What is Cyberspace Definition?

The best way to define cyberspace is the virtual and dynamic space created by the machine clones. According to the cyberspace definition, it is a web consisting of consumer computers, electronics and communication networks by which the consumer is connected to the world.

Cyberspace History

The word cyberspace first made its appearance in Wiliam Gibson's science fiction book Necromancer. The book described an online world filled with computers and associated societal elements. In that book, the author described cyberspace as a 3D virtual landscape created by a network of computers. Although it looked like a physical space, it is generated by a computer, representing abstract data.

After the publication of the book, the word cyberspace became a mainstay in many English dictionaries. The New Oxford Dictionary of English provides cyberspace definition as the notional environment used by the people to communicate over networks of the computer.

As per the cyberspace meaning, cyberspace is a virtual space with no mass, gravity or boundaries. It is the interconnected space between networks of computer systems.

Bits and Bytes- Zeroes and ones are used to define cyberspace. It is a dynamic environment where these values change continuously. It can also be defined as the imaginary location where two parties can converse.

Introduction to cyber crime

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most, but not all, **cybercrime** is committed by cybercriminals or hackers who want to make money. **Cybercrime** is carried out by individuals or organizations.

Types of cybercrime

- Email and internet fraud.
- Identity fraud (where personal information is stolen and used).
- Theft of financial or card payment data.
- Theft and sale of corporate data.
- Cyber extortion (demanding money to prevent a threatened attack).
- **Ransomware attacks (a type of cyberextortion).**

  Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

- Cryptojacking (where hackers mine cryptocurrency using resources they do not own). Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency. Hackers do this by either getting the victim to click on a malicious link in an email that loads cryptomining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser.
- Cyberespionage (where hackers access government or company data). Cyberespionage involves the use of information and communication technology (ICT) by individuals, groups, or businesses for some economic benefit or personal gain

Most cybercrime falls under two main categories:

- Criminal activity that targets
- Criminal activity that uses computers to commit other crimes.

Cybercrime that targets computers often involves viruses and other types of malware.

Cybercriminals may infect computers with viruses and malware to damage devices or stop them working. They may also use malware to delete or steal data.

Malware and its type

Malware and its types

Malware stands for “Malicious Software” and it is designed to gain access or installed into the computer without the consent of the user. They perform unwanted tasks in the host computer for the benefit of a third party. There is a full range of malwares which can seriously degrade the performance of the host machine. There is a full range of malwares which are simply written to distract/annoy the user, to the complex ones which captures the sensitive data from the host machine and send it to remote servers. There are various types of malwares present in the Internet. Some of the popular ones are:

Adware

It is a special type of malware which is used for forced advertising. They either redirect the page to some advertising page or pop-up an additional page which promotes some product or event. These adware are financially supported by the organizations whose products are advertised.

Spyware

It is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine. Mostly it gathers the browsing habits of the user and the send it to the remote server without the knowledge of the owner of the computer. Most of the time they are downloaded in to the host computer while downloading freeware i.e. free application programs from the internet. Spywares may be of various types; It can keeps track of the cookies of the host computer, it can act as a keyloggers to sniff the banking passwords and sensitive information, etc.

Browser hijacking software

There is some malicious software which are downloaded along with the free software offered over the internet and installed in the host computer without the knowledge of the user. This software modifies the browsers setting and redirect links to other unintentional sites.

Virus

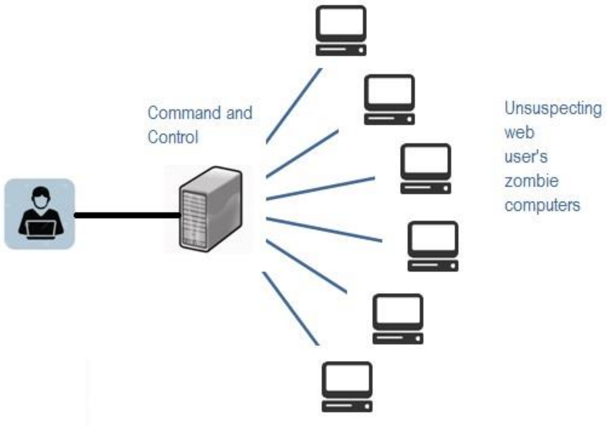
A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, occupy memory space of the computer by replicating the copy of the code, slow down the performance of the computer, format the host machine, etc. It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc. A virus may be present in a computer but it cannot activate itself without the human intervention. Until and unless the executable file(.exe) is execute, a virus cannot be activated in the host machine.

Worms

They are a class of virus which can replicate themselves. They are different from the virus by the fact that they does not require human intervention to travel over the network and spread from the infected machine to the whole network. Worms can spread either through network, using the loopholes of the Operating System or via email. The replication and spreading of the worm over the network consumes the network resources like space and bandwidth and force the network to choke.

Trojan Horse

Trojan horse is a malicious code that is installed in the host machine by pretending to be useful software. The user clicks on the link or download the file which pretends to be a useful file or software from legitimate source. It not only damages the host computer by manipulating the data but also it creates a backdoor in the host computer so that it could be controlled by a remote computer. It can become a part of botnet(robot-network), a network of computers which are infected by malicious code and controlled by central controller. The computers of this network which are infected by malicious code are known as zombies. Trojens neither infect the other computers in the network nor do they replicate.



A typical botnet

Scareware

Internet has changed how we talk, shop, play etc. It has even changed the way how the criminal target the people for ransom. While surfing the Internet, suddenly a pop-up alert appears in the screen which warns the presence of dangerous virus, spywares, etc. in the

KINDS OF CYBER CRIME

Various types of cyber crimes are:

Cyber Stalking

It is an act of stalking, harassing or threatening someone using Internet/computer as a medium. This is often done to defame a person and use email, social network, instant messenger, web-posting, etc. as a using Internet as a medium as it offers anonymity. The behavior includes false accusations, threats, sexual exploitation to minors, monitoring, etc.

Child Pornography

It is an act of possessing image or video of a minor (under 18), engaged in sexual conduct.

Forgery and Counterfeiting

It is a use of computer to forgery and counterfeiting is a document. With the advancement in the hardware and the software, it is possible to produce counterfeit which matches the original document to such an extent that it is not possible to judge the authenticity of the document without expert judgement.

Software Piracy and Crime related to IPRs

Software piracy is an illegal reproduction and distribution for personal use or business. It comes under crime related to IPR infringement. Some of the other crimes under IPR infringement are: download of songs, downloading movies, etc.

Cyber Terrorism

It is defined as the use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives.

Phishing

It is a process of acquiring personal and sensitive information of an individual via email by disguising as a trustworthy entity in an electronic communication. The purpose of phishing is identity theft and the personal information like username, password, and credit card number etc. may be used to steal money from user account. If a telephone is used as a medium for identity theft, it is known as Vishing (voice phishing). Another form of phishing is Smishing, in which sms is used to lure customers.

Computer Vandalism

It is an act of physical destroying computing resources using physical force or malicious code.

Computer Hacking

It is a practice of modifying computer hardware and software to accomplish a goal outside the creator's original purpose. The purpose of hacking a computer system may vary from simply demonstrations of the technical ability, to sealing, modifying or destroying information for social, economic or political reasons. Now the corporate are hiring hackers, a person who is engaged in hacking computers, to intentionally hack the computer of an organization to find and fix security vulnerabilities.

The hackers may be classified as:

- **White Hat:** white hat hackers are the persons who hack the system to find the security vulnerabilities of a system and notify to the organizations so that a preventive action can be taken to protect the system from outside hackers. White hat hackers may be paid employee of an organization who is employed to find the security loop-holes, or may be a freelancer who just wants to prove his mantle in this field. They are popular known as ethical hackers.
- **Black Hat:** in contrast to the white hat, the black hat hack the system with ill intentions. They may hack the system for social, political or economically motivated intentions. They find the security loopholes the system, and keep the information themselves and exploit the system for personal or organizational benefits till organization whose system is compromised is aware of this, and apply security patches. They are popularly known as crackers.
- **Grey Hat:** Grey hat hackers find out the security vulnerabilities and report to the site administrators and offer the fix of the security bug for a consultancy fee.
- **Blue hat:** A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed.

Creating and distributing viruses over internet

The spreading of a virus can cause business and financial loss to an organization. The loss includes the cost of repairing the system, cost associated with the loss of business during downtime and cost of loss of opportunity. The organization can sue the hacker, if found, for the sum of more than or equivalent to the loss borne by the organization.

Spamming

Sending of unsolicited and commercial bulk message over the internet is known as spamming. An email can be classified as spam, if it meets following criteria:

- Mass mailing:- the email is not targeted to one particular person but to a large number of peoples.
- Anonymity:- The real identify of the person not known
- Unsolicited:- the email is neither expected nor requested for the recipient.

These spams not only irritate the recipients and overload the network but also waste the time and occupy the valuable memory space of the mailbox.

Cross Site Scripting

It is an activity which involves injecting a malicious client side script into a trusted website. As soon as the browser executes the malicious script, the malicious script gets access to the cookies and other sensitive information and sent to remote servers. Now this information can be use to gain financial benefit or physical access to a system for personal interest.

Online Auction Fraud

There are many genuine websites who offers online auction over internet. Taking the advantage of the reputation of these websites, some of the cyber criminals lure the customers to online auction fraud schemes which often lead to either over payment of the product or the item is never delivered once the payment is made.

Cyber Squatting

It is an act of reserving the domain names of someone else's trademark with intent to sell it afterwards to the organization who is the owner of the trademark at a higher price.

Logic Bombs

These are malicious code inserted into legitimate software. The malicious action is triggered by some specific condition. If the conditions holds true in future, the malicious action begins and based on the action defined in the malicious code, they either destroy the information stored in the system or make system unusable.

Web Jacking

The hacker gain access to a website of an organization and either blocks it or modify it to serve political, economical or social interest. The recent examples of web jacking are some of the websites of the educational institutes were hacked by Pakistani hackers and an animation which contains Pakistani flags were flashed in the homepage of these websites. Another example is Indian hackers hacked website of Pakistani railways and flashed Indian flag in the homepage for several hours on the occasion of Independence Day of India in 2014.

Internet Time Thefts

Hacking the username and password of ISP of an individual and surfing the internet at his cost is Internet Time Theft.

Denial of Service Attack

It is a cyber attack in which the network is chocked and often collapsed by flooding it with useless traffic and thus preventing the legitimate network traffic.

Salami Attack

It is an attack which proceeds with small increments and final add up to lead to a major attack. The increments are so small that they remain unnoticed. An example of salami attack is gaining access to online banking of an individual and withdrawing amount in such a small amounts that it remains unnoticed by the owner. Often there is default trigger set in the banking website and transactions below say, Rs. 1000 withdrawal are not reported to the owner of the account. Withdrawing amount of Rs. 1000 over a period of time will lead to total withdrawal of a large sum.

Data Diddling

It is a practice of changing the data before its entry into the computer system. Often, the original data is retained after the execution on the data is done. For example, DA or the basic salary of the person is changed in the payroll data of an individual for pay calculation. Once the salary is calculated and transferred to his account, the total salary is replaced by his actual salary in the report.

Email Spoofing

It is a process of changing the header information of an e-mail so that its original source is not identified and it appears to an individual at the receiving end that the email has been originated from source other than the original source.

WHAT IS INFORMATION SECURITY?

Sometimes referred to as computer security, Information Technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

Information security is defined as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction". In essence, it means we want to protect our data and our systems from those who would seek to misuse it. In a general sense, security means protecting our assets. This may mean protecting them from attackers invading our networks, natural disasters, adverse environmental conditions, power failures, theft or vandalism, or other undesirable states. Ultimately, we will attempt to secure ourselves against the most likely forms of attack, to the best extent we reasonably can, given our environment.

When we look at what exactly it is that we secure, we may have a broad range of potential assets. We can consider physical items that we might want to secure, such as those of inherent value (e.g. , gold bullion) or those that have value to our business (e.g., computing hardware). We may also have items of a more ethereal nature, such as software, source code, or data. In today's computing environment, we are likely to find that our logical assets are at least as valuable as, if not more than, our physical assets. Additionally, we must also protect the people who are involved in our operations. People are our single most valuable asset, as we cannot generally conduct business without them. We duplicate our physical and logical assets and keep backup copies of them elsewhere against catastrophe occurring, but without the skilled people to operate and maintain our environments, we will swiftly fail. In our efforts to secure our assets, we must also consider the consequences of the security we choose to implement. There is a well-known quote that says, “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards-and even then I have my doubts". Although we could certainly say that a system in such a state could be considered reasonably secure, it is surely not usable or productive. As we increase the level of security, we usually decrease the level of productivity. With the system mentioned in quote above, the level of security would be very high, but the level of productivity would be near zero.

Various Definitions

The definitions of Information Security suggested in different sources are summarized below :

1. "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009)
2. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010)
3. "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008)
4. "Information Security is the process of protecting the intellectual property of an organisation." (Pipkin, 2000)
5. "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business." (McDermott and Geer, 2001)
6. "A well-informed sense of assurance that information risks and controls are in balance." (Anderson, J., 2003)
7. "Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties." (Venter and Eloff, 2003)
8. "Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organisational, human-oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include: confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability.

Information assurance

It is the act of ensuring that data is not lost when critical issues arise. These issues include, but are not limited to: natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

When Are We Secure?

Defining the exact point at which we can be considered secure presents a bit of a challenge.

- Are we secure if our systems are properly patched?
- Are we secure if we use strong passwords?
- Are we secure if we are disconnected from the Internet entirely?

Even from common-sense, all of these questions can be answered with a "no." Even if our systems are properly patched, there will always be new attacks to which we are vulnerable. When strong passwords are in use, there will be other avenues that an attacker can exploit. When we are disconnected from the Internet, our systems can be physically accessed or stolen. In short, it is very difficult to define when we are truly secure. We can, however, turn the question around.

Defining when we are insecure is a much easier task, and we can quickly list a number of items that would put us in this state:

- Not patching our systems
- Using weak passwords such as "password" or "1234"
- Downloading programs from the Internet
- Opening e-mail attachments from unknown senders
- Using wireless networks without encryption

We could go on for some time creating such a list. The good thing is that once we are able to point out the areas in an environment that can cause it to be insecure, we can take steps to mitigate these issues. This problem is akin to cutting something in half over and over; there will always be some small portion left to cut again. Although we may never get to a state that we can definitively call "100 percent secure”, we can take steps in the right direction.

The bodies of law that define standards for security, vary quite a bit from one industry to another and wildly from one country to another. Organizations that operate globally are very common at present, and we need to take care that we are not violating any such laws in the course of conducting business. We can see exactly such a case when we look at the differences in data privacy laws between the United States and the European Union. When in doubt, consult legal counsel before acting. Some bodies of law or regulations do make an attempt to define what secure is, or at least some of the steps we should take to be "secure enough." We have the Payment Card Industry Data Security Standard (PCI DSS) for companies that process credit card payments, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for organizations that handle health care and patient records, the Federal Information Security Management Act (FISMA) that defines security standards for many federal agencies in the United States, and a host of others. Whether these standards are effective or not is the source of much discussion, but following the security standards defined for the industry in which we are operating is generally considered to be advisable, if not mandated.

Confidentiality

In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes" (Excerpt ISO27000). Confidentiality is a concept similar to, but not the same as, privacy. Confidentiality is a necessary component of privacy and refers to our ability to protect our data from those who are not authorized to view it. Confidentiality is a concept that may be implemented at many levels of a process. As an example, if we consider the case of a person withdrawing money from an ATM, the person in question will likely seek to maintain the confidentiality of the personal identification number (PIN) that allows him, in combination with his ATM card, to draw funds from the ATM. Additionally, the owner of the ATM will hopefully maintain the confidentiality of the account number, balance, and any other information needed to communicate to the bank from which the funds are being drawn. The bank will maintain the confidentiality of the transaction with the ATM and the balance change in the account after the funds have been withdrawn. If at any point in the transaction confidentiality is compromised, the results could be bad for the individual the owner of the ATM, and the bank, potentially resulting in what is known in the information security field as a breach.

Confidentiality can be compromised by the loss of a laptop containing data, a person looking over our shoulder while we type a password, an e-mail attachment being sent to the wrong person, an attacker penetrating our systems, or similar issues.

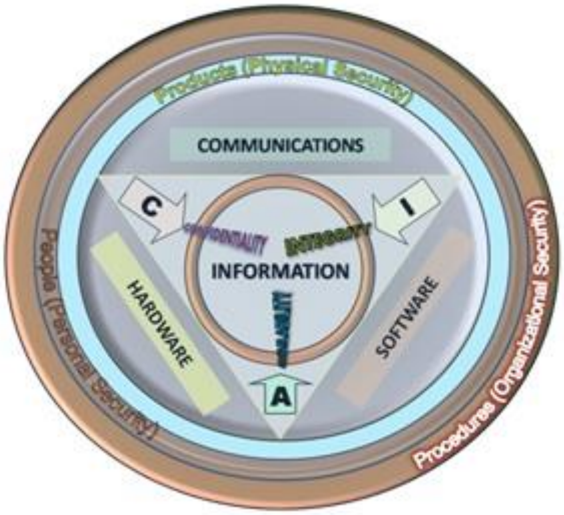

Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
HARDWARE
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

Figure 24: The CIA Triad*

Integrity

Integrity refers to the ability to prevent our data from being changed in an unauthorized or undesirable manner. This could mean the unauthorized change or deletion of our data or portions of our data, or it could mean an authorized, but undesirable, change or deletion of our data. To maintain integrity, we not only need to have the means to prevent unauthorized changes to our data but also need the ability to reverse authorized changes that need to be undone. We can see a good example of mechanisms that allow us to control integrity in the file systems of many modern operating systems such as Windows and Linux. For purposes of preventing unauthorized changes, such systems often implement permissions that restrict what actions an unauthorized user can perform on a given file. Additionally, some such systems, and many applications, such as databases, can allow us to undo or roll back changes that are undesirable. Integrity is particularly important when we are discussing the data that provides the foundation for other decisions. If an attacker were to alter the data that contained the results of medical tests, we might see the wrong treatment prescribed, potentially resulting in the death of the patient.

Availability

The final leg of the CIA triad is availability. Availability refers to the ability to access our data when we need it. Loss of availability can refer to a wide variety of breaks anywhere in the chain that allows us access to our data. Such issues can result from power loss, operating system or application problems, network attacks, compromise of a system, or other problems. When such issues are caused by an outside party, such as an attacker, they are commonly referred to as a denial of service (DoS) attack.

Relating the CIA triad to security

Given the elements of the CIA triad, we can begin to discuss security issues in a very specific fashion. As an example, we can look at a shipment of backup tapes on which we have the only existing, but unencrypted, copy of some of our sensitive data stored. If we were to lose the shipment in transit we will have a security issue. From a confidentiality standpoint, we are likely to have a problem since our files were not encrypted. From an integrity standpoint, presuming that we were able to recover the tapes, we again have an issue due to the lack of encryption used on our files. If we recover the tapes and the unencrypted files were altered, this would not be immediately apparent to us. As for availability, we have an issue unless the tapes are recovered since we do not have a backup copy of the files. Although we can describe the situation in this example with relative accuracy using the CIA triad, we might find that the model is more restrictive than what we need in order to describe the entire situation. An alternative model does exist that is somewhat more extensive.

THE PARKERIAN HEXAD

The Parkerian hexad, named for Donn Parker and introduced in his book Fighting Computer Crime, provides us with a somewhat more complex variation of the classic CIA triad. Where the CIA triad consists of confidentiality, integrity, and availability, the Parkerian hexad consists of these three principles, as well as possession or control, authenticity, and utility for a total of six principles, as shown in Figure 25 below. Although it is considered by some to be a more complete model, the Parkerian hexad is not as widely known as the CIA triad. If we decide to use this model in discussion of a security situation, we should be prepared to explain the difference to the uninitiated.

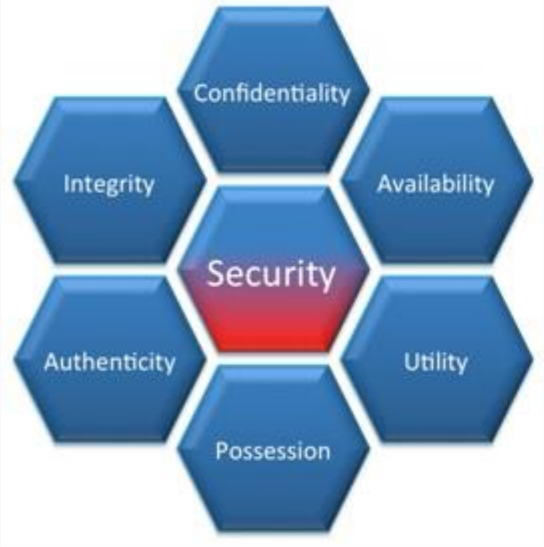


Figure 25: The Parkerian Hexad

Confidentiality, Integrity and Availability

As we mentioned, the Parkerian hexad encompasses the three principles of the CIA triad with the same definitions we just discussed. There is some variance in how Parker describes integrity, as he does not account for authorized, but incorrect, modification of data, and instead focuses on the state of the data itself in the sense of completeness.

Possession or Control

Possession or control refers to the physical disposition of the media on which the data is stored. This enables us, without involving other factors such as availability, to discuss our loss of the data in its physical medium. In our lost shipment of backup tapes, let us say that some of them were encrypted and some of them were not. The principle of possession would enable us to more accurately describe the scope of the incident; the encrypted tapes in the lot are a possession problem but not a confidentiality problem, and the unencrypted tapes are a problem on both counts.

Authenticity

Authenticity allows us to talk about the proper attribution as to the owner or creator of the data in question. For example, if we send an e-mail message that is altered so as to appear to have come from a different e-mail address than the one from which it was actually sent, we would be violating the authenticity of the e-mail. Authenticity can be enforced through the use of digital signatures. A very similar, but reversed, concept to this is non-repudiation. Non-repudiation prevents someone from taking an action, such as sending an e-mail, and then later denying that he or she has done so.

Utility

Utility refers to how useful the data is to us. Utility is also the only principle of the Parkerian hexad that is not necessarily binary in nature; we can have a variety of degrees of utility, depending on the data and its format. This is a somewhat abstract concept, but it does prove useful in discussing certain situations in the security world. For instance, in one of our earlier examples we had a shipment of backup tapes, some of which were encrypted and some of which were not. For an attacker, or other unauthorized person, the encrypted tapes would likely be of very little utility, as the data would not be readable. The unencrypted tapes would be of much greater utility, as the attacker or unauthorized person would be able to access the data.

Interception

Interception attacks allow unauthorized users to access our data, applications, or environments, and are primarily an attack against confidentiality. Interception might take the form of unauthorized file viewing or copying, eavesdropping on phone conversations, or reading e-mail, and can be conducted against data at rest or in motion. Properly executed, interception attacks can be very difficult to detect.

Interruption

Interruption attacks cause our assets to become unusable or unavailable for our use, on a temporary or permanent basis. Interruption attacks often affect availability but can be an attack on integrity as well. In the case of a DoS attack on a mail server, we would classify this as an availability attack. In the case of an attacker manipulating the processes on which a database runs in order to prevent access to the data it contains, we might consider this an integrity attack, due to the possible loss or corruption of data, or we might consider it a combination of the two. We might also consider such a database attack to be a modification attack rather than an interruption attack.

Modification

Modification attacks involve tampering with our asset. Such attacks might primarily be considered an integrity attack but could also represent an availability attack. If we access a file in an unauthorized manner and alter the data it contains, we have affected the integrity of the data contained in the file. However, if we consider the case where the file in question is a configuration file that manages how a particular service behaves, perhaps one that is acting as a Web server, we might affect the availability of that service by changing the contents of the file. If we continue with this concept and say the configuration we altered in the file for our

Web server is one that alters how the server deals with encrypted connections, we could even make this a confidentiality attack.

Fabrication

Fabrication attacks involve generating data, processes, communications, or other similar activities with a system. Fabrication attacks primarily affect integrity but could be considered an availability attack as well. If we generate spurious information in a database, this would be considered to be a fabrication attack. We could also generate e-mail, which is commonly used as a method for propagating malware, such as we might find being used to spread a worm. In the sense of an availability attack, if we generate enough additional processes, network traffic, e-mail, Web traffic, or nearly anything else that consumes resources, we can potentially render the service that handles such traffic unavailable to legitimate users of the system.

Information Security

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

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

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

policy/change management.

Denial of service attack is one of the factor that can hamper the availability of information. Apart from this there is one more principle that governs information security programs. This is Non repudiation.

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

Computer Ethics

The general definition of the word "ethics" defines the elements important to humans' morals. Ethics could be referred to as specific values, standards, rules, and agreements.
For example, not being involved in software piracy is a matter of ethics. Computer ethics is a set of morals that regulate the use of computers. It is important for computer users to be aware of the ethical use of copyrighted material, the ethical use of resources and information, and the ethical use of school, company, and employee information. There are a set of rules called the "Ten Commandments of Computer Ethics" - which are rules that speak for themselves.

These commandments are:

1. Thou shall not use a computer to harm other people.
2. Thou shall not interfere with other people's computer work.
3. Thou shall not snoop around in other people's computer files.
4. Thou shall not use a computer to steal.
5. Thou shall not use a computer to bear false witness.
6. Thou shall not copy or use proprietary software for which you have not paid (without permission).
7. Thou shall not use other people's computer resources without authorization or proper compensation.
8. Thou shall not appropriate other people's intellectual output.
9. Thou shall think about the social consequences of the program you are writing or the system you are designing.
10. Thou shall always use a computer in ways that ensure consideration and respect for your fellow humans

The 10 ethical computer commandments are simple rules to abide by when using a computer.

Common issues of computer ethics are the following:

privacy concerns
how computers affect society
intellectual property rights

EXAMPLE:
It is a very common and easy practice to burn a CD or movie for a friend. However, a better option would be to tell the friend to buy the CD or movie as an ethical alternative. The privacy of another person is also an ethical issue of today. People's information is easily accessible through the computer; the ethical solution would be to not access another person's private information unless given permission. Ethics certainly guide our behavior, and it is the source of the acts we will and will not partake in.

Ethics is a field of study that is concerned with distinguishing right from wrong, and good from bad. It analyzes the morality of human behaviors, policies, laws and social structures. Ethicists attempt to justify their moral judgments by reference to ethical principles of theories that attempt to capture our moral intuitions about what is right and wrong. The two theoretical approaches that are most common in ethics are consequentialism and deontology. Consequentialist approaches assume that actions are wrong to the extent that they have bad consequences, whereas deontological approaches assume that people have moral duties that exist independently of any good or bad consequences that their actions may have. Ethical principles often inform legislation, but it is recognized in ethics that legislation cannot function as a substitute for morality. It is for this reason that individuals and corporations are always required to consider not only the legality but also the morality of their actions. Ethical analysis of security and privacy issues in information technology primarily takes place in computer ethics which emerged in the 1980s as afield. Computer ethics analyzes moral responsibilities of computer professionals and computer users and ethical issues in public policy for information technology development and use. It asks such questions as:

- Is it wrong for corporations to read their employee’s e-mail?
- Is it morally permissible for computer users to copy copyrighted software?
- Should people be free to put controversial or pornographic content online without censorship?

Ethical issues and questions like these require moral or ethical analysis: analysis in which the moral dilemmas contained in these issues are clarified and solutions are proposed for them. Moral analysis aims to get clear on the facts and values in such cases, and to find a balance between the various values, rights and interests that are at stake and to propose or evaluate policies and courses of action.

COMPUTER SECURITY AND ETHICS

We will now turn to ethical issues in computer and information security. In this section, the moral importance of computer security will be assessed, as well as the relation between computer security and national security.

The Moral Importance of Computer Security

Computer security is a field of computer science concerned with the application of security features to computer systems to provide protection against the unauthorized disclosure, manipulation, or deletion of information, and against denial of service. The condition resulting from these efforts is also called computer security. The aim of computer security professionals is to attain protection of valuable information and system resources. A distinction can be made between the security of system resources and the security of information or data. The first may be called system security, and the second information security or data security. System security is the protection of the hardware and software of a computer system against malicious programs that sabotage system resources. Information security is the protection of data that resides on disk drives on computer systems or is transmitted between systems. Information security is customarily defined as concerned with the protection of three aspects of data: their confidentiality, integrity and availability.

How does computer security pose ethical issues?

As explained earlier, ethics is mostly concerned with rights, harms and interests. We may therefore answer this question by exploring the relation between computer security and rights, harms and interests.

- **What morally important benefits can computer security bring?**
- **What morally important harms or violations of moral rights can result from a lack of computer security?**
- **Can computer security also cause harms or violate rights instead of preventing and protecting them?**

Computer Security and National Security

Developments in computer security have been greatly influenced by the September 11, 2001 terrorist attacks in the United States and their aftermath. In response to these attacks, national security has become a major policy concern of Western nations. National security is the maintenance of the integrity and survival of the nation-state and its institutions by taking measures to defend it from threats, particularly threats from the outside. Many new laws, directives and programs protective of national security have come into place in Western nations after 9/11, including the creation in the U.S. of an entire Department of Homeland Security. The major emphasis in these initiatives is the protection of state interests against terrorist attacks. Information technology has acquired a dual role in this quest for national security. First of all, computer security has become a major priority, particularly the protection of critical information infrastructure from external threats. Government computers, but also other public and private infrastructure, including the Internet and telephone network, have been subjected to stepped-up security measures. Secondly, governments have attempted to gain more control over public and private information infrastructures. They have done this through wiretapping and data interception, by requiring Internet providers and telephone companies to store phone and e-mail communications records and make them available to law enforcement officials, by attempting to outlaw certain forms of encryption, or even through attempts to require companies to reengineer Internet so that eavesdropping by the government is made easier. Paradoxically, these efforts by governments to gain more control over information also lessen certain forms of security: they make computers less secure from access by government agencies.

ETHICAL ISSUES IN COMPUTER SECURITY

Hacking and Computer Crime

A large part of computer security is concerned with the protection of computer resources and data against unauthorized, intentional break-ins or disruptions. Such actions are often called hacking. Hacking, is the use of computer skills to gain unauthorized access to computer resources. Hackers are highly skilled computer users that use their talents to gain such access, and often form communities or networks with other hackers to share knowledge and data. Hacking is often also defined, more negatively, as the gaining of such unauthorized access for malicious purposes: to steal information and software or to corrupt data or disrupt system operations. Self-identified hackers, however, make a distinction between non-malicious break-ins, which they describe as hacking, and malicious and disruptive break-ins, which they call cracking. Self-identified hackers often justify their hacking activities by arguing that they cause no real harm and instead have a positive impact. The positive impact of hacking, they argue, is that it frees data to the benefit of all, and improves systems and software by exposing security holes. The reconsideration are part of what has been called the hacker ethic or hacker code of ethics, which is a set of (usually implicit) principles that guide the activity of many hackers. Such principles include convictions that information should be free, that access to computers should be unlimited and total, and that activities in cyberspace cannot do harm in the real world. Various professionals have argued that many principles of the hacker ethic cannot be sustained. The belief that information should be free runs counter to the very notion of intellectual property, and would imply that creators of information would have no right to keep it to themselves and have no opportunity to make a profit from it. It would moreover fundamentally undermine privacy, and would undermine the integrity and accuracy of information, as information could be modified and changed at will by anyone who would access it. A school of thought, that the helpfulness of hacking in pointing to security weaknesses may not outweigh the harm it does, and that activities in cyberspace can do harm in the real world.

Both hacking and cracking tend to be unlawful, and may therefore be classified as a form of computer crime, or cybercrime, as it has also been called. There are many varieties of computer crime, and not all of them compromise computer security. There are two major types of cybercrime that compromise computer security:

Moral Responsibilities of Information Security Professionals

Information security (IS) professionals are individuals whose job it is to maintain system and information security. By standing of their profession, they have a professional responsibility to assure the correctness, reliability, availability, safety and security of all aspects of information and information systems. The discussion in the above sections makes clear that this responsibility has a moral dimension: professional activities in computer security may protect people from morally important harms but could also cause such harms, and may either protect or violate people's moral rights. In case of safety-critical systems, the decisions of information security professionals may even be a matter of life or death. That IS professionals have moral responsibilities as part of their profession is reflected in codes of ethics used by various organizations for computer and information security. These codes of ethics rarely go into detail, however, on the moral responsibilities of IS professionals in specific situations. For instance, the code of ethics of the Information Systems Security Association (ISSA), an international organization of information security professionals and practitioners, only states that members should "perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles" but does not go on to specify what these

Information Technology and Privacy

Privacy is a value in modern societies that corresponds with the ideal of the autonomous individual who is free to act and decide his own destiny. Yet, modern societies are also characterized by surveillance, a practice that tends to undermine privacy. Surveillance is the systematic observation of (groups of) people for specific purposes, usually with the aim of exerting some form of influence over them. Sociologist David Lyon has argued that surveillance has always been an important part of modern societies. The state engages in surveillance to protect national security and to fight crime, and the modern corporation engages in surveillance in the workplace to retain control over the workforce. Computerization from the 1960s onward has intensified surveillance by increasing its scale, ease and speed. Surveillance is partially delegated to computers that help in collecting, processing and exchanging data. Computers have not only changed the scale and speed of surveillance, they have also made a new kind of surveillance possible: dataveillance, which is the large-scale, computerized collection and processing of personal data in order to monitor people's actions and communications. More and more, information technology is not just used to record and process static information about individuals, but to record and process their actions and communications. New detection technologies like smart closed-circuit television (CCTV), biometrics and Intelligent User Interfaces, and new data processing techniques like data mining further exacerbate this trend. As Lyon has argued, the ease with which surveillance now takes place has made it a generalized activity that is routinely performed in all kinds of settings by different kinds of organizations. Corporations, for instance, have extended surveillance from the workplace to their customers (consumer surveillance). In addition, the 9/11 terrorist attacks have drastically expanded surveillance activities by the state. Many privacy disputes in today's society result from tensions between people's right to privacy and state and corporate interests in surveillance. In the information society, privacy protection is realized through all kinds of information privacy laws, policies and directives, or data protection policies, as they are often called in Europe. These policies regulate the harvesting, processing, usage, storage and exchange of personal data. They are often overtaken, however, by new developments in technology. However, privacy protection has also become a concern in the design and development of information technology. Information privacy has also become a major topic of academic study. Studies of information privacy attempt to balance privacy rights against other rights and interests, and try to determine privacy rights in specific contexts and for specific practices. Specialized topics include workplace privacy, medical privacy, genetic privacy, Internet privacy, and privacy in public.

PRIVACY ISSUES IN MODERN DATA MANAGEMENT

Internet Privacy

The Internet raises two kinds of privacy issues. First, the posting and aggregation of personal information on Internet websites sometimes violates privacy. Websites on the Internet contain all sorts of personal information that is made publicly available, often without the bearer's explicit consent. They may contain, for instance, one's phone number and address, archived bulletin board messages from years past, information about one's membership of organizations, online magazines and newspapers in which one is mentioned, online databases with public records, pictures and video clips featuring oneself, etc. Using search engines, this information can easily be located and be used to create elaborate composite records about persons. Should there be limits to this? When should someone's consent be asked when his personal information is posted on the web, or when such information is used for specific purposes?

Record Merging and Matching and Data Mining

It frequently happens that different databases with personal information are combined to produce new data structures. Such combinations may be made in two ways. First, the records in two databases may be merged to produce new composite records. For instance, a credit card company may request information about its prospective customers from various databases (e.g., financial, medical, insurance), which are then combined into one large record. This combined record is clearly much more privacy-sensitive than the records that compose it, as the combined record may generate perceptions and suggest actions that would not have resulted from any of the individual records that make it up. Second, records in databases may be matched. Computer matching is the cross-checking in two or more unrelated databases for information that fits a certain profile in order to produce matching records or "hits". Computer matching is used often by government agencies to detect possible instances of fraud or other crimes. For instance, ownership records of homes or motorized vehicles may be matched with records of welfare recipients to detect possible instances of welfare fraud. Computer matching has raised privacy concerns because it is normally done without the consent of the bearers of personal information that are involved. Moreover, matches rarely prove facts about persons but rather generate suspicions that require further investigation. In this way, record matching could promote stereotyping and lead to intrusive investigations. Data Mining is a technique that is usually defined over a single database. It is the process of automatically searching large volumes of data for patterns, using techniques like statistical analysis, machine learning and pattern recognition. When data mining takes place in databases containing personal information, the new information thus gained may be privacy sensitive or confidential even when the old information is not. It may for instance uncover patterns of behavior of persons that were not previously visible. Data mining may also be used to stereotype whole categories of individuals. For instance, a credit card company may use data mining on its customer database to discover that certain zip codes correlate strongly with loan defaults. It may then decide not to extend credit anymore to customers with these zip codes. In summary, data mining may violate individual privacy and may be used to stereotype whole categories of individuals. Ethical policies are needed to prevent this from happening.

Privacy in Public

It is sometimes believed that privacy is a right that people have when they are in private places like homes, private clubs and restrooms, but that is minimized or forfeited as soon as they enter public space. When you walk in public streets or are on the road with your car, it is sometimes believed, you may retain the right not to be seized and searched without probable cause, but your appearance and behavior may be freely observed, surveilled and registered. Many privacy scholars, however, have argued that this position is not wholly tenable, and that people have privacy rights in public areas that are incompatible with certain registration and surveillance practices. The problem of privacy in public applies to the tracking, recording, and surveillance of public appearances, movements and behaviors by individuals and their vehicles. Techniques that are used for this including video surveillance (CCTV), including smart CCTV for facial recognition, infrared cameras, satellite surveillance, GPS tracking, RFID tagging, electronic checkpoints, mobile phone tracking, audio bugging, and ambient intelligence techniques. Does the use of these techniques violate privacy even when they are used in public places? The problem of privacy in public also applies to publicly available information on the Internet. Does the fact that personal information is available on a public forum make it all right to harvest this information, aggregate it and use it for specific purposes?

Biometric Identification

Biometrics is the identification or verification of someone's identity on the basis of physiological or behavioral characteristics. Biometric technologies provide a reliable method of access control and personal identification for governments and organizations. However, biometrics has also raised privacy concerns. Widespread use of biometrics would have the undesirable effect of eliminating anonymity and pseudonymity in most daily transactions, because people would leave unique traces everywhere they go. Moreover, the biometric monitoring of movements and actions gives the monitoring organization insight into a person’s behaviors which may be used against that person’s interests. In addition, many people find biometrics distasteful, because it involves the recording of unique and intimate aspects of (rather than about) a person, and because biometric identification procedures are sometimes invasive of bodily privacy. The challenge for biometrics is therefore to develop techniques and policies that are optimally protective of personal privacy.

TACTICS TO ENSURE COMPUTER SECURITY AND MAINTAIN PRIVACY

These tactics guides cover the basics of digital security and recommend tools you can use

- Protect your device from malware and hackers :Prevent worms, viruses and trojans
- Protect your information from physical threats : Ensure your workplace and devices are secure
- Create and maintain secure passwords : Learn to manage strong passwords
- Protect the sensitive files on your computer : Learn to encrypt data and files

- Recover from information loss : Back up your devices and data
- Destroy sensitive information : Delete data permanently
- Keep your online communication private : Encrypted chat and email
- Remain anonymous and bypass censorship on the Internet : Using Tor and VPNs
- Protect yourself and your data when using social networking sites : Using Facebook, Twitter and Flickr safely
- Use mobile phones as securely as possible : Staying safe when using cellphones
- Use smartphones as securely as possible : Android and iPhone safety

Web browsers security

Web browsers can be breached in one or more of the following ways:

- Operating system is breached and malware is reading/modifying the browser memory space in privilege mode
- Operating system has a malware running as a background process, which is reading/modifying the browser memory space in privileged mode
- Main browser executable can be hacked
- Browser components may be hacked
- Browser plug-in can be hacked
- Browser network communications could be intercepted outside the machine

Whenever a browser communicates with a website, the website, as part of that communication, collects some information about the browser (in order to process the formatting of the page to be delivered, if nothing else).

Once an attacker is able to run processes on the visitor's machine, then exploiting known security vulnerabilities can allow the attacker to gain privileged access (if the browser isn't already running with privileged access) to the "infected" system in order to perform an even greater variety of malicious processes and activities on the machine or even the victim's whole network.

Browsers can use more secure methods of network communication to help prevent some of these attacks:

HTTP: HTTP Secure with digitally signed public key certificates or Extended Validation Certificates.

Perimeter defenses, typically through firewalls and the use of filtering proxy servers that block malicious websites and perform antivirus scans of any file downloads, are commonly implemented as a best practice in large organizations to block malicious network traffic before it reaches a browser.

Plugins and extensions

Although not part of the browser , browser plugins and extensions extend the attack surface.

STEPS TO SECURE WEB BROWSING

- **ENABLE AUTOMATIC UPDATES: (**Research shows that 88% of publicly disclosed vulnerabilities are exploited within a day of release. Administrator driven manual patching often incurs significant lag time before patches are deployed.)
- **ENABLE REPUTATION SERVICES (**Reputation-based blocking services (such as Microsoft SmartScreen®3F5 or Google®6 Safe Browsing) block browsers from accessing sites known to deliver malware.)
- **DISABLE UNSAFE PLUGINS AND EXTENSIONS (**Web browser plugins and extensions enrich web browsers by embedding extra features)

- **ADVANCED MITIGATIONS (**Well-resourced adversaries have the advantage of time and skill, enabling them to target weaknesses in even properly configured systems.)
- **ENABLE BROWSER ISOLATION (**Browser isolation is a strategy that creates a logical barrier between the web browser and the operating system)
- **DISABLE UNNECESSARY FEATURES (**Some web browser features are not intended for wide spread use in a production environment, resulting in an unnecessarily large attack surface)
- **ENABLE OPERATING SYSTEM LEVEL MITIGATIONS(**Protecting the browser should extend beyond the browsing environment itself**)**

ROLE OF ANTI VIRUS

Antivirus software is designed to prevent computer infections by detecting malicious software, commonly called malware, on your computer and, when appropriate, removing the malware and disinfecting the computer.
The purpose of antivirus (AV) software is to detect, neutralize or eradicate malware (malicious software).
AV software not only will identify and destroy the computer virus, but it's also designed to fight off other kinds of threats such as phishing attacks etc.

How does AV software work?

- It will first scan (either on automatic timer that the user selects or manual) the computer's files to seek out any viruses that fit the description that's in a virus dictionary.
- Using a method called heuristic analysis, it will also try to detect suspicious activity from any program that might seem to be infected.

Antivirus programs come in different flavors, but the common denominator is that they seek out viruses and other malware, and neutralize them.

The computer's hard drive and external drives are also included in the scanning process.

Report of Cybercrimes are more prevalent than ever, says the McAfee Threat Report

Fairly recently (first quarter of 2013) was a time that was the most active, ever, for the entire gamut of malicious software generation.

- More than 14 million new samples were identified by McAfee.
- attachment in an e-mail, not knowing it's poised to infect his computer.
- Every month : about six million new infections.
- Between the first and second halves of 2013, new websites doubled in number.
- Sixty percent of the leading Google search terms returned malicious sites

SECURING COMPUTER USING FREE ANTIVIRUS

As computers become more and more integrated in to our lives, we end up leaving many sensitive data on our computer-from passwords, official email id, bank account to personal notes, business plans and other confidential information. So, good security software is a must for everyone.

Here is a list of 11 free anti-virus software and its common features which you can select (home users) for your online security.

Avast Antivirus– Avast is one of the best free anti-virus software available that provides a complete protection against security threats. This full-featured antivirus package has the following feature: Built in Anti-spyware, Anti-Rootkit, Web shield, Strong self protection, P2P and IM shield, Anti-Virus kernel, resident protection, Network shield, Automatic update, System integration, Windows 64 bit support, Integrated Virus Cleaner. It can be downloaded from https://www.avast.com/index

1. **AVG Antivirus–** AVG anti-virus free edition provides basic antivirus and anti-spyware protection for Windows. Following features included in the free edition: Anti-virus , anti-spyware and Safe surf feature. It can be downloaded from http://free.avg.com/
2. **Avira AntiVir Personal-** Avira is a comprehensive, easy to use antivirus program, designed to reliable free of charge virus protection to home-users. Features included are: Protection from virus worms and Trojans, Anti-rootkit, Anti-fishing, Anti dialers. It can be downloaded from http://www.free-av.com/
3. **BitDefender-** Free Edition uses the same ICSA Labs certified scanning engines found in Pro version of BitDefender , allowing you to enjoy basic virus protection for no cost at all. Features includes: On demand Virus Scanner and Remover and Scheduled scanning. It can be downloaded from http://www.bitdefender.com/PRODUCT-14-en--BitDefender-Free-Edition.html
4. **Blink Personal–** An all-in one security suite with antivirus limited for one year. Blink personal Security suite features – Antivirus and Anti spyware, Anti root kit, Built-in Firewall protection and Identity protection. It can be downloaded from http://free-antivirus.eeye.com/
5. **Calmwin antivirus–** An open source, free Antivirus program for Windows 98/Me/2000/XP/2003 and Vista. Features include - high detection rates for viruses and spyware; automatic downloads of regularly updated Virus Database, Standalone virus scanner. It does not include an on-access real-time scanner. It can be downloaded from http://www.clamwin.com/
6. **Comodo Antivirus-** has all the functionality of a paid AV without the price – Features includes- Detects and remove viruses from computers and networks. On Access Scanning conducts a real-time, scheduled virus scan. Host Intrusion Detection allows you to Intercept viruses, spyware, and other malware before they infect your computer.Get updates of the latest virus definitions everyday so you can stay protected against the latest threats. It can be downloaded from http://antivirus.comodo.com/
7. **Moon Secure Antivirus-** Aims to be the best Free Antivirus for Windows under GPL license. It offers multiple scan engines, Net shield, Firewall, On access, on Exec scanner and rootkits preventions plus features from Commercial Antivirus applications. It can be downloaded from http://sourceforge.net/projects/moonav/
8. **PCTools Antivirus-** with PC Tools AntiVirus Free Edition you are protected against the most nefarious cyber-threats attempting to gain access to your PC and personal information. It protects you fromVirus, worm, Trojan and has Smart Updates, IntelliGuard Protection, file guard and email guard. It can be downloaded from http://www.pctools.com/free-antivirus/
9. **Rising Antivirus–** Rising Antivirus Free Edition is a solution with no cost to personal users for the life of the product while still provides the same level of detection and protection capability as RISING Antivirus . It protects your computers against all types of viruses, Trojans, worms, rootkits and other malicious programs. Ease of use and Smartupdate technology make it an "install and forget" product and entitles you to focus on your own jobs with your computer. It can be downloaded from http://www.freerav.com/

10. **Threatfire Lite**– Provides Comprehensive protection against viruses, worms, Trojans, spyware, rootkits, keyloggers & buffer overflows. And have Real-time behavior-based malware detection, malware quarantine & removal, etc. It can be downloaded from http://www.threatfire.com/download/

Email Security

Email is a fast and efficient way to communicate. It is very useful for sending messages to which you need a timely reply, it's a great way to keep people informed about developments and it also makes it easy for people in different geographical locations and time zones to discuss topics and issues. It can be used as a tool for planning, and for content creation.

You can access an email account in two ways, either using an application dedicated to receiving, sending and managing your messages, such as Outlook Express or Thunderbird, or via your web-browser, using online services like Gmail, Yahoo Mail, or Hotmail. Before doing anything, you will need to open an account with an email provider.

The main thing to remember about email is that all data travels on the internet in a readable format, so if someone intercepts your email along the way, they can read the content easily. You would be surprised by just how many people could view this content if they wanted to. The internet is a huge, worldwide network of computers, all directing traffic among themselves, so there are very many different people who have the opportunity to intercept a message in this way.

Email Security

Few of the webmail providers available offer SSL access to your email. Some of them give you a secure login to protect your password but the messages you send and receive are not secure. Some even insert the IP address of the computer you are using into all of the messages you send. Two providers which are worth considering are Gmail and Riseup.

1. **GMAIL:** can be used entirely through a secure connection, as long as you login to your account from https://mail.google.com (with the HTTPS), rather than http://mail.google.com. To ensure ultimate security, you also need to set a preference that tells Gmail always to use SSL in sending and receiving mail. However, we don't recommend relying entirely on Google for the confidentiality of your sensitive email communication. Google scans and records the content of its users' messages for a wide variety of purposes and has, in the past, conceded to the demands of governments that restrict digital freedom.

2. **RISEUP:** Riseup https://mail.riseup.net. RiseUp offers free email to activists around the world and takes great care to protect the information stored on their servers. They have long been a trusted resource for those in need of secure email solutions. Unlike Google,

they have very strict policies regarding their users' privacy, and no commercial interests that might conflict with those policies. In order to create a new RiseUp account, however, you will need two 'invite codes' which can be given out by anyone who already has a RiseUp account.

Regardless of what secure email tools you decide to use, keep in mind that every message has a sender and one or more recipients. Even if you are accessing your email account securely, your recipients may not be using a secure email account when reading and replying to your messages. To ensure private communication, you and your contacts should all use secure email services. If you want to be certain that messages are not intercepted between your email server and a contact's email server, you might all choose to use accounts from the same provider. In this case, RiseUp is a good one to choose.

E-Mail Security Tips

- Don't open email attachments that you are not expecting, or which have come from someone you do not know. When you open such an email, make sure that your anti-virus software is up-to-date and pay close attention to any warnings from your browser or email program.
- You can use anonymity software which can help you hide your chosen email service from anyone who might be monitoring your internet connection. A good, free software programme to do this is Tor (Find out more about Tor browser using Google). If you don't want to give away information about your identity through your email, do not register a username or 'Full Name' that is related to your personal or professional life.
- You can avoid getting spam (unwanted or junk email) by guarding your email address and distributing it sparingly. Also, never open or reply to any emails you consider to be spam, because spammers will take this as a proof of the legitimacy of the address and will just send you more spam. Consider using a spam filter, but remember that it needs to be monitored as it may mistake a genuine email for spam.
- You should try to avoid your emails being mistaken for spam by the recipients. Spam filters will block messages with certain words in the subject heading. It is worth scanning your spam folder for subject lines that are getting blocked.
- Beware of email scams. Many scam emails pretend to come from a bank, Ebay, Paypal, or other online shops. If you get an email telling you that your account is in danger of being shut down, or that you need to take immediate action by updating your account information, be very suspicious: these messages are usually scams. Another frequent scam has you receiving an email from someone you know which says that they have had an emergency and asks you to send them money. This person's email account is likely to have been compromised by a scammer.
- Pay close attention if your browser suddenly gives you messages about invalid security certificates when you attempt to access a secure webmail account. It could mean that someone is tampering with the communication between your computer and the server in order to intercept your messages.

GENERATING SECURE PASSWORD

Guideline for setting secure Password

Choosing the right password is something that many people find difficult, there are so many things that require passwords these days that remembering them all can be a real problem. Perhaps because of this a lot of people choose their passwords very badly. The simple tips below are intended to assist you in choosing a good password.

Basics

- Use at least eight characters, the more characters the better really, but most people will find anything more than about 15 characters difficult to remember.
- Use a random mixture of characters, upper and lower case, numbers, punctuation, spaces and symbols.
- Don't use a word found in a dictionary, English or foreign.
- Never use the same password twice.

Things to avoid

- Don't just add a single digit or symbol before or after a word. e.g. "apple1"
- Don't double up a single word. e.g. "appleapple"
- Don't simply reverse a word. e.g. "elppa"
- Don't just remove the vowels. e.g. "ppl"
- Key sequences that can easily be repeated. e.g. "qwerty","asdf" etc.
- Don't just garble letters, e.g. converting e to 3, L or i to 1, o to 0. as in "z3r0-10v3"

Tips

- Choose a password that you can remember so that you don't need to keep looking it up, this reduces the chance of somebody discovering where you have written it down.
- Choose a password that you can type quickly, this reduces the chance of somebody discovering your password by looking over your shoulder.

Bad Passwords

- Don't use passwords based on personal information such as: name, nickname, birthdate, wife's name, pet's name, friends name, home town, phone number, social security number, car registration number, address etc. This includes using just part of your name, or part of your birthdate.
- Don't use passwords based on things located near you. Passwords such as "computer", "monitor", "keyboard", "telephone", "printer", etc. are useless.
- Don't ever be tempted to use one of those oh so common passwords that are easy to remember but offer no security at all. e.g. "password", "letmein".
- Never use a password based on your username, account name, computer name or email address.

Choosing a password

- Use good password generator software.
- Use the first letter of each word from a line of a song or poem.
- Alternate between one consonant and one or two vowels to produce words. eg. "taupouti".
- Choose two short words and concatenate them together with a punctuation or symbol character between the words. eg. "seat%tree".

Changing your password

- You should change your password regularly,
- You should also change your password whenever you suspect that somebody knows it Remember, don't re-use a password.

Protecting your password

- Never store your password on your computer except in an encrypted form. Note that the password cache that comes with windows (.pwl files) is NOT secure, so whenever windows prompts you to "Save password" don't.
- Don't tell anyone your password, not even your system administrator
- Never send your password via email or other unsecured channel.
- Yes, write your password down but don't leave the paper lying around, lock the paper away somewhere, preferably off-site and definitely under lock and key.
- Be very careful when entering your password with somebody else in the same room.

Remembering your password

Remembering passwords is always difficult and because of this many people are tempted to write them down on bits of paper. As mentioned above this is a very bad idea. So what can you do?

- Use a secure password manager, see the downloads page for a list of a few that won't cost you anything.
- Use a text file encrypted with a strong encryption utility.
- Choose passwords that you find easier to remember.

Bad Examples

- "fred8" - Based on the users name, also too short.
- "christine" - The name of the users girlfriend, easy to guess
- "kciredref" - The users name backwords
- "indescribable" - Listed in a dictionary
- "iNdesCribaBle" - Just adding random capitalisation doesn't make it safe.
- "gandalf" - Listed in word lists
- "zeolite" - Listed in a geological dictionary
- "qwertyuiop" - Listed in word lists

- "merde!" - Listed in a foreign language dictionary

Good Examples

None of these good examples are actually good passwords, that's because they've been published here and everybody knows them now, always choose your own password don't just use somebody elses.

- "mItWdOtW4Me" - Monday is the worst day of the week for me.

How would a potential hacker get hold of my password anyway?

There are four main techniques hackers can use to get hold of your password:

1. **Steal it:** That means looking over your should when you type it, or finding the paper where you wrote it down. This is probably the most common way passwords are compromised, thus it's very important that if you do write your password down you keep the paper extremely safe. Also remember not to type in your password when somebody could be watching.
2. **Guess it:** It's amazing how many people use a password based on information that can easily be guessed. Psychologists say that most men use 4 letter obscenities as passwords and most women use the names of their boyfriends, husbands or children.
3. **A brute force attack:** This is where every possible combination of letters, numbers and symbols in an attempt to guess the password. While this is an extremely labour intensive task, with modern fast processors and software tools this method is not to be underestimated. A Pentium 100 PC might typically be able to try 200,000 combinations every second this would mean that a 6 character password containing just upper and lower case characters could be guessed in only 27½ hours.
4. **A dictionary attack.:** A more intelligent method than the brute force attack described above is the dictionary attack. This is where the combinations tried are first chosen from words available in a dictionary. Software tools are readily available that can try every word in a dictionary or word list or both until your password is found. Dictionaries with hundreds of thousands of words, as well as specialist, technical and foreign language dictionaries are available, as are lists of thousands of words that are often used as passwords such as "qwerty", "abcdef" etc.

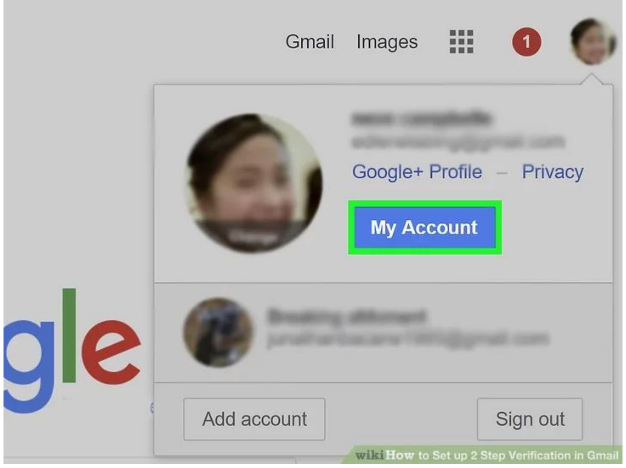
Two step authentication process

How to Set up 2 Step Verification in Gmail

Two-Step Verification is an additional layer of security that you can add onto your Gmail account. When enabled, you will have to enter your password, and enter a special code that is sent to your device, or verify the sign in attempt on your phone. This dramatically increases the security of your account and makes sure that hackers can't get into your account even if the guess or steal your password. This how you how to enable two-step verification on Gmail.

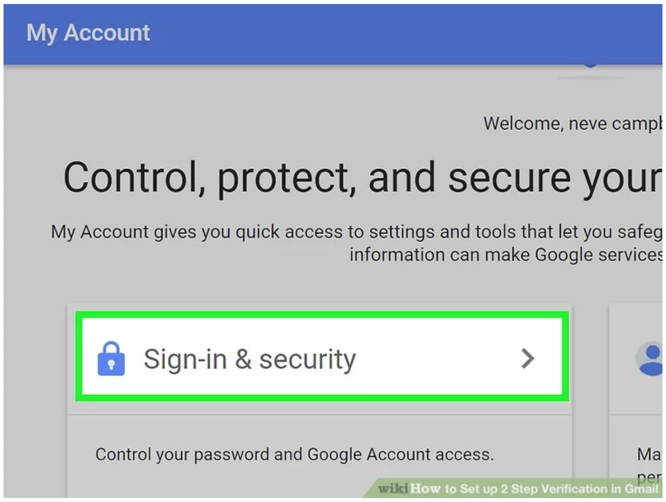
Method 1 Text Message or Voice Call

1 Decide if you want to use the text message or voice call option. With this enabled, a code will be sent to your phone via text, or Google will call your phone and tell you the code. You then enter this code into the sign in prompt in order to sign in.



2 Go to Google's "My Account" page. You can find it at the following address: https://myaccount.google.com/

If you aren't signed into your Google account, click Sign in in the top-right corner of the page and enter your Gmail email address and password.



My Account

Welcome, neve campb

Control, protect, and secure your

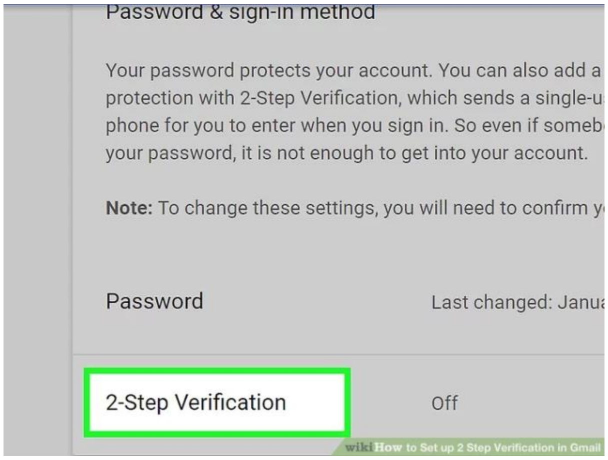
My Account gives you quick access to settings and tools that let you safeg
information can make Google services

Sign-in & security

Control your password and Google Account access.

Ma
per

3 Click Sign-in & security. It's on the left side of the page.



Password & sign-in method

Your password protects your account. You can also add a
protection with 2-Step Verification, which sends a single-u
phone for you to enter when you sign in. So even if someb
your password, it is not enough to get into your account.

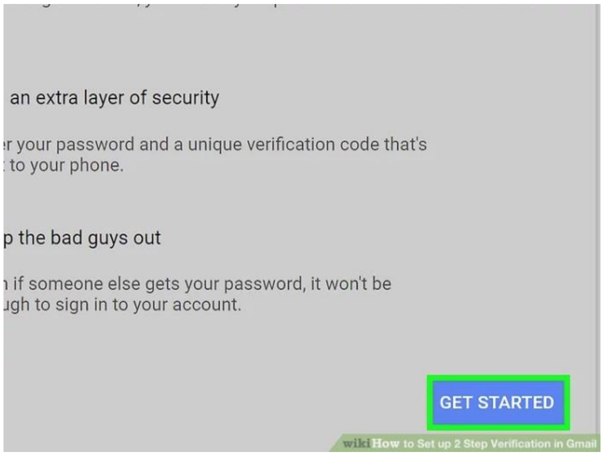
Note: To change these settings, you will need to confirm y

Password Last changed: Janua

2-Step Verification Off

4 Scroll down and click 2-Step Verification. You'll see this option on the right side of the page in the "Password & sign-in method" section.

If you see "On" to the right of 2-Step Verification, it's already set up. You can add this method as another way to verify your sign in attempt. Just access the 2-Step Verification page, and click on Set Up under the option for "Voice or text message".



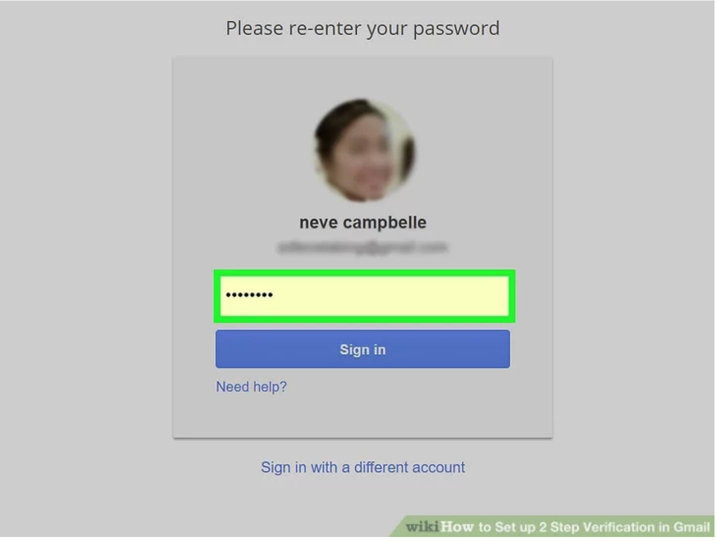
an extra layer of security

r your password and a unique verification code that's
: to your phone.

p the bad guys out

ı if someone else gets your password, it won't be
ıgh to sign in to your account.

5 Click GET STARTED. It's a blue button in the bottom-right corner of the page.



Please re-enter your password

neve campbelle

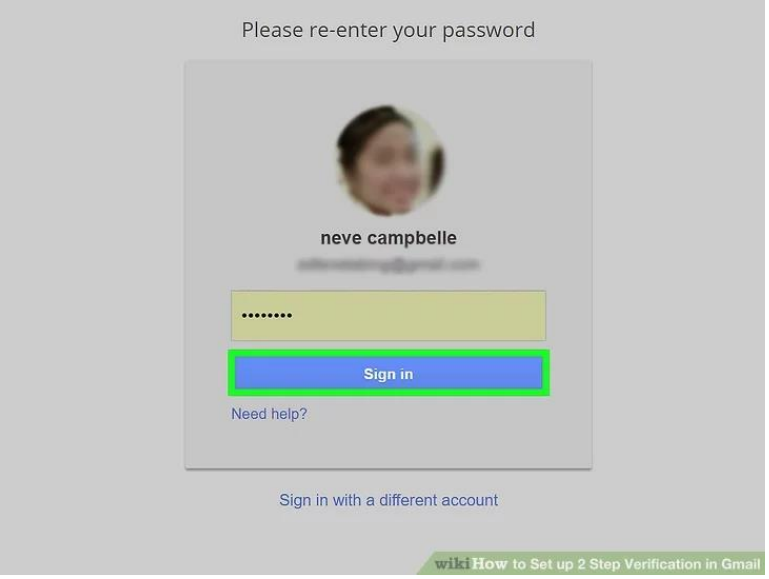
[redacted]

••••••••

6 Enter your Google account password. This step is to confirm your identity with Google before continuing.

If you're signed in on the wrong account, click Sign in with a different account.

Image titled Set up 2 Step Verification in Gmail Step 6



Please re-enter your password

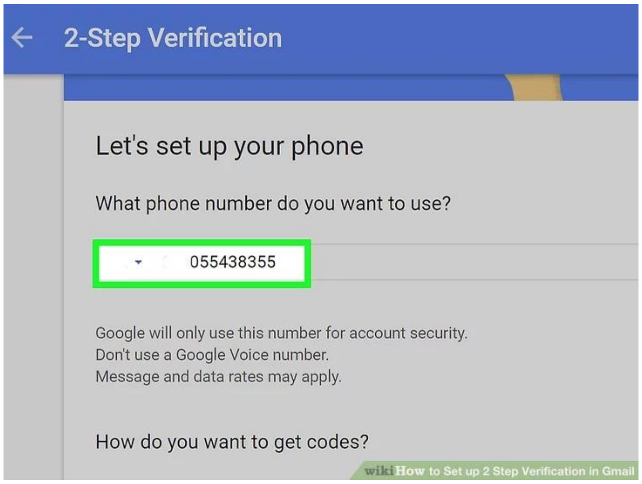
neve campbelle

[redacted]

••••••••

Sign in
Need help?
Sign in with a different account
wikiHow to Set up 2 Step Verification in Gmail

7 Click Sign in. Doing so will confirm your identity and take you to the next page.



2-Step Verification

Let's set up your phone

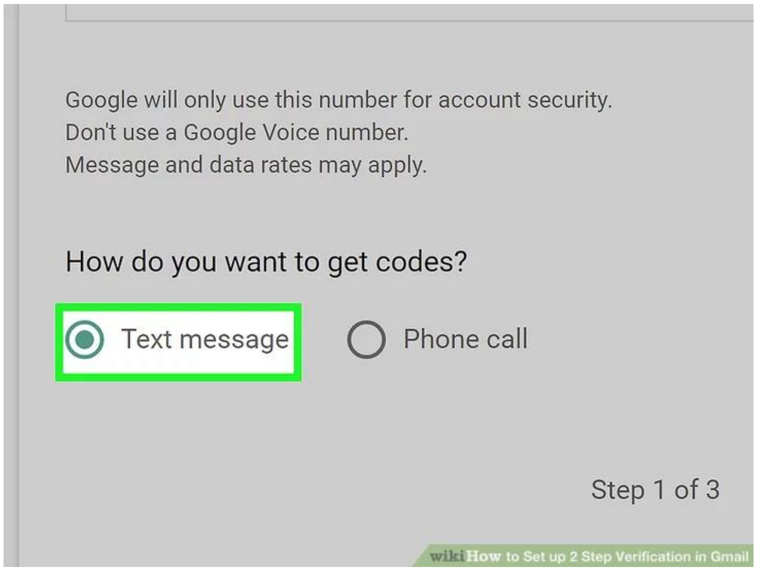
What phone number do you want to use?

055438355

Google will only use this number for account security.
Don't use a Google Voice number.
Message and data rates may apply.

How do you want to get codes?

8 Enter your phone number. Do so in the text field below the "What phone number do you want to use?" heading.



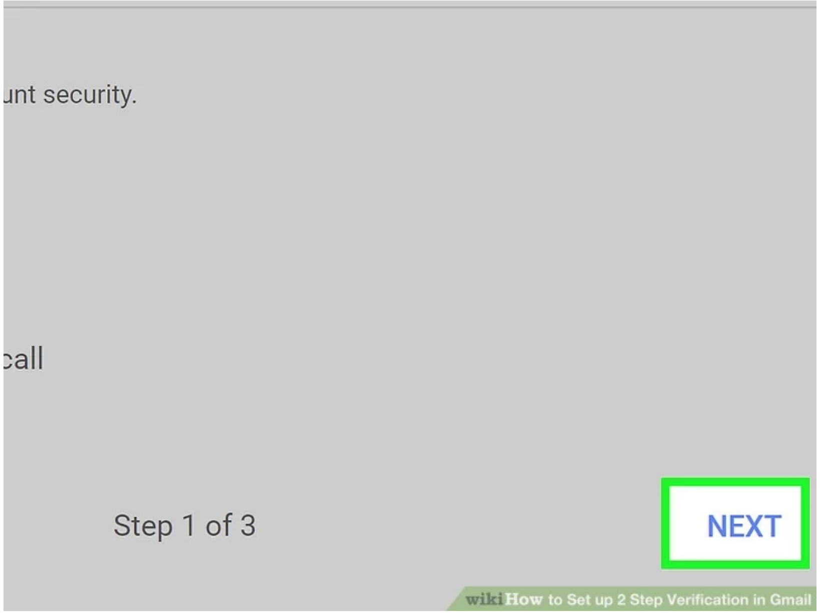
Google will only use this number for account security.
Don't use a Google Voice number.
Message and data rates may apply.

How do you want to get codes?

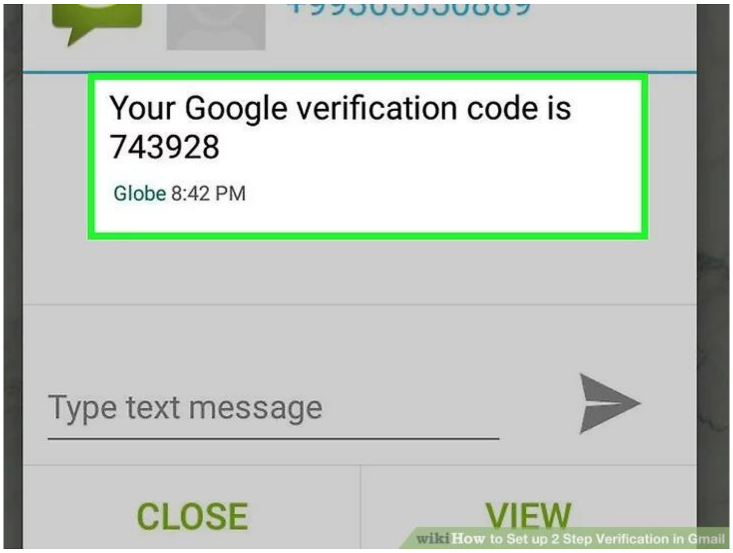
● Text message ○ Phone call

Step 1 of 3

9 Click a code option. You can select Text message to receive a code in text form, or you can click Phone call to receive an audio recording of the code.



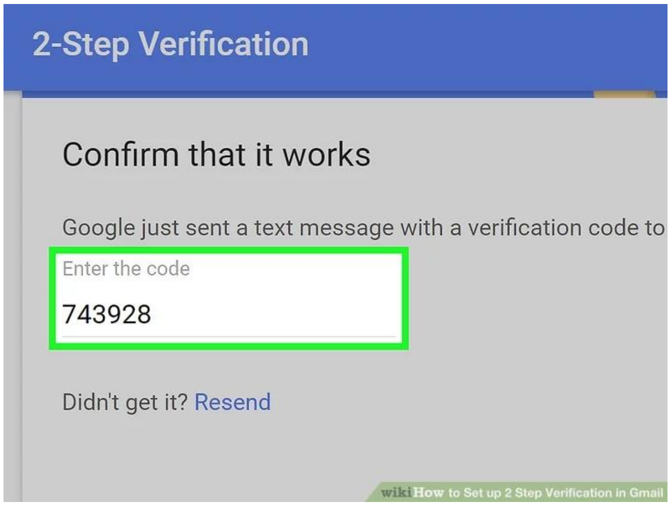
10 Click Next. It's in the bottom-right corner of the screen. Doing so will prompt Google to send a code to you according to your selected option above.



Your Google verification code is 743928

Globe 8:42 PM

11 Retrieve your code from Google. You'll do so either by answering a phone call and listening to the numbers, or by opening your phone's Messages app and reading the new text from a five-digit number.



2-Step Verification

Confirm that it works

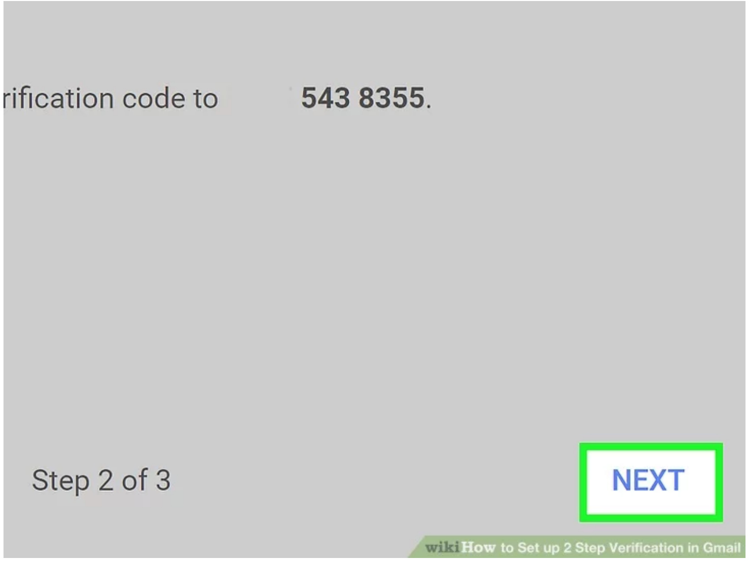
Google just sent a text message with a verification code to

Enter the code

743928

Didn't get it? Resend

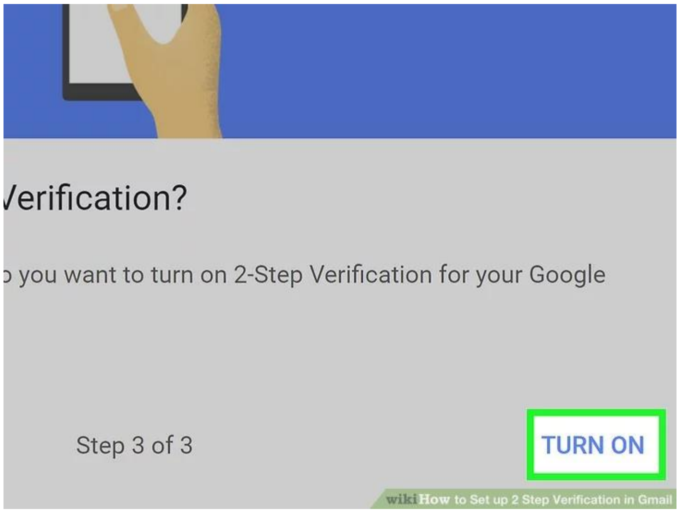
12 Type in your code. You'll do so in the text field in the middle of the page.



rification code to 543 8355.

Step 2 of 3

13 Click Next. It's in the bottom-right corner of the page.



/erification?

› you want to turn on 2-Step Verification for your Google

Step 3 of 3

14 Click TURN ON. This blue button is at the top of the page. Clicking it will enable two-step verification for your Google account; whenever you log into a new device, you'll be prompted to enter a code delivered to your phone.

USING PASSWORD MANAGER

We use passwords to ensure security and the confidentiality of our data. One of the biggest modern day crimes is identity theft, which is easily accomplished when passwords are compromised. The need of the hour is good password management. Have you ever thought of an alternative to remembering your passwords and not repeatedly entering your login credentials? Password managers are one of the best ways to store, back up and manage your passwords. A good password is hard to remember and that’s where a password manager comes in handy. It encrypts all the different passwords that are saved with a master password, the only one you have to remember.

What is a password manager?

A password manager is software that helps a user to manage passwords and important information so that it can be accessed anytime and anywhere. An excellent password manager helps to store information securely without compromising safety. All the passwords are saved using some kind of encryption so that they become difficult for others to exploit.

Why you should use it?

If you find it hard to remember passwords for every website and don’t want to go through the ‘Forgot password?’ routine off and on, then a password manager is what you are looking for. These are designed to store all kinds of critical login information related to different websites.

How does it work?

Password managers may be stored online or locally. Online password managers store information in an online cloud, which can be accessed any time from anywhere. Local password managers store information on the local server, which makes them less accessible. Both have their own advantages, and the manager you use would depend on your need.

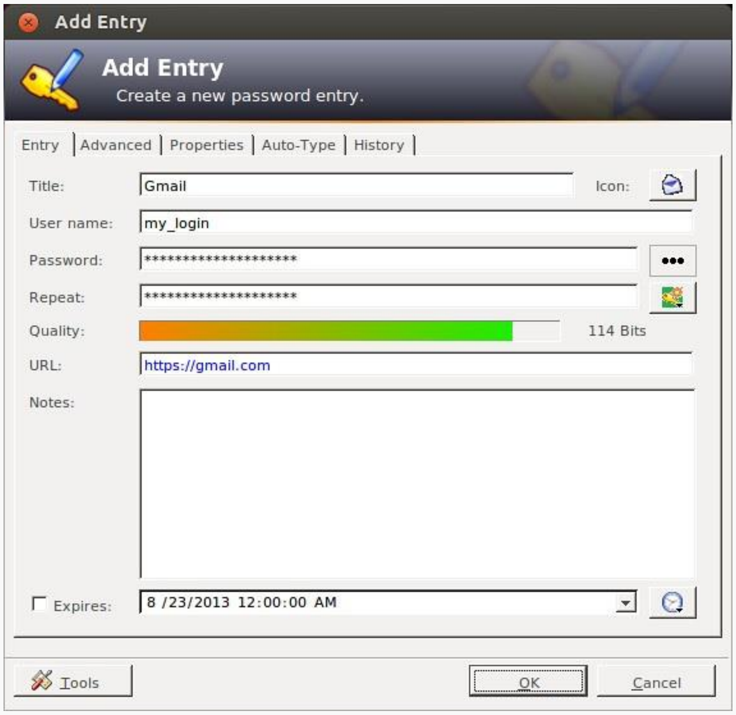
Online password managers use browser extensions that keep data in a local profile, syncing with a cloud server. Some other password managers use removable media to save the password so that you can carry it with you and don’t have to worry about online issues. Both these options can also be combined and used as two-factor authentication so that data is even more secure.

Some popular Password managers

The passwords are saved using different encryptions based on the services that the companies provide. The best password managers use a 256-bit (or more) encryption protocol for better security, which has been accepted by the US National Security Agency for top secret information handling. If you have considered using a password manager and haven’t decided on one, this section features the top five.

KeePassX

KeePassX is an open source, cross-platform and light weight password management application published under the terms of the GNU General Public License. It was built based on the Qt Libraries. KeePassX stores information about user names, passwords and other login information in a secure database. KeePassX uses its own random password generator, which makes it easier to create strong passwords for better security. It also includes a powerful and quick search tool with which a keyword of a website can be used to find login credentials that have been stored in the database. It allows users to customize groups, making it more user friendly. KeePassX is not limited to storing only usernames and passwords but also free-form notes and any kind of confidential text files.



Title: Gmail

User name: my_login

Password: ********************

Repeat: ********************

Quality: 114 Bits

URL: https://gmail.com

Notes:

☐ Expires: 8 /23/2013 12:00:00 AM

KeePassX [Image Courtesy: https://www.flickr.com/photos/xmodulo/9580944074]

Features

- **Simple user interface:** The left pane tree structure makes it easy to distinguish between different groups and entries, while the right pane shows more detailed information.

- **Portable media access:** Its portability makes it easy to use since there's no need to install it on every computer.
- **Search function:** Searches in the complete database or in every group.
- **Auto fill:** There's no need to type in the login credentials; the application does it whenever the Web page is loaded. This keeps it secure from key loggers.
- **Password generator:** This feature helps to generate strong passwords that make it difficult for dictionary attacks. It can be customised.
- **Two factor authentication:** It enables the user to either unlock the database by a master password or by a key from a removable drive.
- **Adds attachments:** Any type of confidential document can be added to the database as an attachment, which allows users to secure not just passwords.
- **Cross-platform support:** It works on all supported platforms. KeePassX is an open source application, so its source code can be compiled and used for any operating system.
- **Security:** The password database is encrypted with either the AES encryption or the Twofish algorithm, which uses 256-bit key encryption.
- **Expiration date:** The entries can be expired, based on a user defined date.
- **Import and export of entries:** Entries: from PwManager or Kwallet can be imported, and entries can be exported as text files.
- Multi-language support: It supports 15 languages.

Password Gorilla

Password Gorilla is an open source, cross-platform, simple password manager and personal vault that can store login information and notes. Password Gorilla is a Tcl/Tk application that runs on Linux, Windows and Mac OS X. Login information is stored in the database, which can be accessed only using a master password. The passwords are SHA256 protected and the database is encrypted using the Twofish algorithm. The key stretching feature makes it difficult for brute force attacks.

Password Gorilla - <New Database>
File Edit Login Security Help
<New Database>
Gmail

Password Gorilla

Features

- **Portable:** Designed to run on a compatible computer without being installed.
- **Import of database:** Can import the password database saved in the CSV format.
- **Locks the database when idle: I**t automatically locks the database when the computer is idle for a specific period of time.
- **Security:** It uses the Twofish algorithm to encrypt the database.
- **Can copy credentials:** Keyboard shortcuts can be used to copy login credentials to the clipboard.
- **Auto clear:** This feature clears the clipboard after a specified time.
- **Organises groups:** Groups and sub-groups can be created to organise passwords for different websites.

Gpassword Manager

Gpassword Manager is a simple, lightweight and cross-platform utility for managing and accessing passwords. It is published under the terms of the Apache License. It allows users to securely store passwords/URLs in the database. The added entries can be marked as favorites, which then can be accessed by right-clicking the system tray icon. The passwords and other login information shown in the screen can be kept hidden based on user preferences.

Gpassword manager

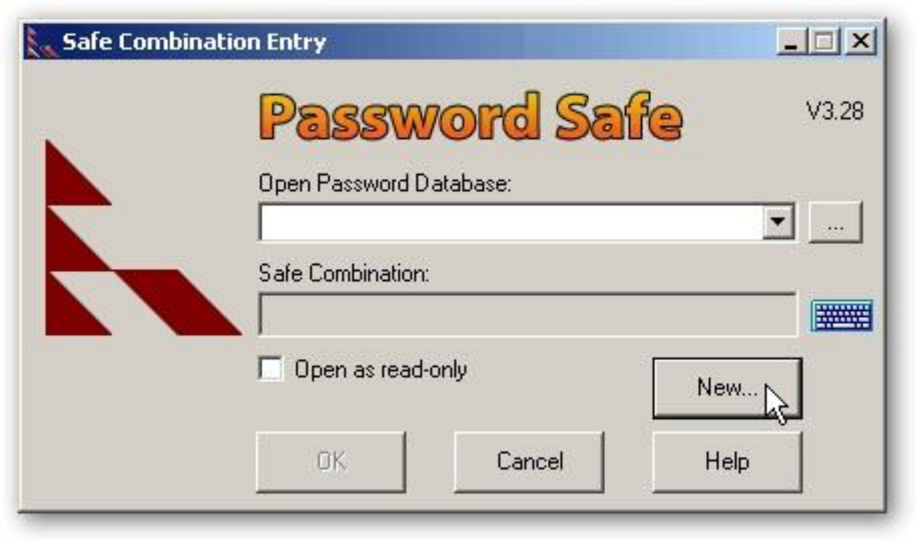
Features

- **Access to favorite sites:** A list of favorite Web pages can be accessed quickly from the convenient ‘tray’ icon.

- **Quick fill:** Passwords and other information can be clicked and dragged onto forms for quick filling out.
- **Search bar:** The quick search bar allows users to search passwords that are needed.
- **Password generator:** Passwords with user-defined options can be generated with just a click.
- **Quick launch:** Favorite websites can be launched by right-clicking the tray icon.

Password Safe

Password Safe is a simple and free open source application initiated by Bruce Schneier and released in 2002. Now Password Safe is hosted on SourceForge and developed by a group of volunteers. It's well known for its ease of use. It is possible to organise passwords based on user preference, which makes it easy for the user to remember. The whole database backup and a recovery option are available for ease of use. Passwords are kept hidden, making it difficult for shoulder surfing. Password Safe is licensed under the Artistic licence.



Password Safe

Features

- **Ease of use:** The GUI is very simple, enabling even a beginner to use it.
- **Multiple databases:** It supports multiple databases. And different databases can be created for each category.
- **Safe decryption:** The decryption of the password database is done in the RAM, which leaves no trace of the login details in the hard drive.
- **Password generator:** Supports the generation of strong, lengthy passwords.
- **Advanced search:** The advanced search function allows users to search within the different fields.
- **Security:** Uses the Twofish algorithm to encrypt the database.

WI-FI SECURITY

Internet users are widely using Wi-Fi devices to access Internet. Every year millions of Wi-Fi devices are sold in the market. Out of these most of the wireless devices are vulnerable in their default configuration mode. Since end users are not fully aware of security levels to be set on these devices, these get rendered vulnerable. By taking advantage of these unsecured Wi-Fi devices terrorists and hackers fulfill their needs.

Anyone with Wi-Fi connectivity in his computer, laptop or mobile can connect to unsecured Access Points (wireless routers).Anyone in the range of Access point can connect to an Access Point if it is unsecured. Once the connection is established the attacker can send mails, download classified/confidential stuff, initiate attack on other computers in the network, send malicious code to others, install a Trojan or botnet on the victims computer to get long term control on it through Internet, etc.

All these criminal acts will naturally be associated with the legal user of Access Point (wireless router). It is up to the legal user of the Access Point to defend himself to prove that he has not been involved in these acts. It now becomes the responsibility of the user to secure his/her own Access Point.

Lets see some real incidents that took place in the recent years.

- Terrorists and hackers used unsecured Access Points to perform illegal activities on the Internet.
- Hackers penetrated into open Wi-Fi network of luxury hotels owned by the Thompson Group in New York, Los Angeles and Washington DC and stole the private emails sent by the guests.The hackers then attempted to extort money from the hotel chain by threatening to publish the emails.(www.crpcc.in)
- Just 5 minutes before Delhi blasts on September 2008 terrorists used an unsecured Wi-Fi connection of a company at Chembur in Mumbai to send terror emails to authorities and news channels. These hackers do not leave a trail of footprints for the investigators to arrive at a logical conclusion. The audit trail ends at Wi-Fi Access Point of the legal user. So it is becomes imperative for the users to secure their own Access Points(wireless router).

Types of Attacks on Wireless Environment

Denial of Service Attack

Denial of service attack aims at preventing the users from accessing the network resources. In a Wireless network, denial of service attack can be applied in various ways.

Man-In-Middle Attack in Wifi Devices

Performing Man-In-Middle Attack in a wireless network is much easier, when compared to wired network. As the transmissons from an accesspoint is broadcasted, it is easy for an unauthorised user to collect the traffic sent by other wireless clients. And the process of collecting the packets in this manner is known as Eavesdropping. Also the third party user can manipulate the packets sent to the legitimate users which results in breaking the users privacy.

So In order to avoid these kind of attacks, Strong encryption should be used for transmitting the data between wireless client and accesspoint.

WarDriving

It is a process of tracking Wi-Fi hotspots located at a particular place, while moving with a hand held device or a laptop in a vehicle. This helps the user in finding out the accesspoints that doesnot use encryption and takes control over it for performing the attacks on the network

How the attack occurs in Wifi Environment ?

- At the physical layer of TCP/IP Model, denial of service attack can be implemented by introducing a device which will generate noise in the same frequency band in which wireless accesspoint is operating. This makes the users who are trying to connect to the accesspoint may not be able to connect to it.

- Also the other possibility of Denial of service Attack is spoofing the accesspoint. Normally wireless clients connect to the wired network with the help of an accespoint. For associating with the accesspoint they require SSID of it. When an unauthorised user places an accesspoint with the same SSID, then there is a chance of authorised user getting associated with the attackers accesspoint. If that happens, the attacker will try to collect sufficient number of packets from the wireless client and cracks the WEP key used by the legitimate accesspoint. Then the attacker gets associated with the legitimate accesspoint and generates large ping requests in the network or generate some abnormal traffic, which may finally result in Denial of Service Attack.

Tips:

- All Wi-Fi equipment support some form of encryption. So, enable them.
- Enable MAC address filtering on Wi-Fi devices.
- Avoid dynamic IP address for home Wi-Fi rather use static IP addresses.
- Use encryption technology for sensitive data in wireless networks.

Guidelines for securing Wireless Communications

- Always use strong password for encryption
- A strong password should have atleast 15 characters, uppercase letters, lowercase letters, numbers and symbol. Also it is recommended to change the encryption key frequently so that it makes difficult for the cracker to break the encryption key. Do not use WEP for encryption, rather use WPA/WPA2.
- Always use the maximum key size supported by accesspoint for encryption
- If the keysize is large enough, then it takes more time to crack the key by the hacker. Also it is recommneded to change the encryption key frequently so that it makes difficult for the cracker to break the encryption key.
- Isolate the wireless network from wired network with a firewall and a antivirus gateway.
- Do not connect the accesspoint directly to the wired network. As there is a chance of comprimised wireless client inturn effecting the systems in the wired network, a firewall and an antivirus gateway should be placed between the accespoint and the wired network.
- Restrict access to the Access Point based on MAC address
- In order to allow authorized users to connect to the Access Point, wireless clients should be provided access based on MAC address.
- Change the default username and Password of the Access Point
- Most of the users do not change the default passwords while configuring the Access Point.But it is recommended to keep a strong password, as this default password information can be known from product manufacturers.
- Shutdown the Access Point when not in use
- Hackers try to brute force the password to break the keys, so it is good practice to turn off the Access points during extended periods of Non-use
- Do not broadcast your network name
- SSID information is used to identify a Access Point in the network and also the wireless clients connect to the network using this information. Hence, in order to allow authorized users to connect to the network, the information should not be provided in public.
- Always maintain a updated firmware
- Updating the firmware of accesspoint is recommended, as it will reduce the number of security loop holes in the accesspoint.
- Use VPN or IPSEC for protecting communication
- When the information flowing from wireless client to the wired network receiver is critical, then it is recommended to use VPN or IPSEC based communication so that the information is protected from sniffers in the network.
- Do not make the SSID information public

- SSID information is used to identify a accesspoint in the network and also the wireless clients connect to the network using this information. Hence, in order to allow authorised users to connect to the network, the information should not be provided in public.
- Disable DHCP service
- When the number of users accessing the Access Point is less, it is recommended to disable the DHCP service. As this may make the attackers easy to connect to the network once they get associated with the Access Point.

References:

Text Books

1. William Easttom II, Computer Security Fundamentals, Pearson, 4th edition.
2. Sunit Belapure Nina Godbole, Cyber Security, Wiley, 1st edition.
3. Christopher Hadnagy, Social Engineering, The Science of Human Hacking, John Wiley & Sons, 2nd edition
4. Thomas A. Johnson, Cyber Security, CNC Press, 1st edition.
5. Sanjib Sinha, Beginning Ethical Hacking, Apress, 1st edition.

Reference Books

1. Nina Godbole, Information Systems Security: Security Management, Metrics, Frameworks and Best Practices, Wile, 1st edition.
2. Jon Erickson, The art of Exploitation, Starch Press, 2nd edition.

E-Books and online learning material:

1. Cyber Attacks and Counter Measures: http://uou.ac.in/progdetail?pid=CEGCS-17Meilir Page-Jones: Fundamentals.
2. Introduction to Cyber Security available at http://uou.ac.in/foundation-course.
3. Fundamentals of Information Security http://uou.ac.in/progdetail?pid=CEGCS-17.
4. Cyber Security Techniques http://uou.ac.in/progdetail?pid=CEGCS-17.
5. https://www.cybersecurity.ox.ac.uk/resources/videos

Online Courses and Video Lectures

1. https://nptel.ac.in/courses/106/106/106106129/
2. https://www.utep.edu/information-resources/iso/security-awareness/videos/security-awareness-videos.html
3. https://www.utep.edu/technologysupport/ServiceCatalog/SEC_EmailEncryption.html
4. https://nptel.ac.in/courses/106/105/106105031/