Vieh Groups Internship

Hybrid Techniques for Data Encryption

Ethical Hacking

Sudhanshu D. Meshram

Started :- 1 february 2023

**Index**

Abstraction……………………………………………………………………………………..….1

Objectives……………………………………………………………………………..…………..2

Benefits……………………………………………………………………………………..……..3

Cryptography…………………………………………………………………………...…………4

* Plaintext
* Ciphertext
* Cipher

Cryptanalysis……………………………………………………………………………….…….5

* Known plaintext
* Chosen plaintext
* Chosen ciphertext

Cryptology………………………………………………………………………………..………7

Brute force attack…………………………………………………………………………………8

Classical encryption techniques…………………………………………………………9

* Ceaser cipher
* Monoalphabetic cipher
* Playfair cipher
* Hill cipher

Malware…………………………………………………………………………….11

* Trojens
* Viruses
* Spyware
* Ransomwares

Causes………………………………………………………………………………13

Prevention……………………………………………………………………………14

How IT Industry works…………………………………………………………….….14

How Goggle identifies 12.4 million phishing users potentials …………………………….15

**Abstraction**

Data encryption is process of securing data through creation of some sort of combination of ciphers and techniques which attempt to change plaintext into a pattern which is not easy to understand for anyone for security purpose. The process involves Generate a symmetric encryption key: A symmetric encryption key is generated by a key generation algorithm. Encrypt the data with symmetric encryption: The data is encrypted with the symmetric encryption key. Encrypt the symmetric encryption key with asymmetric encryption: The symmetric encryption key is encrypted using the public key of the recipient. Send the encrypted data and encrypted symmetric encryption key: The encrypted data and encrypted symmetric encryption key are sent to the recipient. Decrypt the symmetric encryption key with asymmetric encryption: The recipient uses their private key to decrypt the symmetric encryption key. Decrypt the data with symmetric encryption: The recipient uses the decrypted symmetric encryption key to decrypt the data.

**Objectives**

Increased security: By using both symmetric and asymmetric encryption methods, hybrid encryption techniques can provide greater security than either method alone. The symmetric encryption method is used for encrypting the data, while the asymmetric encryption method is used for securely transmitting the symmetric key.

Efficiency: Hybrid encryption is more efficient than asymmetric encryption alone because it uses a symmetric key to encrypt the data, which is faster and more efficient than asymmetric encryption.

Flexibility: Hybrid encryption allows for greater flexibility in terms of key management. Because symmetric encryption keys can be generated and distributed easily, they can be used for short-term secure communication, while asymmetric encryption keys can be used for long-term security and key management.

Compatibility: Hybrid encryption is compatible with existing encryption methods and protocols, making it easy to implement in existing systems and networks

**Benefits**

* Stronger Security: Hybrid encryption combines the advantages of both symmetric and asymmetric encryption, providing stronger security than either method alone. By using a symmetric encryption key to encrypt the data and an asymmetric encryption key to securely transmit the symmetric key, hybrid encryption ensures that the data is secure even if the symmetric key is compromised.
* Better Efficiency: Hybrid encryption is more efficient than asymmetric encryption alone because it uses a symmetric key to encrypt the data, which is faster and more efficient than asymmetric encryption. This makes hybrid encryption particularly useful for securing large amounts of data.
* Key Management Flexibility: Hybrid encryption allows for greater flexibility in terms of key management. Symmetric encryption keys can be generated and distributed easily, allowing for short-term secure communication, while asymmetric encryption keys can be used for long-term security and key management.
* Compatibility: Hybrid encryption is compatible with existing encryption methods and protocols, making it easy to implement in existing systems and networks without the need for major changes.
* Versatility: Hybrid encryption can be used in a wide range of applications, including email, online transactions, and cloud storage, making it a versatile solution for securing data transmissions.

**Hybrid** :- Hybrid means mixer of fields working related to the same field. In data encryption its about mixer of different patterns, sequences, techniques, etc . for data security.

**Techniques** :-Techniques are the different ways to perform a task logically or definitely or uniquely done .

**Data** :- Data is alphabets , numbers, structured or unstructured combination of this for information and knowledge .

**Encryption** :- Encryption is a process of creating a cipher text of plaintext enter by user to provide privacy to user data .

**CRYPTOGRAPHY**

Cryptography is the practice of securing communication from unauthorized access or modification. It involves the use of mathematical algorithms and protocols to transform messages into an unreadable format, which can only be decrypted by authorized individuals who possess the corresponding key. Cryptography is commonly used to protect sensitive information such as financial data, passwords, and personal information. It is also used in digital signatures, secure communication channels, and electronic voting systems. There are several types of cryptography, including symmetric key cryptography, asymmetric key cryptography, and hash functions.

Cryptography is the practice of securing communication from third-party interference. It involves techniques that enable the transformation of plain text into coded or encrypted form, which is difficult to understand by unauthorized persons. The purpose of cryptography is to provide confidentiality, integrity, and authenticity to data.

Cryptography has a long history, dating back to ancient times when people used various methods to keep their messages secret. With the advent of the digital age, cryptography has become an essential aspect of modern communication systems. Cryptography is widely used in areas such as online banking, e-commerce, email communication, and many other areas where secure data transmission is critical.

Cryptography relies on the use of cryptographic algorithms, which are mathematical functions that convert plain text into cipher text. The cipher text is then sent over an insecure channel and can only be deciphered by authorized parties with the appropriate key. There are several types of cryptographic algorithms, including symmetric key algorithms, public key algorithms, and hashing algorithms.

Overall, cryptography plays a vital role in modern communication, ensuring that data is secure and confidential, and preventing unauthorized access and interception of sensitive information.

* **Plaintext** :- Plaintext refers to any text that is easily readable and understandable without any encryption or obfuscation. In other words, plaintext is any information that is not coded or scrambled in any way.

It's important to note that plaintext is vulnerable to unauthorized access and interception by third parties, which is why sensitive information should be encrypted to protect it from being read by anyone who shouldn't have access to it.

* **Ciphertext** :- Ciphertext is the result of applying an encryption algorithm to plaintext to convert it into an unreadable format. In other words, it is the encrypted form of plaintext, which is designed to be unreadable to anyone who doesn't have the decryption key to convert it back into plaintext.

Ciphertext is created by using a mathematical algorithm to transform the original message into a different form that is not easily understood. This process involves using a key or a password to encode the information, so that only those who have access to the key or password can decrypt and read the message.

Ciphertext is commonly used to protect sensitive information, such as passwords, financial transactions, and personal data, from unauthorized access. It can also be used to protect the confidentiality and privacy of communications, such as email, instant messaging, and voice calls, by making it more difficult for attackers to intercept and read the messages.

* **Cipher** :- A cipher is a system or method of encryption that transforms plaintext into ciphertext. It involves the use of mathematical algorithms and keys to convert plaintext into an unreadable form.

There are many different types of ciphers, including substitution ciphers, transposition ciphers, and modern block and stream ciphers. Substitution ciphers replace each letter or character in the plaintext with a different letter or character, while transposition ciphers rearrange the order of the letters or characters in the plaintext. Modern ciphers use complex mathematical functions to encrypt the plaintext, and are often designed to be resistant to cryptanalysis attacks.

Ciphers are used for a variety of purposes, including protecting the confidentiality and integrity of sensitive information, preventing unauthorized access to data, and ensuring the privacy of communications. They have been used throughout history, from ancient times to the present day, and continue to be an important part of cryptography and information security.

**Cryptanalysis** :- Cryptanalysis is the process of analyzing and breaking cryptographic systems, such as ciphers, codes, and encryption algorithms. It involves using mathematical and computational techniques to find weaknesses in the cryptographic systems, and to uncover the plaintext from the ciphertext without knowledge of the key or password.

Cryptanalysis can be divided into two categories: classical cryptanalysis and modern cryptanalysis. Classical cryptanalysis involves breaking classical ciphers, which were used before the advent of computers and modern cryptography. This type of cryptanalysis relies on techniques such as frequency analysis, which involves analyzing the frequency of letters and patterns in the ciphertext to deduce information about the plaintext.

Modern cryptanalysis, on the other hand, involves breaking modern encryption algorithms, which are used to protect data in computer systems and communications networks. This type of cryptanalysis involves using mathematical algorithms and computational power to attack encryption keys, and to find weaknesses in the encryption algorithms themselves.

* **Known Plaintext** :- Known plaintext is a term used in cryptanalysis to refer to a situation in which an attacker has access to both the plaintext and the corresponding ciphertext of one or more messages. This can occur when an attacker intercepts a message, or when they have access to the plaintext and ciphertext in a different context, such as a database or a network capture.

Known plaintext is a powerful tool for cryptanalysis, as it provides the attacker with information about the encryption algorithm and key used to generate the ciphertext. By comparing the plaintext and ciphertext, the attacker can identify patterns and relationships between the two, which can help them to deduce information about the encryption key and algorithm.

One example of a known plaintext attack is frequency analysis, which involves analyzing the frequency of letters and patterns in the plaintext and ciphertext to deduce information about the encryption key. Another example is the known plaintext attack on the Data Encryption Standard (DES) cipher, which was used in the 1970s and 1980s. This attack involved analyzing the plaintext and ciphertext of messages encrypted with DES, and using this information to deduce the encryption key.

**Chosen Plaintext** :- Chosen plaintext is a term used in cryptanalysis to refer to a situation in which an attacker has the ability to choose and encrypt their own plaintext messages, and observe the corresponding ciphertext produced by the encryption algorithm. This can occur in situations where an attacker has direct access to the encryption algorithm or has intercepted communication between two parties.

Chosen plaintext attacks are a powerful tool for cryptanalysis, as they provide an attacker with additional information about the encryption algorithm and key used to generate the ciphertext. By choosing specific plaintexts to encrypt, an attacker can observe the corresponding ciphertext and use this information to deduce information about the encryption algorithm and key.

One example of a chosen plaintext attack is the padding oracle attack, which involves an attacker sending specially crafted plaintext messages to a server that uses padding to encrypt the messages. By analyzing the corresponding ciphertext and the error messages produced by the server, the attacker can deduce information about the encryption key and decrypt other messages.

Chosen plaintext attacks can be a serious threat to the security of a cryptographic system, as they can allow attackers to bypass the encryption and access sensitive information. Therefore, it is important to use strong encryption algorithms and keys, and to protect the confidentiality of plaintext and ciphertext to prevent attackers from obtaining chosen plaintext.

* **Chosen Ciphertext** :- Chosen ciphertext is a term used in cryptanalysis to refer to a situation in which an attacker has the ability to choose and decrypt their own ciphertext messages, and observe the corresponding plaintext produced by the decryption algorithm. This can occur in situations where an attacker has direct access to the decryption algorithm or has intercepted communication between two parties.

Chosen ciphertext attacks are a powerful tool for cryptanalysis, as they provide an attacker with additional information about the decryption algorithm and key used to generate the plaintext. By choosing specific ciphertexts to decrypt, an attacker can observe the corresponding plaintext and use this information to deduce information about the decryption algorithm and key.

One example of a chosen ciphertext attack is the adaptive chosen ciphertext attack, which involves an attacker repeatedly sending ciphertexts to a server and receiving the corresponding plaintext. By analyzing the plaintext produced by the server, the attacker can deduce information about the decryption algorithm and key.

Chosen ciphertext attacks can be a serious threat to the security of a cryptographic system, as they can allow attackers to bypass the decryption and access sensitive information. Therefore, it is important to use strong encryption and decryption algorithms and keys, and to protect the confidentiality of ciphertext and plaintext to prevent attackers from obtaining chosen ciphertext.

**Cryptology** :- Cryptology is the study of techniques for secure communication in the presence of third parties, and encompasses both cryptography and cryptanalysis. It involves the development of mathematical and computational methods for encrypting and decrypting messages, and for breaking encrypted messages without knowledge of the key or password.

Cryptography is the practice of using mathematical algorithms to convert plaintext into ciphertext, which is unintelligible to unauthorized parties. It involves the development and implementation of encryption techniques, such as symmetric-key cryptography, public-key cryptography, and hashing algorithms, to protect data and communications from unauthorized access.

Cryptanalysis, on the other hand, is the study of how to break cryptographic systems, and involves analyzing and attacking encryption algorithms and keys to uncover the plaintext from the ciphertext. It is an important part of cryptology, as it helps to identify and fix vulnerabilities in cryptographic systems, and to develop stronger and more secure encryption algorithms.

Cryptology has a wide range of applications, including securing communications in military and diplomatic contexts, protecting financial transactions, and ensuring the privacy and security of personal data in computer systems and communications networks. It is a constantly evolving field, as new technologies and techniques are developed to address emerging security threats.

**Key** :- In cryptography, a key is a piece of information that is used to control the encryption and decryption of messages. It is a parameter that determines the specific transformation used to convert plaintext into ciphertext, or vice versa.

In symmetric-key cryptography, the same key is used for both encryption and decryption. The key is a secret shared between the sender and the receiver, and is used to convert plaintext into ciphertext before sending the message, and to convert ciphertext back into plaintext upon receipt. The security of the system depends on the secrecy of the key, as anyone who knows the key can decrypt the message.

In public-key cryptography, there are two keys: a public key and a private key. The public key is used to encrypt messages, while the private key is used to decrypt them. The public key is widely distributed and can be used by anyone to encrypt messages for the recipient, while the private key is kept secret and used only by the recipient to decrypt the messages. This system allows for secure communication without the need for a shared secret key.

The strength and security of a cryptographic system depends on the length and randomness of the key used, as well as the encryption algorithm and implementation used. Therefore, generating and managing strong keys is an important aspect of cryptography and information security.

**Brute Force Attack**

Brute force attack is a type of cryptanalytic attack in which an attacker systematically tries all possible keys or passwords until the correct one is found. This attack involves no prior knowledge of the encryption key or password and relies on the attacker's computational power to try all possible combinations.

Brute force attacks are often used against encryption algorithms that use short keys or passwords. For example, if a password is only six characters long and uses only uppercase letters, lowercase letters, and digits, there are only 62^6 (about 56 billion) possible combinations, which can be tried by an attacker in a reasonable amount of time using a powerful computer.

To protect against brute force attacks, cryptographic systems often use longer keys or passwords, or implement additional security measures such as rate limiting or lockouts to prevent repeated attempts. Additionally, many encryption algorithms are designed to be resistant to brute force attacks by using key stretching, salting, or other techniques that make the search space much larger and more difficult to brute force.

In some cases, a brute force attack may be the only viable method of attack, especially if the encryption key or password is weak or poorly chosen. However, with strong encryption and appropriate key or password management, a successful brute force attack can be made computationally infeasible, making it a powerful tool for securing information.

**CLASSICAL ENCRYPTION TECHNIQUES**

* **Ceaser Cipher** :- The Caesar cipher is one of the simplest and most widely known encryption techniques in cryptography. It is named after Julius Caesar, who is believed to have used this technique to communicate with his generals.

The Caesar cipher is a substitution cipher in which each letter in the plaintext is shifted a certain number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on. The method is based on the idea of wrapping around the alphabet, so that Z becomes A again.

The encryption process using the Caesar cipher can be described as follows:

Choose a shift value, which determines how many positions each letter in the plaintext will be shifted.

Take each letter in the plaintext and shift it by the shift value. For example, with a shift of 3, A would become D, B would become E, and so on.

The resulting letters are the ciphertext.

The decryption process is the reverse of the encryption process. The shift value is known to the recipient, who can use it to shift each letter of the ciphertext back to its original position.

* **Monoalphabetic Cipher** :- A monoalphabetic cipher is a type of substitution cipher in which each letter of the plaintext is replaced by a fixed letter in the ciphertext. The substitution is determined by a fixed mapping between the letters of the alphabet. This means that each plaintext letter is replaced by the same ciphertext letter every time it appears in the message.

For example, if the mapping is “a” to “D”, “b” to “F”, “c” to “G”, and so on, then every occurrence of the letter “a” in the plaintext will be replaced by the letter “D” in the ciphertext, and so on.

Monoalphabetic ciphers are relatively easy to implement, but they are not very secure because the same substitution is used for every occurrence of a given plaintext letter. This means that an attacker can use frequency analysis to break the encryption by analyzing the frequency of occurrence of letters in the ciphertext and comparing it to the frequency of letters in the plaintext.

To make monoalphabetic ciphers more secure, various techniques have been developed such as polyalphabetic ciphers, which use multiple substitution mappings, and transposition ciphers, which rearrange the order of letters in the plaintext to create the ciphertext. These techniques help to make the cipher more resistant to frequency analysis and other forms of cryptanalysis.

* **Playfair Cipher** :- The Playfair cipher is a polygraphic substitution cipher that was invented by Sir Charles Wheatstone in 1854, but named after his friend Lyon Playfair who popularized the technique. It uses a 5x5 matrix of letters to encrypt pairs of letters in the plaintext, making it more secure than monoalphabetic substitution ciphers.

The encryption process using the Playfair cipher can be described as follows:

Generate a 5x5 matrix of letters by filling in the letters of a keyword (usually a word or phrase) and then filling in the remaining letters of the alphabet in order, omitting "Q".

Break the plaintext into pairs of letters. If the plaintext contains an odd number of letters, add an "X" at the end to create an even number of pairs.

For each pair of letters, find their corresponding positions in the matrix.

If the two letters are in the same row of the matrix, replace them with the letters to their immediate right, wrapping around to the left side of the row if necessary.

If the two letters are in the same column of the matrix, replace them with the letters immediately below, wrapping around to the top of the column if necessary.

If the two letters are in different rows and columns, replace them with the letters at the opposite corners of the rectangle formed by their positions.

The Playfair cipher is relatively strong against frequency analysis and other traditional cryptanalytic attacks, but it is not secure against modern cryptographic techniques such as brute force attacks or differential cryptanalysis. Nonetheless, it remains an interesting historical cipher and a useful teaching tool for understanding basic principles of polygraphic substitution ciphers.

* **Hill Cipher** :-

(ENCRYOTION)

The Hill cipher is a polygraphic substitution cipher that was invented by Lester S. Hill in 1929. It uses matrix multiplication to encrypt blocks of plaintext letters, making it more secure than monoalphabetic substitution ciphers.

The encryption process using the Hill cipher can be described as follows:

* Choose a key matrix, which is a square matrix of numbers that determines the encryption and decryption rules. The size of the matrix depends on the length of the blocks of plaintext letters to be encrypted.
* Break the plaintext into blocks of letters, with each block having the same length as the key matrix.
* Convert each block of plaintext letters into a column vector by assigning each letter a numerical value (A=0, B=1, C=2, and so on) and arranging them vertically.
* Multiply the key matrix by the column vector modulo 26 to obtain a new column vector representing the encrypted block of letters.
* Convert the resulting column vector back into a block of ciphertext letters by assigning each numerical value a corresponding letter.

(DECRYPTION)

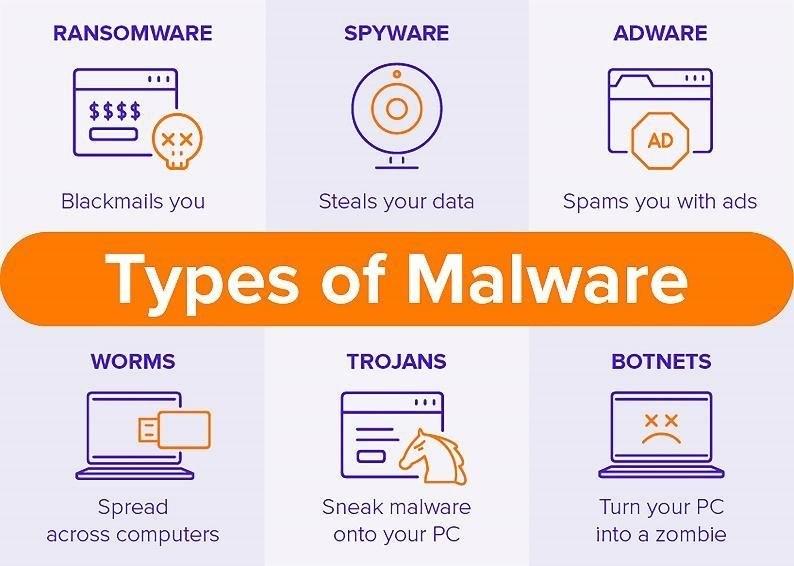
The decryption process for the Hill cipher involves using the inverse of the key matrix to convert the ciphertext back into plaintext. Here are the steps for decrypting a block of ciphertext using the Hill cipher:

* Choose the key matrix used to encrypt the plaintext.
* Calculate the inverse of the key matrix using modular arithmetic. The inverse matrix can be found using various methods such as Gauss-Jordan elimination or the adjugate matrix method.
* Break the ciphertext into blocks of letters, with each block having the same length as the key matrix.
* Convert each block of ciphertext letters into a column vector by assigning each letter a numerical value (A=0, B=1, C=2, and so on) and arranging them vertically.
* Multiply the inverse key matrix by the column vector modulo 26 to obtain a new column vector representing the decrypted block of letters.
* Convert the resulting column vector back into a block of plaintext letters by assigning each numerical value a corresponding letter.

**Malware**

Malware, short for "malicious software," refers to any type of software designed to cause harm to a computer system or network. Malware can take many forms, including viruses, worms, Trojans, ransomware, spyware, adware, and more.

Malware can be spread through a variety of methods, including email attachments, software downloads, infected websites, and social engineering tactics. Once a computer is infected with malware, it can be used to steal sensitive information, damage files, or take control of the entire system.



To protect against malware, it's important to keep your operating system and software up-to-date with the latest security patches, use strong passwords and two-factor authentication, and avoid opening suspicious emails or downloading unknown files. It's also a good idea to use antivirus software and regularly back up important data to prevent data loss in case of a malware attack.

1. **Trojens :-** A Trojan, short for Trojan horse, is a type of malware that disguises itself as legitimate software in order to trick users into installing it on their computers. Once installed, the Trojan can perform a variety of malicious actions, such as stealing sensitive information, modifying files, or giving an attacker remote control of the infected system.

Trojans can be spread through a variety of methods, including email attachments, software downloads, and infected websites. They often rely on social engineering tactics to convince users to download and install them, such as by pretending to be a useful software update or a harmless file attachment.

To protect against Trojans, it's important to be cautious when downloading and installing software, particularly from unknown sources. Keep your operating system and software up-to-date with the latest security patches, use strong passwords and two-factor authentication, and avoid opening suspicious emails or downloading unknown files. It's also a good idea to use antivirus software and regularly back up important data to prevent data loss in case of a Trojan attack.

1. **Spyware**

Spyware is a type of malware that is designed to collect information from a user’s computer or mobile device without their knowledge or consent. The information that spyware collects can include web browsing history, keystrokes, passwords, email addresses, and other sensitive data.

Spyware can be installed on a computer or mobile device in a variety of ways, such as through software downloads, email attachments, or infected websites. Once installed, spyware can run in the background without the user’s knowledge, sending the collected information to a remote server where it can be used for malicious purposes such as identity theft, fraud, or espionage.

To protect against spyware, it’s important to be cautious when downloading and installing software, particularly from unknown sources. Keep your operating system and software up-to-date with the latest security patches, use strong passwords and two-factor authentication, and avoid opening suspicious emails or downloading unknown files. It’s also a good idea to use antivirus software and regularly scan your computer or mobile device for spyware and other types of malware.

1. **Viruses**

A computer virus is a type of malware that is designed to replicate itself and spread from one computer to another. Like a biological virus, a computer virus can cause damage to a computer system or network by corrupting files, stealing data, or taking control of the infected system.

Viruses can be spread through a variety of methods, including email attachments, infected software downloads, and infected websites. Once a computer is infected with a virus, it can spread the virus to other computers through email or file-sharing networks.

To protect against viruses, it’s important to keep your operating system and software up-to-date with the latest security patches, use strong passwords and two-factor authentication, and avoid opening suspicious emails or downloading unknown files. It’s also a good idea to use antivirus software and regularly scan your computer for viruses and other types of malware. Additionally, be cautious when downloading and installing software, particularly from unknown sources, and only download software from trusted sources.

1. **Ransomware**

Ransomware is a type of malware that is designed to encrypt a user’s files and demand a ransom payment in exchange for the decryption key. Ransomware typically spreads through email attachments, infected software downloads, or infected websites, and once installed on a system, it can quickly encrypt all the files on the computer and any connected network drives.

The attackers behind ransomware demand a ransom payment, typically in Bitcoin or another cryptocurrency, in exchange for the decryption key to restore access to the encrypted files. Payment of the ransom is never guaranteed to result in the files being restored, and it can also encourage the attackers to continue their criminal activities.

To protect against ransomware, it’s important to keep your operating system and software up-to-date with the latest security patches, use strong passwords and two-factor authentication, and avoid opening suspicious emails or downloading unknown files. It’s also a good idea to use antivirus software and regularly back up important data to prevent data loss in case of a ransomware attack. Additionally, be cautious when downloading and installing software, particularly from unknown sources, and only download software from trusted sources.

**Causes**

1. Human Error: One of the most common causes of malware is human error, such as clicking on a malicious link, downloading an infected file, or opening an attachment from an unknown sender.
2. Vulnerabilities in Software: Software vulnerabilities are security flaws that can be exploited by hackers to gain access to a system. Malware can exploit these vulnerabilities to infect a system.
3. Outdated Software: If a software is not updated regularly, it can become vulnerable to malware. Malware creators often exploit outdated software to infect systems.
4. Unsecured Networks: Unsecured networks, such as public Wi-Fi hotspots, can be a breeding ground for malware. Hackers can use unsecured networks to gain access to systems and infect them with malware.
5. Social Engineering: Social engineering is a tactic used by hackers to trick people into revealing sensitive information or performing actions that can lead to malware infections. Examples of social engineering include phishing emails and fake software downloads.
6. Malicious Websites: Malicious websites can contain code that can infect .

**Preventions**

1. Install antivirus software: A good antivirus software can detect and remove most malware. Ensure that your antivirus software is updated regularly to keep up with the latest threats.
2. Keep your operating system and software updated: Ensure that your operating system and all software are updated with the latest security patches and updates. These updates often include fixes for vulnerabilities that can be exploited by malware.
3. Be cautious with email attachments and links: Do not open email attachments or click on links from unknown or suspicious sources. Malware can be spread through emails disguised as legitimate messages.
4. Use strong passwords: Use complex and unique passwords for your accounts and change them regularly. This makes it harder for hackers to gain access to your accounts.
5. Use a firewall: A firewall can help block unauthorized access to your computer or network. Ensure that your firewall is enabled and configured properly.
6. Backup your data: Regularly backup your data to an external hard drive or cloud storage. This can help you recover from a malware attack or other data loss incidents.

**How IT industry works**

The IT (Information Technology) industry is a vast and complex field that encompasses a wide range of products and services related to computer hardware, software, and digital communications. Here’s a general overview of how the IT industry works:

* Product Development: The IT industry is driven by innovation, and companies invest heavily in research and development to create new and better products. This can involve designing new computer hardware, developing new software applications, or improving existing products.
* Sales and Marketing: Once products are developed, IT companies need to promote them to potential customers. This involves creating marketing campaigns, identifying target markets, and building relationships with distributors and retailers.
* Distribution: IT products are typically sold through various channels, including online marketplaces, brick-and-mortar stores, and direct sales. Distributors and resellers play an important role in getting products to customers.
* Customer Support: IT companies also need to provide ongoing support to their customers. This includes technical support, troubleshooting, and customer service.
* Maintenance and Upgrades: IT products require ongoing maintenance and upgrades to ensure they continue to function properly and meet the evolving needs of customers. This can involve software updates, hardware repairs, and other types of maintenance.
* Security: As more and more data is stored and transmitted online, IT companies need to prioritize cybersecurity to protect their customers’ sensitive information from hacking and other security threats.

**How Google Identifies 12.4 million potentials phishing**

* Automated systems: Google uses machine learning algorithms to analyze email messages and identify patterns that are indicative of phishing attempts. For example, the system might flag an email that appears to be from a legitimate organization but contains a suspicious link.
* User reporting: Google encourages users to report suspicious emails through its “Report phishing” feature, which allows users to flag emails they believe to be phishing attempts. When a user reports an email, it is automatically flagged for review by Google’s systems.
* Blacklists: Google maintains blacklists of known phishing sites and email addresses that have been associated with phishing attempts. When a user receives an email from a blacklisted address or clicks on a link to a blacklisted site, they will be warned that the site is potentially harmful.
* Human review: In addition to automated systems, Google employs human reviewers who manually review flagged emails to determine whether they are phishing attempts. Reviewers look for signs of deception, such as attempts to impersonate a legitimate organization, and assess the potential harm to users.