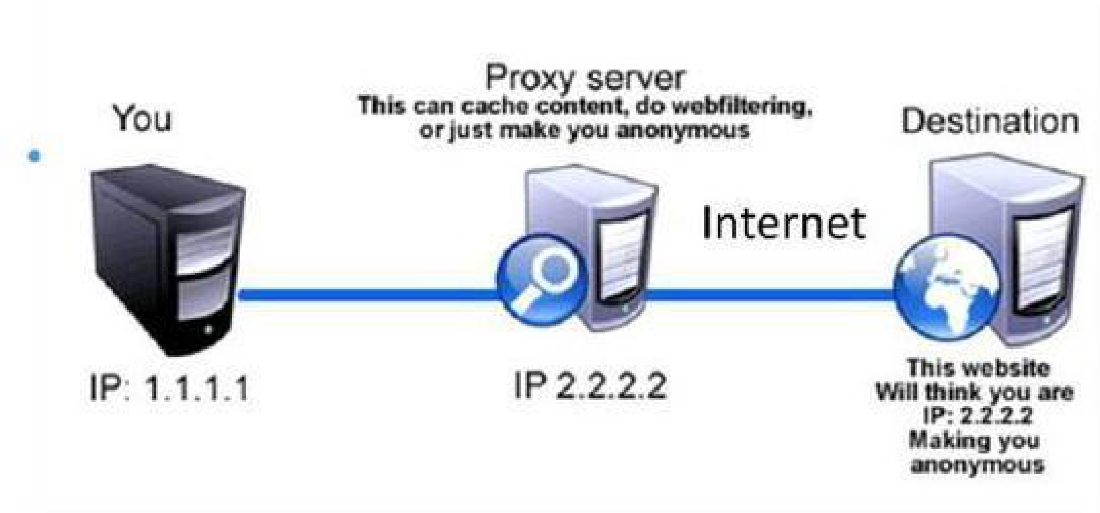
Class Notes - Unit - II

What is a Proxy Server?

A proxy server is another computer on the network which acts as an intermediary between your computer and other computers on the network.


You
Proxy server
This can cache content, do webfiltering, or just make you anonymous
Destination
Internet
IP: 1.1.1.1
IP 2.2.2.2
This website Will think you are IP: 2.2.2.2 Making you anonymous

The attacker machine connects through the proxy to access services provided by other computers (targets) on the network. The proxy server performs the requests on behalf of the attacker machine. The target machines on the network, on receiving the request, can see that the request is coming from a proxy machine but cannot see the actual identity of the attacker machine. Generally, attackers use proxies to hide their identity.

A proxy server has the following uses:

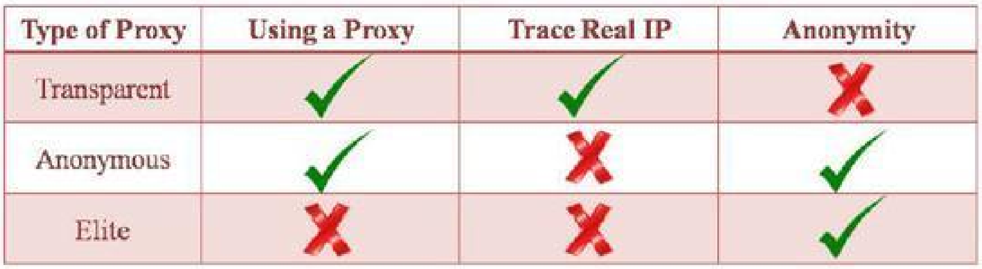
- Hide the company servers or systems
- Cache the frequently accessed web pages to improve the response time for the clients accessing those web pages
- Filtering inappropriate advertisements or for censoring illegal websites

- Can be used as a multiplexer for connecting many computers in a LAN or WAN exposing only one public IP address to the Internet
- Can be used for logging the traffic going in and out of the network

Types of proxies

Following are the types of proxies:

Transparent proxy – Victim will know you are using a proxy and can trace your real IP
Anonymous proxy – Victim will know you are using a proxy, but, cannot trace your real IP
Elite proxy – Victim doesn't know if the communication is from a proxy or not

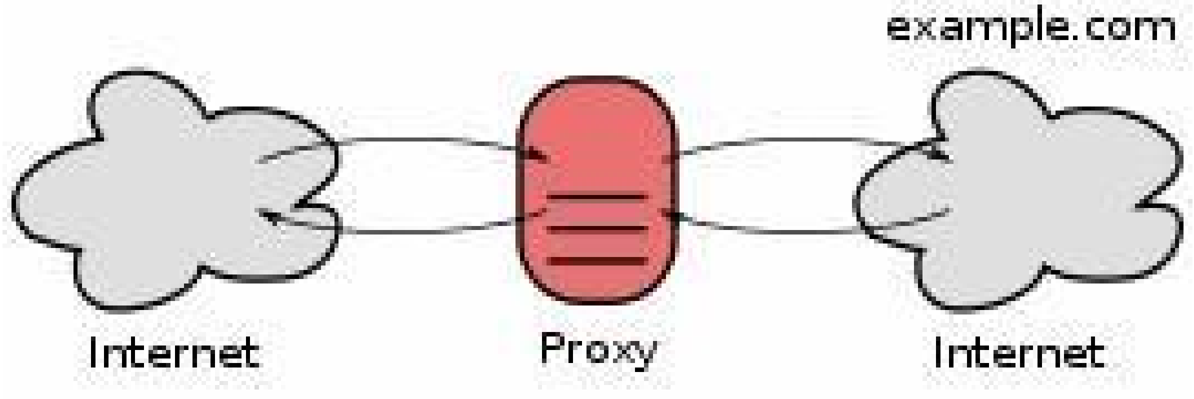


Type of Proxy	Using a Proxy	Trace Real IP	Anonymity
Transparent	✓	✓	✗
Anonymous	✓	✗	✓
Elite	✗	✗	✓

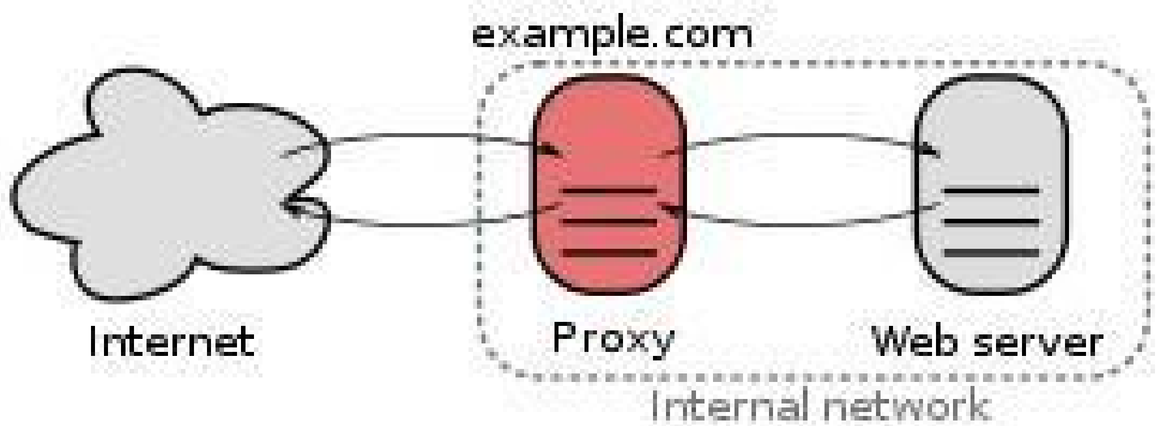
Types of proxy – A proxy server may reside on the user's local computer, or at various points between the user's computer and destination servers on the Internet.

- A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes a tunneling proxy.
- A forward proxy is an Internet-facing proxy used to retrieve from a wide range of sources (in most cases anywhere on the Internet).
- A reverse proxy is usually an Internet-facing proxy used as a front-end to control and protect access to a server on a private network. A reverse proxy commonly also performs tasks such as load-balancing, authentication, decryption or caching.

Open proxies – An open proxy is a forwarding proxy server that is accessible by any Internet user. Gordon Lyon estimates there are "hundreds of thousands" of open proxies on the Internet. An anonymous open proxy allows users to conceal their IP address while browsing the Web or using other Internet services. There are varying degrees of anonymity however, as well as a number of methods of ‘tricking’ the client into revealing itself regardless of the proxy being used.



Reverse proxies – A reverse proxy (or surrogate) is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more proxy servers which handle the request. The response from the proxy server is returned as if it came directly from the original server, leaving the client no knowledge of the origin servers. Reverse proxies are installed in the neighborhood of one or more web servers. All traffic coming from the Internet and with a destination of one of the neighborhood’s web servers goes through the proxy server. The use of “reverse” originates in its counterpart “forward proxy” since the reverse proxy sits closer to the web server and serves only a restricted set of websites.



There are several reasons for installing reverse proxy servers

- Encryption / SSL acceleration: when secure web sites are created, the SSL encryption is often not done by the web server itself, but by a reverse proxy that is equipped with SSL acceleration hardware. See Secure Sockets Layer. Furthermore, a host can provide a single “SSL proxy” to provide SSL encryption for an arbitrary number of hosts; removing the need for a separate SSL Server Certificate for each host, with the downside that all hosts behind the SSL proxy have to share a common DNS name or IP address for SSL connections. This problem can partly be overcome by using the SubjectAltName feature of X.509 certificates.
- Load balancing: the reverse proxy can distribute the load to several web servers, each web server serving its own application area. In such a case, the reverse proxy may need to rewrite the URLs in each web page (translation from externally known URLs to the internal locations).
- Serve/cache static content: A reverse proxy can offload the web servers by caching static content like pictures and other static graphical content.
- Compression: the proxy server can optimize and compress the content to speed up the load time.
- Spoon feeding: reduces resource usage caused by slow clients on the web servers by caching the content the web server sent and slowly “spoon feeding” it to the client. This especially benefits dynamically generated pages.
- Security: the proxy server is an additional layer of defense and can protect against some OS and Web Server specific attacks. However, it does not provide any protection from attacks against the web application or service itself, which is generally considered the larger threat.
- Extranet Publishing: a reverse proxy server facing the Internet can be used to communicate to a firewall server internal to an organization, providing extranet access to some functions while keeping the servers behind the firewalls. If used in this way, security measures should be considered to protect the rest of your infrastructure in case this server is compromised, as its web application is exposed to attack from the Internet.

If the destination server filters content based on the origin of the request, the use of a proxy can circumvent this filter. For example, a server using IP-based geolocation to restrict its service to a certain country can be accessed using a proxy located in that country to access the service.

Web proxies are the most common means of bypassing government censorship, although no more than 3% of Internet users use any circumvention tools. In some cases users can circumvent proxies which filter using blacklists using services designed to proxy information from a non-blacklisted location.

Proxies can be installed in order to eavesdrop upon the data-flow between client machines and the web. All content sent or accessed – including passwords submitted and cookies used – can be captured and analyzed by the proxy operator. For this reason, passwords to online services (such as webmail and banking) should always be exchanged over a cryptographically secured connection, such as SSL. By chaining proxies which do not reveal data about the original requester, it is possible to obfuscate activities from the eyes of the user's destination. However, more traces will be left on the intermediate hops, which could be used or offered up to trace the user's activities. If the policies and administrators of these other proxies are unknown, the user may fall victim to a false sense of security just because those details are out of sight and mind. In what is more of an inconvenience than a risk, proxy users may find themselves being blocked from certain Web sites, as numerous forums and Web sites block IP addresses from proxies known to have spammed or trolled the site. Proxy bouncing can be used to maintain your privacy.

What are Anonymizers?

An anonymizer is a tool that is used to conceal a user's identity when accessing the internet. Anonymizers work by hiding the user's IP address, making it difficult for websites to track the user's online activity.

There are several different types of anonymizers, including:

- VPN - A Virtual Private Network (VPN) is a type of anonymizer that creates an encrypted connection between the user's device and the internet. All traffic between the device and the internet is routed through the VPN, which conceals the user's IP address and provides an additional layer of security.

- TOR - The Onion Router (TOR) is a free software program that is used to conceal a user's online activity by routing their traffic through a network of servers. TOR is designed to be extremely difficult to trace, making it a popular choice for users who need to conceal their identity.
- Web-based anonymizers - Web-based anonymizers are online tools that allow users to browse the internet without revealing their IP address. These tools work by routing traffic through a third-party server, making it difficult for websites to track the user's online activity.

Benefits of Anonymizers

The primary benefits of using anonymizers include:

1. Anonymizers can provide users with a layer of privacy when accessing the internet, helping to conceal their online activity from prying eyes.
2. Anonymizers can help protect users from malware, viruses, and other types of attacks by creating an encrypted connection between the user's device and the internet.
3. Anonymizers can be used to access content that may be blocked or restricted in certain locations, such as geo-restricted content or websites that may be blocked by government or institutional firewalls.
4. Anonymizers can help protect a user's identity and personal information from being tracked and monitored by third parties, such as advertisers or hackers.
5. Anonymizers can also provide improved performance when browsing the internet, as they can reduce load times for certain types of content and reduce bandwidth usage.

Drawbacks of Anonymizers

While there are many benefits to using anonymizers, there are also some potential drawbacks that users should be aware of:

1. Some anonymizers may be created and maintained by individuals or groups with malicious intent, such as stealing personal information or financial data.

2. Anonymizers may not work with all types of internet activity or all websites and services, which can limit their usefulness.
3. Depending on the anonymizer used, there may be a reduction in internet speed due to the encryption process.
4. While anonymizers can often help bypass certain restrictions, there may be some limitations to their effectiveness, particularly if more advanced techniques are used to block access.

Phishing

Cybercrime is defined in simple words as a crime that is done online. Here, the medium used to commit crime digitally is the computer, network, internet, or any electronic device. The main targets of cybercrime are users of the system, websites, company defamation, gaining money, etc.

Some of the activities of cyber-criminals are listed below:

- Spread viruses and malware to cause harm to computers and sensitive data.
- Attacks a computer to reach the target or victim's computer via network.
- Hack the victim's system and steals confidential information from the user's data.
- Gaining unauthorized access to user accounts.
- Paving ways for online scams and frauds.
- Generate profit by selling or locking crucial data.

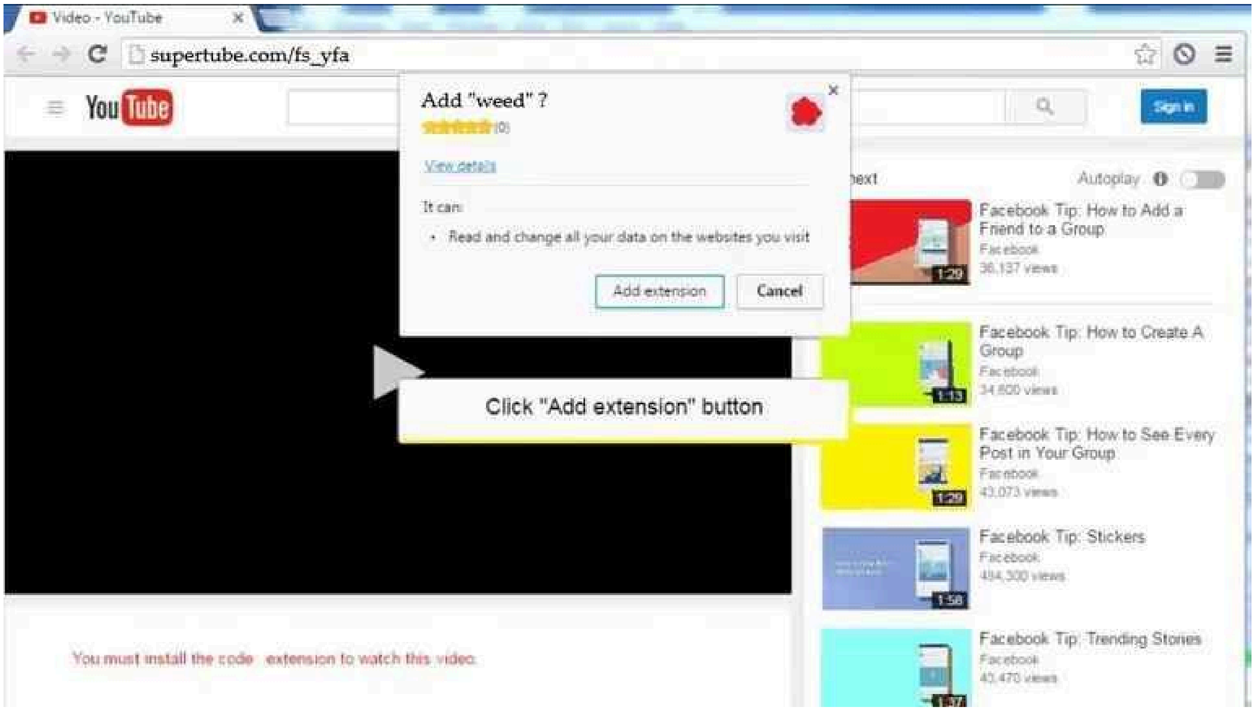
Phishing

Phishing is one type of cyber attack. Phishing got its name from "**phish**" meaning fish. It's a common phenomenon to put bait for the fish to get trapped. Similarly, phishing works. It is an unethical way to dupe the user or victim to click on harmful sites. The attacker crafts the harmful site in such a way that the victim feels it to be an authentic site, thus falling prey to it. The most common mode of phishing is by sending spam emails that appear to be authentic and thus, taking away all credentials from the victim. The main motive of the attacker behind phishing is to gain confidential information like

- Password
- Credit card details

- Social security numbers
- Date of birth

The attacker uses this information to further target the user and impersonate the user and cause data theft. The most common type of phishing attack happens through email. Phishing victims are tricked into revealing information that they think should be kept private. The original logo of the email is used to make the user believe that it is indeed the original email. But if we carefully look into the details, we will find that the URL or web address is not authentic. Let’s understand this concept with the help of an example:



Add "weed" ?

It can:

- Read and change all your data on the websites you visit

Click "Add extension" button

You must install the code extension to watch this video.

In this example, most people believe it’s YouTube just by looking at the red icon. So, thinking of YouTube as a secure platform, the users click on the extension without being suspicious about it. But if we look carefully, we can see the URL is supertube.com and not youtube.com. Secondly, YouTube never asks to add extensions for watching any video. The third thing is the extension name itself is weird enough to raise doubt about its credibility.

How Does Phishing Occur?

Below mentioned are the ways through which Phishing generally occurs. Upon using any of the techniques mentioned below, the user can lead to Phishing Attacks.

- **Clicking on an unknown file or attachment:** Here, the attacker deliberately sends a mysterious file to the victim, as the victim opens the file, either malware is injected into his system or it prompts the user to enter confidential data.
- **Using an open or free wifi hotspot:** This is a very simple way to get confidential information from the user by luring him by giving him free **wifi**. The wifi owner can control the user's data without the user knowing it.
- **Responding to social media requests:** This commonly includes social engineering. Accepting unknown friend requests and then, by mistake, leaking secret data are the most common mistake made by naive users.
- **Clicking on unauthenticated links or ads:** Unauthenticated links have been deliberately crafted that lead to a phished website that tricks the user into typing confidential data.

Types of Phishing Attacks

There are several types of Phishing Attacks, some of them are mentioned below. Below mentioned attacks are very common and mostly used by the attackers.

- **Email Phishing:** The most common type where users are tricked into clicking unverified spam emails and leaking secret data. Hackers impersonate a legitimate identity and send emails to mass victims. Generally, the goal of the attacker is to get personal details like bank details, credit card numbers, user IDs, and passwords of any online shopping website, installing malware, etc. After getting the personal information, they use this information to steal money from the user's account or harm the target system, etc.
- **Spear Phishing:** In spear phishing of phishing attack, a particular user(organization or individual) is targeted. In this method, the attacker first gets the full information of the target and then sends malicious emails to his/her inbox to trap him into typing confidential data. For example, the attacker targets someone(let's assume an employee from the finance department of some organization). Then the attacker pretends to be like the manager of that employee and then requests personal information or transfers a large sum of money. It is the most successful attack.

- **Whaling:** Whaling is just like spear-phishing but the main target is the head of the company, like the CEO, CFO, etc. a pressurized email is sent to such executives so that they don't have much time to think, therefore falling prey to phishing.
- **Smishing:** In this type of phishing attack, the medium of phishing attack is SMS. Smishing works similarly to email phishing. SMS texts are sent to victims containing links to phished websites or invite the victims to call a phone number or to contact the sender using the given email. The victim is then invited to enter their personal information like bank details, credit card information, user id/ password, etc. Then using this information the attacker harms the victim.
- **Vishing:** Vishing is also known as voice phishing. In this method, the attacker calls the victim using modern caller id spoofing to convince the victim that the call is from a trusted source. Attackers also use IVR to make it difficult for legal authorities to trace the attacker. It is generally used to steal credit card numbers or confidential data from the victim.
- **Clone Phishing:** Clone Phishing this type of phishing attack, the attacker copies the email messages that were sent from a trusted source and then alters the information by adding a link that redirects the victim to a malicious or fake website. Now the attacker sends this mail to a larger number of users and then waits to watch who clicks on the attachment that was sent in the email. It spreads through the contacts of the user who has clicked on the attachment.

Impact of Phishing

These are the impacts on the user upon affecting the Phishing Attacks. Each person has their own impact after getting into Phishing Attacks, but these are some of the common impacts that happen to the majority of people.

- **Financial Loss:** Phishing attacks often target financial information, such as credit card numbers and bank account login credentials. This information can be used to steal money or make unauthorized purchases, leading to significant financial losses.
- **Identity Theft:** Phishing attacks can also steal personal information, such as Social Security numbers and date of birth, which can be used to steal an individual's identity and cause long-term harm.

- **Damage to Reputation:** Organizations that fall victim to phishing attacks can suffer damage to their reputation, as customers and clients may lose trust in the company's ability to protect their information.
- **Disruption to Business Operations:** Phishing attacks can also cause significant disruption to business operations, as employees may have their email accounts or computers compromised, leading to lost productivity and data.
- **Spread of Malware:** Phishing attacks often use attachments or links to deliver malware, which can infect a victim's computer or network and cause further harm.

Signs of Phishing

It is very much important to be able to identify the signs of a phishing attack in order to protect against its harmful effects. These signs help the user to protect user data and information from hackers. Here are some signs to look out for include:

- **Suspicious email addresses:** Phishing emails often use fake email addresses that appear to be from a trusted source, but are actually controlled by the attacker. Check the email address carefully and look for slight variations or misspellings that may indicate a fake address.
- **Urgent requests for personal information:** Phishing attacks often try to create a sense of urgency in order to trick victims into providing personal information quickly. Be cautious of emails or messages that ask for personal information and make sure to verify the authenticity of the request before providing any information.
- **Poor grammar and spelling:** Phishing attacks are often created quickly and carelessly, and may contain poor grammar and spelling errors. These mistakes can indicate that the email or message is not legitimate.
- **Requests for sensitive information:** Phishing attacks often try to steal sensitive information, such as login credentials and financial information. Be cautious of emails or messages that ask for sensitive information and verify the authenticity of the re
- quest before providing any information.
- **Unusual links or attachments:** Phishing attacks often use links or attachments to deliver malware or redirect victims to fake websites. Be cautious of links or attachments in emails or messages, especially from unknown or untrusted sources.
- **Strange URLs:** Phishing attacks often use fake websites that look similar to the real ones, but have slightly different URLs. Look for strange URLs or slight variations in the URL that may indicate a fake website.

How To Stay Protected Against Phishing?

Until now, we have seen how a user becomes so vulnerable due to phishing. But with proper precautions, one can avoid such scams. Below are the ways listed to protect users against phishing attacks:

- **Authorized Source:** Download software from authorized sources only where you have trust.

- **Confidentiality:** Never share your private details with unknown links and keep your data safe from hackers.
- **Check URL:** Always check the URL of websites to prevent any such attack. it will help you not get trapped in Phishing Attacks.
- **Avoid replying to suspicious things:** If you receive an email from a known source but that email looks suspicious, then contact the source with a new email rather than using the reply option.
- **Phishing Detection Tool:** Use phishing-detecting tools to monitor the websites that are crafted and contain unauthentic content.
- **Try to avoid free wifi:** Avoid using free Wifi, it will lead to threats and Phishing.
- **Keep your system updated:** It's better to keep your system always updated to protect from different types of Phishing Attacks.
- **Keep the firewall of the system ON:** Keeping ON the firewalls helps you in filtering ambiguous and suspicious data and only authenticated data will reach to you.

How To Distinguish between a Fake Website and a Real Website?

It is very important nowadays to protect yourself from fake websites and real websites. Here are some of the ways mentioned through which you can identify which websites are real and which ones are fake. To distinguish between a fake website and a real website always remember the following points:

- **Check the URL of the website:** A good and legal website always uses a secure medium to protect yourself from online threats. So, when you first see a website link, always check the beginning of the website. That means if a website is started with https:// then the website is secure because https:// s denotes secure, which means the website uses encryption to transfer data, protecting it from hackers. If a website uses http:// then the website is not guaranteed to be safe. So, it is advised not to visit HTTP websites as they are not secure.
- **Check the domain name of the website:** The attackers generally create a website whose address mimic of large brands or companies like www.amazon.com/order_id=23. If we look closely, we can see that it's a fake website as the spelling of Amazon is wrong, that is amazon is written. So it's a phished website. So be careful with such types of websites.

- **Look for site design:** If you open a website from the link, then pay attention to the design of the site. Although the attacker tries to imitate the original one as much as possible, they still lack in some places. So, if you see something off, then that might be a sign of a fake website. For example, www.sugarcube.com/facebook, when we open this URL the page open is cloned to the actual Facebook page but it is a fake website. The original link to Facebook is www.facebook.com.
- **Check for the available web pages:** A fake website does not contain the entire web pages that are present in the original website. So when you encounter fake websites, then open the option(links) present on that website. If they only display a login page, then the website is fake.

Anti-Phishing Tools

Well, it's essential to use Anti-Phishing tools to detect phishing attacks. Here are some of the most popular and effective anti-phishing tools available:

- **Anti-Phishing Domain Advisor (APDA):** A browser extension that warns users when they visit a phishing website. It uses a database of known phishing sites and provides real-time protection against new threats.
- **PhishTank:** A community-driven website that collects and verifies reports of phishing attacks. Users can submit phishing reports and check the status of suspicious websites.
- **Webroot Anti-Phishing:** A browser extension that uses machine learning algorithms to identify and block phishing websites. It provides real-time protection and integrates with other security tools.
- **Malwarebytes Anti-Phishing:** A security tool that protects against phishing attacks by detecting and blocking suspicious websites. It uses a combination of machine learning and signature-based detection to provide real-time protection.
- **Kaspersky Anti-Phishing:** A browser extension that provides real-time protection against phishing attacks. It uses a database of known phishing sites and integrates with other security tools to provide comprehensive protection.

Note: These anti-phishing tools can provide an additional layer of protection against phishing attacks, but it is important to remember that they are not a complete solution. Users should also be cautious of suspicious emails and messages and practice safe browsing habits to minimize their risk of falling victim to phishing attacks.

Password Cracking

Password cracking is the most enjoyable hacks for bad guys. It increases the sense of exploration and useful in figuring out the password. The password cracking may not have a burning desire to hack the password of everyone. The actual password of the user is not stored in the well-designed password-based authentication system. Due to this, the hacker can easily access to user's account on the system. Instead of a password, a password hash is stored by the authentication system. The hash function is a one-way design. It means it is difficult for a hacker to find the input that produces a given output. The comparison of the real password and the comparison of two password hash are almost good. The hash function compares the stored password and the hash password provided by the user. In the password cracking process, we extract the password from an associated passwords hash. Using the following ways, we can accomplish it:

Dictionary attack: Most of the users use common and weak passwords. A hacker can quickly learn about a lot of passwords if we add a few punctuations like substitute $ for S and take a list of words.

Brute-force guessing attack: A given length has so many potential passwords. If you use a brute-force attack, it will guarantee that a hacker will eventually crack the password.

Hybrid Attack: It is a combination of Dictionary attack and Brute force attack techniques. This attack firstly tries to crack the password using the dictionary attack. If it is unsuccessful in cracking the password, it will use the brute-force attack.

How to create a strong password

There are 12 tools for password cracking. These tools use different password cracking algorithm to crack the password. Mostly tools of password cracking are free. So you should maintain a strong password. The following tips are important while creating the password:

- The most important factor is **password length**. The Length of password increases the complexity of password guessing brute force attack. The password can be cracked in a minute if it is made by random 7 characters. If the password is 10 characters, it takes more time as compared to 7 characters.
- The **brute force password guessing** will become more difficult if the user uses a variety of characters. Due to this, the hackers have to try various options for each password's character. Special characters and incorporate numbers also increase the difficulty for the hacker.
- In the **credential stuffing attack**, the hacker uses the stolen password from one online account to the other accounts. So it would be best to use a unique, random and long password for all your online accounts.

What to avoid for a strong password

Cybercriminal or hacker knows all the clever tricks that users use while creating their passwords. Some common avoidable password mistakes are as follows:

Dictionary word: Using the dictionary attacks, every word in the dictionary is tested in seconds.

Personal information: The dictionary words are birthplace, relative's name, birthdate, favorite name, pet's name, your name and so on. If they are not, there are various tools in the market that grab the information of the users from social media and build a wordlist for the hackers.

Patterns: Most commonly used passwords are asdfgh, qwerty, 123457678, 1111111, and so on. Every password cracker has these passwords on their list.

Character Substitution: The well-known character substitutions are $ for S and 4 for A. These substitutions are automatically tested by dictionary attacks.

Number and special character: Most people use a special character and number at the end of the password. The password cracker developer uses these patterns.

Common passwords: Some companies like Splashdata publish a list every year which contains the most commonly used passwords. Just like the attacker, they crack the breached password and create these lists. While creating the password, you should never use these lists.

Random password: You should maintain your online account password as unique, random and long. To store the password for online accounts, you should use the password manager.

Keyloggers

Key loggers also known as keystroke loggers, may be defined as the recording of the key pressed on a system and saved it to a file, and the that file is accessed by the person using this malware. Key logger can be software or can be hardware. **Working:** Mainly key-loggers are used to steal password or confidential details such as bank information etc. First key-logger was invented in 1970's and was a hardware key logger and first software key-logger was developed in 1983.

1. Software key-loggers : Software key-loggers are the computer programs which are developed to steal password from the victims computer. However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Also Microsoft windows 10 also has key-logger installed in it.

1. **JavaScript based key logger –** It is a malicious script which is installed into a web page, and listens for key to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file.
2. **Form Based Key loggers –** These are key-loggers which activates when a person fills a form online and when click the button submit all the data or the words written is sent via file on a computer. Some key-loggers works as a API in running application it looks like a simple application and whenever a key is pressed it records it.

2. Hardware Key-loggers : These are not dependent on any software as these are hardware key-loggers. keyboard hardware is a circuit which is attached in a keyboard itself that whenever the key of that keyboard pressed it gets recorded.

1. **USB keylogger –** There are USB connector key-loggers which has to be connected to a computer and steals the data. Also some circuits are built into a keyboard so no external wire i used or shows on the keyboard.
2. **Smartphone sensors –** Some cool android tricks are also used as key loggers such as android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique accuracy is about 80%. Now a days crackers are using keystroke logging Trojan, it is a malware which is sent to a victims computer to steal the data and login details.

So key-loggers are the software malware or a hardware which is used to steal , or snatch our login details, credentials , bank information and many more. Some keylogger application used in 2020 are:

1. Kidlogger

2. Best Free Keylogger

3. Windows Keylogger

4. Refog Personal Monitor

5. All In One Keylogger

Prevention from key-loggers : These are following below-

1. **Anti-Key-logger –** As the name suggest these are the software which are anti / against key loggers and main task is to detect key-logger from a computer system.
2. **Anti-Virus –** Many anti-virus software also detect key loggers and delete them from the computer system. These are software anti-software so these can not get rid from the hardware key-loggers.
3. **Automatic form filler –** This technique can be used by the user to not fill forms on regular bases instead use automatic form filler which will give a shield against key-loggers as keys will not be pressed .
4. **One-Time-Passwords –** Using OTP's as password may be safe as every time we login we have to use a new password.
5. **Patterns or mouse-recognition –** On android devices used pattern as a password of applications and on PC use mouse recognition, mouse program uses mouse gestures instead of stylus.
6. **Voice to Text Converter** – This software helps to prevent Keylogging which targets a specific part of our keyboard.

These techniques are less common but are very helpful against key-loggers.

Spyware

Spyware is a breach of cyber security as they usually get into the laptop/ computer system when a user unintentionally clicks on a random unknown link or opens an unknown attachment, which downloads the spyware alongside the attachment. It is a best practice to be cautious of the sites that are used for downloading content on the system. Spyware is a type of software that unethically without proper permissions or authorization steals a user's personal or business information and sends it to a third party. Spyware may get into a computer or laptop as a hidden component through free or shared wares.

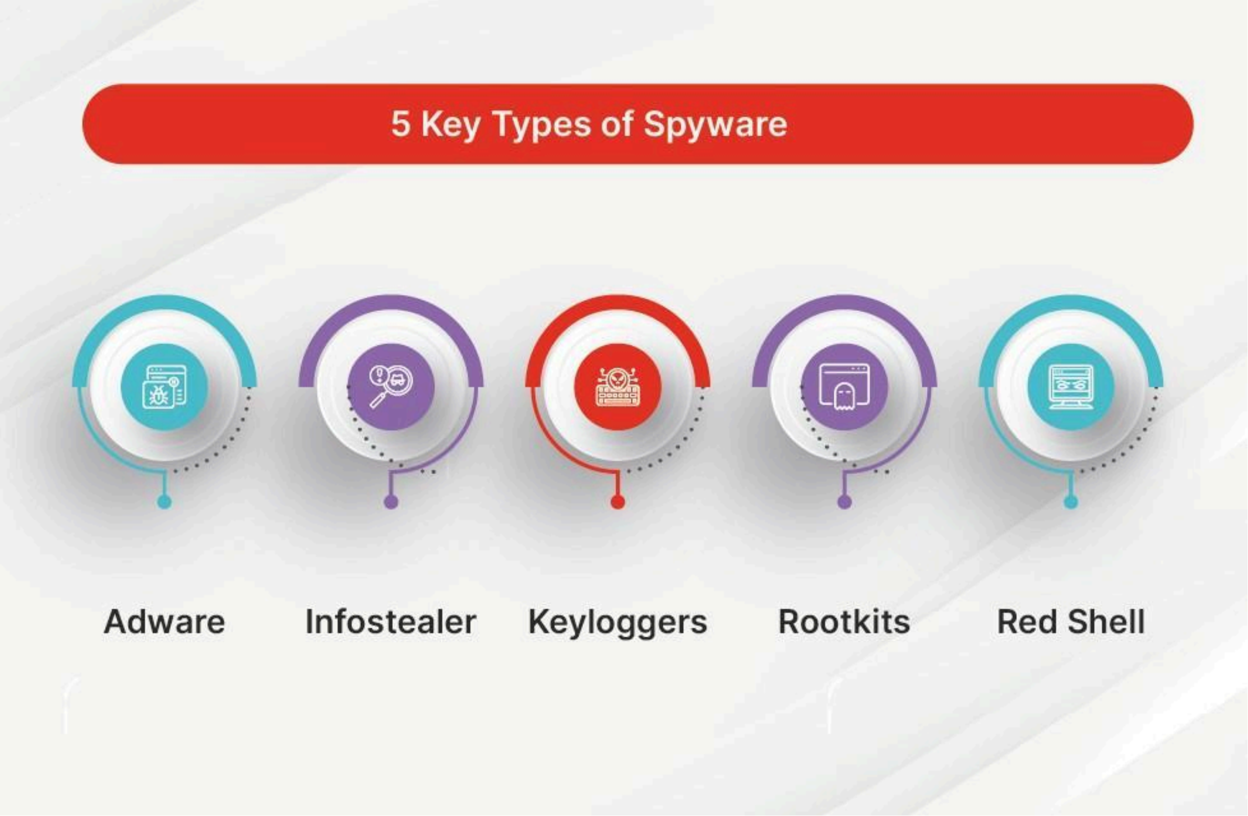
Spywares perform the function of maliciously tracking a user's activity, having access to data, or even resulting in the crashing of the computer/ laptop system. Spyware in many cases runs as a background process and slows down the normal functioning of the computer system.

Spyware enters the laptop/computer system through the below-listed ways:

- **Phishing:** It is a form of a security breach where spyware enters the system when a suspicious link is clicked or an unknown dangerous attachment is downloaded.
- **Spoofing:** It goes alongside phishing and makes the unauthorized emails appear to come from legitimate users or business units.
- **Free Softwares or Shared Softwares:** It gets into the system when a user installs software that is free of cost but has additional spyware added to them.
- **Misleading software:** This is advertised as very beneficial for the system and would boost up the speed of the system but lead to stealing confidential information from the system.

How does Spyware Enter the Computer System?

Spyware entering the system is very dangerous and therefore proper knowledge of them can save a lot of trusted information from being accessible to third-party. Spywares are classified on the basis of the function they perform. There are different types of Spyware, which can attack our system. These are listed as below:



- **Adware:** It is a type of Spyware that keeps track of the user’s activity and gives advertisements based on the tracked activity of the user.
- **Tracking Cookies:** It is a type of Spyware that tracks a user’s activity and supplies the same to third parties.
- **Trojans:** It is a type of Spyware that is the most dangerous. It aims to steal confidential user information such as bank details, passwords and transfers it to a third party to perform illegal transactions or frauds.
- **Keyloggers:** It is a type of Spyware that keeps a track of all the keystrokes that the user enters through the keyboard. It is dangerous as it contributes bro cyber fraud where sensitive passwords can be stolen by keeping an eye on the user who entered the information.
- **Stalkerware:** It is a type of Spyware that is installed on mobile phones to stalk the user. It tracks the movement of the user and sends the same to the third party.

- **System Monitor:** It is a type of Spyware that monitors and keep a track of the entire system including users activity, sensitive information, keystrokes, calls, and chats. It is extremely dangerous to user privacy.

How Spyware Infects Devices?

Spyware gets attached to websites and downloads without going much into the notice of the user. There are many software's that get downloaded without any warning alongside the needed software and are very dangerous for our computer system. Another way of spyware, entering our systems is when the user clicks unverified links or downloads malicious contents on the computer system.

When spyware enters the computer system it unethically accesses the information that it is not authorized to view. In most cases, it also supplies this information to third-party users leading to data leaks. Sensitive information such as passwords and bank information are at much risk if spyware enters the computer system. Data leak, stealing of sensitive information, tracking user's activity/ preferences, making the system slow down, and even crashing the computer system are the effects that can be caused when spyware enters the computer system without the user's consent.

How to Prevent Spyware?

- **Installing Antivirus/ Antispyware:** The best way to protect your system from spyware is to install a good quality Anti-spyware or Antivirus such as MalwareBytes, Adaware, AVG Antivirus, SpywareBlaster, etc. This will help in protecting the computer system in case spyware tries to attach to our system. Installing Antivirus/ Antispyware also protects the system from harmful threats by blocking sites that try to steal data or leak the data to third-party users.
- **Beware of Cookie Settings:** There are some websites that transfer confidential information alongside cookies. It is always advisable to keep a check on the cookie settings and set the settings to high security.
- **Beware of the Pop-ups on Websites:** Don't click on the pop-ups that appear on your website without reading them. Never accept their terms and conditions as it is highly dangerous. Always close the pop-up windows without clicking on 'ok'.

- **Never Install Free Software:** Always be very cautious when you install free software on your systems. Free software mostly has spyware attached to them and it can directly leak confidential user information.
- **Always read Terms & Conditions:** Always read Terms and Conditions before installing apps on your system. Never accept policies that breach privacy. Download only trusted and verified apps from Google PlayStore or Apple PlayStore for mobile phones to protect them from Spyware.

Computer Virus Definition

Chances are you've heard how important it is to keep viruses out, but what is a computer virus exactly? A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software.

Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage. A key thing to know about computer viruses is that they are designed to spread across programs and systems. Computer viruses typically attach to an executable host file, which results in their viral codes executing when a file is opened. The code then spreads from the document or software it is attached to via networks, drives, file-sharing programs, or infected email attachments.

Common Signs of Computer Viruses

Chances are you've heard how important it is to keep viruses out, but what is a computer virus exactly? A computer virus will more than likely have an adverse effect on the device it resides on and may be discoverable through common signs of performance loss, including:

Speed of System

A computer system running slower than usual is one of the most common signs that the device has a virus. This includes the system itself running slowly, as well as applications and internet speed suffering. If a computer does not have powerful applications or programs installed and is running slowly, then it may be a sign it is infected with a virus.

Pop-up Windows

Unwanted pop-up windows appearing on a computer or in a web browser are a telltale sign of a computer virus. Unwanted pop-ups are a sign of malware, viruses, or spyware affecting a device.

Programs Self-executing

If computer programs unexpectedly close by themselves, then it is highly likely that the software has been infected with some form of virus or malware. Another indicator of a virus is when applications fail to load when selected from the Start menu or their desktop icon. Every time that happens, your next step should be to perform a virus scan and remove any files on programs that might not be safe to use.

Accounts Being Logged Out

Some viruses are designed to affect specific applications, which will either cause them to crash or force the user to automatically log out of the service.

Crashing of the Device

System crashes and the computer itself unexpectedly closing down are common indicators of a virus. Computer viruses cause computers to act in a variety of strange ways, which may include opening files by themselves, displaying unusual error messages, or clicking keys at random.

Mass Emails Being Sent from Your Email Account

Computer viruses are commonly spread via email. Hackers can use other people's email accounts to spread malware and carry out wider cyberattacks. Therefore, if an email account has sent emails in the outbox that a user did not send, then this could be a sign of a computer virus.

Changes to Y our Homepage

Any unexpected changes to a computer—such as your system’s homepage being amended or any browser settings being updated—are signs that a computer virus may be present on the device.

How Do Computer Viruses Attack and Spread?

In the early days of computers, viruses were spread between devices using floppy disks. Nowadays, viruses can still be spread via hard disks and Universal Serial Bus (USB) devices, but they are more likely to be passed between devices through the internet.

Computer viruses can be spread via email, with some even capable of hijacking email software to spread themselves. Others may attach to legitimate software, within software packs, or infect code, and other viruses can be downloaded from compromised application stores and infected code repositories. A key feature of any computer virus is it requires a victim to execute its code or payload, which means the host application should be running.

Types of Computer Viruses

There are several types of computer viruses that can infect devices. This section will cover computer virus protections and how to get rid of computer viruses.

Resident Virus

Viruses propagate themselves by infecting applications on a host computer. A resident virus achieves this by infecting applications as they are opened by a user. A non-resident virus is capable of infecting executable files when programs are not running.

Multipartite Virus

A multipartite virus uses multiple methods to infect and spread across computers. It will typically remain in the computer's memory to infect the hard disk, then spread through and infect more drives by altering the content of applications. This results in performance lag and application memory running low.

Multipartite viruses can be avoided by not opening attachments from untrusted sources and by installing trusted antivirus software. It can also be prevented by cleaning the boot sector and the computer's entire disk.

Direct Action

A direct-action virus accesses a computer's main memory and infects all programs, files, and folders located in the autoexec.bat path, before deleting itself. This virus typically alters the performance of a system but is capable of destroying all data on the computer's hard disk and any USB device attached to it. Direct action viruses can be avoided through the use of antivirus scanners. They are easy to detect, as is restoring infected files.

Browser Hijacker

A browser hijacker manually changes the settings of web browsers, such as replacing the homepage, editing the new tab page, and changing the default search engine. Technically, it is not a virus because it cannot infect files but can be hugely damaging to computer users, who often will not be able to restore their homepage or search engine. It can also contain adware that causes unwanted pop-ups and advertisements.

Browser hijackers typically attach to free software and malicious applications from unverified websites or app stores, so only use trusted software and reliable antivirus software.

Overwrite Virus

Overwrite viruses are extremely dangerous. They can delete data and replace it with their own file content or code. Once files get infected, they cannot be replaced, and the virus can affect Windows, DOS, Linux, and Apple systems. The only way this virus can be removed is by deleting all of the files it has infected, which could be devastating. The best way to protect against the overwrite virus is to use a trusted antivirus solution and keep it updated.

Web Scripting Virus

A web scripting virus attacks web browser security, enabling a hacker to inject web-pages with malicious code, or client-side scripting. This allows cyber criminals to attack major websites, such as social networking sites, email providers, and any site that enables user input or reviews. Attackers can use the virus to send spam, commit fraudulent activity, and damage server files.

Protecting against web scripting is reliant on deploying real-time web browser protection software, using cookie security, disabling scripts, and using malicious software removal tools.

File Infector

A file infector is one of the most common computer viruses. It overwrites files when they are opened and can quickly spread across systems and networks. It largely affects files with .exe or .com extensions. The best way to avoid file infector viruses is to only download official software and deploy an antivirus solution.

Network Virus

Network viruses are extremely dangerous because they can completely cripple entire computer networks. They are often difficult to discover, as the virus could be hidden within any computer on an infected network. These viruses can easily replicate and spread by using the internet to transfer to devices connected to the network. Trusted, robust antivirus solutions and advanced firewalls are crucial to protecting against network viruses.

Boot Sector Virus

A boot sector virus targets a computer’s master boot record (MBR). The virus injects its code into a hard disk’s partition table, then moves into the main memory when a computer restarts. The presence of the virus is signified by boot-up problems, poor system performance, and the hard disk becoming unable to locate. Most modern computers come with boot sector safeguards that restrict the potential of this type of virus.

Steps to protecting against a boot sector virus include ensuring disks are write-protected and not starting up a computer with untrusted external drives connected.

Know More About Computer Viruses Through Examples

There are common examples of what computer and internet users believe to be viruses, but are technically incorrect.

Is Trojan a Virus?

A Trojan horse is a type of program that pretends to be something it is not to get onto a device and infect it with malware. Therefore, a Trojan horse virus is a virus disguised to look like something it is not. For example, viruses can be hidden within unofficial games, applications, file-sharing sites, and bootlegged movies.

Is a Worm a Virus?

A computer worm is not a virus. Worms do not need a host system and can spread between systems and networks without user action, whereas a virus requires users to execute its code.

Is Ransomware a virus?

Ransomware is when attackers lock victims out of their system or files and demand a ransom to unlock access. Viruses can be used to carry out ransomware attacks.

Is Rootkit a virus?

A rootkit is not a virus. Rootkits are software packages that give attackers access to systems. They cannot self-replicate or spread across systems.

Is a Software Bug a virus?

"Bug" is a common word used to describe problems with computers, but a software bug is not a virus. A bug is a flaw or mistake in software code, which hackers can exploit to launch a cyberattack or spread malware.

How To Prevent Your Computer from Viruses

There are several ways to protect your computer from viruses, including:

Use a Trusted Antivirus Product

Trusted computer antivirus products are crucial to stop malware attacks and prevent computers from being infected with viruses. These antivirus concepts will protect devices from being infected through regular scans and identifying and blocking malware.

Avoid Clicking Pop-up Advertisements

Unwanted pop-up advertisements are more than likely to be linked to computer viruses and malware. Never click on pop-up advertisements because this can lead to inadvertently downloading viruses onto a computer.

Scan Your Email Attachments

A popular way to protect your device from computer viruses is to avoid suspicious email attachments, which are commonly used to spread malware. Computer antivirus solutions can be used to scan email attachments for potential viruses.

Scan the Files That You Download Using File-sharing Programs

File-sharing programs, particularly unofficial sites, are also popular resources for attackers to spread computer viruses. Avoid downloading applications, games, or software from unofficial sites, and always scan files that have been downloaded from any file-sharing program.

History of computer viruses

Today's malware authors owe a lot to the cybercriminals of yesteryear. All the tactics and techniques employed by cybercriminals creating modern malware were first seen in early viruses. Things like Trojans, ransomware, and polymorphic code. These all came from early computer viruses. To understand the threat landscape of today, we need to peer back through time and look at the viruses of yesteryear.

1949, John von Neumann and "self-reproducing machines"

It was in those salad days of computing that mathematician, engineer, and polymath John von Neumann delivered a lecture on the Theory and Organization of Complicated Automata in which he first argued that computer programs could "self-reproduce." In an era where computers were the size of houses, and programs were stored on mile-long punch tapes, Neumann's ideas must've sounded like something from a sci-fi pulp novel.

1982, The proto computer-virus

In 1982 a fifteen-year-old boy pranking his friends proved Neumann's theory a reality. Rich Skrenta's Elk Cloner is widely regarded as the first proto-computer virus (the term "computer virus" didn't exist just yet). Elk Cloner targeted Apple II computers, causing infected machines to display a poem from Skrenta:

Elk Cloner: The program with a personality
It will get on all your disks
It will infiltrate your chips
Yes, it's Cloner!

It will stick to you like glue
It will modify RAM too
Send in the Cloner!

Other notable firsts—Elk Cloner was the first virus to spread via detachable storage media (it wrote itself to any floppy disk inserted into the computer). For many years to come, that's how viruses travelled across systems—via infected floppy disk passed from user to user.

1984, Computer virus, defined

In 1984 computer scientist Fred Cohen handed in his graduate thesis paper, *Computer Viruses – Theory and Experiments* in which he coined the term "computer virus," which is great because "complicated self-reproducing automata" is a real mouthful. In the same paper, Cohen also gave us our first definition of "computer virus" as "a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself."

1984, Core War

Up to this point, most talk about computer viruses happened only in the rarified air of college campuses and research labs. But a 1984 *Scientific American* article let the virus out of the lab. In the piece, author and computer scientist A.K. Dewdney shared the details of an exciting new computer game of his creation called Core War. In the game, computer programs vie for control of a virtual computer.

The game was essentially a battle arena where computer programmers could pit their viral creations against each other. For two dollars Dewdney would send detailed instructions for setting up your own Core War battles within the confines of a virtual computer. What would happen if a battle program was taken out of the virtual computer and placed on a real computer system?

In a follow-up article for Scientific American, Dewdney shared a letter from two Italian readers who were inspired by their experience with Core War to create a real virus on the Apple II. It's not a stretch to think other readers were similarly inspired.

1986, the first PC virus

The Brain virus was the first to target Microsoft's text-based Windows precursor, MS-DOS. The brainchild of Pakistani brothers and software engineers, Basit and Amjad Farooq, Brain acted like an early form of copyright protection, stopping people from pirating their heart monitoring software.

If the target system contained a pirated version of the brother's software, the "victim" would receive the on-screen message, "WELCOME TO THE DUNGEON . . . CONTACT US FOR VACCINATION" along with the brothers' names, phone number, and business address in Pakistan. Other than guilt tripping victims in to paying for their pirated software, Brain had no harmful effects.

Speaking with *F-Secure*, Basit called Brain a "very friendly virus." Amjad added that today's viruses, the descendants of Brain, are "a purely criminal act."

Worm Virus Definition

A worm virus refers to a malicious program that replicates itself, automatically spreading through a network. In this definition of computer worms, the worm virus exploits vulnerabilities in your security software to steal sensitive information, install backdoors that can be used to access the system, corrupt files, and do other kinds of harm.

Worms consume large volumes of memory, as well as bandwidth. This results in servers, individual systems, and networks getting overloaded and malfunctioning. A worm is different from a virus, however, because a worm can operate on its own while a virus needs a host computer.

Classifications and Names of Worms

Email-Worm

An email-worm refers to a worm that is able to copy itself and spread through files attached to email messages.

IM-Worm

An Instant Messenger (IM) worm is a kind of worm that can spread through IM networks. When an IM-worm is operating, it typically finds the address book belonging to the user and tries to transmit a copy of itself to all of the person's contacts.

IRC-Worm

An IRC-worm makes use of Internet Relay Chat (IRC) networks to send itself over to other host machines. An IRC-worm drops a script into the IRC's client directory within the machine it infects.

Net-Worm

A net-worm refers to a kind of worm that can find new hosts by using shares made over a network. This is done using a server or hard drive that multiple computers access via a local-area network (LAN).

P2P-Worm

A P2P-worm is spread through peer-to-peer (P2P) networks. It uses the P2P connections to send copies of itself to users.

How Do Worm Virus/Computer Worms Work and Spread?

To get a worm in a computer, the worm is often transmitted through vulnerabilities in software. They could also be sent through email attachments or within instant messages or spam emails. After a file is opened, it may link the user to a malicious website or it could download the worm to the user’s device automatically. After the worm is on the device, it infects it without the user being able to tell.

Worms have the ability to delete and modify files. They can also inject more malicious software into a workstation or other device. Sometimes, the worm’s primary mission is to replicate itself again and again—simply to waste system resources, like bandwidth or hard drive space. Worms can also steal sensitive data and pave a way for a hacker to get into the computer by installing a backdoor they can access.

Files Sent as Email Attachments

The user clicks on a file attached to an email and the worm is activated.

Via a Link to a Web or FTP Resource

When the user clicks a link to a web or File Transfer Protocol (FTP) resource, the worm is automatically downloaded to their machine.

Via a Link Sent in an ICQ or IRC Message

An I Seek You (ICQ) or IRC message can contain a link to a worm, which, when clicked, can install the worm on the user’s device.

Through Network Packets

Network packets can penetrate into the computer’s memory. At that point, the worm gets activated, infecting the host computer.

Via Peer-to-Peer (P2P) File-sharing Networks

When users on a P2P network share file, they may accidentally—or intentionally—transmit worms to others. When the recipient clicks on the file to open it, a worm gets installed.

How To Tell if Your Computer Has a Worm

Monitor Speed and Performance

If your computer has been running sluggishly, there is a chance it has a worm. Also, if some programs are crashing or running improperly, a worm could be the cause.

Be on the Lookout for Missing or New Files

Worms can delete files on your computer and then replace them with something else. If you see new files or notice some that are missing, it may be because of a worm.

Keep an Eye on Your Hard Drive Space

Because worms replicate, again and again, they often take up large amounts of hard drive space. If your free space is getting eaten up, it could be due to a worm.

Stay Protected Against Computer Worms

Invest in a Strong Internet Security Software Solution

One of the best ways to get malware protection from computer viruses and worms is to use powerful security software.

A strong antivirus product will be able to combat phishing, spyware, malware, Trojans, and other cyber threats.

Be Extra Cautious Against Phishing

Anytime you open an email you are not expecting, particularly from senders you do not know, check for suspicious attachments or links. They may contain worms or a command that automatically downloads a worm onto your computer.

Update Your Operating System

If your operating system is up-to-date with the most recent version, you are more likely to be protected from worms and other malware. Manufacturers are constantly on the lookout for vulnerabilities, and they often release patches that address them in operating system updates.

What is the Difference Between a Worm, Virus, and a Trojan Horse?

A virus attaches to a file or program, and it gets sent to another computer because that file or program is transferred. In other words, a virus goes along for the ride, using a host file or application to get from one place to another.

A worm also spreads from one computer to the next, but it does this all on its own, without the help of an additional file or program. A Trojan horse is very different from both a worm and a virus, particularly in how it is spread. A Trojan will look like a legitimate program, but when it is executed, it infects your computer, causing different kinds of harm. Trojans also have the ability to set up backdoors—similar to worms—that allow a hacker to gain access to your system.

Steganography?

A steganography technique involves hiding sensitive information within an ordinary, non-secret file or message, so that it will not be detected. The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection. Steganography is an additional step that can be used in conjunction with encryption in order to conceal or protect data.

Steganography is a means of concealing secret information within (or even on top of) an otherwise mundane, non-secret document or other media to avoid detection. It comes from the Greek words steganos, which means “covered” or “hidden,” and graph, which means “to write.” Hence, “hidden writing.”

You can use steganography to hide text, video, images, or even audio data. It’s a helpful bit of knowledge, limited only by the type of medium and the author’s imagination.

Different Types of Steganography

1. Text Steganography − There is steganography in text files, which entails secretly storing information. In this method, the hidden data is encoded into the letter of each word.

2. Image Steganography − The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography.

Since the computer description of an image contains multiple bits, images are frequently used as a cover source in digital steganography.

The various terms used to describe image steganography include:

- Cover-Image - Unique picture that can conceal data.

- Message - Real data that you can mask within pictures. The message may be in the form of standard text or an image.

- Stego-Image − A stego image is an image with a hidden message.

- Stego-Key - Messages can be embedded in cover images and stego-images with the help of a key, or the messages can be derived from the photos themselves.

3. Audio Steganography − It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction. Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier"). Its typical uses involve media playback, primarily audio clips.

4. Video Steganography − Video steganography is a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform (DCT) is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye. Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI.

5. Network or Protocol Steganography − It involves concealing data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object. Steganography can be used in the case of covert channels, which occur in the OSI layer network model.

Steganography Examples Include

- Writing with invisible ink

- Embedding text in a picture (like an artist hiding their initials in a painting they’ve done)

- Backward masking a message in an audio file (remember those stories of evil messages recorded backward on rock and roll records?)

- Concealing information in either metadata or within a file header

- Hiding an image in a video, viewable only if the video is played at a particular frame rate

- Embedding a secret message in either the green, blue, or red channels of an RRB image

Steganography can be used both for constructive and destructive purposes. For example, education and business institutions, intelligence agencies, the military, and certified ethical hackers use steganography to embed confidential messages and information in plain sight.

On the other hand, criminal hackers use steganography to corrupt data files or hide malware in otherwise innocent documents. For example, attackers can use BASH and PowerShell scripts to launch automated attacks, embedding scripts in Word and Excel documents. When a poor, unsuspecting user clocks one of those documents open, they activate the secret, hidden script, and chaos ensues. This process is a favored ransomware delivery method.

Steganography has a huge advantage over standard cryptographic methods. When someone uses cryptography, they're passively calling attention to the fact that there's secret information present in the medium in question. Thus, the very presence of encrypted data tells intruders, "Aha! Here's some secret information!" Steganography, however, hides the sensitive information in an otherwise innocuous document. Therefore, would-be hackers have no idea that there is anything secret and enticing in the first place.

Steganography vs. Cryptography

It's fair to say that steganography and cryptography aim to shield messages and data from prying eyes at their most fundamental level. However, they employ an alternative means of security.

Information is converted into unintelligible ciphertext in cryptography. Someone intercepting this message could tell immediately that encryption was used. In contrast, steganography hides a message without altering its original format.

Factors	Steganography	Cryptography

Explanation	It's a method to conceal the fact that communication is taking place	It's a method for making information unintelligible
Aim	Maintain communication security	Enable data protection
Key	Optional, but increases security when utilized	Necessary prerequisite
Data Visibility	No	Yes
Failure	Once hidden information is decoded, the data can be used by anyone	You can recover the original message from the ciphertext if you can access the decryption key
Data Structure	Does not modify the data's general structure	Modifies the overall data structure

How Steganography Differs From Obfuscation?

Obfuscation, like steganography, is defined as hiding information, but the big difference is that the former method deliberately makes the message hard to interpret, read, or decode. That makes sense since to obfuscate means to render something unclear, unintelligible, or obscure.

Cyber-security professionals employ obfuscation to protect sensitive information such as programming codes. The process makes it difficult for hackers to read the codes in the first place, which in turn prevents them from exploiting the data.

To sum it up, while steganography is a form of obfuscation, the reverse doesn’t apply.

Steganography Techniques Explained

Now that we have a better grasp on what steganography is, what forms it comes in, and who uses it, let's take a closer look at a sample of the available techniques.

- **Secure Cover Selection**

Secure Cover Selection involves finding the correct block image to carry malware. Then, hackers compare their chosen image medium with the malware blocks. If an image block matches the malware, the hackers fit it into the carrier image, creating an identical image infected with the malware. This image subsequently passes quickly through threat detection methods.

- **Least Significant Bit**

That phrase almost sounds like a put-down, doesn't it? However, in this case, it refers to pixels. Grayscale image pixels are broken into eight bits, and the last bit, the eighth one, is called the Least Significant Bit. Hackers use this bit to embed malicious code because the overall pixel value will be reduced by only one, and the human eye can't detect the difference in the image. So, no one is even aware that anything is amiss, and that the image is carrying something dangerous within.

- **Palette-Based Technique**

Like the Least Significant Bit technique, the Palette-Based Technique also relies on images. Hackers embed their message in palette-based images such as GIF files, making it difficult for cybersecurity threat hunters or ethical hackers to detect the attack.

Steganography Tools

Various tools or software that support steganography are now readily accessible. Though most hide information, some provide additional security by encrypting it beforehand. You can find the following free steganography resources online:

- Steghide: Steghide is a free tool that uses steganography to conceal information in other files, such as media or text.
- Stegosuite: It is a Java-based, free steganography tool. Stegosuite makes it simple to obfuscate data in pictures for covert purposes.
- OpenPuff: It is a high-quality steganographic tool that allows you to conceal data in other media types like images, videos, and Flash animations.
- Xiao Steganography: To conceal information in BMP images or WAV files, use the free Xiao Steganography tool.
- SSuite Picsel: The free portable program SSuite Picsel is yet another option for hiding text within an image file; however, it uses a somewhat different method than other programs.

These are only a few of the steganography tools available. However, these instruments will help you achieve your goals.

Advantages of Steganography

Steganography is a method that makes it easy to conceal a message within another to keep it secret. The result is that the hidden message remains hidden. A steganography approach can benefit images, videos, and audio files. Further advantages include:

- Unlike other methods, steganography has the added benefit of hiding communications so well that they receive no attention. However, in countries where encryption is illegal, sending an encrypted message that you can easily decipher will raise suspicion and may be risky.
- Steganography is a form of encryption that protects the information within a message and the connections between sender and receiver.
- The three essential elements of steganography—security, capacity, and robustness—make it worthwhile to covert information transfer via text files and develop covert communication channels.
- You can store an encrypted copy of a file containing sensitive information on the server without fear of unauthorized parties gaining access to the data.
- Government and law enforcement agencies can communicate secretly with the help of steganography corporations.

Using Steganography to Deliver Attacks

These days, attacks are typically automated using PowerShell or BASH scripts. And so are hackers. Excel and Word documents with macros enabled have been a common vector for attacks. The hidden script is triggered when the target opens the malicious Word or Excel file.

The attacker can access the system without the victim being duped into installing Steghide. The intruder is using a steganographic program to take advantage of widespread Windows tools like Excel and PowerShell. Once the victim reads the document, it becomes easier for the hacker to attack the system.

Artificial Intelligence and Steganography

Hackers are also using artificial intelligence (AI). Steganography is just one of the many methods that artificial intelligence is increasingly employing to conceal its activities. AI implementations have tweaked even steganographic techniques to make attacks harder to detect.

Detecting Steganography

In their line of work, security analysts look for indicators of standard attack and penetration testing strategies (TTPs). The common signatures used by steganographic software have been uncovered over time. Because of this, antivirus software, for example, can easily spot the common behaviors of steganographic programs.

As a result, penetration testers and attackers constantly adjust their methods to stay undetected. Likewise, security researchers continuously look for new signatures and attack tactics, while cybercriminals continually adapt their tools and approaches.

Real-World Attacks That Used Steganography

In 2020, businesses in the United Kingdom, Germany, Italy, and Japan were hit by a campaign using steganographic documents.

Hackers could avoid detection by using a steganographic image uploaded on a good platform, like Imgur, to infect an Excel document. Mimikatz, a malware that steals Windows passwords, was downloaded via a secret script included in the picture.

Mitigating Steganography-Based Attacks

Steganography is simple to implement during a cyber attack. However, it's much harder to prevent since the people who pose a threat are getting more resourceful and ingenious, which makes developing countermeasures more difficult.

Code disguised in images and other sorts of obfuscations are more likely to be discovered dynamically by a behavioral engine. Therefore businesses should use modern endpoint protection solutions that extend beyond static checks, elemental signatures, and other old-fashioned components.

Employees should be aware of the risk of opening image files, as they may contain viruses. In addition, the newest security patches should be installed whenever they become available, and firms should use web filtering to ensure their employees can safely browse the web.

Let’s Check Out Some Popular Steganography Applications

There are many kinds of dedicated software applications available to facilitate steganography. Here is a partial list of the more well-known steganography applications:

- Image Steganography: This application is a JavaScript tool used to hide images in other image files

- OpenStego: This program is an open-source steganography tool
- Xiao Steganography: Xiao hides secret files in WAV or BMP files
- Crypture: This application is a command-line tool used to conduct steganography
- NoClue: This application is an open-source tool that hides text information in both video and image carrier files
- Steganography Master: This app is an Android-based open-source tool that can hide text in an image and gives you a decoding tool to pull hidden text messages from image files. It supports multiple image formats (BMP, JPG, ICO, PNG)
- Steghide: Steghide is an application that hides data in different audio and image files, including JPEG, BMP, AU, and WAV

What Is the Difference Between DoS Attacks and DDoS Attacks?

A **denial-of-service (DoS) attack** floods a server with traffic, making a website or resource unavailable. A **distributed denial-of-service (DDoS) attack** is a DoS attack that uses multiple computers or machines to flood a targeted resource. Both types of attacks overload a server or web application with the goal of interrupting services.

As the server is flooded with more Transmission Control Protocol/User Datagram Protocol (TCP/UDP) packets than it can process, it may crash, the data may become corrupted, and resources may be misdirected or even exhausted to the point of paralyzing the system.

The principal difference between a DoS attack and a DDoS attack is that the former is a system-on-system attack, while the latter involves several systems attacking a single system. There are other differences, however, involving either their nature or detection, including:

1. Ease of detection/mitigation: Since a DoS comes from a single location, it is easier to detect its origin and sever the connection. In fact, a proficient firewall can do this. On the other hand, a DDoS attack comes from multiple remote locations, disguising its origin.
2. Speed of attack: Because a DDoS attack comes from multiple locations, it can be deployed much faster than a DoS attack that originates from a single location. The increased speed of attack makes detecting it more difficult, meaning increased damage or even a catastrophic outcome.

3. Traffic volume: A DDoS attack employs multiple remote machines (zombies or bots), which means that it can send much larger amounts of traffic from various locations simultaneously, overloading a server rapidly in a manner that eludes detection.
4. Manner of execution: A DDoS attack coordinates multiple hosts infected with malware (bots), creating a botnet managed by a command-and-control (C&C) server. In contrast, a DoS attack typically uses a script or a tool to carry out the attack from a single machine.
5. Tracing of source(s): The use of a botnet in a DDoS attack means that tracing the actual origin is much more complicated than tracing the origin of a DoS attack.

Types of DoS Attacks and DDoS Attacks

DoS and DDoS attacks can take many forms and be used for various means. It can be to make a company lose business, to cripple a competitor, to distract from other attacks, or simply to cause trouble or make a statement. The following are some common forms taken by such attacks.

Teardrop Attack

A teardrop attack is a DoS attack that sends countless Internet Protocol (IP) data fragments to a network. When the network tries to recompile the fragments into their original packets, it is unable to.

For example, the attacker may take very large data packets and break them down into multiple fragments for the targeted system to reassemble. However, the attacker changes how the packet is disassembled to confuse the targeted system, which is then unable to reassemble the fragments into the original packets.

Flooding Attack

A flooding attack is a DoS attack that sends multiple connection requests to a server but then does not respond to complete the handshake.

For example, the attacker may send various requests to connect as a client, but when the server tries to communicate back to verify the connection, the attacker refuses to respond. After repeating the process countless times, the server becomes so inundated with pending requests that real clients cannot connect, and the server becomes “busy” or even crashes.

IP Fragmentation Attack

An IP fragmentation attack is a type of DoS attack that delivers altered network packets that the receiving network cannot reassemble. The network becomes bogged down with bulky unassembled packets, using up all its resources.

Volumetric Attack

A volumetric attack is a type of DDoS attack used to target bandwidth resources. For example, the attacker uses a botnet to send a high volume of request packets to a network, overwhelming its bandwidth with Internet Control Message Protocol (ICMP) echo requests. This causes services to slow down or even cease entirely.

Protocol Attack

A protocol attack is a type of DDoS attack that exploits weaknesses in Layers 3 and 4 of the OSI model. For example, the attacker may exploit the TCP connection sequence, sending requests but either not answering as expected or responding with another request using a spoofed source IP address. Unanswered requests use up the resources of the network until it becomes unavailable.

Application-based Attack

An application-based attack is a type of DDoS attack that targets Layer 7 of the OSI model. An example is a Slowloris attack, in which the attacker sends partial Hypertext Transfer Protocol (HTTP) requests but does not complete them. HTTP headers are periodically sent for each request, resulting in the network resources becoming tied up.

The attacker continues the onslaught until no new connections can be made by the server. This type of attack is very difficult to detect because rather than sending corrupted packets, it sends partial ones, and it uses little to no bandwidth.

DDoS Threats

DDoS attacks pose a serious threat to companies of all sizes and in all industries. Some of the potential impacts of a successful attack include:

- **Financial Losses:** A successful DDoS attack can cause decreased productivity, downtime, and potential violation of SLAs as well as costing money to mitigate and recover.
- **Operational Disruption:** A DDoS attack may render an organization unable to perform core operations, or it may degrade customers’ ability to access its services.
- **Reputational Damage:** DDoS attacks may cause churn as customers choose competitors if they can’t reach an organization’s website or distrust its ability to provide products and services.

In recent years, the threat of DDoS attacks has grown significantly. One contributor is the greater availability of DDoS attack tools, making it easier for anyone to carry out an attack. Also, botnets have grown more popular and powerful, enabling them to perform record-breaking attacks to take down websites or entire networks. As DDoS attacks grow more common, larger, and more sophisticated, they are increasingly difficult and costly for an organization to mitigate.

DDoS Attack Prevention and Protection

The best way to manage the DDoS threat is to implement defense in depth. A combination of on-prem and cloud-based DDoS mitigation solutions will enable an organization to identify and block a wide range of DDoS attacks, including volumetric, application, reflective, and resource-exhaustive DDoS attacks.

Rapid detection and response are also important to reducing the impact of a DDoS attack. Proactive DDoS detection and prevention combined with an incident response team capable of deploying additional resources as needed can minimize the disruption and cost of a DDoS attack.

Protect Against DDoS Attacks with DDoS Protector

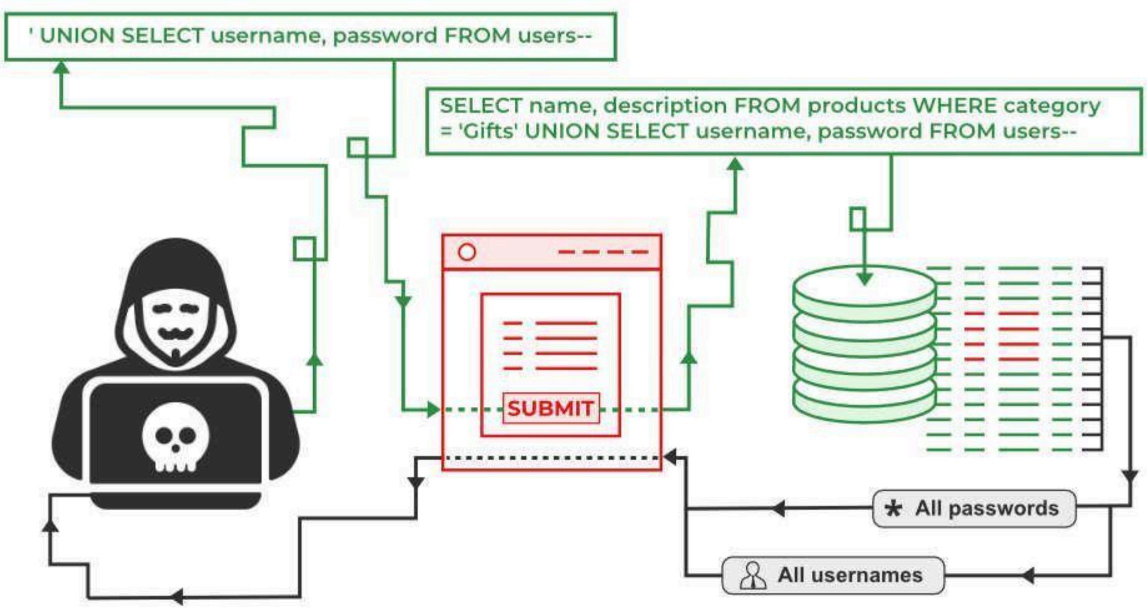
DDoS attacks are an ongoing threat to an organization's security. Stay vigilant, continuously assess your security measures, and leverage reliable DDoS protection solutions to ensure the resilience of your infrastructure.

Furthermore, Check Point offers a free scan to analyze your organization's resiliency against DDoS attacks. If you'd like to deploy additional defenses and reduce your DDoS risk.

SQL Injection

SQL injection is a technique used to extract user data by injecting web page inputs as statements through SQL commands. Basically, malicious users can use these instructions to manipulate the application's web server.

1. SQL injection is a code injection technique that can compromise your database.
2. SQL injection is one of the most common web hacking techniques.
3. SQL injection is the injection of malicious code into SQL statements via web page input.


' UNION SELECT username, password FROM users--
SELECT name, description FROM products WHERE category = 'Gifts' UNION SELECT username, password FROM users--
SUBMIT
All passwords
All usernames

The Exploitation of SQL Injection in Web Applications

Web servers communicate with database servers anytime they need to retrieve or store user data. SQL statements by the attacker are designed so that they can be executed while the web server is fetching content from the application server. It compromises the security of a web application.

Example of SQL Injection

Suppose we have an application based on student records. Any student can view only his or her own records by entering a unique and private student ID.
Suppose we have a field like the one below:

Student id: The student enters the following in the input field: **12222345 or 1=1**.
Query:
SELECT * from STUDENT where
STUDENT-ID == 12222345 or 1 = 1
Now, this **1=1** will return all records for which this holds true. So basically, all the student data is compromised. Now the malicious user can also delete the student records in a similar fashion. Consider the following SQL query.

Query:

SELECT * from USER where
USERNAME = “” and PASSWORD=””

Now the malicious can use the ‘=’ operator in a clever manner to retrieve private and secure user information. So instead of the above-mentioned query the following query when executed retrieves protected data, not intended to be shown to users.

Query:

Select * from User where
(Username = “” or 1=1) AND
(Password=”” or 1=1).

Since **1=1** always holds true, user data is compromised.

Impact of SQL Injection

The hacker can retrieve all the user data present in the database such as user details, credit card information, and social security numbers, and can also gain access to protected areas like the administrator portal. It is also possible to delete user data from the tables.

Nowadays, all online shopping applications and bank transactions use back-end database servers. So in case the hacker is able to exploit SQL injection, the entire server is compromised.

Preventing SQL Injection

- User Authentication: Validating input from the user by pre-defining length, type of input, of the input field and authenticating the user.
- Restricting access privileges of users and defining how much amount of data any outsider can access from the database. Basically, users should not be granted permission to access everything in the database.
- Do not use system administrator accounts.

SQL in Web Pages

SQL injection typically occurs when you ask a user for input, such as their username/user ID, instead of their name/ID, and the user gives you an SQL statement that you execute without the knowledge about your database.

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users
WHERE UserId = " + txtUserId;
```

SQL Injection Based on Batched SQL Statements

1. Most databases guide batch SQL statements.
2. A batch of SQL statements is a collection of two or more square statements separated by using semicolons.

The SQL declaration underneath will return all rows from the “users” desk after which delete the “Employees ” table.

Query:

```
SELECT * FROM Users;
DROP TABLE Employees
```

Look at the following example:

Syntax:

```
txtEmpId = getRequestString("EmpId");
txtSQL = "SELECT * FROM Users
WHERE EmpId = " + txtEmpId;
```

The valid SQL statement would look like this:

Query:

```
SELECT * FROM Users WHERE EmpId = 116;
DROP TABLE Employees;
```

9 Best Practices to Protect Your Database from SQL Injection

When developing your website or web application, you can incorporate security measures that limit your exposure to SQL injection attacks. For example, the following security prevention measures are the most effective ways to prevent SQL injection attacks:

1. Install the latest software and security patches from vendors when available.
2. Give accounts that connect to the SQL database only the minimum privileges needed.
3. Don't share database accounts across different websites and applications.
4. Use validation for all types of user-supplied input, including drop-down menus.
5. Configure error reporting instead of sending error messages to the client web browser.
6. Use prepared statements with parameterized queries that define all the SQL code and pass in each parameter so attackers can't change the intent of a query later.
7. Use stored procedures to build SQL statements with parameters that are stored in the database and called from the application.
8. Use allowlist input validation to prevent unvalidated user input from being added to query.
9. Escape all user-supplied input before putting it in a query so that the input isn't confused with SQL code from the developer.

In general, organizations should avoid using shared accounts so that attackers can't gain further access if one account is compromised. Organizations should also avoid sending database error messages to the client web browser because attackers can use that information to understand technical details about the database.

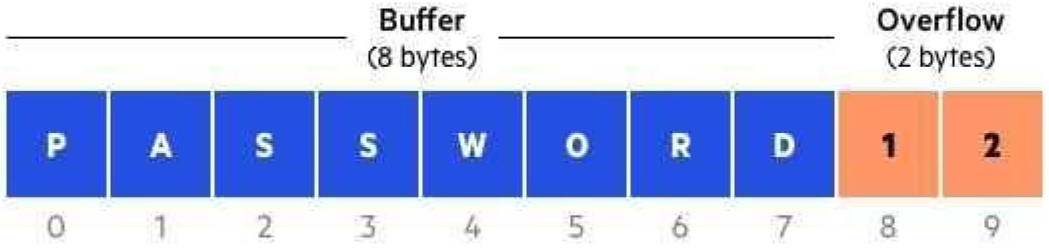
Buffer Overflow Attack

What is Buffer Overflow

Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.

Buffer overflows can affect all types of software. They typically result from malformed inputs or failure to allocate enough space for the buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.



Buffer overflow example

What is a Buffer Overflow Attack

Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information. For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.

If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program.

Types of Buffer Overflow Attacks

Stack-based buffer overflows are more common, and leverage stack memory that only exists during the execution time of a function.

Heap-based attacks are harder to carry out and involve flooding the memory space allocated for a program beyond memory used for current runtime operations.

What Programming Languages are More Vulnerable?

C and C++ are two languages that are highly susceptible to buffer overflow attacks, as they don't have built-in safeguards against overwriting or accessing data in their memory. Mac OSX, Windows, and Linux all use code written in C and C++.

Languages such as PERL, Java, JavaScript, and C# use built-in safety mechanisms that minimize the likelihood of buffer overflow.

How to Prevent Buffer Overflows

Developers can protect against buffer overflow vulnerabilities via security measures in their code, or by using languages that offer built-in protection.

In addition, modern operating systems have runtime protection. Three common protections are:

- **Address space randomization (ASLR)**—randomly moves around the address space locations of data regions. Typically, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes this virtually impossible.
- **Data execution prevention**—flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.
- **Structured exception handler overwrite protection (SEHOP)**—helps stop malicious code from attacking Structured Exception Handling (SEH), a built-in system for managing hardware and software exceptions. It thus prevents an attacker from being able to make use of the SEH overwrite exploitation technique. At a functional level, an SEH overwrite is achieved using a stack-based buffer overflow to overwrite an exception registration record, stored on a thread's stack.

Security measures in code and operating system protection are not enough. When an organization discovers a buffer overflow vulnerability, it must react quickly to patch the affected software and make sure that users of the software can access the patch.

Identity Theft Definition

A common identity theft meaning is when someone takes someone else's personal information and then uses it for their own benefit, particularly without getting the individual's permission. Identity theft can take many forms, and each one affects the victim in different ways. Regardless of how you define identity theft, in every instance, the target's reputation, financial security, or financial future is put at risk.

Because there are so many ways someone can steal your identity, it is virtually impossible to prevent becoming a target altogether. Even if you do not have a lot of liquid assets, an impressive credit score, or access to valuable targets, such as people or secured systems, a thief can still make a profit off your identity.

In many cases, what happens after your identity has been stolen may have a minimal financial impact. However, a thief can make anywhere from a few to hundreds of dollars by selling your identity. Therefore, identity thieves typically go after anyone because each identity has an intrinsic value on the black market. In other situations, the thief aims to personally exploit your identity. If this is the case, they may be more surgical regarding who they choose to target.

In either case, you can minimize your chances of falling victim to identity thieves by learning how it happens, the different kinds of identity theft, signs you have been targeted, and how to protect yourself from these kinds of attacks.

How Identity Theft Happens

The term "identity theft" encompasses a broad range of methods of stealing other people's information. However, it is common for a thief to target high-value information, such as a Social Security number, and use it to buy something, open an account, or commit fraud that involves impersonating the individual, particularly online.

There are several ways this happens.

Data Breaches

A data breach is when a thief or hacker is able to access the data of an organization without receiving the proper authorization. The company may have sensitive information stored in a central location. The thief targets the database or file holding that information and tries to penetrate any cyber defenses in place. In many cases, the thief will focus on getting credit card or Social Security numbers, as well as the complete names of the owners.

Files containing other information can be highly sought-after targets as well, particularly because that information can be used to correlate the identity of each person. For example, where the individual lives, has lived in the past, their phone number, old phone numbers, or maiden names can all be the targets of a data breach.

In 2019, there were 1,506 data breaches in the United States, resulting in the exposure of 164.68 million sensitive records. It is difficult to avoid having some of your information included in one of the many data breaches that occur each year. This is because most people have their personal data stored within the databases and files of multiple companies with whom they do business.

However, as discussed below, there are things you can do to protect yourself, your reputation, and your finances from the effects of a data breach.

Unsecure Browsing

In most cases, the websites you visit are safe. They are protected by security measures that prevent hackers from gaining access to the information you enter. The protection often involves encrypting the data that gets entered. This way, if a thief were to intercept data, they would only get a jumbled arrangement of letters, numbers, and symbols instead of your Social Security number, name, address, etc.

However, if you use websites that are not as well-known, you may be putting yourself at risk. Even if the website's designer had good intentions, the website itself may have been compromised by a hacker. In other cases, a hacker can design a fake website that looks like a real one. When you enter your information, it goes straight to the hacker instead of the company you thought you were sending it to.

Often, your browser can detect fraudulent websites and alert you to the danger. If you get an alert, it is best to take action by leaving the website and closing your browser.

Dark Web Marketplaces

The dark web consists of a network of websites hidden from regular internet users. When someone visits the dark web, they can use software to hide who they are, as well as what they are doing while connected. This makes the dark web an ideal place for thieves, hackers, and others looking to defraud users.

As a result, the dark web is a prime selling ground for your personal information. Hackers recognize the elevated risk associated with trying to exploit personal information themselves, so they often head to the dark web to sell it off to someone else. The initial buyer may use it or sell it to another malicious actor to make a quick profit. Therefore, if your information goes to the dark web, it is virtually impossible to say how it will be used.

Malware Activity

With malware, or malicious software, a hacker can accomplish any number of things—from taking over a computer system to controlling a network, to providing backdoor access and more. Malware can also be used specifically to steal personal information.

The most common way malware is used to execute identity theft or fraud is when it is programmed to spy on the target's computer activity. The attack may begin with a phishing email or other trap designed to get the user to click on a link or image that automatically installs the malware.

An attack can be performed using a number of methods, such as keyloggers, which can keep track of which keys a user strikes. When the user accesses a particular website or logs in to their computer, the keylogger can record their keystrokes and report them back to the thief. In this way, the attacker can ascertain their password to a specific site, workstation, or application. Once the attacker uses that login information, they may be able to collect the target's personal information.

Malware can also be used to provide backdoors for attackers who wish to gain access to a database or file that contains personal information. The malware, once installed, allows the hacker to get behind the system's defenses. The hacker uses this avenue to penetrate the system and then glean the personal information of internal users or the company's clients and customers.

Credit Card Theft

Credit card theft is one of the simplest ways a thief can steal your identity. Once they have access to your credit card, they often do not need any other aspect of your identity—the card itself is enough to make purchases under the target's identity. A thief may even make relatively large purchases the user could not possibly pay off. They could then sell the item to someone else at a steep discount, banking a profit along the way.

Credit card theft can also be used to grab card numbers for resale on the dark web. A credit card number may go for a few dollars or far more. The thief gets your credit card information and then sells it to someone else. It is important to instantly cancel any credit cards that have been lost or stolen, but often, a data breach is used to get ahold of your card information.

Companies store long lists of credit card information to help their customers make quicker purchases. When the customer first does business with the company, the credit card information is obtained and kept in a secure location. When the customer returns, because their card information is already in the company's system, their next purchase is quicker and easier. This convenience comes at a cost, however, because if someone is able to penetrate the defenses protecting customers' card information, they can get a storehouse of account numbers.

Mail Theft

Even before the internet, identity thieves were busy taking people's personal information and using it for their benefit. A common method was mail theft. In this kind of attack, the thief grabs the target's credit card or other information from their mailbox. They then try to use it to make purchases—or sell it to another thief for a quick profit.

A thief does not have to go into your mailbox to take your credit card or gather personal information. It is just as easy to go through your trash. Often, people throw out letters, notices, or account statements that contain sensitive information. Even if the information in the trashed document is not enough to execute a complete theft of your identity, it can be used by the thief to confirm who you are. It is best to shred your old mail instead of just throwing it in the garbage.

Phishing and Spam Attacks

An attacker may send an email or text message that looks like it is coming from a legitimate source. When the target clicks on a link, they are taken to a fake website that asks you for your username, password, or other personal information like your Social Security or credit card number. The hacker can then use that information to assume your identity or make purchases.

Wi-Fi Hacking

Anytime you use your computer or mobile device on a public network, you may be vulnerable to a hacker that can eavesdrop on your communications with the network. This is a particularly prevalent issue at places like coffee shops, department stores, or airports where anybody can get onto the network, often without a password.

Once the hacker has started spying on your communications, they watch to see if you enter your personal information. They may specifically be after your Social Security, credit card, or bank account number. Once they have it, they can use it to make purchases, masquerade as you online while opening accounts, or sell the information to someone on the dark web.

Mobile Phone Theft

Some people use their mobile phones to log in to sites automatically, without having to enter their username or password. If someone gets ahold of your mobile phone, they may be able to access these same sites, especially if they do not need to enter a password or use biometric verification, such as a fingerprint or facial scan.

Mobile phone theft is also popular because people often store their personal information, including passwords and account numbers, in applications on their phones. This may include an app where you can manage and edit notes or email and text apps. If a thief can take your phone and get into it, they can easily navigate to your emails and text messages to steal information.

Further, if they want to execute a more sophisticated attack, they can use your phone to fulfill the second stage of a two-factor authentication (2FA) access procedure. When the site or application sends a text to you, the thief receives it and can then enter a verification number to gain access to the application or site.

Card Skimming

Credit card theft may also involve skimming. In a skimming attack, a fake credit card machine is installed on a gas pump or another point-of-sale (POS) device. It is then used to collect the card information of customers as they swipe their cards. A skimming attack often uses a hidden camera to record the target's password, particularly if they are using a debit card.

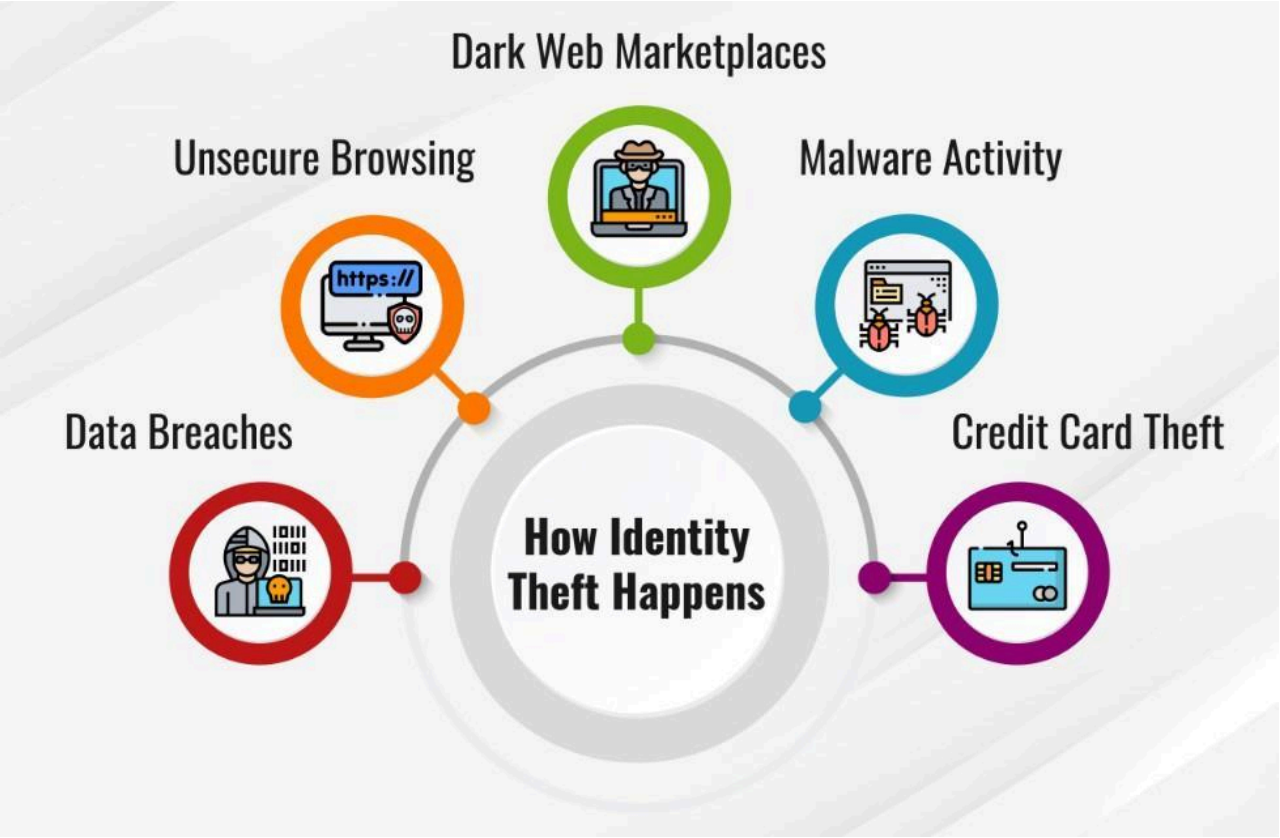
It is important to keep an eye out for any credit card machine that looks out of the ordinary. For example, the card-swiping device may protrude excessively from the machine or the device may be loose when you shake it. If anything seems suspicious, stop using the machine, check around for small cameras pointed toward it, then alert the proper authorities. Letting them know the reasons why you suspected a skimming machine, as well as the exact location, can help them track down the perpetrator and protect your information and that of others.

Child ID Theft

With child ID theft, the child's personal information is used to execute the attack. This may include the child's Social Security number, which can be mailed to you soon after they are born. The attacker may not use the information for many years, waiting until the child is old enough to get a credit card. When they reach the right age, the thief then uses the information to open an account or obtain credit in the name of the child.

Tax ID Theft

With tax ID theft, the attacker uses your social security number and other necessary information to file taxes and then collect your refund. They may also alter the tax information they enter to inflate the refund they get. If this happens to you, there is a chance you will not know until you try to file your taxes. The Internal Revenue Service (IRS) will then alert you that someone has already filed a tax return in your name. After an investigation, you should be able to file your taxes and get the refund you are entitled to.



What is Identity Fraud?

Identity fraud and identity theft are similar, and the terms can sometimes be used interchangeably. However, identity fraud is different in that it specifically refers to using the stolen information, while identity theft may only involve stealing your personal information. There are several different types of identity fraud, including using a credit card, taxes, employment, phone or utility bills, bank account information, leases or loans, and government benefits or documents.

Regardless of the type of fraud, the execution of the attack is similar: The thief uses account numbers, Social Security numbers, and other personal information to make another entity believe they are you. They then use that to make or take money.

Effects of Identity Theft

There are several ways identity thieves can use your personal information to their advantage. Some involve using it to steal money from you, while others require multiple steps before the thief realizes a profit.

Stolen Money or Benefits

A criminal can use your credit card number, address, and name to buy things with your card. They can also file a tax return or even use your insurance and other information to get medical treatment while pretending to be you. If you have airline miles or can get access to government services like the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) or Social Security checks, the thief could use your information to take advantage of those provisions as well.

Identity Sold on the Dark Web

Once your data has been taken, particularly during a data breach where the thief can grab many victims' information at once, it may be sold on the dark web. Even though each piece of information may only yield a few dollars, if a thief has thousands of account numbers, addresses, and names, their profits can add up quickly.

Impersonation

A thief may pretend to be you on social media or to get a job or apartment. This is particularly true when there is an element of their own identity that gets in the way of what they are trying to do, such as a criminal record.

Possible Signs of Identity Theft

Keep an eye out for the following signs that may indicate your identity has been stolen:

1. Discrepancies in your financial statements
2. Unauthorized purchases in your bank statements
3. You get calls from debt collectors about charges you did not initiate
4. You get a letter from the IRS about multiple tax returns
5. You get medical bills for services you never used
6. You see strange charges on your credit card statement
7. You are not getting bills in the mail, which could be because the thief has changed your address, resulting in your mail getting routed somewhere else
8. You get rejected for a loan even though you usually have good credit, which could mean a thief was borrowing money in your name and not repaying it

How To Protect Yourself from Identity Theft Attacks

To protect yourself from identity theft, you can implement the following measures:

1. Use complex passwords for all your accounts and devices. This should include multiple, non-sequential or logical letters, numbers, and symbols
2. Enable multi-factor authentication (MFA)
3. Never provide personal information, especially over the phone, to someone who calls unexpectedly
4. Shred all documents prior to putting them in the trash
5. Use paperless billing to prevent account numbers from getting to your mailbox or trash
6. Store your debit, credit, Social Security, Medicare, and other cards in a secure area in your home
7. Frequently check your bank and credit card accounts for unusual activity
8. Never click suspicious links
9. Arrange for your bank or credit card company to alert you every time a withdrawal has been made from your account

What To Do if You Think You Are a Victim

If you think you have been targeted, you should immediately cancel your credit and debit cards. Also, reach out to the credit bureaus Experian, Equifax, and TransUnion. If you report the situation to one, it is required by law to pass the information on to the others. This way, your credit score can be protected if unauthorized transactions are performed in your name.You should then alert the authorities. You can use the website of the Federal Trade Commission (FTC) to figure out how to proceed.