**INTRODUCTION AND BASIC CONCEPTS OF CYBER SECURITY**

**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. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

OR

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.

## The cyber security principles

### Purpose of the cyber security principles

The purpose of the cyber security principles is to provide strategic guidance on how an organisation can protect their systems and data from cyber threats. These cyber security principles are grouped into four key activities: govern, protect, detect and respond.

* **Govern:** Identifying and managing security risks.
* **Protect:** Implementing controls to reduce security risks.
* **Detect:** Detecting and understanding cyber security events to identify cyber security incidents.
* **Respond:** Responding to and recovering from cyber security incidents.

### Govern principles

The govern principles are:

* **G1:** A Chief Information Security Officer provides leadership and oversight of cyber security.
* **G2:** The identity and value of systems, applications and data is determined and documented.
* **G3:** The confidentiality, integrity and availability requirements for systems, applications and data are determined and documented.
* **G4:** Security risk management processes are embedded into organisational risk management frameworks.
* **G5:** Security risks are identified, documented, managed and accepted both before systems and applications are authorised for use, and continuously throughout their operational life.

### Protect principles

The protect principles are:

* **P1:** Systems and applications are designed, deployed, maintained and decommissioned according to their value and their confidentiality, integrity and availability requirements.
* **P2:** Systems and applications are delivered and supported by trusted suppliers.
* **P3:** Systems and applications are configured to reduce their attack surface.
* **P4:** Systems and applications are administered in a secure and accountable manner.
* **P5:** Security vulnerabilities in systems and applications are identified and mitigated in a timely manner.
* **P6:** Only trusted and supported operating systems, applications and computer code can execute on systems.
* **P7:** Data is encrypted at rest and in transit between different systems.
* **P8:** Data communicated between different systems is controlled and inspectable.
* **P9:** Data, applications and configuration settings are backed up in a secure and proven manner on a regular basis.
* **P10:** Only trusted and vetted personnel are granted access to systems, applications and data repositories.
* **P11:** Personnel are granted the minimum access to systems, applications and data repositories required for their duties.
* **P12:** Multiple methods are used to identify and authenticate personnel to systems, applications and data repositories.
* **P13:** Personnel are provided with ongoing cyber security awareness training.
* **P14:** Physical access to systems, supporting infrastructure and facilities is restricted to authorised personnel.

### Detect principles

The detect principles are:

* **D1:** Event logs are collected and analysed in a timely manner to detect cyber security events.
* **D2:** Cyber security events are analysed in a timely manner to identify cyber security incidents.

### Respond principles

The respond principles are:

* **R1:** Cyber security incidents are reported both internally and externally to relevant bodies in a timely manner.
* **R2:** Cyber security incidents are contained, eradicated and recovered from in a timely manner.
* **R3:** Business continuity and disaster recovery plans are enacted when required.

## **What is Authentication, Authorization, and Accounting (AAA)**

Authentication, authorization, and accounting (AAA) is a security framework that controls access to computer resources, enforces policies, and audits usage.

### Authentication

Authentication involves a user providing information about who they are. Users present login credentials that affirm they are who they claim. As an identity and access management (IAM) tool, a AAA server compares a user’s credentials with its database of stored credentials by checking if the username, password, and other authentication tools align with that specific user.

### Authorization

Authorization follows authentication. During authorization, a user can be granted privileges to access certain areas of a network or system. The areas and sets of permissions granted a user are stored in a database along with the user’s identity. The user’s privileges can be changed by an administrator. Authorization is different from authentication in that authentication only checks a user’s identity, whereas authorization dictates what the user is allowed to do.

For example, a member of the IT team may not have the privileges necessary to change the access passwords for a company-wide virtual private network (VPN). However, the network administrator may choose to give the member access privileges, enabling them to alter the VPN passwords of individual users. In this manner, the team member will be authorized to access an area they were previously barred from.

### Accounting

Accounting keeps track of user activity while users are logged in to a network by tracking information such as how long they were logged in, the data they sent or received, their Internet Protocol (IP) address, the Uniform Resource Identifier (URI) they used, and the different services they accessed.

Accounting may be used to analyze user trends, audit user activity, and provide more accurate billing. This can be done by leveraging the data collected during the user’s access. For example, if the system charges users by the hour, the time logs generated by the accounting system can report how long the user was logged in to the router and inside the system, and then charge them accordingly.

## **What is the CIA triad?**

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.

## Confidentiality, integrity, availability

The following is a breakdown of the three key concepts that form the CIA triad:

* **Confidentiality** is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories.
* **Integrity** involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).
* **Availability** means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

## **How Does Cybersecurity Work?**

Cybersecurity is designed to provide multiple layers of protection across all of the computers, networks, and programs used by a business. In order to create a unified defence against potential cyberattacks, it is important that the business, employees, processes, and technology are designed to work seamlessly together. Cybersecurity systems that function properly will be able to detect, investigate, and resolve potential weaknesses and vulnerabilities in the system before they can be exploited by a hacker or malicious software.

## **Types Of Cybersecurity**

The different types of cybersecurity include:

### **Application Security**

Application security is the implementation of various defences within business software and services to protect against a range of different threats. This type of cybersecurity requires the design of secure applications to minimize unauthorized access and modification.

### **Data Security**

Data security involves implementing strong data storage systems that are specifically designed to secure information while it is being stored and while it is in transit.

### **Network Security**

Network security focuses on protecting a business from both external and internal threats by implementing hardware and software systems that are specifically designed to protect a business’ network and infrastructure from misuse, disruptions, and unauthorized access.

### **Mobile Security**

Businesses that use mobile devices, such as cell phones, laptops, and tablets, should use mobile security measures to protect the information that is being stored on those devices from a range of different threats.

### **Cloud Security**

Most cloud applications and system—AWS, Google, Microsoft, etc.—use cloud security measures to protect users against various threats.

## **What is a cyber-attack?**

A cyber-attack is a deliberate attempt by external or internal threats or attackers to exploit and compromise the confidentiality, integrity and availability of information systems of a target organization or individual(s). Cyber-attackers use illegal methods, tools and approaches to cause damages and disruptions or gain unauthorized access to computers, devices, networks, applications and databases.

Cyber-attacks come in a wide variety and the following list highlights some of important ones that criminals and attackers use to exploit software:

1. Malware
2. Ransomware
3. Injection attacks (e.g., [cross-site scripting](https://www.synopsys.com/glossary/what-is-cross-site-scripting.html), [SQL injection](https://www.synopsys.com/glossary/what-is-sql-injection.html), command injection)
4. Session management and Man-in-the-Middle attacks
5. [Phishing](https://www.synopsys.com/glossary/what-is-phishing.html)
6. Denial of service
7. Privilege escalations
8. Unpatched/Vulnerable software
9. Remote code execution
10. Brute force

## **Types of cyber threats**

The threats countered by cyber-security are three-fold:

1. [**Cybercrime**](https://www.kaspersky.co.in/resource-center/threats/cybercrime) includes single actors or groups targeting systems for financial gain or to cause disruption.

2. **Cyber-attack** often involves politically motivated information gathering.

3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

### **Malware**

**Malware means malicious software.** One of the most common cyber threats, **malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user’s computer**. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

**There are a number of different types of malware, including:**

**virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

·        [**Trojans**](https://www.kaspersky.co.in/resource-center/threats/trojans)**:**A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

**Viruses vs. Trojans**

A virus cannot execute or reproduce unless the app it has infected is running. This dependence on a host application makes viruses different from trojans, which require users to download them, and worms, which do not use applications to execute. Many instances of malware fit into multiple categories: for instance, Stuxnet is a worm, a virus and a rootkit.

·        **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

·        **Ransomware:** Malware which locks down a user’s files and data, with the threat of erasing it unless a ransom is paid.

·        **Adware:** Advertising software which can be used to spread malware.

·        **Botnets:**Networks of malware infected computers which cybercriminals use to perform tasks online without the user’s permission.

### **SQL injection**

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

### **Phishing**

[Phishing](https://www.kaspersky.co.in/resource-center/threats/spam-phishing) is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

### **Man-in-the-middle attack**

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim’s device and the network.

### **Denial-of-service attack**

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

### Worms

Worms target vulnerabilities in operating systems to install themselves into networks. They may gain access in several ways: through backdoors built into software, through unintentional software vulnerabilities, or through flash drives. Once in place, worms can be used by malicious actors to launch [DDoS attacks](https://www.crowdstrike.com/cybersecurity-101/what-is-a-ddos-attack/), steal sensitive data, or conduct ransomware attacks.

### Rootkits

A [rootkit](https://www.crowdstrike.com/cybersecurity-101/malware/rootkit-malware/) is software that gives malicious actors remote control of a victim’s computer with full administrative privileges. Rootkits can be injected into applications, kernels, hypervisors, or firmware. They spread through phishing, malicious attachments, malicious downloads, and compromised shared drives. Rootkits can also be used to conceal other malware, such as keyloggers.

**Rootkit Example:**

[Zacinlo](https://www.eweek.com/security/more-nefarious-strain-of-zacinlo-malware-infecting-windows-10-machines) infects systems when users download a fake VPN app. Once installed, Zacinlo conducts a security sweep for competing malware and tries to remove it. Then it opens invisible browsers and interacts with content like a human would — by scrolling, highlighting and clicking. This activity is meant to fool behavioral analysis software. Zacinlo’s payload occurs when the malware clicks on ads in the invisible browsers. This advertising click fraud provides malicious actors with a cut of the commission.

## **Cyber safety tips - protect yourself against cyberattacks**

 How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

1.     **Update your software and operating system:**This means you benefit from the latest security patches.

2.     **Use anti-virus software:**Security solutions like [Kaspersky Total Security](https://www.kaspersky.co.in/total-security) will detect and removes threats. Keep your software updated for the best level of protection.

3.     **Use strong passwords:**Ensure your passwords are not easily guessable.

4.     **Do not open email attachments from unknown senders:**These could be infected with malware.

5.     **Do not click on links in emails from unknown senders or unfamiliar websites:**This is a common way that malware is spread.

**6.     Avoid using unsecure WiFi networks in public places:**Unsecure networks leave you vulnerable to man-in-the-middle attacks.

## Hacking definition: What is hacking?

Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks. And while hacking might not always be for malicious purposes, nowadays most references to hacking, and hackers, characterize it/them as unlawful activity by cybercriminals—motivated by financial gain, protest, information gathering (spying), and even just for the “fun” of the challenge.

**Who is a Hacker?**

A hacker is ideally a person who is skilled in information technology. He uses his technical knowledge to overcome an obstacle or sometimes even achieve a goal within a computerized system. However, in recent times, the term hacker is always associated with a security hacker – someone who is always on the lookout for ways to acquire and exploit sensitive personal, financial and organizational information, which is otherwise not accessible to them. Legitimate figures often use hacking for legal purposes.

**How does Hacking Work?**

Hackers are highly skilled in breaching securities to gain unauthorized access to phones, tablets, computers, IoT devices, networks, or the networking system of an entire organization. They are generally very proficient in exploiting weaknesses in network security, taking advantage of the same. These weaknesses can be technical or social in nature.

* **Technical weaknesses:**Hackers are extremely talented in exploiting software vulnerabilities or weak security practices. They do this to gain unauthorized access or even sometimes to inject malware that would crumple the entire system.
* **Social weaknesses:** This kind of social engineering is done to convince those with privileged access to click on malicious links, open infected files, or reveal personal information. This allows them access to otherwise hardened infrastructures

.

## Hacking tools: How do hackers hack?

Hacking is typically technical in nature (like creating malvertising that deposits malware in a drive-by attack requiring no user interaction). But hackers can also use psychology to trick the user into clicking on a malicious attachment or providing personal data. These tactics are referred to as “[social engineering](https://www.malwarebytes.com/social-engineering).”

In fact, it's accurate to characterize hacking as an over-arching umbrella term for activity behind most if not all of the malware and malicious cyberattacks on the computing public, businesses, and governments. Besides social engineering and malvertising, common hacking techniques include:

* [Botnets](https://www.malwarebytes.com/botnet)
* [Browser hijacks](https://blog.malwarebytes.com/detections/hijack/)
* [Denial of service (DDoS) attacks](https://www.malwarebytes.com/ddos)
* [Ransomware](https://www.malwarebytes.com/ransomware)
* [Rootkits](https://www.malwarebytes.com/rootkit)
* [Trojans](https://www.malwarebytes.com/trojan)
* [Viruses](https://www.malwarebytes.com/computer-virus)
* [Worms](https://www.malwarebytes.com/computer-worm)
* **Why Do Hackers Hack?**
* 1. Steal/Leak Information  
  One of the most common reasons for hackers to hack is to steal or leak information. This could be data and information about your customers, your internal employees or even private data specific to your business. These are cases where hackers typically go after big targets in order to get the most attention.
* **2. Disrupt Services**
* Hackers just love to take something down. And then also leave a statement on the website - more on that later. But hackers have successfully taken down many services by creating bots that overwhelm a server with traffic, thus, leading to a crash. It is known as a DoS (Denial of Service) attack and can put a company’s website out of service for a while. These days, there's also DDoS or Distributed Denial of Service attacks which use multiple infected systems to take down a single major system leading to a denial of service.
* **3. Make a Point** -The hackers who fall into this category are very interesting. They don't care about money or data. They seem to feel that they have a higher purpose in life. They want to steal information or disrupt your network in order to make a point.
* **4. Money** -This is what everyone usually fears about. We've seen many businesses reach out to us at the stage when they have already been hacked and a hacker is demanding money. Hackers not only hack businesses and ask for ransom but they also try hacking into regular user accounts and try to take advantage of things like online banking, online retail, etc. where financial transactions are involved.
* **5. Driven by Purpose** - Hacktivism, Idealism, Political Motives Many hackers are also drive by a specific purpose. Sometimes, this comes out only when they get caught. Some of them aim to be idealists and take it upon themselves to expose injustice, some have political motives, some simple target the government, and so on. A major example is a hacktivist group called Anonymous who have been popular around the world for challenging and taking down many governments. These hackers can target religious groups, governments, movements, to promote a particular agenda.  
  Read more at: <https://www.appknox.com/blog/why-do-hackers-hack>  
  **Hacker’s Methodology:**

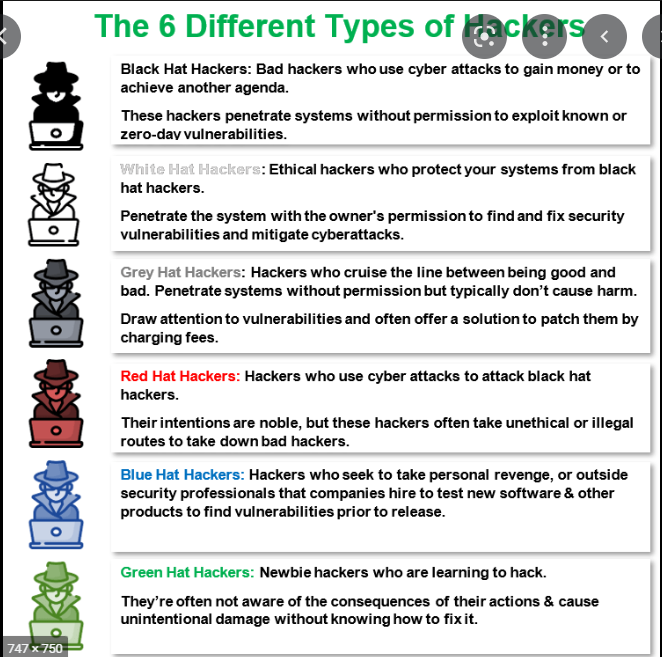
1. **Footprinting**: This is a method that conducts a target analysis, identification and discovery typically through the use of open-source tools. This include dumpster diving, social engineering and the use of utility such as website hacking, treasurers, pings, network lookups etc.
2. **Scanning**: This step extracts information from footprinting and explores more data from it. This step includes pore scanning, operating system identification and determining whether or not a machine is accessible.
3. **Enumeration**: This is a phase where the hacker further interrogates a specific server to determine an operating system’s software. It includes searching for network shared information, the specific version of the application running, user account, traffic and more.
4. **Network Mapping**: This step is exactly as the name implies. Laying out an illustration of the target network includes taking all the resources, logs, target surveys, etc. to create a visualization of the target environment, this often looks different from the exploitative perspective.
5. **Gaining Access**: This step is the exploitation process. This is about gaining access to a machine or network by the client’s side, insider threat, supply interdiction or remote exploitation opportunity. Hackers use spearphishing, device exploitation and many more methods to conduct the exploitation.
6. **Privilege Escalation**: Depending on the exploitation opportunity, hackers decide the intensity of the exploitation, what kind of privileges he wants to escalate. They conduct it through local exploit opportunity in order to gain system-level privileges, the highest possible user.
7. **Post Exploitation**: This step is a compilation of many steps and is dependent upon the objective of the mission. It includes any combination of target surveys and remote forensic analysis, cover track (cleaners), data collection, backdoor implant resistance, computer network attacks, delay target survey and more.
8. **Forensic Analysis**: This step is to conduct analysis on the target machine for potential security mechanisms, fires or users which could either assist in obtaining the objective or harmed assessment. It basically analyses the target’s operating environment.
9. **Cover Tracks**: This is the process of removing any forensic relevant residue that was left behind as a result of exploitation. This is one of the most important steps that the hacker can perform.
10. ***Data Collection:*** The attacker is in the present to perform some activity, which involves extracting as much data as possible. Network traffic analysis is the key to this phase.

### **Common mistakes which you can avoid, save your data from being accessible or penetrable by hackers!**

1. **Same password for multiple accounts**: If the [**hacker**](https://www.cybervie.com/) hacks one of your accounts, all your other accounts are up for a toss. The hacker most likely will gain access to other accounts as well. We recommend you to have different passwords for all your accounts, thereby not giving the hacker any sort of leverage.
2. **Short Passwords**: When you use multiple passwords that are not complex, you expose yourself to the risks of attacks. It is the kind of attack when a hacker is using special software to hack your account.
3. **Using weak or no wireless encryption on your wireless network**: If you have a wireless network in your home and that is not encrypted or using encryption then you are basically letting everyone to your internet connection. You are also helping potential hackers to enter your system. You might have your encryption turned on, but if it is outdated it will not help you anyhow. WEP can be cracked by most hacks, consider implementing WPA based [encryption](https://portal.cybervie.com/forms/enrolment-form) with a strong wireless network password.
4. **Using unknown flash drives**: Backing up is important but be careful when inserting someone else’s flash drive or using it on your computer. External devices are risky to use and can be fooled with. Scan your device regularly for viruses to ensure that you are not a victim of hacking.
5. **Responding to Pop-up Messages and/or Unsolicited Emails**: It is easy to hack your computer by this method. Treat such emails and messages with suspicion. Turn on your browser pop up blocking feature and consider using browser plugin such as nose clip to protect yourself.
6. ***Answering Phishing Emails***: 80000 users fall for phishing scams every single day. Most email systems have spare filters to catch such spams, but always check the sender’s name and email.
7. ***Using unpatched OS and Applications***: The timely application of security patches is extremely important these days. Hackers and cybercriminals are relying on the fact that many of their potential victims likely have unpatched vulnerabilities present on their system. Hackers will exploit these vulnerabilities to gain entrance into the victim’s system. You can prevent these attacks if you keep your system up to date with the latest available security patches.
8. ***Using Public Wifi***: Do not use any public wifi to access your personal information. These networks are not secure and can be a trap. As soon as connect to the wifi, you can give a hacker accessed password. This would harm your system and give easy access to the hacker.
9. **Turning off Security Features**: People might disable their firewall to access a particular application, rather than troubleshooting the problem. They might forget to turn the firewall back on after they have finished working on that particular application. Anti-virus application is another application that frequently gets turned off, some people think it would boost their computer’s performance or another resource-intensive application. This feature secures your computer and data.
10. **Mistakes by Web Developers**: Developing their own security methods which have flaws and vulnerable, moreover discoverable by hackers. Focusing on companies and not the overall system, adding security at the end of development. One must not store data and passwords unencrypted in the database.

## **TYPES OF HACKERS**

1. [**White Hat / Ethical Hackers**](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#White-Hat-Hackers)
2. [**Black Hat Hackers**](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Black-Hat-Hackers)
3. [**Gray Hat Hackers**](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Gray-Hat-Hackers)
4. [**Script Kiddies**](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Script-Kiddies)
5. [**Green Hat Hackers**](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Green-Hat-Hackers)
6. [**Blue Hat Hackers**](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Blue-Hat-Hackers)
7. [**Red Hat Hackers**](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Red-Hat-Hackers)
8. [**State/Nation Sponsored Hackers**](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#State/Nation-Sponsored-Hackers)
9. [**Hacktivist**](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Hacktivist)
10. [**Malicious insider or Whistleblower**](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Malicious-insider-or-Whistleblower)

****

### 1) **White Hat Hackers**

White hat hackers are types of hackers who’re professionals with expertise in cybersecurity. They are authorized or certified to hack the systems. These White Hat Hackers work for governments or organizations by getting into the system. They hack the system from the loopholes in the cybersecurity of the organization. This hacking is done to test the level of cybersecurity in their organization. By doing so, they identify the weak points and fix them to avoid attacks from external sources. White hat hackers work per the rules and regulations the government sets. White hat hackers are also known as ethical hackers.

**Motives & Aims:** The goals of these types of hackers are helping businesses and an appetite for detecting gaps in networks’ security. They aim to protect and assist companies in the ongoing battle against cyber threats. A White Hat hacker is any individual who will help protect the company from raising cyber crimes. They help enterprises create defences, detect vulnerabilities, and solve them before other cybercriminals can find them.

### 2) **Black Hat Hackers**

Black hat hackers are also knowledgeable computer experts but with the wrong intention. They attack other systems to get access to systems where they do not have authorized entry. On gaining entry they might steal the data or destroy the system. The hacking practices these types of hackers use depend on the individual’s hacking capacity and knowledge. As the intentions of the hacker make the hacker a criminal. The malicious action intent of the individual cannot be gauged either can the extent of the breach while hacking

**Motives & Aims:** To hack into organizations’ networks and steal bank data, funds or sensitive information. Normally, they use the stolen resources to profit themselves, sell them on the black market or harass their target company.

### 3) **Gray Hat Hackers**

The intention behind the hacking is considered while categorizing the hacker. The Gray hat hacker falls between the black and white hat hackers. They are not certified, hackers. These types of hackers work with either good or bad intentions. The hacking might be for their gain. The intention behind hacking decides the type of hacker. If the intention is for personal gain, the hacker is considered a gray hat hacker.

**Motives & Aims:** The difference is, they don’t want to rob people nor want to help people in particular. Rather, they enjoy experimenting with systems to find loopholes, crack defenses, and generally find a fun hacking experience.

### 4) **Script Kiddies**

It is a known fact that half knowledge is always dangerous. The Script Kiddies are amateurs types of hackers in the field of hacking. They try to hack the system with scripts from other fellow hackers. They try to hack the systems, networks, or websites. The intention behind the hacking is just to get the attention of their peers. Script Kiddies are juveniles who do not have complete knowledge of the hacking process.

**Motives & Aims:** One standard Kiddie Script attack is a DoS (Denial of Service) or DDoS attack (Distributed Denial of Service). This simply means that an IP address is flooded with too much excessive traffic that it collapses. Consider several Black Friday shopping websites, for instance. It creates confusion and prevents someone else uses the service.

### 5) **Green Hat Hackers**

Green hat hackers are types of hackers who learn the ropes of hacking. They are slightly different from the Script Kiddies due to their intention. The intent is to strive and learn to become full-fledged hackers. They are looking for opportunities to learn from experienced hackers.

### 6) **Blue Hat Hackers**

Blue Hat Hackers are types of hackers who’re similar to Script Kiddies. The intent to learn is missing. They use hacking as a weapon to gain popularity among their fellow beings. They use hacking to settle scores with their adversaries. Blue Hat Hackers are dangerous due to the intent behind the hacking rather than their knowledge.

### 7) **Red Hat Hackers**

Red Hat Hackers are synonymous with Eagle-Eyed Hackers. They are the types of hackers who’re similar to white hackers. The red hat hackers intend to stop the attack of black hat hackers. The difference between red hat hackers and white hat hackers is that the process of hacking through intention remains the same. Red hat hackers are quite ruthless when dealing with black hat hackers or counteracting malware. The red hat hackers continue to attack and may end up having to replace the entire system setup.

### 8) **State/Nation Sponsored Hackers**

Government appoints hackers to gain information about other countries. These types of hackers are known as State/Nation sponsored hackers. They use their knowledge to gain confidential information from other countries to be well prepared for any upcoming danger to their country. The sensitive information aids in being on top of every situation but also in avoiding upcoming danger. They report only to their governments.

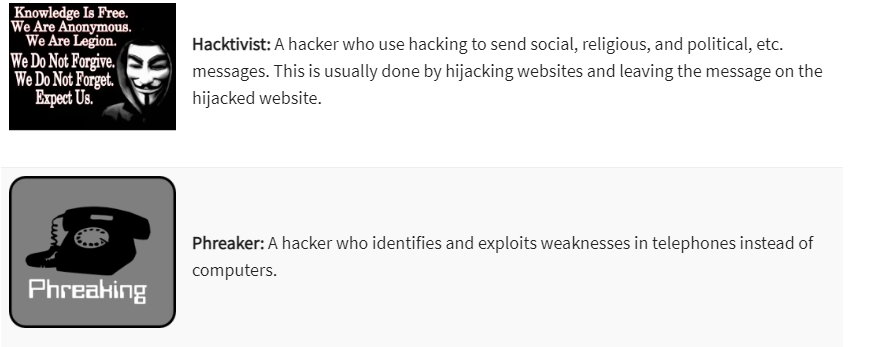
### 9) **Hacktivist**

These types of hackers intend to hack government websites. They pose themselves as activists, so known as a hacktivist. Hacktivists can be an individual or a bunch of nameless hackers whose intent is to gain access to government websites and networks. The data gained from government files accessed are used for personal political or social gain.

### 10) **Malicious insider or Whistleblower**

These types of hackers include individuals working in an organization who can expose confidential information. The intent behind the exposure might be a personal grudge against the organization, or the individual might have come across illegal activities within the organization. The reason for exposure defines the intent behind the exposure. These individuals are known as whistleblowers.

## 



What is infiltration in cyber security?

An Infiltration is **a piece of malicious software that attempts to enter and/or damage a user's computer**.

Analysing a Cyber Attack

Types of Malwares

Spyware

Malware

Backdoor

Ransomware

Scareware

Rootkit

Virus

Trojan horse

Worms

Symptoms of attack

**Methods of Infiltration**

## Social Engineering

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions.

## Pretexting

Pretexting is form of [social engineering](https://www.csoonline.com/article/2124681/what-is-social-engineering.html) in which an attacker tries to convince a victim to give up valuable information or access to a service or system. The distinguishing feature of this kind of attack is that the scam artists comes up with a story — or pretext — in order to fool the victim.

# Tailgating

During these attacks, a cyber criminal will attempt to enter a restricted area without going through an authentication process, such as a passcode-protected door or biometric scanner.

They can do this by locating a secure area, waiting outside for an authorized employee to enter, and asking them to hold the door so they can slip through the defenses designed to protect the perimeter.

## DDoS

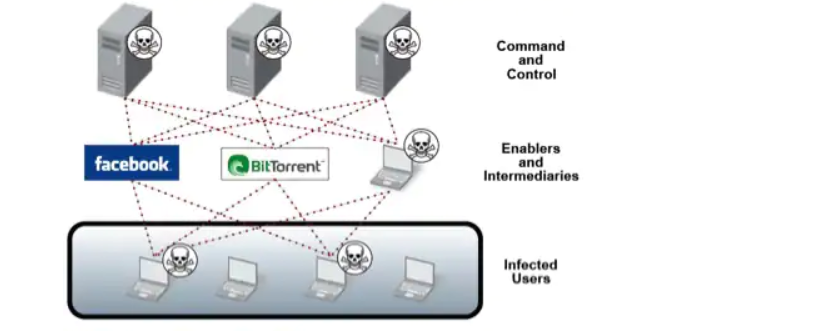
A **distributed denial-of-service (DDoS**) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic

# Botnet

A bot is a piece of malware that infects a computer to carry out commands under the remote control of the attacker.

A **botnet** (short for “robot network”) is a network of computers infected by [**malware**](https://www.paloaltonetworks.com/cyberpedia/what-is-malware) that are under the control of a single attacking party, known as the “bot-herder.” Each individual machine under the control of the bot-herder is known as a bot. From one central point, the attacking party can command every computer on its botnet to simultaneously carry out a coordinated criminal action.



SEO Poisoning

SEO poisoning, also known as search engine poisoning or search poisoning, is an attack method that involves [cybercriminals](https://securuscomms.co.uk/cybercriminal-gangs-causing-havoc-worldwide/) creating malicious websites and using several SEO tactics to make them rank highly in search results.

These ‘fake’ websites appear legitimate and often are near copies of existing sites and rank for search terms that significant numbers of people are looking for, such as phrases related to holidays, current events, breaking news, and viral videos.

**Wi-Fi Password Cracking**

**Wireless networks are accessible to anyone within the router’s transmission radius.**This makes them vulnerable to attacks. Hotspots are available in public places such as airports, restaurants, parks, etc.

You will need a wireless network enabled device such as a laptop, tablet, smartphones, etc. You will also need to be within the transmission radius of a wireless network access point. Most devices (if the wireless network option is turned on) will provide you with a list of available networks. If the network is not password protected, then you just have to click on connect. If it is password protected, then you will need the password to gain access.

## How to Crack WiFI (Wireless) Networks

### WEP(WIRED EQUIVALENT PRIVACY) cracking

Cracking is the process of exploiting security weaknesses in wireless networks and gaining unauthorized access. WEP cracking refers to exploits on networks that use WEP to implement security controls. There are basically two types of cracks namely;

* **Passive cracking**– this type of cracking has no effect on the network traffic until the WEP security has been cracked. It is difficult to detect.
* **Active cracking**– this type of attack has an increased load effect on the network traffic. It is easy to detect compared to passive cracking. It is more effective compared to passive cracking.

## WiFi Password Hacker (WEP Cracking) Tools

* **Aircrack**– network sniffer and WEP cracker. This WiFi password hacker tool can be downloaded from [http://www.aircrack-ng.org/](https://www.aircrack-ng.org/)
* **WEPCrack**– this is an open source Wi-Fi hacker program for breaking 802.11 WEP secret keys. This WiFi hacker app for PC is an implementation of the FMS attack. <http://wepcrack.sourceforge.net/>
* **Kismet**– this WiFi password hacker online detects wireless networks both visible and hidden, sniffer packets and detect intrusions. <https://www.kismetwireless.net/>
* **WebDecrypt**– this WiFi password hack tool uses active dictionary attacks to crack the WEP keys. It has its own key generator and implements packet filters for hacking WiFi password. <http://wepdecrypt.sourceforge.net/>

## WPA(WIFI PROTECTED ACCESS) Cracking

WPA uses a 256 pre-shared key or passphrase for authentications. Short passphrases are vulnerable to dictionary attacks and other attacks that can be used to crack passwords. The following WiFi hacker online tools can be used to crack WPA keys.

* **CowPatty**– this WiFi password cracker tool is used to crack pre-shared keys (PSK) using brute force attack. [http://wirelessdefence.org/Contents/coWPAttyMain.htm](https://sourceforge.net/projects/cowpatty/)
* **Cain & Abel**– this WiFi hacker for PC tool can be used to decode capture files from other sniffing programs such as Wireshark. The capture files may contain WEP or WPA-PSK encoded frames. <https://www.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml>

## General Attack types

* **Sniffing**– this involves intercepting packets as they are transmitted over a network. The captured data can then be decoded using tools such as Cain & Abel.
* **Man in the Middle (MITM) Attack**– this involves eavesdropping on a network and capturing sensitive information.
* **Denial of Service Attack**– the main intent of this attack is to deny legitimate users network resources. FataJack can be used to perform this type of attack. More on this in [article](https://www.guru99.com/how-to-hack-web-server.html)

## Cracking Wireless network WEP/WPA keys

It is possible to crack the WEP/WPA keys used to gain access to a wireless network. Doing so requires software and hardware resources, and patience. The success of such WiFi password hacking attacks can also depend on how active and inactive the users of the target network are.

We will provide you with basic information that can help you get started. Backtrack is a Linux-based security operating system. It is developed on top of Ubuntu. Backtrack comes with a number of security tools. Backtrack can be used to gather information, assess vulnerabilities and perform exploits among other things.

Some of the popular tools that backtrack has includes;

* Metasploit
* Wireshark
* Aircrack-ng
* NMap
* Ophcrack

Cracking wireless network keys requires patience and resources mentioned above. **At a minimum, you will need the following tools**

A **wireless network adapter with the capability to inject packets** (Hardware)

* **Kali Operating System**. You can download it from here <https://www.kali.org/downloads/>
* **Be within the target network’s radius**. If the users of the target network are actively using and connecting to it, then your chances of cracking it will be significantly improved.
* Sufficient **knowledge of Linux based operating systems and working knowledge of Aircrack** and its various scripts.
* **Patience**, cracking the keys may take a bit of sometime depending on a number of factors some of which may be beyond your control. Factors beyond your control include users of the target network using it actively as you sniff data packets.

## Password attacks

Password attacks involve exploiting a broken authorization vulnerability in the system combined with automatic password attack tools that speed up the guessing and cracking passwords. The attacker uses various techniques to access and expose the credentials of a legitimate user, assuming their identity and privileges. The username-password combination is one of the oldest known account authentication techniques, so adversaries have had time to craft multiple methods of obtaining guessable passwords. Additionally, applications that use passwords as the sole authentication factor are vulnerable to password attacks since the vulnerabilities are well understood.

Top 10 password attacks and how to stop them

Here are the 10 most common password attacks and mitigations businesses can use to prevent them from leading to network compromise and loss of business-critical data.

1. Brute-force Attack
2. Dictionary Attack
3. Password Spraying
4. Credential Stuffing
5. Phishing
6. Keylogger Attack
7. Social Engineering
8. Password Reset
9. Old fashioned theft
10. Password Reuse

### 1. Brute Force Attacks

A brute-force attack is a basic password attack carried out by hackers when they make high-volume attempts to gain access to a network using large lists of common or compromised passwords. Even a "gaming" class computer can "guess" billions of passwords each second, using today's high-powered CPU power. It proactively tries to guess the password for legitimate user accounts "by force."

* Prevention of brute-force attacks involves account lockouts, password length & passphrases greater than 20 characters, blocking of incremental passwords and common patterns, and breached password protection, custom dictionaries, and MFA.
* Example of a real-world brute force attack - [Attackers used brute force to gain unauthorized access to the accounts of 19715 users](https://www.makeuseof.com/brute-force/) within five days stealing money.

## 2. Dictionary Attack

A Dictionary attack is a brute-force hacking method described above that uses large databases of common passwords as its source, much like a dictionary. It is used to break into password-protected assets by entering every word in a dictionary and derivatives of those words known as leetspeak and previously leaked passwords or key phrases. For instance, hackers know that users often substitute spellings for words using numbers and characters as substitutions. An example is the password P@$$w0rd.

* Prevention steps - Password length/passphrases greater than 20 characters, block incremental/common patterns, breached password protection, custom dictionary, MFA.
* A dictionary attack was used on [January 4th, 2009 by a hacker known only as GMZ](https://cisserv1.towson.edu/~cssecinj/links-resources/real-life-examples/) to compromise an administrator account and then change the passwords of famous accounts, including President elect Barack Obama, Britney Spears, and others.

## 3. Password Spraying

A password spraying attack avoids detection or lockout on an individual account by attempting one or two common passwords across many different accounts, services, and organizations. Attackers use this method to avoid the account lockout threshold that may be set from three to five incorrect attempts commonly found in many organizations.

By attempting just one password fewer than the lockout threshold, the attacker can successfully try many passwords across the organization without being stopped by default protective mechanisms found in Active Directory. The attacker picks passwords commonly used by end-users, mathematical formulas to guess passwords, or use breached passwords that have already been exposed in password dumps online.

* Prevention steps - Password length/passphrases greater than 20 characters, block incremental/common patterns, breached password protection, custom dictionary, MFA.
* [Microsoft recently warned of an uptick in password spraying attacks](https://www.zdnet.com/article/microsoft-warns-over-uptick-in-password-spraying-attacks/) by state-sponsored hackers and cybercriminals.

## 4.What is a keylogger?

Keyloggers are a particularly insidious type of [spyware](https://www.malwarebytes.com/spyware) that can record and steal consecutive keystrokes (and much more) that the user enters on a device. The term keylogger, or "keystroke logger," is self-explanatory: Software that logs what you type on your keyboard. However, keyloggers can also enable cybercriminals to eavesdrop on you, watch you on your system camera, or listen over your smartphone's microphone

### Hardware vs. software keyloggers

Keyloggers come in at least two broad flavors—hardware devices and the more familiar software variety. Hardware devices can be embedded in the internal PC hardware itself, or be an inconspicuous plugin that’s secretly inserted into the keyboard port between the CPU box and the keyboard cable so that it intercepts all the signals as you type. But that means that the cybercriminal has to have physical access to the PC while you’re not present in order to plant the hardware keyloggers.

Software keyloggers are much easier to introduce to and install on victims’ devices, which is why that variety is much more common. Unlike other kinds of malware, software keyloggers are not a threat to the systems they infect themselves. In fact, the whole point of keyloggers is to work behind the scenes, sniffing out the keystrokes while the computer continues to operate normally. But even if they don’t harm the hardware, keyloggers are definitely a threat to users, especially when they steal sensitive data.

## **Traffic Interception**

Traffic interception, a variation on the man-in-the-middle attack, involves the threat actors eavesdropping on network traffic to monitor and capture data. A common way of doing that is through unsecured Wi-Fi connections or connections that don’t use encryption, such as HTTP.

Even SSL traffic is vulnerable. For example, a hacker can use a man-in-the-middle attack in what’s called SSL hijacking. SSL hijacking is when someone tries to connect to a secure website, and the attacker creates a bridge of sorts between the user and the intended destination and intercepts any information passing between the two, such as passwords.

What is a rainbow table in cybersecurity?

A rainbow table is **a password hacking tool that uses a precomputed table of reversed password hashes to crack passwords in a database**.

Password Cracking Time

* On average, it takes a hacker about two seconds to crack an 11-character password that uses only numbers. Throw in some upper- and lower-case letters, and it will take a hacker one minute to hack into a seven-character password.
* Hive Systems developed a handy chart to illustrate the time it takes for a hacker to brute force your password. A brute force attack on your login details is when cybercriminals use trial-and-error to guess your details.
* Cybercriminals use sophisticated software that can run thousands of password combinations a minute, and their tools are only getting better. A general rule is that your password should be at least 11 characters and use numbers, along with upper and lowercase letters. That combination will take hackers 41 years to crack.
* 

# Advanced persistent threat (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](https://www.imperva.com/learn/data-security/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](https://www.imperva.com/learn/application-security/ethical-hacking/) 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

Executing an APT assault requires more resources than a standard web application attack. The perpetrators are usually teams of experienced cybercriminals having substantial financial backing. Some APT attacks are government-funded and used as cyber warfare weapons.

APT attacks differ from traditional web application threats, in that:

* They’re significantly more complex.
* They’re not hit and run attacks—once a network is infiltrated, the perpetrator remains in order to attain as much information as possible.
* They’re manually executed (not automated) against a specific mark and indiscriminately launched against a large pool of targets.
* They often aim to infiltrate an entire network, as opposed to one specific part.

More common attacks, such as [remote file inclusion (RFI)](https://www.imperva.com/learn/application-security/rfi-remote-file-inclusion/), [SQL injection](https://www.imperva.com/learn/application-security/sql-injection-sqli/) and [cross-site scripting (XSS)](https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/), are frequently used by perpetrators to establish a foothold in a targeted network. Next, Trojans and backdoor shells are often used to expand that foothold and create a persistent presence within the targeted perimeter.

### **What is a Security Vulnerability?**

A security vulnerability is a weakness an adversary could take advantage of to compromise the confidentiality, availability, or integrity of a resource.

OR

A **security vulnerability** is a software code flaw or a system misconfiguration such as [**Log4Shell**](https://snyk.io/blog/log4j-rce-log4shell-vulnerability-cve-2021-4428/) through which attackers can directly gain unauthorized access to a system or network. Once inside, the attacker can leverage authorizations and privileges to compromise systems and assets.

An **exploit**is the means through which hackers use a vulnerability to mount an attack. An exploit is typically a piece of specially crafted software or a sequence of commands. For example, vulnerabilities in Microsoft IIS (Internet Information Services) and MS-SQL server have been exploited over the years by [**network worms**](https://encyclopedia.kaspersky.com/knowledge/vulnerabilities-examples/) such as CodeRed, Spida, and Slammer.

There are even exploit kits out there (e.g., Rig, Magnitude, and Fallout) that can be embedded in compromised web pages where they continuously scan for vulnerabilities. As soon as a weakness is detected, the kit immediately attempts to deploy an exploit, such as injecting malware into the host system.

A **threat**is the actual or hypothetical event in which one or more exploits use a vulnerability to mount an attack. For example the CodeRed exploit on the Microsoft IIS vulnerability has been actively used to infect more than 300,000 targets. These threats have caused huge financial losses around the globe.

Hardware Vulnerabilities

A hardware vulnerability is **an exploitable weakness in a computer system that enables attack through remote or physical access to system hardware**. Any means by which code can be introduced to a computer is inherently a hardware vulnerability.

# Meltdown and Spectre

Vulnerabilities in modern computers leak passwords and sensitive data.

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers.

#### **Meltdown**

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.

If your computer has a vulnerable processor and runs an unpatched operating system, it is not safe to work with sensitive information without the chance of leaking the information. This applies both to personal computers as well as cloud infrastructure. Luckily, there are [software patches against Meltdown](https://meltdownattack.com/#faq-fix).

[Meltdown Paper](https://meltdownattack.com/meltdown.pdf)

[Cite](https://meltdownattack.com/meltdown.bib)

[arXiv](https://arxiv.org/abs/1801.01207)

#### **Spectre**

Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre

Spectre is harder to exploit than Meltdown, but it is also harder to mitigate. [However, it is possible to prevent specific known exploits based on Spectre through software patches.](https://meltdownattack.com/#faq-fix)

[Spectre Paper](https://spectreattack.com/spectre.pdf)

[Cite](https://meltdownattack.com/spectre.bib)

[arXiv](https://arxiv.org/abs/1801.01203)

## Who reported Meltdown?

Meltdown was independently discovered and reported by three teams:

* [Jann Horn](https://twitter.com/tehjh) ([Google Project Zero](https://googleprojectzero.blogspot.com/)),
* [Werner Haas](mailto:werner.haas@cyberus-technology.de), [Thomas Prescher](mailto:thomas.prescher@cyberus-technology.de) ([Cyberus Technology](https://www.cyberus-technology.de/" \t "_blank)),
* [Daniel Gruss](https://gruss.cc/), [Moritz Lipp](https://mlq.me/), [Stefan Mangard](https://www.iaik.tugraz.at/content/about_iaik/people/mangard_stefan/), [Michael Schwarz](https://misc0110.net/) ([Graz University of Technology](https://www.iaik.tugraz.at/))

## Who reported Spectre?

Spectre was independently discovered and reported by two people:

* [Jann Horn](https://twitter.com/tehjh) ([Google Project Zero](https://googleprojectzero.blogspot.com/)) and
* [Paul Kocher](https://paulkocher.com/) in collaboration with, in alphabetical order, [Daniel Genkin](https://www.cis.upenn.edu/~danielg3/) ([University of Pennsylvania](https://www.upenn.edu/) and [University of Maryland](https://www.umd.edu/)), [Mike Hamburg](https://www.shiftleft.org/) ([Rambus](https://www.rambus.com/)), [Moritz Lipp](https://mlq.me/) ([Graz University of Technology](https://www.iaik.tugraz.at/)), and [Yuval Yarom](https://cs.adelaide.edu.au/~yval) ([University of Adelaide](https://www.adelaide.edu.au/) and [Data61](https://www.data61.csiro.au/))

# Software Vulnerability

# A software vulnerability is a defect in software that could allow an attacker to gain control of a system. These defects can be because of the way the software is designed, or because of a flaw in the way that it’s coded.

# Software update

A software update (also known as patch) is a set of changes to a software to update, fix or improve it. Changes to the software will usually either fix bugs, fix security vulnerabilities, provide new features or improve performances and usability. Infrequently, patches may also be used to limit functionality, remove or disable features.

Depending on the software, updates can either be installed manually or automatically if the device is connected to the internet and has the appropriate capabilities (for instance, an Android phone that updates its software on its own). Software updates are particularly important when applied to the Operating System given the reliance of other software (such as apps or drivers) on it. For example, a major release of an Operating System such as Android or iOS might render a number of apps obsolete, if all version released after the update aren't compatible with the previous version of the OS. This could prevent people from accessing important services as illustrated with some covid-19 track and track apps which were only compatible with specific versions of iOS and Android.

From a security standpoint, software updates have important implications. When an update includes a fix for security vulnerabilities, any device running an out-of-date version of the software is particularly vulnerable. This allows malicious actors to know what vulnerabilities exist on a given system and, consequently, puts devices running this software (version) more at risk. For example, using an outdated version of Android (such as version 4) means that all the security vulnerabilities spotted and fixed in following versions still exist on any device that uses the older version 4.

Lack of software update might also have a negative impact on a device's functionalities for example by making some its function obsolete (e.g.: a browser that do not support the latest security protocols and therefor can't display websites properly). It might also mean that identified bugs and problem might never be fixed (e.g.: poor battery).

Current market practices don't impose minimum software support for a device or software version on release, meaning a device can be produced, released and sold while embeding an outdated Operating System or without offering regular software updates. This fundamentally allow manufacturers to sell devices that might become outdated and vulnerable within a couple of month of their release. This is [a practice that's reguylarly observed](https://privacyinternational.org/node/4605) which puts users' security and privacy at a very high risk.

## **Defense in depth**

Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack. This multi-layered approach with intentional redundancies increases the security of a system as a whole and addresses many different attack vectors. Defense in Depth is commonly refered to as the "castle approach" because it mirrors the layered defenses of a medieval castle. Before you can penetrate a castle you are faced with the moat, ramparts, draw-bridge, towers, battlements and so on.

The digital world has revolutionized how we live, work and play. However, it's a digital world that is constantly open to attack, and because there are so many potential attackers, we need to ensure we have the right security in place to prevent systems and networks being compromised. Unfortunately, there is no single method that can successfully protect against every single type of attack. This is where a defense in depth architecture comes into play.

## **How defense in depth works**

A layered approach to security can be applied to all levels of IT systems. From the lone laptop accessing the internet from the coffee shop to the fifty thousand user enterprise WAN, Defense in Depth can significantly improve your security profile.

No organization can be ever be fully protected by a single layer of security. Where one door may be closed, others will be left wide open, and hackers will find these vulnerabilities very quickly. However, when you use a series of different defenses together, such as firewalls, malware scanners, intrusion detection systems, data encryption and integrity auditing solutions, you effectively close the gaps that are created by relying on a singular security solution.

EXAMPLES

### **Antivirus Software**

**Antivirus software** is the cornerstone of a holistic defense in depth **[cybersecurity strategy](https://heimdalsecurity.com/blog/how-to-build-effective-cybersecurity-strategy/)** due to its ability to not only prevent but also detect and remove malware. While initially designed to combat computer viruses only (hence its name), nowadays an antivirus is a jack of all trades, defending users from Trojans, worms, spyware, adware, and other common [**examples of malicious code**](https://heimdalsecurity.com/blog/examples-of-malicious-code/).

A**firewall** is another essential piece of a successful approach to defense in depth that goes hand in hand with antivirus software nowadays. A firewall monitors both incoming and outgoing network traffic, detecting malicious activity according to a predetermined set of rules.

**Multi-factor authentication** is a verification method that allows a user to login into an account only after presenting two or more pieces of evidence. Popular steps include device confirmation, PIN codes, or biometric data such as facial recognition or fingerprint scanning. As for **password hashing**, it represents an encryption process that turns the credential into a scrambled version of itself that is nearly impossible to read or decipher.

## What Is a Honeypot?

A honeypot is a cybersecurity mechanism that uses a manufactured attack target to lure cybercriminals away from legitimate targets. They also gather intelligence about the identity, methods and motivations of adversaries.

A honeypot can be modeled after any digital asset, including software applications, servers or the network itself. It is intentionally and purposefully designed to look like a legitimate target, resembling the model in terms of structure, components and content. This is meant to convince the [adversary](https://www.crowdstrike.com/blog/meet-the-adversaries/) that they have accessed the actual system and encourage them to spend time within this controlled environment.

The honeypot serves as a decoy, distracting cybercriminals from actual targets. It can also serve as a reconnaissance tool, using their intrusion attempts to assess the adversary’s techniques, capabilities and sophistication.

The intelligence gathered from honeypots is useful in helping organizations evolve and enhance their cybersecurity strategy in response to real-world threats and identify potential blind spots in the existing architecture, information and network security.

### What Is a Honeynet?

A honeynet is a network of honeypots that is designed to look like a real network, complete with multiple systems, databases, servers, routers and other digital assets. Since the honeynet, or honeypot system, mimics the sprawling nature of a typical network, it tends to engage cybercriminals for a longer period of time.

Given the size of the honeynet, it is also possible to manipulate the environment, luring adversaries deeper into the system in order to gather more intelligence about their capabilities or their identities.

**Email Gateway.**

An email gateway is a type of email server that protects an organizations or users internal email servers. This server acts as a gateway through which every incoming and outgoing email passes through. A Secure Email Gateway (SEG) is a device or software used for [email monitoring](https://www.proofpoint.com/us/products/archiving-and-compliance/supervision) that are being sent and received. Email gateway protection is designed to prevent unwanted email and deliver good email. Messages that are unwanted include [spam](https://www.proofpoint.com/us/threat-reference/spam), [phishing attacks](https://www.proofpoint.com/us/threat-reference/phishing), [malware](https://www.proofpoint.com/us/threat-reference/malware) or fraudulent content. Outgoing messages can be analyzed to prevent sensitive data from leaving the organization or to automatically [encrypt emails](https://www.proofpoint.com/us/products/information-protection/email-encryption) that contain sensitive information. SEG functionality can be deployed as a cloud service, or as an on-premises appliance, depending on requirements.

### **What is data maintenance?**

Data maintenance is the ongoing process of running regular checks to identify and correct data that does not follow company standards in your CRM database. The goal is to improve the quality and organization of your data to improve your business’s growth and profitability.

## **What Is a Data Backup?**

Data backup is the practice of copying data from a primary to a secondary location, to protect it in case of a disaster, accident or malicious action. Data is the lifeblood of modern organizations, and losing data can cause massive damage and disrupt business operations. This is why backing up your data is critical for all businesses, large and small.

# How Do You Delete Your Data Permanently?

# To permanently delete files on Windows, send them to the Recycle Bin and then empty the Recycle Bin to delete them for good. Once the bin is empty, you can’t recover the files unless you have data or file recovery software. And even that may not work, because recovery software is no guarantee.

# Data Policy

A data policy contains a set of rules, principles, and guidelines that provide a framework for different areas of data management throughout the enterprise, including but not limited to data governance, data quality, and data architecture.

# Terms of service

Terms of service (also known as terms of use and terms and conditions, commonly abbreviated as TOS or ToS, ToU or T&C) are **the legal agreements between a service provider and a person who wants to use that service**. The person must agree to abide by the terms of service in order to use the offered service

**Privacy settings**

## Featured snippet from the web

Privacy settings are "**the part of a social networking website, internet browser, piece of software, etc.** **that allows you to control who sees information about you**". With the growing prevalence of social networking services, opportunities for privacy exposures also grows.

# Two-factor authentication (2FA)

## What Is Two Factor Authentication And How Does It Work

Everyone these days uses the internet at least once every day. People tend to have on the internet a lot of their personal information which is why it is important to make sure they are safe from hackers or third parties. Passwords are the most famous and the old fashioned way to access our accounts and keep it, along with our data and personal information safe. However, a new system emerged, known as two factor authentication, also known as 2FA. It delivers extra protection and safety to your accounts here we will discuss its importance and how two factor authentication works.

## **What is two factor authentication?**

Two step authentication is a system that works to provide two ways to verify that it is you who is accessing your account. In fact, it adds an extra layer of security to your accounts on the internet.

Two factor authentication or 2FA consists of you providing some sort of proof or private information. Any information that only you would know and you will have access to your account only after you enter this specific information.

## **Why is two factor authentication important?**

The rates of cybercrime are rising each and every day and everyone has most of his life on his laptop or cellphone such as his bank account details, his contacts, his messages and other important and private matters. Old ways are not the most secure when it comes to protecting  your data and the old ways of protection are not effective in the face of more modern and advanced threats. Making sure that all of your data is safe should be your top priority.

2FA works really well when it comes to protection and is a good way to keep everything secure. Their whole point is to increase your privacy and provide you with the security a simple password can’t.

After knowing what two factor authentication does and its importance, you might ask yourself how does two factor authentication work, and here is the answer to your question.

## **How does two factor authentication work?**

There are different types of 2FA and each one of them works in a certain way to make sure that you are the only one who can have access to your accounts and your data. Here is an overview on what are the most popular types of 2FA and how they work to provide you with extra security:

**1- Text messages on your phone number**

This one is probably the most popular method and here is how it works. You will have to register your mobile’s phone number while signing up into your account. Whenever you sign in to your account, you will receive a text message containing a code that you will have to enter to be able to access your account. It is also possible to receive a voice message or even a phone call depending on the option you choose.

**2- Applications**

Applications are the second way. You will have to link the application to your account. The application will generate a different code each time you log in to your account that you will have to enter to access it. A new code will be generated every 30 seconds or so. It is crucial to be fast when logging in and most importantly, to keep the app and the codes private.

**3- The biometric method**

For this method to work, you will have to provide physical proof of your identity. An example of that can be a fingerprint scan or iris recognition. You will have to introduce this information when you create your account and scan your fingerprint or iris everytime you want to access it. Face recognition is also a popular option.

**4- Notifications**

Notifications are another popular method of 2FA. Whenever a new device tries to log into your account, you will receive a notification informing you about it. Here, you will have the option to either approve or decline the request. If it is you, you should click on approve and if it is not you and someone you do not know is trying to access your account you should click on deny.

## **How safe is two factor authentication**

There is no doubt that 2FA definitely adds more security, privacy or safety to your accounts. And of course, doing everything we can to keep our accounts and personal information secure is very important to keep you safe from frauds and hackers.

Of course, 2FA is prone to different attacks and cyber threats. However, it is still better than the old ways of protection on the internet and is always recommended to anyone who uses the internet.

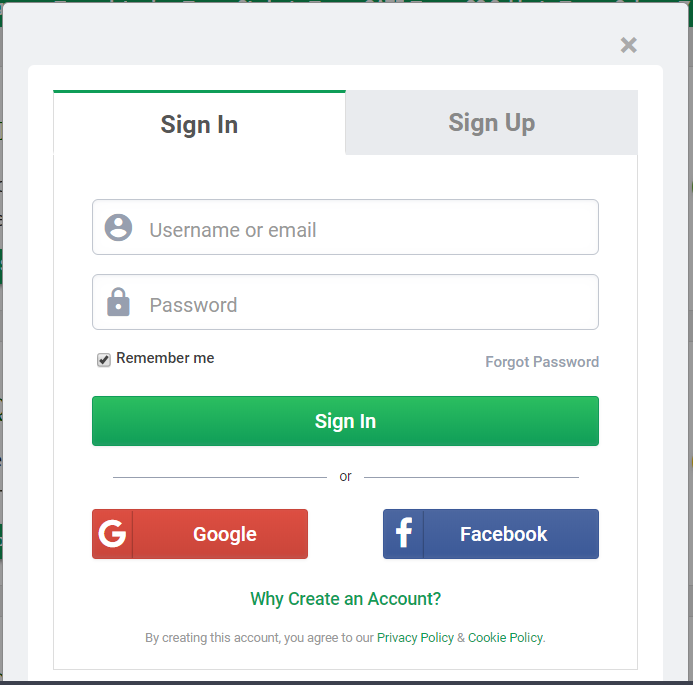
To be more safe, it is advised to not link your 2FA to your personal phone number or email address since they are easy to track and hack. It is also possible to add more than 2FA methods for better protection. But whatever you choose to do, remember that safety comes before anything on the internet and it is crucial to protect yourself and your data as much as possible.



# What is OAuth (Open Authorization) ?

**OAuth (Open Authorization)** is an open standard protocol for authorization of an application for using user information, in general, it allows a third party application access to user related info like name, DOB, email or other required data from an application like Facebook, Google etc. without giving the third party app the user password. It is pronounced as **oh-auth**.

You might have seen a “login with Google” or “login with Facebook” button on the login/signup page of a website that makes easier to get using the service or website by simply logging into one of the services and grant the client application permission to access your data without giving Password. This is done with the OAuth.

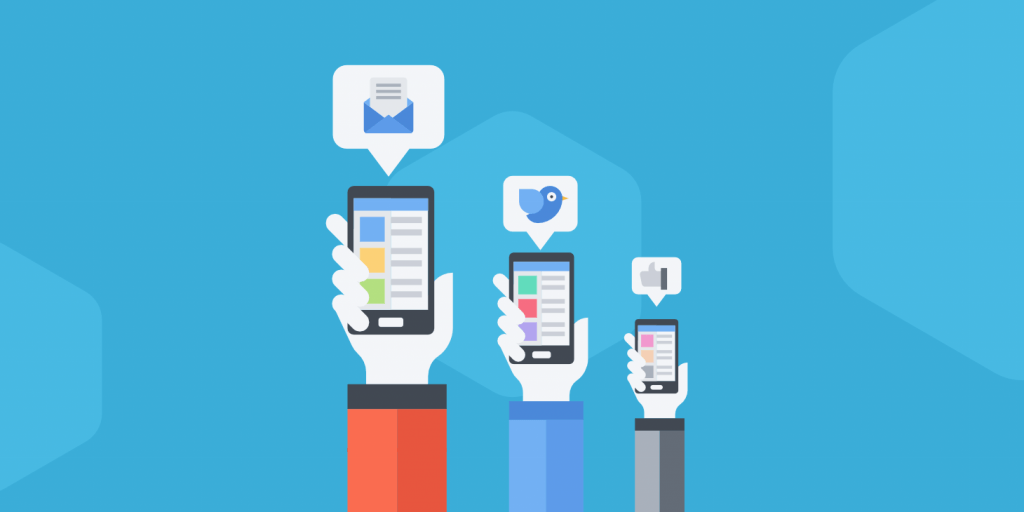


It is designed to work with [HTTP(Hyper Text Transfer Protocol)](https://www.geeksforgeeks.org/what-are-the-differences-between-http-ftp-and-smtp/) and it allows access tokens to be issued to the third party application by an authorization server with the approval from the owner.

# Social sharing : Its Definition, Benefits & Examples

## **What does social sharing mean?**

Simply put, the word “social sharing” is made up of “social” and “sharing”. Commonly, you could understand the word by explaining it. Social means social networks, sharing refers to the spread of information on those social networks. **Briefly, the social sharing definition is known as social media users broadcasting web content on multiple social platforms to their connections, groups, or specific individuals.**

Social sharing means the spread of information in social networks

The purpose of conducting social sharing by e-commerce websites is so wide. However, the primary aim of it is to generate brand awareness, get more people involved in the promotion, campaigns or whichever related to the purpose of the sales of your business.

## **Benefits of social sharing**

According to Social Media Examiner, about 96% of e-commerce businesses are now joined in social media marketing. The key advantage that they want from this tactic is to get more people to know about their company. Speaking of that to let you know that social sharing is crucial for any businesses in their social media marketing. Below are 5 key benefits that social sharing brings to your organization:

### **Reach more organic interaction**

Social sharing plays an important role in the digital era. It helps to generate organic interaction among users on social media networks. Through social sharing buttons available on the posts, customers share products’ information, blog posts, inspirational images, etc. relating to your business. As a result, it resonates more than a message displayed directly by a business.

Social sharing icons commonly appear on your posts

Besides, when social sharing happens, your business campaign is considered to be effectively run. Once a post is shared, your customers’ friends, families or coworkers will connect to your store quickly. It brings to your business a huge benefit. When your social posts (any form) is repetitively shared, they become viral. And that is what a business wants.

According to Social Media Examiner, about 96% of e-commerce businesses are now joined in social media marketing. The key advantage that they want from this tactic is to get more people to know about their company. Speaking of that to let you know that social sharing is crucial for any businesses in their social media marketing. Below are 4 key benefits that social sharing brings to your organization:

### **Higher Conversion Rates**

With the increase in visibility, your business gains more chances for conversion. For instance, people easily buy a product because they are impressed with it. For your social content, when it is viral or widely shared, more people get to know your products, and also more chances of conversion rates will come. To conclude, the more your business approach to customers, the more chances of conversion your business may get.

According to a study, social media has a 100% higher lead-to-close rate than outbound marketing. Therefore, optimizing your brand on social platforms is really effective, getting more sales.

### **Increase Brand Awareness**

Innumerous people actively participate in social media today leading to a huge opportunity for business to get their targeted audience. Implementing social media to get it shared widely on these social platforms helps your business approach thousands of customers a month. Therefore, effectively conducting social sharing allows your business to increase brand awareness.

For example, commonly, you create a post on your social page aiming at your targeted audiences. But if your content is triggered and interesting, they share it. A lot of people connected to that customer (including friends, family, coworkers, etc.) on social media will know about that post. This leads to more people knowing about your brand and your messages. Automatically, brand awareness would be increased in a cost-efficient way.

### **Better Customer Satisfaction**

Customers love to “cooperate” with a brand that is positive and popular. Therefore, creating a significant voice for your business is important to show them that you are a good option among other competitors. With social sharing, you are about to become what a customer requires in an organization.

Shares, likes and comments on your posts make them feel that you are a competent brand that is closely connected to customers. Moreover, social sharing also makes your brands stand out, providing customers with the best experience ever.

Also, when a post is shared, it touches your customers. This shows that your brand has compassion for them. By that, it makes them feel a sense of satisfaction.

### **Brand Authority**

What is brand authority? It is described as your brand is a good one, and has authority in the market compared to other brands. What else? When your social media platforms get popular because of social sharing, it appears to be more credible. Literally, your brand becomes powerful and is always considered to be the best choice in the customers’ mind.

Moreover, the credibility that your business has thanks to the authority it gets makes your customers satisfied. As a result, your conversion rates will be increased greatly.

**Email and Web Browser Privacy**

People are using web browsers for various purposes like shopping, social networking, E-mailing, reading, finding directions, banking etc. Web browser (Some of the most popular web browsers, like Internet Explorer, Mozilla Firefox and Google Chrome) are the most common points of entry for attackers. As web browsers are used so frequently, it is important to configure them securely to enhance web browser protection. Often, the web browser that comes with an operating system is not set up in a secure default configuration. If a user does not secure a system web browser, it can lead to some kind of computer problems like spyware being installed without any knowledge of user to criminals taking control of computer.

Technique of intrusion is not always same, which is why user needs to harden the **security of web browser and must consider few security practices during reading and opening attachment from email**. Weak web browser protection leads to many issues and system compromising is the main one.

#### **How attackers target users mail account/machine:**

There is no magic key but few common techniques which an attacker uses to break into target user email/computer machine. Given below are common tricks which attacker use now-a-days.

##### [**Phishing**](https://heimdalsecurity.com/blog/abcs-detecting-preventing-phishing/)**technique:**

Case 1 (Phishing Mail): Phishing mail is a technique in which attackers craft one email having a malicious document or zip file attached to it and sends the crafted email to targeted victim. As soon, user opens the attachment, a malicious program starts its execution and start working as per its algorithm i.e start performing a task for which it was designed for.

Case 2 (Fake domain): In this case, cyber criminal creates fake website which looks likes a original website and send it to targeted victim through email ,in which the victims are told the enter their confidential details like username ,passwords and bank details.

**Outdated web browser:**

Flash player and java scripts are two common components used for web development. If the flash player or other plugins are not updated with recent security patches, the major risks come in the form of risks of cyber attacks and Trojan horse viruses—particular in conjunction with visiting sites that are infested with malware. They can wreak havoc on user computers, destroy productivity, and compromise the integrity of private information about user customers.

##### **Drive-by-download:**

This is a technique that makes user to redirect vulnerable web browser and force them to download malware binary into the system without of knowledge of user.It is widely used way of breaking web browser protection.

**Ways to protect Email and web browser:**

##### **Implement the sender policy framework:**

Implement the sender policy framework (SPF) by developing SPF records in DNS and enabling receiver-side verification in mail servers.It will reduced the chance of spoofed email messages.

Scan and block all email attachments entering the organization’s email gateway if they contain malicious code or file types that are unnecessary for the organization’s business.This scanning should be done before the email is placed in user’s inbox.

##### **Stay away from phishing attacks:**

* Don’t open any attachment you are not expecting ,even it comes from a trusted source,such as a family member,co-worker, or friend.
* If you do not know the sender of a message that includes an attachment, delete the message without reading it.
* Do not open any attached file ending in .exe,.vbs or .lnk.
* Do not send any personal information and bank details through email, even if you are close with the receiver.You never know who may gain access to your email account, or to the person’s account to whom you are emailing.

##### **Keep the browser up-to-date with the latest patches:**

Use a current web browser and keep automatic updates enabled.Don’t use an outdated web browser like Apple’s safari and older versions of Microsoft’ts Internet Explorer. Use Google Chrome or Mozilla Firefox,leave automatic updates enabled and always keep updated version of web browser (whichever in use ). Web browser protection is most important for user’s online security.

##### **Uninstall Plug-ins You Don’t Need:**

Uninstall any plug-ins you don’t need to secure user web browser. Check your web browser’s list of installed plug-ins and uninstall the plug-ins you don’t need. Java is particularly dangerous and used by few websites — uninstall that unless you really need it. The one plug-in you’re most likely to need is Flash, and   even it is becoming less necessary.

##### **Use a good antivirus program against viruses:**

It is important to have a good security software on user system, one which should include a real-time scanning engine. That means that files you download from online locations are analyzed as soon as they are on your computer. Find the best solution by checking the test results run by important names in the security industry, such as McAfee Antivirus, Kaspersky Anti-Virus Plus, Avira Antivirus Pro  select the best antivirus solution for your system.

##### **Block the scripting languages:**

Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities.

##### **Use secure websites for sensitive operations:**

User should be very careful when running financial transactions on any web location.To visit a secure website, make sure the web address starts with “https://”. Https indicates user are connected to a website where data, which is sent and received in the encrypted manner.

##### **Monitor your bank account with Online Banking Alerts:**

You can set up alerts for any change in your banking account, such as when you receive money or when money are taken from your account. Normally, you will be informed when your salary is received or when an automatic payment has been done.But it is useful also in case someone tries to remove unauthorized money from the account.

Online user must consider web browser protection and should never think it won’t be a threat for the system if user don’t take care of web browser protection policies. User email is the thing which may have sensitive information or even a compromised email account can lead to compromising of other online account which are registered using that mail account. **Web browser protection and email account security is a serious issue and it should be consider before attacker take advantage of the weakness in any of these things.**

**PLEASE REFER PREVIOUS SEM NOTES FOR**

**1.OSI MODEL**

**2.TCP/IP MODEL**

**3.INTERNET PROTOCOLS**

**4.NETWORK RESOURCES**

**5.ROUTER AND FIREWALL,HUB,SWITCH-SECURITY ISSUES**

**6.BASIC NETWORK TERMINOLOGIES**