymity, you can [combine Tor and a VPN](#). Note that it's not recommended you use a web proxy or a free VPN service, as these can often harm your online security more than they help it.

### 4) MAINTAIN GOOD DIGITAL HYGIENE

- 'Digital hygiene' is a new term but represents a very important topic, especially with regard to social networks. Maintaining good digital hygiene helps protect you from cyber harassment, cyberbullying and cyberstalking.
- [Adjusting privacy settings](#) is one of the first steps you can take to "clean up" your accounts. Most social media platforms and some other types of online accounts will let you adjust who can see your profile and contact you.
- It's also a good idea to keep things like your timelines, feeds and message threads free from negative comments. Aside from potentially fueling more negativity from others, these can have a significant emotional impact when you re-read them. For example, psychological support is regularly provided to website moderators, as they seriously suffer from reading aggressive messages, even those that aren't sent to them personally.
- Social media hygiene is especially important for girls and women. [Studies show](#) that although the majority of internet attacks are aimed at men, cyberstalking, in particular, is mostly aimed at women.

### 5) AVOID DISCLOSING SENSITIVE INFORMATION

- Surprisingly, many people constantly share personal information about themselves, even outside of social media platforms. By filling out questionnaires or submitting applications for coupons, you are increasing the likelihood of someone getting their hand on your personal data and possibly making cyberstalking more accessible.

## What to do in case you are being cyberstalked?????

- **Block the person**
- Don't hesitate to apply all measures permitted by law, especially those offered by web services. If the tools are there, block anyone who you wish to stop hearing from, even if these messages are just annoying and not yet threatening. Only you can decide when this boundary has been passed.
- **Report to the platform involved**
- If someone is harassing or threatening you, you should block them immediately and report their behavior to the platform involved. Twitter, Facebook, LinkedIn, and many other platforms have created easy-to-use buttons to quickly report abusive behavior.
- Even if you think you are rid of the perpetrator, they may come back or pursue more victims. Law enforcement agencies do not always have the technical ability to protect you from cyberstalking, but platform moderators usually respond quickly and delete attackers' profiles.
- **Call the police**
- If you believe their behavior is illegal or you fear for your safety, then you should contact the police and report the cyberstalker. Even if you don't have enough information or evidence for them to prosecute immediately, the report will go on record and the police can offer advice about what to do if the perpetrator persists.

- Obscenity refers to a narrow category of pornography that violates contemporary community standards and has no serious literary, artistic, political or scientific value.
- For adults at least, most pornography — material of a sexual nature that arouses many readers and viewers — receives constitutional protection.
- Federal law makes it illegal to distribute, transport, sell, ship, mail, produce with intent to distribute or sell, or engage in a business of selling or transferring obscene matter.
- Convicted offenders face fines and imprisonment.
- Although the law generally does not criminalize the private possession of obscene matter, the act of receiving such matter could violate federal laws prohibiting the use of the mails, common carriers, or interactive computer services for the purpose of transportation.

# Security Issues of Smart Phones

- <http://publications.lib.chalmers.se/records/fulltext/128680.pdf>
- Smartphones are more at risk in certain areas — hotels, coffee shops, airports, cars, trains, etc. And home Wi-Fi connections can be potential risk areas if users don't properly secure them. An attacker could easily access confidential personally identifiable information (PII) and data, such as:
  - ❖ Personal or professional data (emails, documents, contacts, calendar, call history, SMS, MMS).
  - ❖ User identification and passwords (to emails, social networks, etc.).
  - ❖ Mobile applications that record PII.
  - ❖ Geolocation data about the smartphone user.
- ❖ READ: <https://www.kaspersky.co.in/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store> (IMPORTANT)

## 10 major risks for smartphone users:

- ✓ Data leakage resulting from device loss or theft.
- ✓ Unintentional disclosure of data.
- ✓ Attacks on decommissioned smartphones.
- ✓ Phishing attacks.
- ✓ Spyware attacks.
- ✓ Network spoofing attacks.
- ✓ Surveillance attacks.
- ✓ Diallerware attacks: an attacker steals money from the user by means of malware that makes hidden use of premium short message services or numbers.
- ✓ Financial malware attacks.
- ✓ Network congestion.

Here are various measures that can help reduce the risks associated with mobile devices:

- Encrypt mobile devices.
- Regularly update mobile devices' applications and operating systems.
- Set strong passwords. Each personal identification number (PIN) should be at least eight digits long because a four-digit PIN can be easily broken. Alphanumeric passwords should be at least eight characters long and shouldn't use common names or words. An easy way to help create a memorable password is to use a favorite sentence. For example, you can create a password from "The ACFE is reducing business fraud worldwide and inspiring public confidence." Use the first letters of each word and replace "a" and "i" with "@" and "1," respectively. Following this method, the password would be: "t@1rbfw@1pc."
- Also avoid using a password that you've used for another account (a Yahoo! or Google email account, for example). Change your passwords (to access your phone and your various accounts) after a trip, especially if you used it in high-risk areas such as public hotspots in hotels, coffee shops and airports.

Here are a few more steps to better protect smartphones:

- Consider deactivating smartphone functionalities such as Siri on iPhone, "Ok Google" on Android or Cortana on Windows Phone as they could be used to gain PII or control over your phone or computer.
- Activate an immediate automatic lock of your smartphone screen when you're not using it.
- Deactivate any smartphone features that display messages on a locked screen.
- Don't ignore error messages about the validity of certificates, for example, when you try connecting to a Wi-Fi hotspot. You should always ensure that the website you're visiting or the hotspot you're connecting to is legitimate. They could be malicious Wi-Fi connections pretending to be legitimate hotspots. Hackers can plan and deliver these attacks at a relatively low cost.

- Staying diligent helps decrease risk
- Smartphone antivirus protection applications can provide a false sense of security because their effectiveness varies greatly. Thus, you have to be responsible to ensure the safety of your professional and personal smartphones and possibly those your organization supplies to its employees.
- organizations must train all employees — including high-level employees who have access to sensitive company information — in smartphone security.
- Your organization can conduct online training in social engineering, smartphone specificities, malware and passwords.
- Smartphone instructions often are outdated. Stay current about security risks and remedies because smartphone attack schemes are always evolving. You can do this by checking specialized websites and blogs or by doing a simple web search.

## SMARTPHONE THREATS AND ATTACKS

- In a smartphone threat model, a malicious user publishes malware disguised as a normal application through an app store or website.
- Users will unintentionally download the malware to a smartphone, which carries a large amount of sensitive data.
- After infiltrating a smartphone, the malware attempts to control its resources, collect data, or redirect the smartphone to a premium account or malicious website.

## Affected services

- Malware's impact can range from minor issues, such as degraded performance, spam messages, and slow operation, to more significant challenges, such as the user not being able to receive and make phone calls or incurring financial loss.
- The impact to any one smartphone user might be completely different from that experienced by other subscribers.

## Jeopardized resources

Resources containing sensitive data are attractive to hackers. Once malware finds a way into the smartphone, it will try to gain privileges to access and control these resources.

- Threats and attacks Smartphone threats and attacks include sniffing, spam, attacker spoofing, phishing, pharming, vishing, and data leakage.

For various reasons, smartphones are also vulnerable to DoS attacks:

- Because they are based on radio communication technology, smartphones can incur an attack in which a jamming device is used to disrupt the communication between the smartphone and its base station.
- Flooding attacks can generate hundreds of text messages or incoming calls, thus disabling a smartphone.
- A battery exhaustion attack on a smartphone causes more battery discharge than is typically necessary.
- A malicious user could use a smartphone's blocking features to start a DoS attack. If a malicious user keeps calling a smartphone from a blocked phone number, the subscriber cannot use any of the smartphone's functions.

## Limited battery life

- A smartphone is a resource-constrained device that is powered by a battery with a limited life and that must be recharged when drained. Any security solution must consider this limitation as enhanced security cannot sacrifice battery life.

## Vulnerability to theft and loss

- Among all potential security issues, loss and theft are two primary concerns for smartphone users. Losing control of a smartphone, even temporarily—say, by loaning it to someone—can have catastrophic consequences. With some simple setup, a malicious user can reprogram a smartphone's firmware and flash memory, physically clone the memory card, or install spyware. Some simple techniques can help protect against smartphone theft and loss. For example, the user can add a password or enable auto-lock. Antitheft technology that remotely deletes sensitive data when a smartphone leaves a secure zone is also available through third-party applications

## Multiple-entrance open system

- Smartphones are multiple-entrance open systems, and each entrance is a potential back door for malware access.
- Each smartphone communication channel is a potential path for malware disguised as an application. Because smartphones offer multiple entrances, an attack loop can consist of many combinations, but an attack loop cannot be formed if malware is detected, prevented, and removed from the smartphone.
- Securing a smartphone requires using one of many possible approaches to break the attack loop. For example, resource control could break the attack loop by preventing the malware from gaining access to the smartphone's resources to manipulate its data

## DESIRED SECURITY FEATURES

- Confidentiality, integrity, and authentication are three of the most desirable security features in a smartphone.
- Most smartphones support synchronization between the device and a computer. This function makes it possible for another user to access the smartphone file system. Thus, to keep data confidential, users should employ encryption techniques and avoid storing sensitive information in plaintext on a smartphone.
- Integrity applies to both data and the system. App stores should verify software integration to avoid malicious modification. Further, smartphones should provide mechanisms to protect system integrity. They should also block unauthorized data access requests.
- A smartphone authentication service could protect smartphone users against malware attacks that spoof caller IDs and MMS.

# Security issues of Smart Phones, digital tablets and smart Devices

- When it comes to security, most mobile devices are a target waiting to be attacked. That's pretty much the conclusion of a report to Congress on the status of the security of mobile devices this week by watchdogs at the Government Accountability Office.
- Combine the lack of security with the fact that mobile devices are being targeted by cybercriminals and you have a bad situation.
- Mobile devices face an array of threats that take advantage of numerous vulnerabilities commonly found in such devices. These vulnerabilities can be the result of inadequate technical controls, but they can also result from the poor security practices of consumers. Private [companies] and relevant federal agencies have taken steps to improve the security of mobile devices, including making certain controls available for consumers to use if they wish and promulgating information about recommended mobile security practices. However, security controls are not always consistently implemented on mobile devices, and it is unclear whether consumers are aware of the importance of enabling security controls on their devices and adopting recommended practices.

- **Problems**
1. Mobile devices often do not have passwords enabled. Mobile devices often lack passwords to authenticate users and control access to data stored on the devices. Many devices have the technical capability to support passwords, personal identification numbers (PIN), or pattern screen locks for authentication. Some mobile devices also include a biometric reader to scan a fingerprint for authentication. However, anecdotal information indicates that consumers seldom employ these mechanisms. Additionally, if users do use a password or PIN they often choose passwords or PINs that can be easily determined or bypassed, such as 1234 or 0000. Without passwords or PINs to lock the device, there is increased risk that stolen or lost phones' information could be accessed by unauthorized users who could view sensitive information and misuse mobile devices.
  2. Two-factor authentication is not always used when conducting sensitive transactions on mobile devices. According to studies, consumers generally use static passwords instead of two-factor authentication when conducting online sensitive transactions while using mobile devices. Using static passwords for authentication has security drawbacks: passwords can be guessed, forgotten, written down and stolen, or eavesdropped. Two-factor authentication generally provides a higher level of security than traditional passwords and PINs, and this higher level may be important for sensitive transactions. Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors" something you know, something you have, or something you are before being granted access. Mobile devices can be used as a second factor in some two-factor authentication schemes. The mobile device can generate pass codes, or the codes can be sent via a text message to the phone. Without two-factor authentication, increased risk exists that unauthorized users could gain access to sensitive information and misuse mobile devices.

- 3. Wireless transmissions are not always encrypted. Information such as e-mails sent by a mobile device is usually not encrypted while in transit. In addition, many applications do not encrypt the data they transmit and receive over the network, making it easy for the data to be intercepted. For example, if an application is transmitting data over an unencrypted WiFi network using http (rather than secure http), the data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted.
- 4. Mobile devices may contain malware. Consumers may download applications that contain malware. Consumers download malware unknowingly because it can be disguised as a game, security patch, utility, or other useful application. It is difficult for users to tell the difference between a legitimate application and one containing malware. For example, an application could be repackaged with malware and a consumer could inadvertently download it onto a mobile device. When a wireless transmission is not encrypted, data can be easily intercepted by eavesdroppers, who may gain unauthorized access to sensitive information.
- 5. Mobile devices often do not use security software. Many mobile devices do not come preinstalled with security software to protect against malicious applications, spyware, and malware-based attacks. Further, users do not always install security software, in part because mobile devices often do not come preloaded with such software. While such software may slow operations and affect battery life on some mobile devices, without it, the risk may be increased that an attacker could successfully distribute malware such as viruses, Trojans, spyware, and spam to lure users into revealing passwords or other confidential information.

- 6. Operating systems may be out-of-date. Security patches or fixes for mobile devices' operating systems are not always installed on mobile devices in a timely manner. It can take weeks to months before security updates are provided to consumers' devices. Depending on the nature of the vulnerability, the patching process may be complex and involve many parties. For example, Google develops updates to fix security vulnerabilities in the Android OS, but it is up to device manufacturers to produce a device-specific update incorporating the vulnerability fix, which can take time if there are proprietary modifications to the device's software. Once a manufacturer produces an update, it is up to each carrier to test it and transmit the updates to consumers' devices. However, carriers can be delayed in providing the updates because they need time to test whether they interfere with other aspects of the device or the software installed on it.
- In addition, mobile devices that are older than two years may not receive security updates because manufacturers may no longer support these devices. Many manufacturers stop supporting smartphones as soon as 12 to 18 months after their release. Such devices may face increased risk if manufacturers do not develop patches for newly discovered vulnerabilities.
- 7. Software on mobile devices may be out-of-date. Security patches for third-party applications are not always developed and released in a timely manner. In addition, mobile third-party applications, including web browsers, do not always notify consumers when updates are available. Unlike traditional web browsers, mobile browsers rarely get updates. Using outdated software increases the risk that an attacker may exploit vulnerabilities associated with these devices.
- 8. Mobile devices often do not limit Internet connections. Many mobile devices do not have firewalls to limit connections. When the device is connected to a wide area network it uses communications ports to connect with other devices and the Internet. A hacker could access the mobile device through a port that is not secured. A firewall secures these ports and allows the user to choose what connections he wants to allow into the mobile device. Without a firewall, the mobile device may be open to intrusion through an unsecured communications port, and an intruder may be able to obtain sensitive information on the device and misuse it.

- 9. Mobile devices may have unauthorized modifications. The process of modifying a mobile device to remove its limitations so consumers can add features (known as "jailbreaking" or "rooting") changes how security for the device is managed and could increase security risks. Jailbreaking allows users to gain access to the operating system of a device so as to permit the installation of unauthorized software functions and applications and/or to not be tied to a particular wireless carrier. While some users may jailbreak or root their mobile devices specifically to install security enhancements such as firewalls, others may simply be looking for a less expensive or easier way to install desirable applications. In the latter case, users face increased security risks, because they are bypassing the application vetting process established by the manufacturer and thus have less protection against inadvertently installing malware. Further, jailbroken devices may not receive notifications of security updates from the manufacturer and may require extra effort from the user to maintain up-to-date software.
- 10. Connecting to an unsecured WiFi network could let an attacker access personal information from a device, putting users at risk for data and identity theft. One type of attack that exploits the WiFi network is known as man-in-the-middle, where an attacker inserts himself in the middle of the communication stream and steals information.9. Communication channels may be poorly secured. Having communication channels, such as Bluetooth communications, "open" or in "discovery" mode (which allows the device to be seen by other Bluetooth-enabled devices so that connections can be made) could allow an attacker to install malware through that connection, or surreptitiously activate a microphone or camera to eavesdrop on the user. In addition, using unsecured public wireless Internet networks or WiFi spots could allow an attacker to connect to the device and view sensitive information.

## Fight Back

- A number of ideas including:
- Enable user authentication: Devices can be configured to require passwords or PINs to gain access. In addition, the password field can be masked to prevent it from being observed, and the devices can activate idle-time screen locking to prevent unauthorized access.
- Verify the authenticity of downloaded applications: Procedures can be implemented for assessing the digital signatures of downloaded applications to ensure that they have not been tampered with. Enable two-factor authentication for sensitive transactions: Two-factor authentication can be used when conducting sensitive transactions on mobile devices. Two-factor authentication provides a higher level of security than traditional passwords. Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors" something you know, something you have, or something you are before being granted access. Mobile devices themselves can be used as a second factor in some two-factor authentication schemes used for remote access. The mobile device can generate pass codes, or the codes can be sent via a text message to the phone. Two-factor authentication may be important when sensitive transactions occur, such as for mobile banking or conducting financial transactions.
- Install antimalware capability: Antimalware protection can be installed to protect against malicious applications, viruses, spyware, infected secure digital cards, and malware-based attacks. In addition, such capabilities can protect against unwanted (spam) voice messages, text messages, and e-mail attachments.

- Install a firewall: A personal firewall can protect against unauthorized connections by intercepting both incoming and outgoing connection attempts and blocking or permitting them based on a list of rules.
- Install security updates: Software updates can be automatically transferred from the manufacturer or carrier directly to a mobile device. Procedures can be implemented to ensure these updates are transmitted promptly.
- Remotely disable lost or stolen devices: Remote disabling is a feature for lost or stolen devices that either locks the device or completely erases its contents remotely. Locked devices can be unlocked subsequently by the user if they are recovered.
- Enable encryption for data stored on device or memory card: File encryption protects sensitive data stored on mobile devices and memory cards. Devices can have built-in encryption capabilities or use commercially available encryption tools.
- Enable whitelisting: Whitelisting is a software control that permits only known safe applications to execute commands.
- Establish a mobile device security policy: Security policies define the rules, principles, and practices that determine how an organization treats mobile devices, whether they are issued by the organization or owned by individuals. Policies should cover areas such as roles and responsibilities, infrastructure security, device security, and security assessments. By establishing policies that address these areas, agencies can create a framework for applying practices, tools, and training to help support the security of wireless networks.
- Provide mobile device security training: Training employees in an organization's mobile security policies can help to ensure that mobile devices are configured, operated, and used in a secure and appropriate manner.
- Establish a deployment plan: Following a well-designed deployment plan helps to ensure that security objectives are met.
- Perform risk assessments: Risk analysis identifies vulnerabilities and threats, enumerates potential attacks, assesses their likelihood of success, and estimates the potential damage from successful attacks on mobile devices.
- Perform configuration control and management: Configuration management ensures that mobile devices are protected against the introduction of improper modifications before, during, and after deployment.

# Social network Account Attack

- The following are ways to hack any online account, not just social networking sites, in order of difficulty.
- **Guessing Passwords (Bruteforce Attack):**
  - This is arguably the most common and easiest type of attack, because it can be launched against any website.
  - The attacker would try to login by trying different passwords.
  - There are tools/utilities that automate this process, so the attacker would just need to give said tool/utility a list of words/passwords to try.
- **Phishing Attack:**
  - This is when an attacker tries to obtain sensitive information (eg username, password, DoB, security questions & answers ...etc) from the victim by posing as a legitimate entity. Phishing attacks encompasses other attack types, such as *social engineering* and/or *cross-site scripting* attacks.
  - The simplest form of phishing is cloning the targeted website and sending the URL to the victim. The unsuspecting victim would then type in the sensitive information in the cloned website.
- **Social Engineering:**
  - This type of attack requires some creativity and due-diligence from the attacker.
  - In this type of attack, an attacker would try to get the victim to do something the victim otherwise would not be willing to do.
  - In the context of trying to hack an account, the attacker could pose as a Security Engineer/Analyst from the website's corporate office informing you that your account has been compromised and asking you to "confirm your identity" by asking you a series of questions for your name, DoB, username, address ...etc.
  - In this context, the attacker could use email, phone, or instant messaging to carry out their attack, but in other contexts, the attacker could even try to carry social engineering attacks out in person.

- **Cross-Site Scripting Attack:**
  - This type of attack can be carried out against any website. The website must meet certain conditions in order for this attack to work. Specifically, the website must not sanitize user inputs.
  - Once the attacker confirms that the site is susceptible, the attacker would typically send a URL to the victim. Upon clicking on the URL, some malicious code runs in the victim's browser that extracts and sends sensitive information from victim to the attacker.
  - 
  -
- **Man-in-the-Middle Attack:**
  - This is a highly sophisticated attack and could be carried out in many different ways. Essentially, this is when the attacker embeds themselves between the victim and the website.
  - If the attacker is in the same network as the victim, then the attacker could fool the victim's machine into thinking that the attacker's machine is the access point/router, or hacking the router to forward all traffic to attacker's machine ([ARP spoofing](#)). Once this is established, the victim's traffic goes through the attacker's machine before it goes to the final destination and goes through the attacker's machine first before reaching your machine on its way back. This means the hacker could, at the very least, passively sniff your packets or, at most, intercept your packets and alter them before forwarding them along. This could lead to the attacker obtaining more than just username/password, but potentially anything else that is being transmitted over the Internet.

# Hacking of social network account

## using password cracking

- Password cracking is one of the most enjoyable hacks for the bad guys. It fuels their sense of exploration and desire to figure out a problem. A hacker can use low-tech methods to crack passwords. These methods include using social engineering techniques, shoulder surfing, and simply guessing passwords from information that he knows about the user.
- **SOCIAL ENGINEERING**
  - The most popular low-tech method for gathering passwords is *social engineering*. Social engineering takes advantage of the trusting nature of human beings to gain information that later can be used maliciously. A common social engineering technique is simply to con people into divulging their passwords. It sounds ridiculous, but it happens all the time.
- **TECHNIQUES**
  - To obtain a password through social engineering, you just ask for it. For example, you can simply call a user and tell him that he has some important-looking e-mails stuck in the mail queue, and you need his password to log in and free them up. This is often how hackers and rogue insiders try to get the information!
  - A common weakness that can facilitate such social engineering is when staff members' names, phone numbers, and e-mail addresses are posted on your company websites. Social media sites such as LinkedIn, Facebook, and Twitter can also be used against a company because these sites can reveal employees' names and contact information.
- **COUNTERMEASURES**
  - User awareness and consistent security training are great defenses against social engineering. Security tools are a good fail-safe if they monitor for such e-mails and web browsing at the host-level, network perimeter, or in the cloud.
  - Train users to spot attacks and respond effectively. Their best response is not to give out any information and to alert the appropriate information security manager in the organization to see whether the inquiry is legitimate and whether a response is necessary. Oh, and take that staff directory off your website or at least remove IT staff members' information.

- **SHOULDER SURFING**
  - *Shoulder surfing* (the act of looking over someone's shoulder to see what the person is typing) is an effective, low-tech password hack.
- TECHNIQUES
  - To mount this attack, the bad guys must be near their victims and not look obvious. They simply collect the password by watching either the user's keyboard or screen when the person logs in.
  - An attacker with a good eye might even watch whether the user is glancing around his desk for either a reminder of the password or the password itself. Security cameras or a webcam can even be used for such attacks. Coffee shops and airplanes provide the ideal scenarios for shoulder surfing.
  - You can try shoulder surfing yourself. Simply walk around the office and perform random spot checks. Go to users' desks and ask them to log in to their computers, the network, or even their e-mail applications. Just don't tell them what you're doing beforehand, or they might attempt to hide what they're typing or where they're looking for their password. Just be careful doing this and respect other people's privacy.
- COUNTERMEASURES
  - Encourage users to be aware of their surroundings and not to enter their passwords when they suspect that someone is looking over their shoulders. Instruct users that if they suspect someone is looking over their shoulders while they're logging in, they should politely ask the person to look away or, when necessary, hurl an appropriate epithet to show the offender that the user is serious.
  - It's often easiest to just lean into the shoulder surfer's line of sight to keep them from seeing any typing and/or the computer screen. [\*\*3M Privacy Filters\*\*](#) work great as well.

- **INFERENCE**
- *Inference* is simply guessing passwords from information you know about users — such as their date of birth, favorite television show, or phone numbers. It sounds silly, but criminals often determine their victims' passwords simply by guessing them!
- The best defense against an inference attack is to educate users about creating secure passwords that don't include information that can be associated with them. Outside of certain password complexity filters, it's often not easy to enforce this practice with technical controls. So, you need a sound security policy and ongoing security awareness and training to remind users of the importance of secure password creation.
- **WEAK AUTHENTICATION**
- External attackers and malicious insiders can obtain — or simply avoid having to use — passwords by taking advantage of older or unsecured operating systems that don't require passwords to log in. The same goes for a phone or tablet that isn't configured to use passwords.
- **BYPASSING AUTHENTICATION**
- On older operating systems that prompt for a password, you can press Esc on the keyboard to get right in. Okay, it's hard to find any Windows 9x systems these days, but the same goes for any operating system — old or new — that's configured to bypass the login screen.
- After you're in, you can find other passwords stored in such places as dialup and VPN connections and screen savers. Such passwords can be cracked very easily using [Elcomsoft's Proactive System Password Recovery tool](#) and [Cain & Abel](#). These weak systems can serve as *trusted* machines — meaning that people assume they're secure — and provide good launching pads for network-based password attacks as well.
- **COUNTERMEASURES**
- The only true defense against weak authentication is to ensure your operating systems require a password upon boot. To eliminate this vulnerability, *at least* upgrade to Windows 7 or 8 or use the most recent versions of Linux or one of the various flavors of UNIX, including Mac OS X.

# SOCIAL NETWORKING SAFETY

- Social networking is a method of communication with people through online platforms such as Facebook, LinkedIn, and Twitter. Over the years, social networking has become an important part of life for both adults and teens. The popularity is due to the ability of meeting the needs and interests of a vast majority of people.
- For teens it is a way to socialize with friends, by sharing the latest events, photos and videos. Adults use social platforms for the same reason as teens, while also utilizing each platform in a professional manner as well. It is a valuable tool for businesses in that it allows them to interact with like-minded professionals, customers and other businesses.
- With all the benefits social networking offers, it is easy to overlook the risks that are involved. Said risks include threats of criminal activity, such as, stalking, bullying, identity theft, and hacking. Also, users may fall prey to impersonators who can cause damage to their reputation and standing with the very people they are trying to network with. To make the best use of social networking while avoiding the risks, users will need to understand and follow a set of basic safety tips that are easy to remember and highly effective.

- **1. Be Cautious of Sharing Too Much**
- When utilizing a social networking website, people have the option of sharing personal details with friends and followers. While sharing some information is okay, other facts can reveal too much about who a person is. For the sake of personal safety, one should never reveal their date and place of birth, home address or phone number, as this could put them at serious risk for identity theft and fraud. In addition, it is extremely important that a person never reveal their credit card numbers, banking information, passwords, or social security number on any networking site. If such information is shared it would be very easy to fall victim to crimes ranging from stalking to identity theft.
- 
- **2. Adjust Privacy Settings**
- Nearly all social networking sites have pre-set or default privacy settings. People often feel that these setting are sufficient enough and never put forth the effort to make changes. Altering one's privacy settings can allow the account holder to block strangers and people who are not friends with them from viewing his or her private information. These settings also limit what information is available in search results; for example, Facebook allows the account holder to modify their settings so only their friends, friends and networks, specific groups, or no one can see their status, photos, videos, likes, etc.. Privacy settings can be adjusted at any time; however, the account holder must log in to make adjustments.

- **3. Limit Details About Work History**
- On some social networking sites, such as LinkedIn, people are able to post resumes and other information that pertains to their work history. Work related information can reveal too much about a person's personal life and can give criminals such as hackers personal information which may help them to hack into one's account. The information that is found on resumes can also be used in identity theft.
- 
- **4. Verify Who You're Connecting With**
- There are a number of reasons why a person may put up a false account. If there is ever uncertainty about the authenticity of an account that claims to belong to a friend, it is important to check with the individual for verification. These accounts may be setup in efforts to misrepresent themselves as another person in order to make false statements. This may be done to embarrass someone or to create problems that either of a legal or personal nature. False accounts may also be set up to for the purpose of sending people to malicious sites or with the intent of committing fraud.
- 
- **5. Keep Control of Comments – Be Aware of Impersonators**
- Impersonation can be a problem when it comes to comments on networking websites. Typically, people who are misrepresented online only need to ask that the impersonator be removed. This can be a hassle, however, networking sites are beginning to require commenter's to go through an authentication process in which they are identified as registered users or not.
- 
- **6. Don't Share Personal Details**
- Microblogging websites encourage people to share in the moment activities and slices of life. For people who enjoy this sort of social interaction, they may find that they are revealing too much about what is happening and as a result making themselves the ideal victim for thieves and other criminals. Because these networks are visible to practically everyone, a person should not reveal information that alerts criminals to their whereabouts or other actions. For example, a person should never reveal where they are vacationing, shopping, or traveling. It should also never be revealed when they expect to leave or return home.

- **7. Check Out Your Own Account**
- In order to ensure the security of one's account, it is wise to search for their profile from the prospective of someone who is conducting a search. This step will let the account holder know what others are able to view. When using a search engine to look for one's profile they will also be able to see if there are any false accounts set up in his or her name.
- 
- **8. Know Employer Boundaries or Acceptable Use Policies**
- More and more frequently there are reports of people who have lost their jobs as a result of their activities on social networking sites. This can easily be avoided when employees review what policies their employer has in place. These policies may affect what a person can share in terms of pictures and/or writing. This is done to not only protect their reputation, but to also prevent data loss or loss of intellectual property.
- 
- **9. Control What Information is Shared with Outside Sources**
- When a person joins a social networking site, they should understand how that site uses their private information. A user's personal details may be shared with partners, advertisers, or other outside companies. Reading the privacy policy of the social networking platform will explain exactly how private information is used. Unfortunately, people do not fully read these policies before agreeing to them. The privacy terms should be rechecked in the event that a company is sold as these policies may change.
- 
- **10. Be Careful of Over-Friending**
- As a member of a social networking group, it can be exciting to gain new "friends" or followers. Looking through the network it is easy to find members with high numbers of friends, which can inspire a competitive streak in some. A high number of friends, however, is not always positive. Some "friends" can be problematic by introducing spam into one's timeline or some may even have criminal intentions. When accepting friends, choose people who are actual friends.
- 
- **11. Consider Forming a New Social Network**
- Respected networking sites like Facebook and Twitter, are not the only social networking platforms available. The popularity of these sites make them larger than life and attract a large assortment of people with various agendas. However, people who are interested in interacting with a smaller, more intimate group of people should look into joining MeetUp, Ning, or FamilyLeaf. In some cases people are able to go through MeetUp to create a niche social network that will attract like-minded individuals within one's own community.
-

- **12. Single Sign-On: Open ID**
- Using a single sign-on for multiple platforms is one way people can reduce the likelihood of their passwords getting into the hands of identity thieves and hackers. OpenID is the most common single sing-on to manage various accounts.
- 
- **13. What Goes Online Stays Online**
- When sharing information online it is important for people to realize the permanence of what they type or download. Once information goes on the Internet, through social networking, microblogging, etc., it is difficult, if not impossible to remove. In some instances, the information may even be captured via screen shot and used on blogs or news sites. Depending on what was originally submitted, the information can prove detrimental for future job prospects, relationships, and may even leave a person vulnerable to crimes.
- 
- **14. Know How to Block Unfriendly Followers**
- Nearly every social networking platforms gives users a way to protect themselves from harassment or unwanted contact. When joining a social network one should familiarize themselves with how to block another member. Once a person has been blocked, he or she will no longer have the ability to interact with the individual who has done the blocking.
- 
- **15. Keep Passwords Strong**
- Security is as important for one's social network account as it is for their computer or any other account. Creating a strong password will prevent hackers from gaining access to one's account and using it to post spam or malicious attacks. When creating a password it is important to choose one that consists of no less than eight characters. The characters should consist of both letters and numbers and should be changed approximately every three months.

Here are our top 10 tips to stay safe on social media:

- Use a strong password. The longer it is, the more secure it will be.
- Use a different password for each of your social media accounts.
- Set up your security answers. This option is available for most social media sites.
- If you have social media apps on your phone, be sure to password protect your device.
- Be selective with friend requests. If you don't know the person, don't accept their request. It could be a fake account.
- Click links with caution. Social media accounts are regularly hacked. Look out for language or content that does not sound like something your friend would post.
- Be careful about what you share. Don't reveal sensitive personal information ie: home address, financial information, phone number. The more you post the easier it is to have your identity stolen.
- Become familiar with the privacy policies of the social media channels you use and customize your privacy settings to control who sees what.
- Protect your computer by installing antivirus software to safeguard. Also ensure that your browser, operating system, and software are kept up to date.
- Remember to log off when you're done.

- Social networking websites like [MySpace](#), [Facebook](#), [Twitter](#), and [Windows Live Spaces](#) are services people can use to connect with others to share information like photos, videos, and personal messages.
- As the popularity of these social sites grows, so do the risks of using them. Hackers, spammers, virus writers, identity thieves, and other criminals follow the traffic.
- Read these tips to help protect yourself when you use social networks.
- **Use caution when you click links** that you receive in messages from your friends on your social website. Treat links in messages on these sites as you would links in e-mail messages.
- **Know what you've posted about yourself.** A common way that hackers break into financial or other accounts is by clicking the "Forgot your password?" link on the account login page. To break into your account, they search for the answers to your security questions, such as your birthday, hometown, high school class, father's middle name, on your social networking site. If the site allows, make up your own password questions, and don't draw them from material anyone could find with a quick search.
- **Don't trust that a message really is from whom it says it's from.** Hackers can break into accounts and send messages that look like they're from your friends, but aren't. If you suspect that a message is fraudulent, use an alternate method to contact your friend to find out. This includes invitations to join new social networks.
- **To avoid giving away e-mail addresses of your friends, do not allow social networking services to scan your e-mail address book.** When you join a new social network, you might receive an offer to enter your e-mail address and password to find out if your contacts are on the network. The site might use this information to send e-mail messages to everyone in your contact list or even everyone you've ever sent an e-mail message to with that e-mail address. Social networking sites should explain that they're going to do this, but some do not.
- **Type the address of your social networking site directly into your browser or use your personal bookmarks.** If you click a link to your site through e-mail or another website, you might be entering your account name and password into a fake site where your personal information could be stolen.
- **Be selective about who you accept as a friend on a social network.** Identity thieves might create fake profiles in order to get information from you.
- **Choose your social network carefully.** Evaluate the site that you plan to use and make sure you understand the privacy policy. Find out if the site monitors content that people post. You will be providing personal information to this website, so use the same criteria that you would to select a site where you enter your credit card.
- **Assume that everything you put on a social networking site is permanent.** Even if you can delete your account, anyone on the Internet can easily print photos or text or save images and videos to a computer.
- **Be careful about installing extras on your site.** Many social networking sites allow you to download third-party applications that let you do more with your personal page. Criminals sometimes use these applications to steal your personal information. To download and use third-party applications safely, take the same safety precautions that you take with any other program or file you download from the Web.
- **Think twice before you use social networking sites at work.**
- **Talk to your kids about social networking.**

- **The four major dangers of using social networking websites are**
- Over sharing information. When creating a profile page, most websites will ask for personal information such as home addresses, birthdays, and phone numbers. Giving this information can be very dangerous and will be made public to anyone who visits a user's profile page, especially if privacy settings are not set correctly. Even if account settings are set to private, users are still at risk of their accounts being hacked. If someone hacks into an account he or she will be able to view and use the information. Sharing simple things like your favorite color can tip off a hacker to try to see if you used that as a password on your account. The biggest threat of over sharing information is identity theft. Identity theft is not uncommon in the world of online social networking. Online computer criminals look to steal identities in obvious and not so obvious ways. An obvious way would be someone asking for your social security number. A not so obvious way is luring a user to click on a link that will allow the criminal to download all of the user's personal information. The anonymity provided online makes it easier for computer criminals to go undetected.
- He's not who you think he is. Social networking sites make it very easy to pretend to be someone else. Even if an individual may be friends with someone on the site, anyone can take control of a user's account if he or she can obtain the user's password. As a result, someone who is a "Friend" can ask for money or gain personal information that can be used to hack into other accounts. For example, you may get a message from a relative asking you for your banking information because he or she would like to wire you some money for your birthday. You may think you're talking to your relative, but in fact the information is being requested by someone who has hacked into your relative's account.
- Location-based services. Location-based services can be one of the most dangerous features provided by social networking sites. It exposes the profile user's location and whereabouts. The service also has a feature that allows users to tag who they are with at any given time. While it can be fun to share your location with friends and family, it can also increase your vulnerability, potentially opening you up to being robbed, sexually assaulted, or worse. Predators can use this tool to track your movements and determine when you are alone or when you are not at home.
- Posting photos. One of the features of online social networking that many teens enjoy is the photo-sharing feature. This feature allows you to post photos 24 hours a day. Whether it is from your computer or mobile device, posting photos can be done in seconds. The Internet makes it easy to obtain photos and use the images in any way a person may choose. Posting inappropriate photos that may be deemed as fun, cute, or sexy, can end up where one least expects it. Photo tampering is a big threat when it comes to posting photos online. The use of photo editing tools allows people to manipulate online images in any way they choose, whether it's used for good or bad purposes. While posting pictures and sharing them with friends can be fun, it can also be risky.

- **Teaching Your Teen Three Simple Steps To Increase Safety**
- Don't give optional information-When creating a profile, you do not need to enter all of the information that is requested. The set-up page usually requires you to fill out basic information, such as your name and email. Everything else is optional. Do not feel obligated to put your address and telephone number.
- Third level of privacy- There are three levels of privacy settings to choose from for your profile. There is “open to everyone,” “open to friends of friends” and “friends only.” The best setting to use is the “friends only” setting on all of your privacy choices. “Friends only” is the strictest level of security; it only allows people that you have accepted as a friend to view information about you.
- Accept only people you know- Accepting only people you know and trust is a great way to ensure safety when using social networking sites. Doing this can protect you from spammers, pedophiles, and other people who use social networking sites to commit crimes.

- When discussing social networking safety with your child, encourage him or her to always use discretion when posting any type of photo, location status, and message. Tell your teen to ask him or herself these four questions before posting to the world: "Think Before They Post"
- Should I share this? Will the information you share put yourself or someone else in danger?
- Do people really need to know where I am and who I am with? - Is it a good idea to let everyone know my exact location?
- Am I selecting friends online that I can trust? –Always keep in mind that it's not just about what you post, but how others may use that content.
- Is the information I am sharing transparent? - Before sharing information to the public, does your post give out too much personal information?
- Having a discussion with your teen about social networking sites can ease some anxiety about your child's safety. Social networking sites help us stay connected to family and friends. However, it's important to make sure your child knows how to be safe while online. Encourage them to enjoy the sites but to be safe at all times.

# Privacy issues on Social Network sites

- Social media is possibly the most vital sector of the Internet, but, being open and social creates legitimate concerns about privacy and safety. Headlines warning of online security breaches are just one reminder of the vulnerability of all websites, including social media outlets.
- Despite these justifiable security concerns about the Web, some of the reasons a person's social media account is compromised are self-induced. Five common mistakes that can expose an account include:
  - **1. Forgetting to Log Out**  
Increase the security of your social media account by always logging out when you step away from your laptop or computer. It's best to go one step further and close down the browser you were using to view your account. If you leave your account logged in, you set yourself up to be hacked because anyone who can get to your computer can access your account, change the password or even post items and communicate with your friends as if they are you. Logging out and shutting down the browser is even more important if you use a public computer.
  - **2. Clicking on Enticing Ads**  
Viruses and malware often find their way onto your computer through those annoying, but sometimes enticing ads. However, on the Web, just like in real life, if an offer seems to good to be true, then it probably is. Save yourself a potential security headache - don't click.
  - **3. Connecting With Strangers**  
Be careful of who you accept invitations from when building your online network. Connecting and sharing information with people you don't know can be dangerous. If you receive friend requests from strangers, it's best to stay away.
  - Further, if you receive friend requests from people you do know, but are already connected with via the same site, it's possible that someone has set up a fake account. Avoid accepting duplicate requests, instead checking in with the 'real' person to see if the request is legitimate.
  - You should also be careful when connecting with a celebrity's account, as scammers sometimes pose as famous people. Make sure it is their official, legitimate account and not a stranger pretending to be them before you accept their 'friend' invitation.

- **4. Using Third Party Apps**
  - Part of the appeal of social media sites are all the various games and apps. Even though a significant number of them are safe, you do grant the app a certain level of permission concerning your information. Make sure you know what the app is viewing and sharing before agreeing to the terms.
- **4. Exposing Too Much Information**
  - Make sure you understand the level of privacy - or lack of privacy - you are agreeing to when volunteering personal information. Do you really want an app badly enough to allow it to announce where you are?
  - Also, participating in seemingly innocent games, like posting answers to a list of 20 questions, may actually also allow cyber-criminals gather important personal information. For example, the question, "What is your most embarrassing moment?" is probably fine to answer, but answering questions like, "What is your pet's name?" or "Where did you and your significant other meet?" may expose answers you gave to security questions for legitimate sites like Amazon or your bank.
- **5. Failing to Utilize Security Settings**
  - Social media sites provide you with the ability to restrict who has access to your information. For example, Facebook (like others) lets you decide who your friends are and what content they can view. One practice to increase your account's security is to disable most of the options and then re-open them once you understand what the settings specifically mean to your account.
  - In reality, you probably want different types of content to be displayed to different people, with the most being available to known friends and the least to acquaintances.

- **What to Do if Your Account Is Hacked**
  - Regardless whether your account is compromised because the social networking site was hacked or just your individual account was infected, you need to take several steps to resolve the issue.
  - Clean Your Device
    - The aforementioned hack that compromised Facebook and Google was caused by malware on users machines. In cases like this, use well-known quality [malware removal software](#) to scan your machine. The software will contain and/or destroy known and suspicious files. You may even consider [reformatting your computer](#).
  - Once your machine is clean, the best way to prevent it from becoming infected again is to keep your antivirus software and browsers current. Set them to automatically install updates.
- **Change Your Passwords**
  - Once an account has been compromised, it is best to presume all your passwords are compromised. Some [security experts advise](#) using a different, strong password for each site.
- **Get a Password Manager**
  - Since security is dependent on multiple strong passwords, it can become difficult to remember them all -- although there are [tricks to make it possible](#). Consider using a [password manager](#) to reduce your vulnerability. You can use the program's password generator to create strong, hard-to-break passwords and you only need to remember one password to access the manager.
- **Report It**
  - Make sure you report the situation to the social network site. This is especially true if you have been locked out of your account. If this happens, you may have to prove to the social networking site the account belongs to you, but be persistent and follow through. If you don't, someone could potentially post information as if they are you - which, at the very least, can damage your online reputation.
  - If a crime has been committed, such as banking information stolen, also report the incident to local authorities and [appropriate federal law enforcement agencies](#).

- **Use Two-Step Verification**
- If the social media site offers a [two-step verification](#) process, use it. The added layer of security makes it much harder for a would-be hacker to access your account. The extra log-in steps will save you time and headaches in the long run.

# Cyber Warfare

- Cyber attacks offer terrorists the possibility of greater security and operational flexibility. Theoretically they can launch a computer assault from almost anywhere in the world, without directly exposing the attacker to physical harm...
- **Cyberwar**, also spelled **cyber war**, also called **cyberwarfare** or **cyber warfare**, war conducted in and from computers and the networks connecting them, waged by states or their proxies against other states.
- Cyberwar is usually waged against government and military networks in order to disrupt, destroy, or deny their use. Cyberwar should not be confused with the terrorist use of cyberspace or with cyberespionage or cybercrime.
- Even though similar tactics are used in all four types of activities, it is a misinterpretation to define them all as cyberwar.
- Some states that have engaged in cyberwar may also have engaged in disruptive activities such as cyberespionage, but such activities in themselves do not constitute cyberwar.

- Computers and the networks that connect them are collectively known as the domain of cyberspace.
- Western states depend on cyberspace for the everyday functioning of nearly all aspects of modern society, and developing states are becoming more reliant upon cyberspace every year.
- Everything modern society needs to function—from critical infrastructures and financial institutions to modes of commerce and tools for national security—depends to some extent upon cyberspace.
- Therefore, the threat of cyberwar and its purported effects are a source of great concern for governments and militaries around the world, and several serious cyberattacks have taken place that, while not necessarily meeting a strict definition of cyberwar, can serve as an illustration of what might be expected in a real cyberwar of the future.

- **What would be attacked?**
- 1. Information - such as stealing information from storage devices for instance.
- 2. Information based processes - attack on processes that collect, analyze, and disseminate information using any medium or form and attack on the networking.
- 3. Information and communication systems - attack on the infrastructure, organizations, personnel and components that collect, process, store, transmit, display, disseminate and act on information

- **What would be defended (protected)?**
- 1. Information - such as protect from being stolen for instance.
- 2. Information based processes - protect the processes that collect, analyze, and disseminate information from being attacked and protect our networking.
- 3. Information and communication systems - protect our infrastructure, organizations, personnel and components that collect, process, store, transmit, display, disseminate from being attacked.

# CyberTerrorism

- **Cyberterrorism** is the use of the [Internet](#) to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through [threat](#) or [intimidation](#).
- It is also sometimes considered an act of Internet terrorism where [terrorist](#) activities, including acts of deliberate, large-scale disruption of [computer networks](#), especially of personal computers attached to the Internet by means of tools such as [computer viruses](#), [computer worms](#), [phishing](#), and other malicious software and hardware methods and programming scripts.
- Cyberterrorism can be also defined as the intentional use of computers, networks, and public internet to cause destruction and harm for personal objectives. Experienced cyberterrorists, who are very skilled in terms of [hacking](#) can cause massive damage to government systems and might leave a country in fear of further attacks.

# Types of cyberterror capability

- **Simple-Unstructured:** the capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target-analysis, command-and-control, or learning capability.
- Advanced-Structured: the capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking-tools. The organization possesses an elementary target-analysis, command-and-control, and learning capability.
- Complex-Coordinated: the capability for a coordinated attack capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target-analysis, command-and-control, and organization learning-capability.

# Hacktivism

## What Is Hacktivism?

- Hacktivism is a social or political activist act that is carried out by breaking into and wreaking havoc on a secure computer system. Hacktivism is a mix of “hacking” and “activism” and is said to have been coined by the hacktivist group Cult of the Dead Cow.
- Hacktivism involves breaking into a computer system and making changes that affect a person or organization.
- Targets range from religious organizations to drug dealers and pedophiles.
- Hacktivists use a wide range of techniques to work towards their goals including doxing, denial of service attacks (DoS), anonymous blogging, information leaks, and website replication.
- Hacktivism’s goals include circumventing government censorship by helping citizens get around national firewalls (or helping protestors organize) and using social media platforms to promote human rights.
- Some of the most widely known hacktivist groups include Anonymous, Legion of Doom (LOD), Masters of Deception (MOD), and Chaos Computer Club.

- Hacktivism is usually directed at corporate or government targets. The people or groups that carry out hacktivism are referred to as hacktivists. Hacktivists' targets include religious organizations, terrorists, drug dealers, and pedophiles.
- An example of hacktivism is a [denial of service attack](#) (DoS) which shuts down a system to prevent customer access. Other examples involve providing citizens with access to government-censored web pages or providing privacy-protected means of communication to threatened groups (such as Syrians during the Arab Spring).
- Hacktivists' methods may include distributed denial of service (DDoS) attacks, which flood a website or email address with so much traffic that it temporarily shuts down; data theft; website defacement; computer viruses and worms that spread protest messages; taking over social media accounts, and stealing and disclosing [sensitive data](#).
- There is disagreement within the hacktivist community over which techniques are appropriate and which are not. For example, while hacktivists may claim supporting free speech as an important cause, the use of DoS attacks, website defacements, and data theft that hinder or prevent free speech may be at odds with that goal.

- The methods hacktivists use are illegal and are a form of cybercrime. Yet they often are not prosecuted because they are rarely investigated by law enforcement. It can be difficult for law enforcement to identify the hackers and damages that ensue tend to be minor.
- Hacktivist attacks themselves are not violent and don't put protestors at risk of physical harm, unlike participating in a street protest, but hacktivism might incite violence in some cases.
- Hacktivism also makes it possible to support geographically distant causes without having to travel there and allows geographically dispersed people with common goals to unite and act in support of a shared goal.

- **Types of Hacktivism**
- Hacktivists use a wide range of tools and techniques to work towards their goals. They can include actions like:
- **Doxing:** In this method, hacktivists gather sensitive information about a specific person or organization and make it public.
- **Blogging anonymously:** This tactic is primarily used by whistleblowers, journalists, and activists to bring light to a specific issue while maintaining privacy.
- **DoS and DDoS attacks:** This tactic aims to flood targeted computer systems or networks to prevent users from accessing them.
- **Information leaks:** In this tactic, an insider source with access to sensitive or classified information (that implicates a specific individual or organization) makes it public.
- **Website replication:** This method seeks to mirror a legitimate website, using a slightly different URL, to circumvent censorship rules.

## Hacktivism Goals

- Hacktivism's goals include the following:
- Circumventing government censorship by helping citizens get around national firewalls or helping protestors to organize online
- Using [social media](#) platforms to promote human rights or help censored citizens of oppressive regimes communicate with the outside world
- Taking down government websites that pose a danger to politically active citizens
- Protecting free speech online
- Promoting access to information
- Supporting citizen uprisings
- Assisting computer users in protecting their privacy and avoiding surveillance through secure and anonymous networks such as [Tor](#) and the Signal messaging app
- Disrupting corporate or government power
- Helping illegal immigrants cross borders safely
- Supporting democracy
- Protesting globalization and capitalism
- Protesting acts of war
- Halting the financing of terrorism.

# UNIT 3

# Securing PC

- Keeping your PC secure is critical to protecting the personal, business, and financial information it contains. Fortunately, securing your computer is easy if you take the proper precautions.
- Using secure passwords and verification processes will make it more difficult for another person or program to impersonate you and access your information.
- Using protective software will make it harder for a hacker, virus, or malicious software to penetrate your PC. In addition to protective programs, using encryptions and safe practices will help keep your data secure when you're using the Internet.

# Method 1: Encrypting Your Data

General Labels Inbox Accounts and Import Filters Forwarding and POP/IMAP

Language: Gmail display language: English (UK)

Maximum page size: Show 50 conversations per page  
Show 250 contacts per page

Keyboard shortcuts:  Keyboard shortcuts off  
 Keyboard shortcuts on

External content:  Always display external content (such as images)  
 Ask before displaying external content

Browser connection:  Always use https  
 Don't always use http

Default reply behaviour:

Conversation View:  Conversation view on [wikiHow to Secure Your PC](#)

**1** Select "Always use https" in Gmail. To make sure your Gmail page is always using a secure HTTPS connection, click on the gear icon in the top-right corner. Scroll to the tab labeled "General." In the general menu, choose the option to always use an HTTPS connection.<sup>[1]</sup>

- Your Gmail settings will be saved so anytime you use it, you'll be using an HTTPS connection.
- Your Gmail likely contains a lot of your important and personal information, so keep it secure with an HTTPS connection.

Search

General  
**Security and Login**  
Your Facebook Information

Privacy  
Timeline and Tagging  
Stories  
Location  
Blocking  
Language and Region  
Face Recognition

Notifications  
Mobile  
D. My Profile

**Recommended**

Where You're Logged In

wikiHow to Secure Your PC

**2** Set your Facebook to use an HTTPS connection. To change your Facebook settings to use an HTTPS connection, click on the down arrow in the top right corner of your screen and select the "Account Settings" option. In the menu for your account settings, click on the option labeled "Security" to bring up the menu. In the "Secure Browsing" section, check the box labeled "Browse Facebook on a secure connection (https) when possible" to change the settings.<sup>[2]</sup>

- Viruses and malware can breach your PC by using your Facebook account.

## HTTPS Everywhere

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure.

**Encrypt the web: Install HTTPS Everywhere today.**



[Install in Firefox](#)



[Install in Firefox](#)



[Install in Chrome](#)



[Install in Opera](#)

[for Android](#)

HTTPS Everywhere is produced as a collaboration between [The Tor Project](#) and the

[Electronic Frontier Foundation](#). Many sites on the web offer some limited support for HTTPS. [How to Secure Your PC](#)

- 3** **Install the HTTPS Everywhere extension for your browser.** If you use Google Chrome, Opera, or Firefox as your web browser, you can add an extension that will automatically request an encrypted connection whenever you visit a web page. If the page supports an HTTPS connection, then your browser will automatically use an encrypted connection. Download the extension to add it to your browser.<sup>[3]</sup>

- Visit <https://www.eff.org/https-everywhere> to download the extension.

**Tip:** After you install the extension, make sure it's turned on by clicking on the icon in the corner of your browser window.

The screenshot shows a Windows Start Menu search interface. At the top, there is a navigation bar with tabs: All, Apps, Documents, Email, Web, and More. Below this is a search bar containing the text "tunne". Underneath the search bar, the text "Best match" is displayed above a list item. The list item "TunnelBear" is highlighted with a green rectangular border. To the left of the list item is a small icon of a brown bear in a yellow hat. To the right of the list item is the text "App". Further down the screen, there is a section titled "Search the web" with a magnifying glass icon and the text "tunne - See web results". On the right side of the screen, there is a vertical list of actions for the selected item: "Open", "Run as administrator", "Open file location", "Pin to Start", "Pin to taskbar", and "Uninstall". At the bottom right of the screen, there is a small green banner with the text "wikiHow to Secure Your PC".



Getting Started

# wikiHow to do anything

## Method 3

### Encrypting Your Data

wikiHow to Secure Your PC

**5** Use an HTTPS connection on websites to secure your PC. Hypertext transfer protocol secure (HTTPS) is an encrypted website connection that your browser uses when you're accessing and viewing a web page. You can tell that the website you're viewing is using an HTTPS connection if you see "https:" at the beginning of the website's address in your web browser's address bar.<sup>[5]</sup>

- Many websites use an HTTPS connection that will keep your PC safer from viruses and malware.

# Method 2: Setting up Secure Password Protection

Manage how you sign in to Microsoft

Edit date of birth

Edit country/region

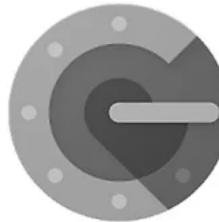
wikiHow to Secure Your PC

1 Turn on the “Two-step Verification” option for your Windows account. Open your web browser and log in to your account on the Microsoft website. Look for the security settings option at the top of the page and click on it to access the menu. When the expanded security menu pops up, look for the option labeled “Two-step Verification.” Click the button to turn it on.<sup>[6]</sup>

- Sign into your account at <https://account.microsoft.com/profile>.
- The two-step verification system adds another way for you to verify that it's really you using the account, which adds another level of security to your PC.
- You don't have to use Outlook or other Windows apps in order to set up the two-step verification system.

**Tip:** In order to add the second verification, you need a device or email for Microsoft to send you a code that you can use to prove that it's you. Enter your phone number if you want to receive a code by text or type in your email address if you want to receive the access code by email.

1



Google Authenticator

Google LLC Tools

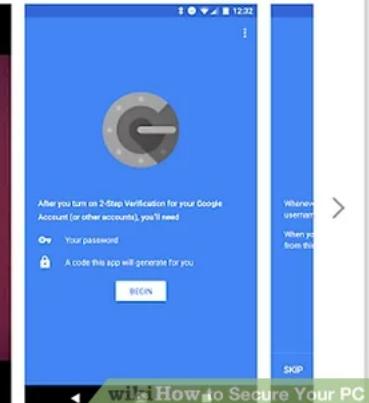
★ ★ ★ ★ 179,074

PEGI 3

⚠ You don't have any devices.

Add to Wishlist

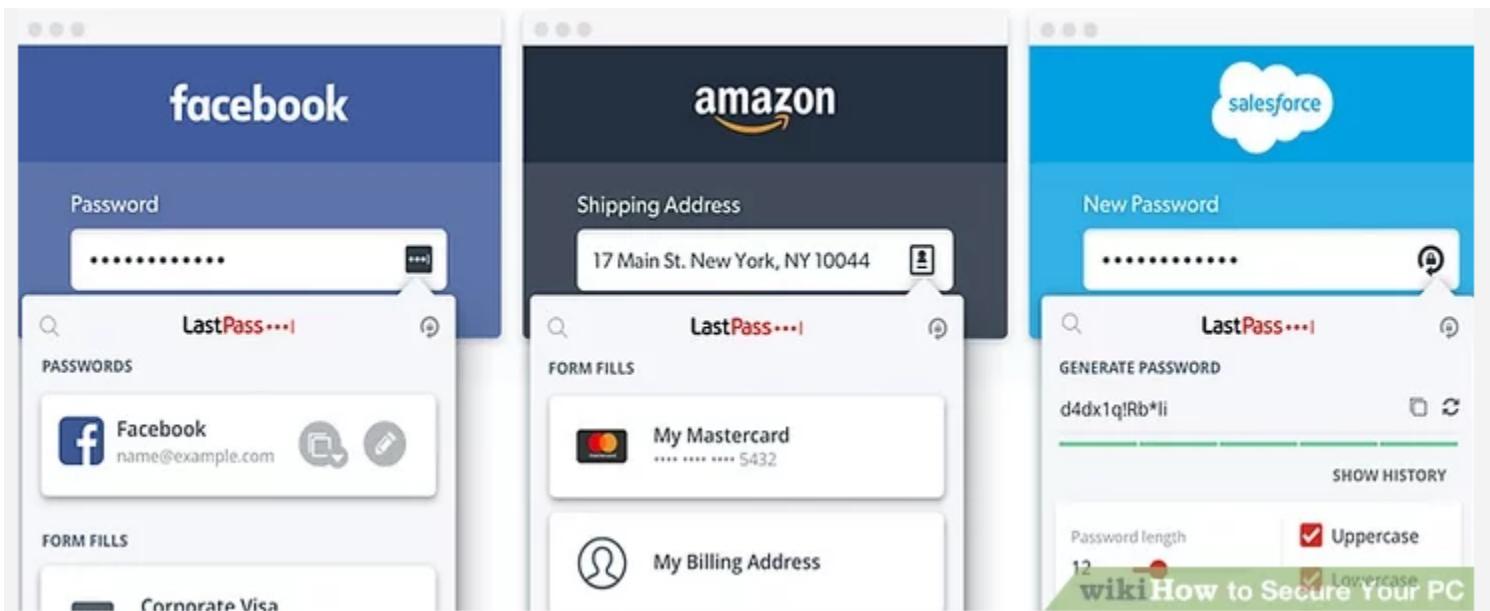
Install



2

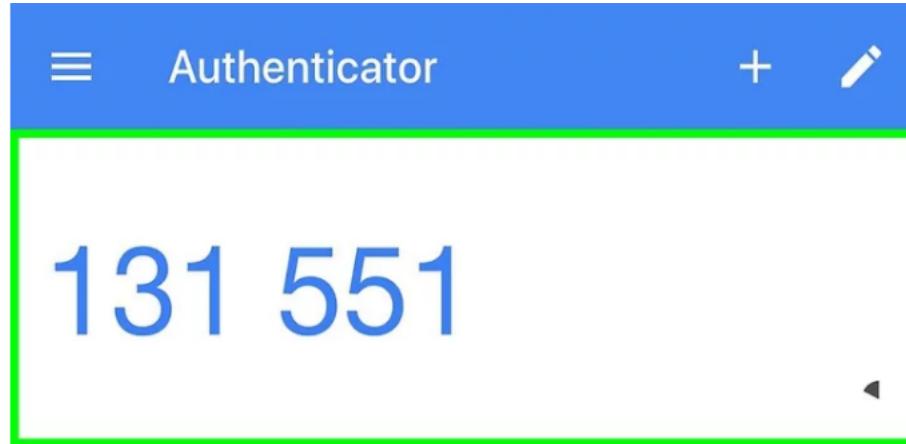
Download an authenticator app to secure the apps that you use. Download an authenticator app to your smartphone or tablet so you don't have to receive codes via text message or email every time you want to verify that it's you accessing an app or account. Add all of the apps that you use to the app so you can easily verify yourself and secure your apps.<sup>[7]</sup>

- Popular authenticator apps include Google Authenticator, Authy, and LastPass.
- Add your social media accounts to your authenticator app to create another layer of security.



**3** **Use a password manager to keep track of your passwords.** Password managers don't just store and keep track of your passwords, they allow you to generate and use strong and unique passwords whenever you sign up for a new website or app. When you log in, you can pull up your password generator, copy your password, and paste it into the login box.<sup>[8]</sup>

- Some password managers come with browser extensions that will automatically fill in your passwords.
- Popular password managers include LastPass, 1Password, and Dashlane.
- You may need to pay a monthly or yearly subscription fee to download some password managers.



747 337

wikiHow to Secure Your PC

**4** Add your phone to your Google account to activate 2-Step Verification. Google uses a two-factor authentication system called 2-Step Verification, which makes your account more secure. Go to your account security settings in the browser and add your smartphone to your account to activate it. You'll receive a code by text, phone call, or with an authenticator app.<sup>[9]</sup>

- Download the Google Authenticator app from your app store after you activate the 2-Step Verification to generate a verification code even when you're not connected to the internet.

## Two-Factor Authentication

### Use two-factor authentication

We'll ask for a security code if we notice a login from an unusual device

**Edit**

### Authorized Logins

Review a list of devices where you won't have to use a login code

**View**

### App passwords

Use special passwords to log into your apps instead of using your Facebook password or login codes.

**Add**

## Setting Up Extra Security

### Get alerts about unrecognized logins

We'll let you know if anyone logs in from a device or browser you don't usually use

**Edit**

### Choose 3 to 5 friends to contact if you get locked out

On • Your trusted contacts can send a code and URL from Facebook to help you log back in

**Edit**

## Advanced

### Encrypted notification emails

Add extra security to notification emails from Facebook (only you can decrypt these emails)

**Edit**

### Recover external accounts

Recover access to other sites with your Facebook account

**Edit**

wikiHow to Secure Your PC

## 5 Change your Facebook settings to set up a two-factor authentication.

To keep your Facebook account more secure, go the "Security and Login" menu under your account settings. Click "Edit" on the right of the "Two-Factor Authentication" option to choose how you want to receive your second form of authentication. You can receive a code via text message or use an authenticator app.<sup>[10]</sup>

- Your Facebook account is full of personal information that you want protected, but it can also be a way for hackers or malware to breach your PC.

# Method 3: Using Protective Software

- **1. Install antivirus software to protect your PC.** Antivirus software is a security utility designed to keep your PC safe against viruses, spyware, malware, and other online threats. Quality antivirus software needs to be purchased and installed onto your PC. Popular antivirus software include Avast, AVG, McAfee, and Symantec.
  - Set your software setting to automatically scan for viruses and malware so you can keep your PC clear of them.
  - Many programs can also block ads and spam from websites to keep your PC safer while you're browsing the internet.
- 2. Enable your firewall to filter information from the internet.** A firewall is a program that monitors information coming through the internet connection to your PC to block harmful programs. Go to your PC's control panel and open up the "System and Security" menu. Click on the Windows Firewall shortcut and make sure it's turned on. Your built-in Windows firewall is just as good as any antivirus program's firewall.
- Make sure you're connected to the internet when you turn your firewall on so it connects.
  - If you can't find the shortcut, type in "firewall" in the search bar of the System and Security menu.

- **3. Clean up your PC using malware-removal products.**
- Firewalls and antivirus software are designed to prevent your computer from becoming infected, but they can't remove viruses or malware once they infect your computer. Use an anti-malware program to clean up your system after an attack or infection. Download the software and run periodic scans to check for harmful programs.
- Popular malware-removal products include Spybot Search & Destroy and Malwarebytes Anti-Malware.
- Schedule regular scans to check for spyware, malware, and viruses.

# Method 4: Following Safe Practices

## Windows Update



Updates available

Last checked: Yesterday, 9:08 PM

2019-08 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 1903 for x64 (KB4511555)  
**Status:** Pending download

Updates are ready to download

[Download](#)

### Optional updates available

- 2019-08 Cumulative Update for Windows 10 Version 1903 for x64-based Systems (KB4512941)

[Download and install now](#)



**Pause updates for 7 days**

Visit Advanced options to change the pause period



**Change active hours**

Currently 8:00 AM to 5:00 PM

wikiHow to Secure Your PC

**1 Keep your PC up to date.** It's important that your PC has all of the latest tools and updates to stay secure. Access the Windows Update option in your control panel and click on "Check for Updates." Choose the option to install any updates that are available.<sup>[14]</sup>

- Some updates may take up to an hour to complete, especially if you haven't updated your PC in a while.
- Restart your computer when it's done updating so the updates take effect.

[Sent from Yahoo Mail on Android](#)



wa-agreeme....pdf

152.8kB



[Reply](#), [Reply All](#) or [Forward](#)

wikiHow to Secure Your PC

**2 Scan email attachments before you open them.** Even if an email appears to be sent by somebody that you know, it could be a tactic called "spear phishing," which disguises itself as one of your contacts in order to gain access to your email and PC. Right-click on any attachments and choose the option to scan the file manually to make sure it's safe.<sup>[15]</sup>

**Tip:** Never open attachments in emails from people or companies that you don't know.

# Settings

General Labels Inbox Accounts and Import Filters and Blocked Addresses Forwarding and POP/IMAP

**Default reply behavior:**

[Learn more](#)

- Reply**  
 **Reply all**

**Hover actions:**

- Enable hover actions** - Quickly gain access to archive, move, and delete options  
 **Disable hover actions**

**Images:**

- Always display external images** - [Learn more](#)  
 **Ask before displaying external images** - This option

**Dynamic email:**

[Learn more](#)

- Enable dynamic email** - Display dynamic email content from your contacts  
[Developer settings](#)

**Smart Compose personalization:**

(Smart Compose is personalized to your writing style)

- Personalization on**  
 **Personalization off**

**Smart Compose:**

(predictive writing suggestions appear as you compose an email)

- Writing suggestions on**  
 **Writing suggestions off**

[Feedback on Smart Compose suggestions](#)  
wiki How to Secure Your PC

**3** **Disable images in your email for extra security.** Harmful programs can use loopholes to gain access to your email and PC. To help keep out unwanted software, disable the images in your received messages. Go the account settings in your email and choose the option to ask you before your email displays images.<sup>[16]</sup>

- In Gmail, click on the settings option in the upper right corner of the screen. Choose the mail settings and click the box to "Ask before displaying external content."

# Family & other users

## Your family

Add your family so everybody gets their own sign-in and desktop. You can help kids stay safe with appropriate websites, time limits, apps and games.



Add a family member

[Learn more](#)

## Other users

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.



Add someone else to this PC

wikiHow to Secure Your PC

**4** **Use a non-administrator Windows account to block malware.** If you set up your PC without changing any settings, you may be using an administrator account, which can leave your PC exposed to potential attack. Choose the "Manage another account" option in the User Accounts menu and create a new account. Select the "Standard user" option when you create the account.<sup>[17]</sup>

- Using a standard account adds an extra level of security to your PC.

**Cookies and Site Data**

Your stored cookies, site data, and cache are currently using 783 MB of disk space. [Learn more](#)

Delete cookies and site data when Firefox is closed

**Clear Data...** **Manage Data...** **Manage Permissions...**

**Logins and Passwords**

Ask to save logins and passwords for websites

**Exceptions...** **Saved Logins...** **Change Master Password...**

Use a master password

**History**

Firefox will Remember history

wikiHow to Secure Your PC

**5** **Clear cookies that you don't want or need from your browser.** Cookies are a way for websites to retain information about you and your browser to make browsing their site easier and more convenient. But they can also be used by hackers or harmful software. Go to your browser settings and clear out any cookies that you don't want.<sup>[18]</sup>

- Having cookies for some websites may be helpful so you don't have to reenter information into a site you visit often.



Getting Started

# wikiHow to do a

wikiHow to Secure Your PC

**6** **Avoid websites that don't have HTTPS in their address.** If a website seems suspicious or if it asks you to enter personal information, avoid visiting it to keep your PC safe from a potential breach. A clear sign that a website isn't safe is if it doesn't have HTTPS in its web address.<sup>[19]</sup>

- Not all websites without HTTPS in their web address are dangerous, but they aren't encrypted, so don't input any personal or financial information into them to be safe.

# 8 easy steps to secure your computer

- **1. Keep up with system and software security updates**
- While software and security updates can often seem like an annoyance, it really is important to stay on top of them. Aside from adding extra features, they often cover security holes. This means the provider of the operating system (OS) or software has found vulnerabilities which give hackers the opportunity to compromise the program or even your entire computer.
- Typically if an update is available for your OS, you'll get a notification. You can often opt to update immediately or set it to run at a later time. While it can be inconvenient to stop what you're doing for half an hour for an update to take place, it's often best to just get it done out of the way.
- It's not just your OS that should be kept up-to-date. All software that you run on your computer could potentially have flaws. When updates are available, you might see a popup when you open the software.
- Even though they are usually a good thing, it's prudent to be wary of updates. Sometimes software companies will offer pre-release versions to try. These may be unstable and should be used at your own risk. Even with stable release versions, you may want to wait a day or two in case there are any obvious bugs. Just remember to go back to it when you're ready.
- Another thing to watch out for is a fake update. These might be used by hackers to persuade you to click a link or enter credentials. You can avoid falling prey to these by doing a little research into the latest updates from the software company. Simply search for the latest version to see if the alert you received makes sense. Alternatively, you can plug the popup text in a search engine to find out if it's a known scam.

- **2. Have your wits about you**
- It should go without saying, being suspicious is one of the best things you can do to keep your computer secure. Admittedly, with hacker techniques becoming increasingly sophisticated, it can be difficult to tell when you're under attack. All it takes is one email open or link click and your computer could be compromised.
- Make sure you have your wits about you and think twice about opening or clicking on anything that doesn't look legit. Don't rely on spam filters to always catch sketchy emails. Criminals are constantly trying to outsmart these settings and now and again they'll get through.
- **3. Enable a firewall**
- A firewall acts as a barrier between your computer or network and the internet. It effectively closes the computer ports that prevent communication with your device. This protects your computer by stopping threats from entering the system and spreading between devices. It can also help prevent your data leaving your computer.
- If your computer ports are open, anything coming into them could be processed. This is bad if it's a malicious program sent by a hacker. While it's possible to [close ports manually](#), a firewall acts as a simple defence to close all ports. The firewall will open the ports only to trusted applications and external devices on an as needed basis.
- If your operating system comes with a firewall (e.g. Windows XP onward), you can simply enable the built-in firewall. In Windows, this can be found by navigating to **Control Panel>System and Security**. You might choose to install an additional firewall as an extra layer of defense or if your OS doesn't already have one. A couple of free options are [Comodo](#) and [TinyWall](#). Antivirus software often comes with a built-in firewall too.
- The firewalls discussed above are software firewalls. There is a second type known as a hardware firewall. While these can be purchased separately, they often come built into home routers. It could just be a simple case of [checking if yours is turned on](#).

- **4. Adjust your browser settings**
  - Most browsers have options that enable you to adjust the level of privacy and security while you browse. These can help lower the risk of malware infections reaching your computer and malicious hackers attacking your device. Some browsers even enable you to tell websites not to track your movements by blocking cookies.
  - However, many of the options are disabled by default, so you could unwittingly be exposing far more than you need to each time you browse. Thankfully, it should only take a few minutes to go into your browser settings and make the necessary adjustments. [Chrome](#), [Firefox](#), [Safari](#), and [Edge](#) all provide detailed instructions to help. While using these browsers you can add an additional layer of protection by installing an anti-tracking browser extension like [Disconnect](#) or [uBlock Origin](#).
  - On the topic of browsers, you should choose yours carefully. The ones mentioned above are generally considered safe. But since updates and patches occur all the time, you never know when a new hole could appear and how big it will be. If you want more privacy, you can consider steering away from traditional options and look at privacy-focused alternatives like [Epic Privacy Browser](#), [Comodo Dragon](#), or [Tor](#) Browser.
- **5. Install antivirus and anti spyware software**
  - Any machine connected to the internet is inherently vulnerable to viruses and other threats, including malware, ransomware, and Trojan attacks. An antivirus software isn't a completely foolproof option but it can definitely help. There are free options out there, but they're limited, and besides, the paid programs won't set you back a whole lot. [Bitdefender](#) is a popular option that I recommend. For alternatives take a look at this data backed [comparison of antivirus](#).
  - Spyware is a specific type of malware that is designed to secretly infect a computer. It then sits in the system, gathers information, and sends it to a third party. The information is typically of a sensitive nature, such as credentials or banking information. This can ultimately lead to identity theft, a multi-billion dollar industry.
  - In the spyware category, you have adware (often causing popups), [Trojans](#) (posing as a harmless software), and system monitors (such as keyloggers), all of which pose a pretty serious threat. Other forms of spyware like tracking cookies are typically harmless albeit annoying. Thankfully, many antivirus programs have anti spyware built in, but there are some dedicated solutions.
  - If spyware has found its way onto your computer, then it's very possible you can remove it. There are a [ton of options](#) for spyware removal, including many free offerings and some paid single use tools.

- **6. Password protect your software and lock your device**
- Most web-connected software that you install on your system requires login credentials. The most important thing here is not to use the same password across all applications. This makes it far too easy for someone to hack into all of your accounts and possibly steal your identity.
- If you're having trouble remembering a whole bunch of passwords, then you could try a password manager. This will keep all of your passwords safe and you only have to remember one. A password can be combined with an email or SMS as part of a two-step verification (2SV) method for extra security. 2SV usually kicks in when you log into a website or app from a new or unrecognized device requiring you to verify your identity with a PIN code.
- While many security steps relate to intangible threats, there is always the possibility that someone could get their hands on your actual computer. A simple line of defence here is to have a strong computer password to at least make it more difficult for them to enter.
- Other forms of verification include biometric methods like a fingerprint or retina scan. Alternative physical verification methods might involve key cards and fobs, such as those offered by [Yubico](#). Any of these can be combined with each other and/or a password as part of a two-step authentication (2FA) process.
- If you're concerned about someone actually walking away with your computer, another option is a physical lock. This is an ideal solution for laptops but can also be used on home or work computers. [Kensington locks](#) and other similar brands are small locks that insert into a special hole in the device. Some require a physical key while others work using a code. There *are* solutions for tablets, although these tend to be more cumbersome and more suitable for things like point-of-sale.
- **7. Encrypt your data**
- Whether your computer houses your life's work or a load of files with sentimental value like photos and videos, it's likely worth protecting that information. One way to ensure it doesn't fall into the wrong hands is to encrypt your data. Encrypted data will require resources to decrypt it; this alone might be enough to deter a hacker from pursuing action.
- There are a plethora of tools out there to help you encrypt things like online traffic and accounts, communication, and files stored on your computer. For full disk encryption, some popular tools are [VeraCrypt](#) and [BitLocker](#). You can find separate tools to help you encrypt your mobile device, with various apps available for both Android and iOS.

- **8. Use a VPN**
- A Virtual Private Network (VPN) is an excellent way to step up your security, especially when browsing online. While using a VPN, all of your internet traffic is encrypted and tunneled through an intermediary server in a separate location. This masks your IP, replacing it with a different one, so that your ISP can no longer monitor your activity.
- What's more, you can typically choose the server location based on your needs, such as getting the fastest speeds or unblocking geo-locked content. Additionally, a VPN can help you browse securely while using open wifi networks and access censored material (e.g. Facebook in China).
- When it comes to choosing a provider, there are some okay free offerings out there, but monthly rates for paid services can be pretty low, even as little at \$3 per month. The free ones are typically limited in features but can be good for getting a feel for what's available. Some paid options have free trial periods for the full service and most offer generous money-back guarantee periods.
- No matter what you store on your computer, it's simply prudent to protect its content from criminals and snoopers. Although nothing is ever completely secure, following the steps above will provide most people with ample protection and safeguard their data.

# Securing Smart Phone

- In addition to storing sensitive information on laptops and desktops, today's small businesses rely heavily on mobile devices, like smartphones, to get work done. Business smartphones, either provided by the business or the employee, are used for a range of commercial operations: inventory control, customer relations, advertising and marketing, banking and more.
- As such, they become repositories for valuable data that can be targeted by hackers and malware. Taking the appropriate precautions to protect data is much like investing in an insurance policy, and most of it comes down to instilling best practices across your business, not investing in expensive products.

- **1. Update your OS and apps promptly.**
- Most people are guilty of postponing or ignoring operating system updates and app updates, but doing so on a regular basis can open you up to a data breach. Hackers know how to identify and exploit vulnerabilities in systems; as those vulnerabilities are made known to the company, improvements are made to increase security and eliminate weaknesses. The longer you wait to update your phone or laptop, the more out of date your systems are, making you an easier target for hackers.
- If your small business utilizes a BYOD (bring your own device) policy, establish a training and awareness program for your employees. Make sure your staff understands that they are expected to take reasonable security precautions when using their smartphones and tablets, including running regular updates and being discerning about app downloads.
- **2. Lock your devices.**
- Sure, it's a lot easier to keep your phone unlocked all the time because you can get to your email, camera, texts, and other features more quickly, but just think how you would feel if a stranger found your phone on a bus seat or in a coffee shop and could just tap on your business apps, contacts, and even banking information. If your phone contains client information, you could even end up in the embarrassing position of informing your clients that their data has been compromised, essentially due to negligence.
- To prevent that from happening, always engage the four- or six-digit passcode – or set up a longer alphanumeric code – so that if you ever lose track of your phone, it won't open your entire business to a stranger. Utilizing fingerprint scanning and facial identification is also an excellent option, as it's faster and easier than memorizing an unlock code. Also, be sure to password-protect all mobile apps that contain personal data, such as banking, email and your Amazon account. Don't use the same password for all your accounts, and change your passwords occasionally for good measure.

- **3. Utilize mobile device management, small business style.**
- If a work phone gets lost or stolen, you can contain the damage using basic smartphone features. Both Apple and Google offer find device services, such as [Find My iPhone](#) and Android's [Find My Device](#), that can locate your phone on a map and automatically disable it. These services can also make your phone ring, either alarming the thief or just locating a phone you have temporarily lost track of. You can even arrange for the phone to delete all information after five to 10 false passcode tries.
- For small business owners who want more control, affordable mobile device management software is a good option. If your business currently uses Microsoft Office 365, you should already have access to MDM features through [Mobile Device Management for Office 365](#). There are also stand-alone MDM products like AirWatch's [Workspace ONE](#) (a VMware product) and [Hexnode](#), but despite offering SMB solutions, Office 365's MDM is far more suitable for most small business owners.
- **4. Use Wi-Fi and Bluetooth wisely.**
- Most people don't think twice about jumping on a free public Wi-Fi connection, but people operating devices with sensitive business information on them should exercise caution. Business travelers often use hotel or conference center Wi-Fi. In general, this is an OK practice as businesses like reputable hotels and event venues have a vested interest in maintaining the security of their Wi-Fi users. However, free public Wi-Fi in areas like shopping centers, cafes, airports, parks or gyms, is often far less secure.
- Try to use only your private cell connection whenever possible and switch off Wi-Fi on your mobile phone whenever you are in a public place. And, of course, do not sign on to unencrypted open networks. If that is not possible, consider using a VPN, but choose carefully, as all are not created equal. A VPN tunnels your network traffic through an encrypted connection to a server based in another location. Unless you are wearing a smartwatch that requires a Bluetooth connection for functionality, it's also a good idea to disable Bluetooth when you're out and about.

- **5. Use two-factor authentication wherever possible.**
- Two-factor authentication (2FA) is one of the least-favorite security options around because, as the name implies, it requires an extra step. However, it offers another solid barrier to accessing your private information, and two-factor authentication is much easier to use now (thanks to biometric scanners and save-password features) than it used to be.
- **6. Manage app permissions.**
- Check the apps on your phone to determine whether they have more privileges than they need to get the job done. You can grant apps permissions like access to the camera, the microphone, your contacts and your location. Keep track of which permissions you've given to which apps, and revoke permissions that are not needed.
- For iPhones, go to Settings and tap on Privacy, where you'll see a list of all permissions and the apps you've granted them to. Android users can find app permissions in the Application Manager under Device > Application in some Android versions.
- **7. Ignore spam and phishing emails.**
- One of the easiest ways for hackers to access your company's information is through your employee's email inboxes. Even major corporations have suffered breaches due to phishing scams. Incorporate email security training as part of your basic onboarding procedure, and make sure employees are aware that they shouldn't click on links in promotional emails, open suspicious attachments or run updates that are prompted through email (including those that say they come directly from a company, like Microsoft).
- Make sure employees understand company policy. For example, let them know that your business will never ask them for personal information or send them links regarding their 401(k) accounts and that if they see such emails, they should assume they are fraudulent. If they want to cross-check their accounts, to make sure their 401(k) or other sensitive information is OK, tell them to go directly to the financial institution's website and log into their accounts directly, rather than clicking on a link in an email.

- **8. Back up your data.**
- Bad stuff happens, but don't compound the problem by not being prepared. Always back up your data. This is a general good practice, and it protects your important documents and images in case of any loss.
- For an Android phone, make sure "Back up my data" and "Automatic restore" are enabled in the settings and then sync your data with Google. For an iPhone, choose your device in the settings and then back up to iCloud.
- **9. Use an antivirus app.**
- Hackers typically use malware to steal passwords and account information. There are plenty of smartphone antivirus apps — some of which are linked to companion desktop apps. These provide enhanced security by ensuring apps, PDFs, images and other files you download aren't infected with malware before you open them. Antivirus apps like [Avast](#), [McAfee](#) and [Panda](#) can halt such threats.
- **10. Know where your apps come from.**
- Don't just download any app to your phone. While iPhones only run apps from Apple's App Store, which vets all apps sold from the platform, standards are not quite as high on Android. The Google Play Store has made progress in ensuring its apps aren't running malware, but the Android platform allows installation from various, less-regulated environments. The best way to avoid malware on Android is to stick with the Google Play Store, unless you are sure you can trust an independent app from somewhere else.

# Securing Laptops/Tabs

- More employees with more [laptops](#) can mean greater exposure of your network to roaming security threats. And, in a worst-case scenario, a stolen laptop with sensitive customer data or proprietary company information can also expose the company to liabilities, legal or otherwise. Lost customer data can lead to identity theft and open the company to lawsuits. Lost proprietary information can damage the company's competitive edge, if not its business altogether.
- Large organizations have sophisticated network defenses and firewalls to block malware from compromised laptops. For outbound threats, they may also employ complex content control systems to prevent the loss of customer data or company information. Not so for small and medium-sized businesses (SMBs), which [may operate simple firewall networks](#) on a shoestring and don't have the cash to spend on expensive content filtering systems and software.

- There are three parts to laptop security: physical security, administrative access and technical controls.
- **Physical security:** A laptop should never be left unattended. If you have to get up, for any reason, power down the laptop and take it with you. Unattended laptops have been targets of thieves in airport lounges and at Starbucks.
- If it's absolutely necessary to leave the laptop, use a good lock. The Defcon SCL cable lock from Targus Inc. is especially designed for laptops. It consists of a cable with a combination lock that plugs into the locking port of any laptop. The cable can be used to lock the laptop to a table, if you have to step away for a minute.
- Other physical security measures for laptops include carrying them in nondescript briefcases rather than laptop bags, especially those emblazoned with big logos from the laptop manufacturer. Another thing to watch out for is shoulder surfing. Working on a laptop in a public place leaves you open to let people see everything you're doing. Try to work away from crowds in a secluded area like an empty gate at an airport or a table facing a wall -- not a window -- in a coffee shop. Shoulder surfers have been known to even peer through windows.
- Privacy filters also protect against unwanted wandering eyes. Privacy filters are screens that stick to a laptop monitor with adhesive tape. Only someone looking directly at the screen can see it, but to others it looks dark. Privacy filters range in price from \$50 to \$90 and are available from 3M Co. and Fellowes Inc.

- **Administrative access:** The best administrative controls are an inventory system for keeping track of who has a company laptop, and what they're doing with it. Every employee allowed a laptop should be required to sign it out, whether it's given for temporary or long-term purposes. The laptop's make, model and serial number should be recorded along with the name and signature of the employee using it. The records should be kept by your IT staff, which is already probably managing the issuing and maintenance of your company's laptops.
- Personal laptops should never be allowed on a company network. You never know what's on a personal laptop that could infect your network.
- **Technical controls:** Technical controls include encryption, personal firewalls and antivirus software and virtual private network (VPN) connections. Also, all laptops should have a standard build and be required to authenticate to your network like any workstation. In fact, look at a laptop as an extension of your company network, not something separate from it.
- Encryption is vital for making sure data on the laptop doesn't fall into the wrong hands, in case the laptop is lost or stolen. Full disk encryption makes the laptop unusable to anyone who doesn't have the encryption key. Even if the disk is foisted out of the machine and installed on a test bed, the data is gibberish.
- Products such as SafeBoot Device Encryption provide full disk encryption and are designed specifically for laptops. SafeBoot N.V.'s product requires the user to authenticate with a user ID and password before the operating system loads. Because it loads before the operating system, it can't be defeated by Linux boot disks, such as Knoppix, which bypass operating system logons to access machines.

- SafeBoot works behind the scenes, continually encrypting the hard drive while the user is working. Similar products are offered by PGP Corp. and GuardianEdge Technologies Inc.
- All laptops, like their stationary desktop counterparts, should be outfitted with personal firewalls and antiviral software. They should be up-to-date with the latest security patches. If you use Active Directory for authentication, laptops can be further locked down using Group Policy Objects, again like the desktops that are also connected to the network.
- Consider a VPN for secure communication back to the office for those on the road. A Secure Sockets Layer VPN doesn't require any software installed on the laptop but could cost more than an IT professional at an SMB is willing to spend. Products include those from Aventail Corp. and Juniper Networks Inc., and the open source OpenVPN.
- If the worst happens, and a laptop is lost or stolen, a theft should be reported to the police and to the incident response team, if you have one, in your IT department. Even without a dedicated information security team, an SMB's IT staff should be informed of what happened. Free tools, like LaptopLock, can be used to register your laptops and can then remotely delete files or encrypt and disable the machine.
- With these options, laptop security can be part of an SMB's overall IT security program with existing staff at minimal cost.

- **Turn on your firewall.** When you're on an open Wi-Fi network, make sure you have your laptop's firewall on and blocking unwanted incoming connections. In Windows' Control Panel, click on Windows Firewall. On your Mac, in System Preferences, go to Security and click on the Firewall tab to turn it on.
- **Password protect — or unshare — shared folders.** When you're at home, sharing a document folder with other computers behind your firewall is a fine idea. But when you're out and about, you may not want everyone to be able to see your collection of family vacation photos. Make sure your shared folders are password protected when you're not on a safe network. Even better, turn off all sharing when you're on a public network.
- **Use https (secure connections to web sites) whenever possible.** When you're checking your webmail like Gmail or Yahoo Mail, or visiting any site with the option, make sure you're using the https:// (instead of http://) connection to encrypt any information you submit there, like your password. Most modern webmail and calendar programs like Gmail and Google Calendar offer an https:// option.

- **Don't save your web site passwords in your browser without encrypting them.** Sure, if you save your web site passwords inside your browser, you save a whole lot of time. However, if a thief, co-worker, or relative uses your computer, it's also dead simple for that person to log into your accounts. Three weeks ago I ran down how to [secure your browser's saved passwords](#) with an encrypted master password — do it.
- **Lock down your laptop with an actual lock.** If you work in a public place often and tend to leave your laptop unattended, invest \$15 to \$30 on [a physical laptop lock](#) to anchor your notebook to the desk. It's a simple way to deter thieves.
- **Always have a current backup of your important data.** Backing up your computer will help you restore things in the event of theft or a hard drive crash or coffee spill. When your laptop is docked back at home or the office, use an external hard drive to back up your documents. If you're constantly on the go, a remote backup service like [Mozy](#) or [Carbonite](#) works over the internet in the background, and can restore your files from anywhere.
- **Run anti-virus and malware protection software.** Like a backup system, this is a best practice for all computers, not just your laptop. Just last week Microsoft released their new and free [Security Essentials software](#). Download that and scan your notebook on a regular basis.

## Advanced Security

The super-paranoid and technically-inclined can use hacker-level techniques for locking down files and disks. Those include:

- **Encrypting folders and disks.** Using free tools you can encrypt an entire hard drive or just a folder full of files. When you encrypt data, you use a secret key to scramble it into an unreadable format, which foils any thieves' attempts to read your private files. To decrypt it, you need a master password. On a Mac, you can create an encrypted disk image by using the Disk Utility application. Macs also come with File Vault (in System Preferences, Security), which encrypts your home folders' contents keeping unwanted eyes out. Windows Vista and the upcoming Windows 7 offers [BitLocker](#), a data encryption application. Alternately, you can use a free utility called [TrueCrypt](#) to [encrypt a folder or drive](#).
- **Securing your network traffic via an SSH tunnel.** Another common technique among the tech elite is the use of an SSH tunnel, or a secure connection to an outside computer (like your home server or office computer) to connect to the internet. From the network you're already on, it looks like you're sending encrypted information to a single destination; in reality, you're using a trusted remote server as a proxy for all your network activity. Here's more on [how to encrypt your web browsing session with an SSH SOCKS proxy](#).

# Securing Pen Drives

- How do most corporate data breaches happen? Lost laptops and USB drives.
- Now many businesses have some kind of security practice in place for lost corporate computers, whether it's encrypted drives with remote wipe, or a call lost-and-reporting procedure. But how many have USB drive best practices on the books? Not many.
- Yet USBs, because of their size, are more likely to be lost than laptops or smartphones. And loaded with sophisticated malware and virus, USB drives have been used to penetrate some of the world's most sensitive networks, from the Department of Defense on down.
- So how do you prevent against lost data or network intrusions associated with USB storage devices or thumb drives? Here are the best practices for designing your company's USB drive policy:
  - **1. Enable USB functionality on a need-to-have basis.** Disable storage devices on computers with access to sensitive information. It will limit exposure and reduce the risk of unauthorized data being transferred away from your organization.
  - **2. If your business needs USB drives, issue devices that provide whole drive encryption and are passphrase protected.**
  - **3. Make sure those drives have remote management options, such as remote wipe or remote lock.** Drives like those from Iron Key have remote administration tools that also enforce strong passwords, have strict re-entry limits, disable portable applications and, believe it or not, even self-destruct.
  - **4. Look for drives that provide event logging and geotagging,** so information on what computer, and where, is retained on every use.

- 5. **Enforce USB scanning on all corporate computers whenever a thumb drive is plugged in.** This can help ensure no malware or malicious programs are on the drive. Allow only corporate signed and approved applications to be run from the drive.
- 6. **Regularly audit USB devices** to ensure that only documents in compliance with acceptable usage are being stored. This is a snatch and scan. It only takes of few of these kinds of trips around the office before everyone is very aware of the seriousness of the new USB policy.
- 7. **Perform regular backups of USB devices internally**, including encryption keys, for data recovery purposes. Ensure that backups are properly safeguarded, and have separate procedures and security controls for backup of encryption keys. It's also another excellent way to monitor what information is being moved to and from the device.
- 8. **Test data recovery procedures** to ensure that the corporate security office can unlock and access any USB drive, even if an end user or malware maliciously disables the USB drive.
- 9. **Ensure that mobile devices with USB storage cards—such as digital cameras and SD Card readers—have the same controls as any USB drive.**
- 10. **If possible, issue USB devices with unique serial numbers** tagged in the firmware, as well as etched on the outside cover.
- 11. **Know your assets.** Have a precise count of the USB devices at your organization. List them by owner and use. Ban use of all personal USB devices, without question, on any work computers or for any work use.
- 12. **If a USB device is lost, take a look at that latest secure backup to review what was lost and the potential risk.** Consider recovering the drive through those geotagging features or wiping, or destroying the device with remote administration tools.
- Portable and mobile storage devices are significant players in most corporate offices. Ensuring proper protection with a best practices policy and strict enforcement offers significant risk reduction—and can prevent long nights on data breach investigations.

## **Situations in Which USB Flash Drives Pose a Security Risk:**

- When employees unknowingly share USB sticks that carry malware infections
- When employees pick up unknown thumb drives and plug them into their computers (Dropping USB flash drives with malware on them is a common tactic used by black hat developers).
- When employees leave the organization and still retain a USB holding sensitive information
- When USB flash drives are lost or stolen and information is leaked
- But knowing that USB flash drives can pose a threat to your organization isn't enough. You need to put proactive steps in place to ensure that potential security risks are identified and addressed quickly.

## **3 Steps to Secure USB Flash Drives**

- Only allow employees to download company information onto hardware- and/or software- encrypted USB flash drives.
- Issue warnings to employees about using USB flash drives that they are unsure about.
- Deploy software or leverage corporate that only allows company-owned and/or recognized USB flash drives.

## 1. Use an Encrypted USB Drive

- There is a very simple solution to the problem, and it only costs a few dollars more than the drive you may be using now. Everyone should seriously consider an encrypted USB drive with strong password protection so that if you do lose your USB drive, the data cannot be accessed. Although your drive is gone, you'll have the peace of mind knowing your private information remains safe and sound, locked away on the USB drive.

## 2. Educate Yourself

- If you are not paying attention to what is going on and how to protect yourself, your information, quite frankly, is more prone to be compromised. In other words, educate yourself on the benefits/differences of using a quality USB flash drive as opposed to a cheap handout.

## 3. Encrypt Confidential Data

- Encryption is the most trustworthy means of protecting your confidential or sensitive data. Encrypted USB drives combine the mobility advantages of using a USB while protecting the information on the drive. Be sure to check that the user storage space is 100-percent encrypted; no non-secured storage space should be provided.
- Encrypted USB drives are powerful tools in closing security gaps and helping ensure security by offering complex password protection, data wiping when password attempts are exceeded, anti-tampering technology to protect against hackers accessing the drive's internal components, and availability in a wide range of capacities.

## 4. Know the Best USB Flash Drive Available for Your Unique Needs

- A simple analysis of what you are using the USB drive for and the data stored on it, along with knowing there is a range of easy-to-use, cost-effective, encrypted USB flash-drive solutions can go a long way toward managing your security risks and, quite possibly, saving yourself some cash and loads of stress. Don't overpay for your needs.

## **5. Confirm Anti-Virus/Malware Protection is Present at Every Entry Point**

- Let's face it, new threats emerge at anytime and from anywhere – email, websites, and removable media like USB drives and CDs. Up-to-date anti-virus software is critical in keeping your valuable data safe from known and unknown threats. Ensure that all endpoint-host computer systems (i.e., any device outside your personal firewall) are equipped with up-to-date anti-virus software. Likewise, give consideration to software programs that extend protection against malware on USB devices when used in a computer other than your own.

## **6. Require Hardware-based Encrypted USB Drives**

- A USB drive with hardware-based encryption is an excellent, non-complicated, and simple solution to protect your data from breaches. Such devices meet tough industry security standards and offer the ultimate security in data protection to confidently manage threats and reduce risks. They are self-contained and do not require a software element on the host computer. No software vulnerability eliminates the possibility of brute-force, sniffing, and memory hash attacks. Software encryption is no longer considered a best practice and the new norm is hardware encryption.
- Hardware-centric/software-free encryption eliminates the most commonly used attack routes. This same software-free method also provides complete cross-platform compatibility with any OS or embedded equipment possessing a USB port and file storage system.

# Wi-Fi Security

- Wi-Fi is one entry-point hackers can use to get into your network without setting foot inside your building because wireless is much more open to eavesdroppers than wired networks, which means you have to be more diligent about security.
- But there's a lot more to Wi-Fi security than just setting a simple password. Investing time in learning about and applying enhanced security measures can go a long way toward better protecting your network. Here are six tips to better secure your Wi-Fi network.

- **Step 1. Change the name of your default home network**
- If you want to better secure your home network, the first thing you should do is to change the name of your Wi-Fi network, also known as the **SSID** (Service Set Identifier).
- While giving your Wi-Fi a somewhat provocative name such as “Can’t hack this” may backfire at times, other names such as “this is not a wifi” or “too fly for a wifi” are perfectly acceptable.
- Changing your Wi-Fi’s default name makes it harder for malicious attackers to know what type of router you have. If a cybercriminal knows the manufacturer name of your router, they will know what vulnerabilities that model has and then try to exploit them.
- We strongly advise not to call your home network something like “John’s Wi-Fi”. You don’t want them to know at first glance which wireless network is yours when there are probably three or four other neighboring Wi-Fis.
- Also, remember that **disclosing too much personal information on a wireless network name may expose you to an identity theft operation.**

- **Step 2. Make sure you set a strong and unique password to secure your wireless network**
- You probably know that every wireless router **comes pre-set with a default username and password**, which is needed in the first place to install and connect your router. The worst part: it's easy for hackers to guess it, especially if they know the manufacturer.
- So, make sure you **change them both immediately**.
- A good wireless password should be **at least 20 characters long and include numbers, letters, and various symbols**.

### **Step 3. Increase your Wi-Fi security by activating network encryption**

- Wireless networks come with multiple encryption languages, such as WEP, WPA or WPA2.
- To better understand this terminology, **WPA2** stands for Wi-Fi Protected Access 2 and is both a **security protocol** and a current standard in the industry (WPA2 networks are almost everywhere) and encrypts traffic on Wi-Fi networks. It also replaces the older and less secure **WEP (Wired Equivalent Privacy)** and is an upgrade of the original **WPA** (Wi-Fi Protected Access) technology. Since 2006, all Wi-Fi certified products should use WPA2 security.
- WPA2 AES is also a standard security system now, so all wireless networks are compatible with it. If you want to enable WPA2 encryption on your Wireless router, use these [\*\*six steps\*\*](#). If you are using a [\*\*TP-Link wireless router\*\*](#), here's how to secure your wireless network.
- The good news is that [\*\*the WPA3\*\*](#) is already here and will replace WPA2. The Wi-Fi Alliance recently announced its next-generation wireless network security standard which aims to solve a common security issue: open Wi-Fi networks. More than that, it comes with **security enhancements** and includes a suite of features to simplify Wi-fi security configuration for users and service providers.

### **Step 4. Turn off the wireless home network when you're not at home**

- In order to secure your network, we strongly recommend you to **disable the wireless home network**, in case of extended periods of non-use. You should do the same thing with [\*\*all your devices\*\*](#) that are using Ethernet cables or when you won't be at home.
- By doing this, you are closing any windows of opportunity malicious hackers might attempt to get access to it while you are away.
- Here are a few [\*\*advantages\*\*](#) of disabling your wireless network:
- **Security reasons** – Turning off your network devices, it minimizes the chances of becoming a target for hackers.
- **Surge protection** – When you power off your network device, you also lower the possibility of being damaged by electric power surges;
- **Noise reduction** – Although the modern home networks are much quieter these days, disabling your wireless home network can add calmness to your home.

- **Step 5. Where is the router located in your home?**
- You probably haven't thought about this in the first, but **where is your Wi-Fi place** in your home can also have an impact on your security.
- **Place the wireless router as close as possible to the middle of your house.** Why? First of all, it will provide equal access to the Internet to all the rooms in your home. Secondly, you don't want to have your wireless signal range reach too much outside your home, where it can be easily intercepted by malicious persons.
- For this reason, we recommend not to place your wireless router close to a window since there's nothing to block the signal going outside your home.
- **Step 6. Use a strong network administrator password to increase Wi-Fi security**
- To set up your wireless router, you usually need to access an online platform or site, where you can make several changes to your network settings.
- Most Wi-fi routers come with **default credentials such as “admin” and “password”** which are such an easy for malicious hackers to break into.
- **Did you know that** the number of wireless networks has increased dramatically over the last 8 years? In 2010 there were **20 million Wi-Fi networks** around the globe, and **in 8 years, that number increased** to 400 million. Smartphones, laptops, tablets and other devices have driven this growth, and because of how expensive data plans are, most people choose to connect their device **to wireless Internet connections.**

- **Step 7. Change your default IP address on the Wireless router**
- Changing the default IP address to a less common one is another thing you should consider doing to better secure your home network and make it more difficult for hackers to track it.
- To change the IP address of a router, you should follow these steps:
  - Log into your router's console as an administrator. These [\*\*basic steps\*\*](#) will teach you how to easily connect to your home network as an admin. Usually, the address bar type looks like <http://192.168.1.1> or <http://192.168.0.1>
  - Once you are there, insert the username and password on the login page;
  - Then select **Network > LAN** which is in the menu of the left side;
  - Change the IP address to preference, then click **Save**.
  - **Note:** After you've changed the IP address, you'll need to type the new IP address into the web browser bar.
  - You can also change the [\*\*DNS server\*\*](#) that your Wireless router is using to filter the Internet traffic and this [\*\*guide\*\*](#) will show how to do it.
- **Step 8. Turn off the DHCP functionality on the router**
  - To enhance the wireless network security, you should turn off the Dynamic Host Configuration Protocol (DHCP) server in your router which is what IP addresses are assigned to each device on a network. Instead, you should make use of a static address and enter your network settings.
  - This means that you should enter into your device and assign it an IP address that is suitable to your router.
- **Step 9. Disable Remote Access**
  - Most routers allow you to access their interface only from a connected device. However, some of them allow access even from remote systems.
  - Once you turned off the remote access, malicious actors won't be able to **access your router's privacy settings from a device not connected to your wireless network**.
  - To make this change, access the web interface and search for "Remote access" or "Remote Administration".

- **Step 10. Always keep your router's software up-to-date**
- The software is an essential part of your wireless network security. The wireless router's firmware, like any other software, contains flaws which can become major vulnerabilities and be ruthlessly exploited by hackers, as [this unfortunate family would find out.](#)
- Unfortunately, many wireless routers don't come with the option to auto-update their software, so you have to go through the hassle of doing this manually.
- And even for those Wi-Fi networks that can auto-update, it still requires you to switch on this setting. But, we remind you about the importance of software patching and how neglecting to do this can leave open doors for cybercriminals to exploit various vulnerabilities.
- **Step 11. A firewall can help secure your Wi-fi network**
- [Firewalls](#) aren't just software programs used on your PC, they also come in the hardware variety.
- A hardware firewall does pretty much the same thing as a software one, but its biggest advantage is that it adds one extra layer of security.
- The best part about hardware firewalls is that most of the **best wireless routers have a built-in firewall** that should protect your network from potential cyber attacks.

- **Step 12. Enhance protection for the devices most frequently connected to your home network**
- **Important: Do not leave any exposed vulnerabilities for online criminals to pick on!**
- Even though you've increased protection for your router and home network, you need to **make sure you don't have any security holes that can be exploited by online criminals.**
- Here's what we recommend you to do:
- Remember to always keep your devices up to date with the **most recent software available;**
- Always apply the **latest security patches** to ensure no security hole is left open to malicious actors.
- check which devices connect most often to your home network and make sure they have **antivirus and/or an anti-malware security software installed.** If you don't know which one should you choose, this [\*\*guide\*\*](#) will be very useful.
- Make sure [\*\*to protect your devices using multiple security layers\*\*](#) consisting of **specialized security software** such as updated antivirus programs and [\*\*traffic filtering software\*\*](#). You may consider using an antimalware software program like our [\*\*Thor Foresight\*\*](#) or Malwarebytes.

# Email Security

- Email security refers to the collective measures used to secure the access and content of an email account or service. It allows an individual or organization to protect the overall access to one or more email addresses/accounts.
- An email service provider implements email security to secure subscriber email accounts and data from hackers - at rest and in transit.
- Email security is a broad term that encompasses multiple techniques used to secure an email service. From an individual/end user standpoint, proactive email security measures include:
  - Strong passwords
  - Password rotations
  - Spam filters
  - Desktop-based anti-virus/anti-spam applications
- Similarly, a service provider ensures email security by using strong password and access control mechanisms on an email server; encrypting and digitally signing email messages when in the inbox or in transit to or from a subscriber email address. It also implements firewall and software-based spam filtering applications to restrict unsolicited, untrustworthy and malicious email messages from delivery to a user's inbox.

## **How can email messages be compromised?**

- While many cybersecurity professionals are aware of common email security threats like [phishing](#), [ransomware](#), business email compromise, and other inbound threats, it's important to also consider data protection and securing outbound traffic. That is, putting measures in place to prevent users from sending sensitive data via email to external parties. There are four main components of an email message that can be compromised or manipulated:
  - The body of the email
  - The attachments of the email
  - URLs contained within the email
  - The sender's email address

## **What are email security best practices?**

- Email security best practices include the use of a robust email security posture that contains layers of security measures, including effective security intelligence across your entire architecture, retrospective remediation, and encryption to prevent data leakage among other features.

## **Run regular phishing exercises**

- Your employees are your greatest defense against phishing, especially the most tailored phishing attempts. Employees who can learn to recognize a phishing attempt outright can stop the number one source of endpoint compromise.

## **Use multifactor authentication**

- In the event that a corporate email account's credentials are successfully stolen, multifactor authentication can prevent an attacker from gaining access to the account and wreaking havoc.

## **Ensure you can quarantine and remediate**

- Message quarantine functionality is useful to hold a message while a file attachment is analyzed prior to either releasing the message to the recipient, removing the malicious attachment, or removing the message completely. Email remediation helps if a file is detected as malicious after delivery to the recipient. It allows you to go back and quarantine the message with a malicious attachment from within a mailbox.

## **Harness threat intelligence**

- External email threat feeds in Structured Threat Information Expression (STIX) are now commonly used by email security products, which is helpful should an organization want to use a vertical-focused threat feed beyond the native threat intelligence in the product.

## **Consider an integrated cybersecurity solution**

- Integration of email security with broader security portfolios is also becoming common to determine if advanced malware or messages in an environment may have been delivered to particular users or inboxes.

## 1. Familiarize Yourself with Common Phishing Schemes

- Phishing is a common scamming practice that is quite sneaky. Scammers pose as well known companies and request private information about its recipients.
- Since these emails often seem to come from reputable sources, such as PayPal, banks and other large companies, they often are effective in their data collection. Many people don't think twice before entering their information in order to continue their subscriptions or collect a prize or payment.
- One of the telltale signs of a phishing email is poor spelling, improper grammar and an uncomfortable or robot-like writing style.
- There are a few major phishing practices that you should look out for so that you can avoid jeopardizing your email security.
- 5 Common Phishing Practices
  - 
  - **Deceptive Phishing:** Deceptive fishing is when a scammer sends an email under the guise of a reliable company.
  - **Spear Phishing:** Spear phishing uses information about the target in order to build trust and increase the chances of the scam working.
  - **Whaling:** This type of phishing targets CEOs so that hackers can penetrate the company from the top.
  - **Pharming:** Pharming is when scammers redirect safe domains to unsafe ones by toying with IP addresses.
  - **Google Drive/Dropbox Phishing:** This type of phishing is among the most difficult to detect. It duplicates cloud folder login pages and requests your login info. When scammers have these login credentials, it usually opens access to a plethora of sensitive information.

## 2. Protect Your Account with an Unbeatable Password

- The days of using “password123” as your password are long gone. (Yes, some people actually used passwords like these because they are easy to remember).
- Many sites have upped the password requirements to include a number, special symbol and both uppercase and lowercase letters.
- It is suggested that you don’t use your name, phone number, address or company name in your password. You do not want something that is easy to guess.

## 3. Prohibit Personal Use of Company Emails

- Let your employees know that their company email addresses should be used for business and nothing more.
- If people list their work email addresses on personal accounts, more mail is being sent and received. This greatens the chances of a bad apple spoiling the whole account.
- Minimizing personal use of the company emails makes for a more secure email.

## 4. Implement Two-Factor Authentication

- Two-step authentication is a major tool against phishing. This way you can be sure that your login information is being used to log you into your intended site or portal, not a phony form used to steal your precious data.
- The extra step may take a little bit more time, but it puts up an extra wall of protection around your accounts.

## 5. Avoid Opening Unfamiliar Attachments

- Never ever open an attachment from an unfamiliar sender. Unsafe links, malware and viruses are often hidden in unsuspecting attachments.
- If you are unsure about an attachment, you should run a virus and malware scan to see if it’s safe or not.
- Take note that dangerous attachments can come in any format, but .HTML attachments are a commonly used phishing tactic.

## **6. Run Malware and Virus Scans**

- Malware and virus scans are essential since many unsafe links and attachments are hidden quite carefully.
- Some of the best virus and malware scans include McAfee Total Protection, Kaspersky Anti-Virus, Bitdefender Total Security and Check Point ZoneAlarm Anti-Ransomware.
- This sort of software is worth investing in. It could save you quite a bit of pain and hassle in the long run.

## **7. Don't Open Your Inbox When Connected to Public Wifi**

- Connecting to public WiFi networks makes all of the sensitive information on your computer vulnerable to anybody else connected to the same network. Your email is no exception.
- Avoid checking your email on the internet at coffee shops or internet cafes at all costs. Predators like to hack people who are working in these places.
- If you are checking your email while you're out and about, the best bet is to open it using your internet data on your phone or using your connecting your laptop to your phone's wireless hotspot.

## **8. Use a Powerful Spam Filter**

- Most email platforms, including Google and Office 365, have built-in spam filters. Often times, you have the ability to turn the spam filter on and off.
- Users also have the ability to customize their spam filters to weed out emails that include certain words or come from certain senders.
- This helps to protect your email from scammers and phishers.

## **9. Avoid Clicking the “Unsubscribe” Button in Unsafe Emails**

- Unsubscribing when you get an email that you wish you hadn't received may seem like the most logical action, and that is why many phishers disguise their unsafe links as an “Unsubscribe” buttons.
- While hitting the “Unsubscribe” button may be tempting, resist the urge. Instead of unsubscribing, mark unwanted emails as junk and delete them promptly.
- The best way to unsubscribe from an email that you believe you've signed up for is heading directly to the website and logging in a secure portal. You'll likely have the ability to change your communication options. Do not follow the link from the email.

## **10. Educate Your Entire Company**

- Unless your entire company gets on board with the best email security practices, your inboxes may still be at risk. After all, you're only as strong as your weakest link.
- Include email security lessons in your company's new member orientation and employee handbooks. Make sure that the whole team is well-informed. This is certainly the most important part of ensuring your email security.

# Browser Security

- Web browsers are designed to store information for your convenience, but that information can also fall into the wrong hands.
- The web browser is inarguably the most common portal for users to access the internet for any given array of consumer or business purposes. Innovative advances have allowed many traditional "thick client" apps to be replaced by the browser, enhancing its usability and ubiquity. User-friendly features such as recording browsing history, saving credentials and enhancing visitor engagement through the use of cookies have all helped the browser become a "one stop shopping" experience.
- However, the browser also has the potential to betray the user through the very same options which are intended to make life easier since it serves as a ripe target for the theft of confidential data because it holds so many proverbial eggs in its basket.

Here is a summary of their findings along with some other tips for protection:

## 1. Accessing browser history

- Your browser history is a veritable map of where you go on the internet and for what purpose. And it's not only possible to tell where you've been, but when you've been there, establishing your behavioral patterns.
- Knowing you access certain sites can lead to phishing attacks against you to obtain your credentials for those sites (assuming you haven't stored this information in the browser), establishing your purchasing habits (for instance if you are a football fan and visit NFL sites, your credit card company isn't likely to raise an eyebrow if a slew of charges for football merchandise start showing up on your compromised credit card) or even blackmail if the site(s) in question prove illegal or unethical, or allegations thereof can be made.

### Recommendations:

- Clearing the browser cache is a good way to flush potentially damaging information, especially after engaging in confidential activities such as conducting online banking. This can be performed manually or set to do so automatically such as when closing the browser (Google the details for your browser version and operating system to carry out this and the other recommendations as the steps involved may be subject to change).
- Use incognito mode (private browsing) since no harvestable data is stored (if you must use a public system, always make sure to do so with incognito mode).

## 2. Harvesting saved login credentials

- Saved logins paired with bookmarks for the associated sites you visit are a deadly combination. Two mouse clicks might be all it takes for a criminal to have access to your banking/credit card website. Some sites do use two-factor authentication, such as texting access codes to your mobile phone, but many of them utilize this on a one-time basis so you can confirm your identity on the system you're connecting from. Unfortunately, that system is then deemed trusted, so subsequent access may go entirely unchallenged.
- Saved credentials associated with your email account is basically like Kryptonite to Superman in a scenario like this. An attacker who can get into your email can reset your password on almost any other website you access. And keep in mind they might not need to be on your system to do so - if they obtain your email address and password they can work at leisure from any other system they choose.
- Just taking a series of screenshots (or even utilizing the camera on a mobile phone) can allow an attacker on your system to record all of your saved passwords. Firefox lets you view these quite easily. While Chrome at least requests your logon password to do so, as stated resetting this is quite easy with administrative access (which can be simple to obtain thanks to password reset utilities such as [Offline NT Password and Registry Editor](#)).

### Recommendations:

- Don't save credentials in the browser. Instead, take advantage of free password managers such as [KeePass](#) or [Password Safe](#) to store passwords (never write them down) via a central master password. These password managers can securely store all your website passwords. A password manager can even access a saved URL and login for you, adding to the convenience and security of your information.

## 3. Obtaining autofill information

- Autofill information can also be deadly. Chrome can save your home address information to make it easier to shop online, but what if your device fell into the wrong hands? Now an attacker knows where you live - and probably whether you're home.

### Recommendations:

- Turn off autofill for any confidential or personal details.

- **4. Analyzing cookies**
  - Cookies (files stored locally which identify users/link them to sites) are another potential attack vector. Like the browsing history, they can reveal where you go and what your account name might be.
  - As with #1, incognito mode can also come in handy here.
- **Recommendations:**
  - Disabling cookies is touted as a potential solution, but this has been a problematic "fix" for years since many sites depend on cookies or at least severely limit your functionality (or possibly annoy you with nagging prompts) if these are turned off.
  - Instead, purging cookies periodically can help protect you, though be prepared to enter information repeatedly as prompted by websites.
- **5. Exploring the browser cache**
  - The browser cache involves storing sections of web pages for easier access/loading on subsequent visits, which can outline where you've been and what you've seen. Malware can be tailored to prey upon cache data as well.
  - Exabeam also considered location history and device discovery to be risky elements in their blog post, stating these could expose user location and other devices used.
- **Recommendations:**
  - As with #1 and #4, incognito mode can also come in handy here, or manually clear the cache as needed, particularly after sensitive operations.

# Browser Security

- **Don't rely on your browser to protect you from malicious Websites.** Browsers only warn you about sites but cannot stop you from going there. Even if you have high security settings and anti-virus software, visiting a risky Web site can result in viruses, spyware or worse.
- **Keep your browser software up-to-date.** New patches are often released to fix existing vulnerabilities in browser software, so having the most up-to-date versions is critical.
- **Run anti-virus software and scan files before downloading.** Anti-virus software provides protection by scanning for and removing malicious files on your computer and avoid downloading anything until you're confident that it is secure. If you have any suspicion that a file may not be legitimate or may be infected, scan it with anti-virus software before downloading.
- **Use HTTPS.** The “s” in “https” stands for secure, meaning that the Website is employing SSL encryption. Check for an “https:” or a padlock icon in your browser’s URL bar to verify that a site is secure before entering any personal information.
- **Don't reuse passwords.** Using the same password for multiple sites only makes it easier for attackers to compromise your sensitive information. Instead, keep track of your different passwords with a handwritten list that you keep in a safe place or come up with your own algorithm for creating unique passwords that only you would know. It is also recommended that you change your passwords every 90 days.

- **Disable *auto-complete* for forms or remember your passwords features.** Nearly all browsers and many websites in general offer to remember your passwords for future use and Web sites can use hidden fields to steal the data from forms. Enabling these features make them easier for an attacker to discover if your system gets compromised. Also, criminals can hijack your browsing session and steal your information if you stay logged-in to a site. If you have these features enabled, disable them and clear your stored passwords.
- **Read privacy policies.** Websites' privacy policies and user agreements should provide details as to how your information is being collected and protected as well as how that site tracks your online activity. Websites that don't provide this information in their policies should generally be avoided.
- **Regularly monitor your bank statements.** Keeping an eye on your online statements will allow you to react quickly in the event that your account has been compromised.
- **Avoid public or free Wi-Fi.** Attackers often use wireless sniffers to steal users' information as it is sent over unprotected networks. The best way to protect yourself from this is to avoid using these networks altogether.
- **Turn on your browser's popup blocker.** Popup blocking is now a standard browser feature and should be enabled any time you are surfing the Web. If it must be disabled for a specific program, turn it back on as soon as that activity is complete.

# What is Cloud

- The cloud is a virtual space that exists on the internet. It is a storage space where people can place their digital resources such as software, applications and files. So in simplified terms, we can say that the cloud is a virtual storage space on the internet.
- A lot of people do get the cloud mixed up with the internet. However, the cloud is only one part of the internet and not the whole thing.

- "The cloud" refers to servers that are accessed over the Internet, and the software and databases that run on those servers. Cloud servers are located in data centers all over the world. By using cloud computing, users and companies don't have to manage physical servers themselves or run software applications on their own machines.
- The cloud enables users to access the same files and applications from almost any device, because the computing and storage takes place on servers in a data center, instead of locally on the user device. This is why a user can log into their Instagram account on a new phone after their old phone breaks and still find their old account in place, with all their photos, videos, and conversation history. It works the same way with cloud email providers like Gmail or Microsoft Office 365, and with cloud storage providers like Dropbox or Google Drive.
- For businesses, switching to cloud computing removes some IT costs and overhead: for instance, they no longer need to update and maintain their own servers, as the cloud vendor they are using will do that. This especially makes an impact for small businesses that may not have been able to afford their own internal infrastructure but can outsource their infrastructure needs affordably via the cloud. The cloud can also make it easier for companies to operate internationally, because employees and customers can access the same files and applications from any location.

- What is Cloud Security?
- Cloud computing is the delivery of hosted services, including software, hardware, and storage, over the Internet. The benefits of rapid deployment, flexibility, low up-front costs, and scalability, have made cloud computing virtually universal among organizations of all sizes, often as part of a hybrid/multi-cloud infrastructure architecture.
- Cloud security refers to the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure from threats.

- Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion. Methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections. Cloud security is a form of cybersecurity.

- Cloud security is a set of control-based safeguards and technology protection designed to protect resources stored online from leakage, theft, or data loss.
- Protection encompasses cloud infrastructure, applications, and data from threats. Security applications operate as software in the cloud using a Software as a Service (SaaS) model.
- Topics that fall under the umbrella of security in the cloud include:
  - [Data center security](#)
  - Access control
  - Threat prevention
  - Threat detection
  - Threat mitigation
  - Redundancy
  - Legal compliance
  - Security policy

- **What are the Benefits of a Cloud Security System?**
- Now that you understand how cloud computing security operates, explore the ways it benefits your business.
- Cloud-based security systems benefit your business through:
  - Protecting your business from threats
  - Guarding against internal threats
  - Preventing data loss
  - Top threats to systems include malware, ransomware, and DDos.

# OS Security

- OS security encompasses many different techniques and methods which ensure safety from threats and attacks. OS security allows different applications and programs to perform required tasks and stop unauthorized interference.

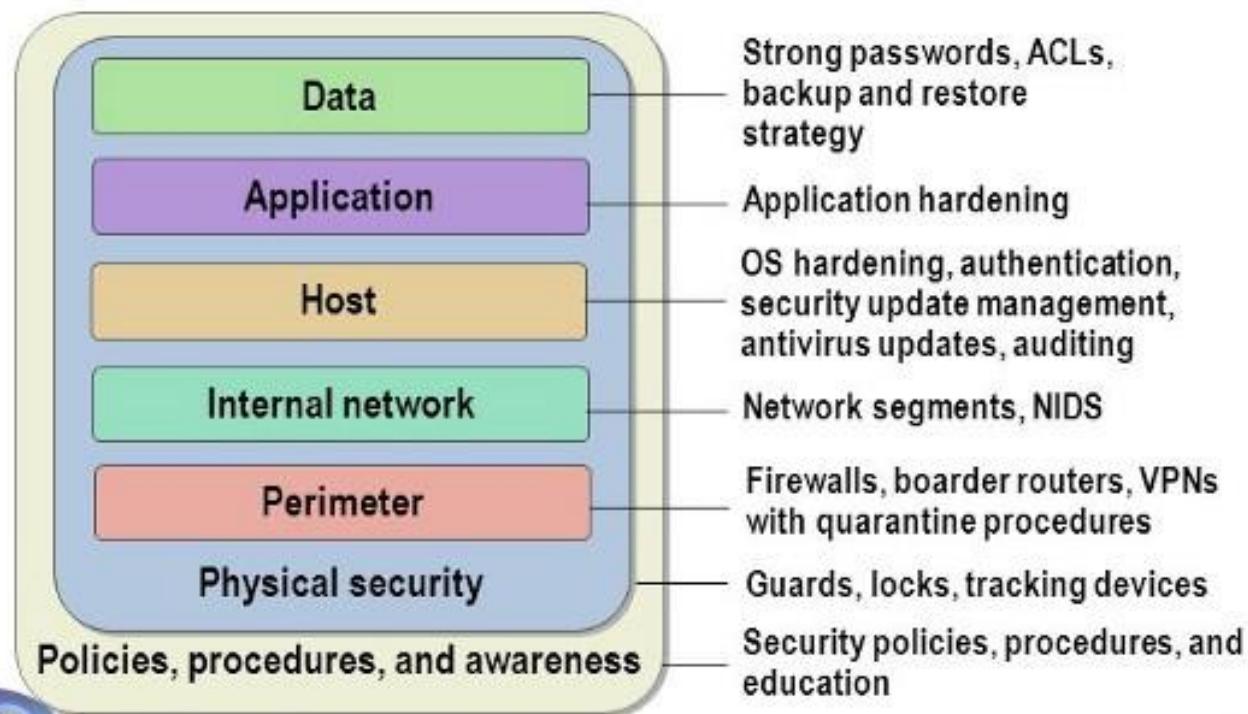
OS security may be approached in many ways, including adherence to the following:

- Performing regular OS patch updates
- Installing updated antivirus engines and software
- Scrutinizing all incoming and outgoing network traffic through a firewall
- Creating secure accounts with required privileges only (i.e., user management)

# Understanding Defense-in-Depth

## Using a layered approach:

- Increases an attacker's risk of detection
- Reduces an attacker's chance of success



# What is Data Security?

- Data security refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle. Data security includes data encryption, hashing, tokenization, and key management practices that protect data across all applications and platforms.
- Why Data Security?
- Organizations around the globe are investing heavily in information technology (IT) cyber security capabilities to protect their critical assets. Whether an enterprise needs to protect a brand, intellectual capital, and customer information or provide controls for critical infrastructure, the means for incident detection and response to protecting organizational interests have three common elements: people, processes, and technology.

- ## Data Security Solutions

- Micro Focus drives leadership in [data security solutions](#) with over 80 patents and 51 years of expertise. With advanced data encryption, tokenization, and key management to protect data across applications, transactions, storage, and big data platforms, [big data solutions](#), Micro Focus simplifies the protection of sensitive data in even the most complex use cases.
- [Cloud data security](#) – Protection platform that allows you to move to the cloud securely while protecting data in cloud applications.
- [Data encryption](#) – Data-centric and tokenization security solutions that protect data across enterprise, cloud, mobile and big data environments.
- [Hardware security module](#) -- Hardware security module that guards financial data and meets industry security and compliance requirements.
- [Key management](#) -- Solution that protects data and enables industry regulation compliance.
- [Enterprise Data Protection](#) – Solution that provides an end-to-end data-centric approach to enterprise data protection.
- [Payments Security](#) – Solution provides complete [point-to-point encryption](#) and [tokenization](#) for retail payment transactions, enabling [PCI scope reduction](#).
- Big Data, Hadoop and IoT data protection – Solution that protects sensitive data in the Data Lake – including [Hadoop](#), [Teradata](#), Micro Focus [Vertica](#), and other Big Data platforms.
- [Mobile App Security](#) - Protecting sensitive data in native mobile apps while safeguarding the data end-to-end.
- [Web Browser Security](#) - Protects sensitive data captured at the browser, from the point the customer enters cardholder or personal data, and keeps it protected through the ecosystem to the trusted host destination.
- [eMail Security](#) – Solution that provides end-to-end encryption for email and mobile messaging, keeping Personally Identifiable Information and Personal Health Information secure and private.

# Database Security

What is database security

- Database security refers to the range of tools, controls, and measures designed to establish and preserve database confidentiality, integrity, and availability. This article will focus primarily on confidentiality since it's the element that's compromised in most data breaches.

Database security must address and protect the following:

- The data in the database
- The database management system (DBMS)
- Any associated applications
- The physical database server and/or the virtual database server and the underlying hardware
- The computing and/or network infrastructure used to access the database

- Database security is a complex and challenging endeavor that involves all aspects of information security technologies and practices.
- It's also naturally at odds with database usability. The more accessible and usable the database, the more vulnerable it is to security threats; the more invulnerable the database is to threats, the more difficult it is to access and use

- By definition, a data breach is a failure to maintain the confidentiality of data in a database. How much harm a data breach inflicts on your enterprise depends on a number of consequences or factors:
- **Compromised intellectual property:** Your intellectual property—trade secrets, inventions, proprietary practices—may be critical to your ability to maintain a competitive advantage in your market. If that intellectual property is stolen or exposed, your competitive advantage may be difficult or impossible to maintain or recover.
- **Damage to brand reputation:** Customers or partners may be unwilling to buy your products or services (or do business with your company) if they don't feel they can trust you to protect your data or theirs.
- **Business continuity (or lack thereof):** Some business cannot continue to operate until a breach is resolved.
- **Fines or penalties for non-compliance:** The financial impact for failing to comply with global regulations
- **Costs of repairing breaches and notifying customers:** In addition to the cost of communicating a breach to customer, a breached organization must pay for forensic and investigative activities, crisis management, triage, repair of the affected systems, and more.

## Common threats and challenges

- Many software misconfigurations, vulnerabilities, or patterns of carelessness or misuse can result in breaches. The following are among the most common types or causes of database security attacks and their causes.
- Insider threats
- An insider threat is a security threat from any one of three sources with privileged access to the database:
  - A malicious insider who intends to do harm
  - A negligent insider who makes errors that make the database vulnerable to attack
  - An infiltrator—an outsider who somehow obtains credentials via a scheme such as phishing or by gaining access to the credential database itself
- Insider threats are among the most common causes of database security breaches and are often the result of allowing too many employees to hold privileged user access credentials.

### Human error

- Accidents, weak passwords, password sharing, and other unwise or uninformed user behaviors continue to be the cause of nearly half (49%) of all reported data breaches.

- **Exploitation of database software vulnerabilities**
- Hackers make their living by finding and targeting vulnerabilities in all kinds of software, including database management software. All major commercial database software vendors and open source database management platforms issue regular security patches to address these vulnerabilities, but failure to apply these patches in a timely fashion can increase your exposure.
- **SQL/NoSQL injection attacks**
- A database-specific threat, these involve the insertion of arbitrary SQL or [non-SQL](#) attack strings into database queries served by web applications or HTTP headers. Organizations that don't follow secure web application coding practices and perform regular vulnerability testing are open to these attacks.
- **Buffer overflow exploitations**
- Buffer overflow occurs when a process attempts to write more data to a fixed-length block of memory than it is allowed to hold. Attackers may use the excess data, stored in adjacent memory addresses, as a foundation from which to launch attacks.
- **Denial of service (DoS/DDoS) attacks**
- In a denial of service (DoS) attack, the attacker deluges the target server—in this case the database server—with so many requests that the server can no longer fulfill legitimate requests from actual users, and, in many cases, the server becomes unstable or crashes.

- Malware
- Malware is software written specifically to exploit vulnerabilities or otherwise cause damage to the database. Malware may arrive via any endpoint device connecting to the database's network.
- Attacks on backups
- Organizations that fail to protect backup data with the same stringent controls used to protect the database itself can be vulnerable to attacks on backups.

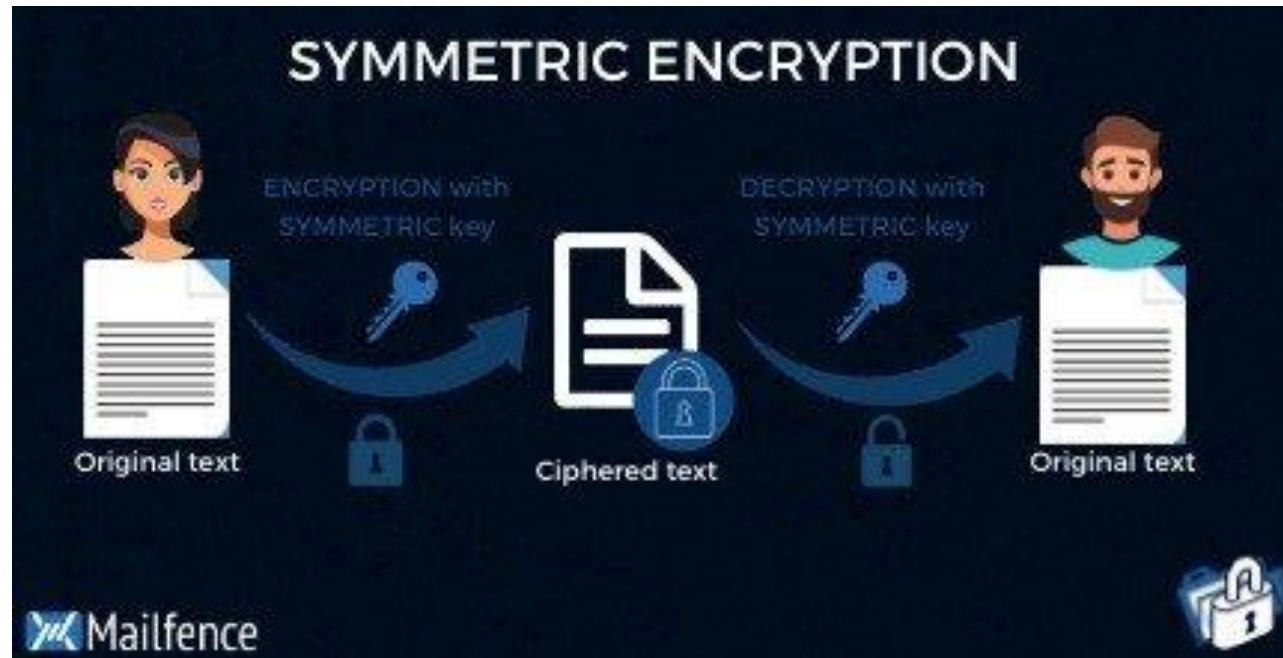
- **Best practices**

- When evaluating database security in your environment to decide on your team's top priorities, consider each of the following areas:
- **Physical security:** Whether your database server is on-premise or in a cloud data center, it must be located within a secure, climate-controlled environment. (If your database server is in a cloud data center, your cloud provider will take care of this for you.)
- **Administrative and network access controls:** The practical minimum number of users should have access to the database, and their permissions should be restricted to the minimum levels necessary for them to do their jobs. Likewise, network access should be limited to the minimum level of permissions necessary.
- **End user account/device security:** Always be aware of who is accessing the database and when and how the data is being used. Data monitoring solutions can alert you if data activities are unusual or appear risky. All user devices connecting to the network housing the database should be physically secure (in the hands of the right user only) and subject to security controls at all times.
- **Encryption:** ALL data—including data in the database, and credential data—should be protected with best-in-class encryption while at rest and in transit. All encryption keys should be handled in accordance with best-practice guidelines.
- **Database software security:** Always use the latest version of your database management software, and apply all patches as soon as they are issued.

- **Application/web server security:** Any application or web server that interacts with the database can be a channel for attack and should be subject to ongoing security testing and best practice management.
- **Backup security:** All backups, copies, or images of the database must be subject to the same (or equally stringent) security controls as the database itself.
- **Auditing:** Record all logins to the database server and operating system, and log all operations performed on sensitive data as well. Database security standard audits should be performed regularly.

# Cryptography

- What is symmetric encryption?
- Symmetric encryption aka symmetric key cryptography uses one single key to encrypt and decrypt data. You have to share this key with the recipient. Let's say you want to say I love you Mom, you would write your email, then set a secret key to encrypt it. When mom receives the message she would enter the secret key to decrypt the email.



- Pros and cons of Symmetric Encryption
- The advantages of **symmetric encryption** are that it **is easy to set up** and can be done in a jiffy. Moreover, it is pretty straightforward, **all ages and backgrounds can use it**. Asymmetric encryption is more difficult to comprehend and use.
- Because the algorithm behind symmetric encryption is less complex and executes faster, this is the preferred technique when transmitting data in bulk.
- The plaintext is encrypted using a key, and the same key is used at the receiving end to decrypt the received ciphertext. The host in the communication process would have received the key through external means.
- Widely used symmetric encryption algorithms include AES-128, AES-192, and AES-256.
- **The drawback is that the secret key needs to be shared with the recipient.**

- **Asymmetric Key Encryption:**

Asymmetric Key Encryption is based on public and private key encryption technique. It uses two different key to encrypt and decrypt the message. It is more secure than symmetric key encryption technique but is much slower.



- Pros and cons of Asymmetric encryption
- The advantage of **Asymmetric encryption** is that it **does not force the user to share (secret) keys**. Therefore, removing the necessity of key distribution. Asymmetric encryption supports digital signing which authenticates the recipient identity and makes sure that message was not tampered with in transit.
- The **cons of Asymmetric encryption are that it is time-intensive and it requires considerably more effort**. What's more, you can send encrypted emails only if the other person has created key pairs. Finally, if you lose your private key – you will lose it forever. The private key is irrecoverable which could create a whole series of new problems for you to deal with.
- This type of encryption is relatively new as compared to symmetric encryption, and is also referred to as public-key cryptography.
- Asymmetric encryption is considered to be more secure than symmetric encryption as it uses two keys for the process.
- The public key used for encryption is available to everyone but the private key is not disclosed.
- This encryption method is used in everyday communication over the internet.
- When a message is encrypted using a public key, it can only be decrypted using a private key. However, when a message is encrypted using a private key, it can be decrypted using a public key.
- Digital certificates in the client-server model can be used to discover public keys.
- The drawback of this encryption is that it takes more time than the symmetric encryption process.
- Common asymmetric encryption techniques include RSA, DSA, and PKCS.

## **Symmetric Key Encryption**

It only requires a single key for both encryption and decryption.

The size of cipher text is same or smaller than the original plain text.

The encryption process is very fast.

It is used when a large amount of data is required to transfer.

It only provides confidentiality.

Examples: 3DES, AES, DES and RC4

In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.

## **Asymmetric Key Encryption**

It requires two key one to encrypt and the other one to decrypt.

The size of cipher text is same or larger than the original plain text.

The encryption process is slow.

It is used to transfer small amount of data.

It provides confidentiality, authenticity and non-repudiation.

Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

In asymmetric key encryption, resource utilization is high.

# Key management

- Key Management deal with the creation, exchange, storage, deletion, and refreshing of keys.
- In cryptography it is a very tedious task to distribute the public and private key between sender and receiver. If key is known to the third party (forger/eavesdropper) then the whole security mechanism becomes worthless. So, there comes the need to secure the exchange of keys.
- There are 2 aspects for Key Management:
- Distribution of public keys.
- Use of public-key encryption to distribute secret.
- **Distribution of Public Key:**
- Public key can be distributed in 4 ways: Public announcement, Publicly available directory, Public-key authority, and Public-key certificates. These are explained as following below.
- **Public Announcement:**  
Here the public key is broadcasted to everyone. Major weakness of this method is forgery. Anyone can create a key claiming to be someone else and broadcast it. Until forgery is discovered can masquerade as claimed user.

- **Publicly Available Directory:**

In this type, the public key is stored at a public directory. Directories are trusted here, with properties like Participant Registration, access and allow to modify values at any time, contains entries like {name, public-key}.Directories can be accessed electronically still vulnerable to forgery or tampering.

- **Public Key Authority:**

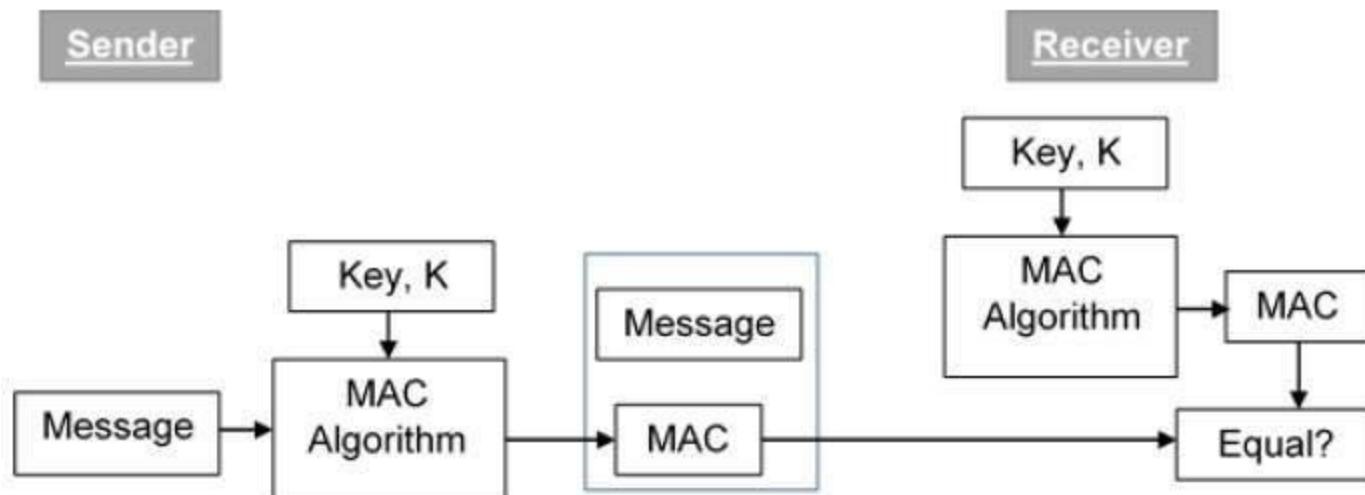
It is similar to the directory but, improve security by tightening control over distribution of keys from directory. It requires users to know public key for the directory. Whenever the keys are needed, a real-time access to directory is made by the user to obtain any desired public key securely.

- **Public Certification:**

This time authority provides a certificate (which binds identity to the public key) to allow key exchange without real-time access to the public authority each time. The certificate is accompanied with some other info such as period of validity, rights of use etc. All of this content is signed by the trusted Public-Key or Certificate Authority (CA) and it can be verified by anyone possessing the authority's public-key.

# Message Authentication Code

- MAC algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K.
- Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.
- The process of using MAC for authentication is depicted in the following illustration –



- Let us now try to understand the entire process in detail –
- The sender uses some publicly known MAC algorithm, inputs the message and the secret key K and produces a MAC value.
- Similar to hash, MAC function also compresses an arbitrary long input into a fixed length output. The major difference between hash and MAC is that MAC uses secret key during the compression.
- The sender forwards the message along with the MAC. Here, we assume that the message is sent in the clear, as we are concerned of providing message origin authentication, not confidentiality. If confidentiality is required then the message needs encryption.
- On receipt of the message and the MAC, the receiver feeds the received message and the shared secret key K into the MAC algorithm and re-computes the MAC value.
- The receiver now checks equality of freshly computed MAC with the MAC received from the sender. If they match, then the receiver accepts the message and assures himself that the message has been sent by the intended sender.
- If the computed MAC does not match the MAC sent by the sender, the receiver cannot determine whether it is the message that has been altered or it is the origin that has been falsified. As a bottom-line, a receiver safely assumes that the message is not the genuine.

- **Limitations of MAC**
- There are two major limitations of MAC, both due to its symmetric nature of operation –
- **Establishment of Shared Secret.**
  - It can provide message authentication among pre-decided legitimate users who have shared key.
  - This requires establishment of shared secret prior to use of MAC.
- **Inability to Provide Non-Repudiation**
  - Non-repudiation is the assurance that a message originator cannot deny any previously sent messages and commitments or actions.
  - MAC technique does not provide a non-repudiation service. If the sender and receiver get involved in a dispute over message origination, MACs cannot provide a proof that a message was indeed sent by the sender.
  - Though no third party can compute the MAC, still sender could deny having sent the message and claim that the receiver forged it, as it is impossible to determine which of the two parties computed the MAC.

# Properties of Message Authentication Codes

## 1. Cryptographic checksum

A MAC generates a cryptographically secure authentication tag for a given message.

## 2. Symmetric

MACs are based on secret symmetric keys. The signing and verifying parties must share a secret key.

## 3. Arbitrary message size

MACs accept messages of arbitrary length.

## 4. Fixed output length

MACs generate fixed-size authentication tags.

## 5. Message integrity

MACs provide message integrity: Any manipulations of a message during transit will be detected by the receiver.

## 6. Message authentication

The receiving party is assured of the origin of the message.

## 7. No nonrepudiation

Since MACs are based on symmetric principles, they do not provide nonrepudiation. P