18AIS102J - SMART MANUFACTURING

Cyber Security Systems

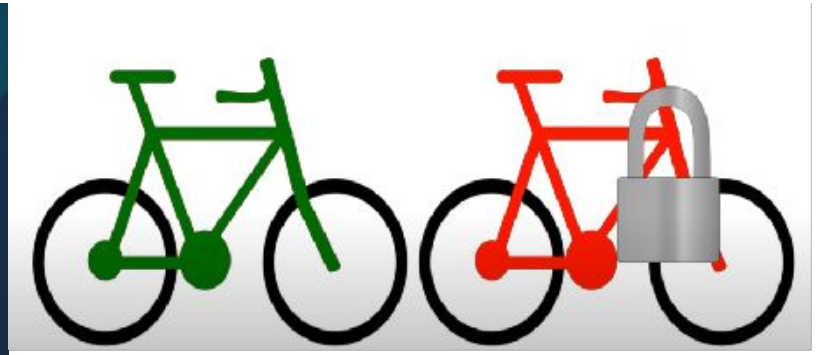
What is Cyber Crime?

- Cybercrime is **any criminal activity that involves a computer, networked device or a network**.

- While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them.

What is Cyber Security?

- Cyber Security is the process and techniques involved in protecting sensitive data, computer systems, networks and software applications from cyber attacks.



“WHAT ARE WE TRYING TO PROTECT OURSELVES AGAINST?”

Main aspects we are trying to control

- Unauthorised Access
- Unauthorised Deletion
- Unauthorised Modification

Cyber Attack

- A cyber attack is any offensive maneuver that targets computer information systems, computer networks, infrastructures, or personal computer devices.

OR

- An attempt by hackers to damage or destroy a computer network or system.

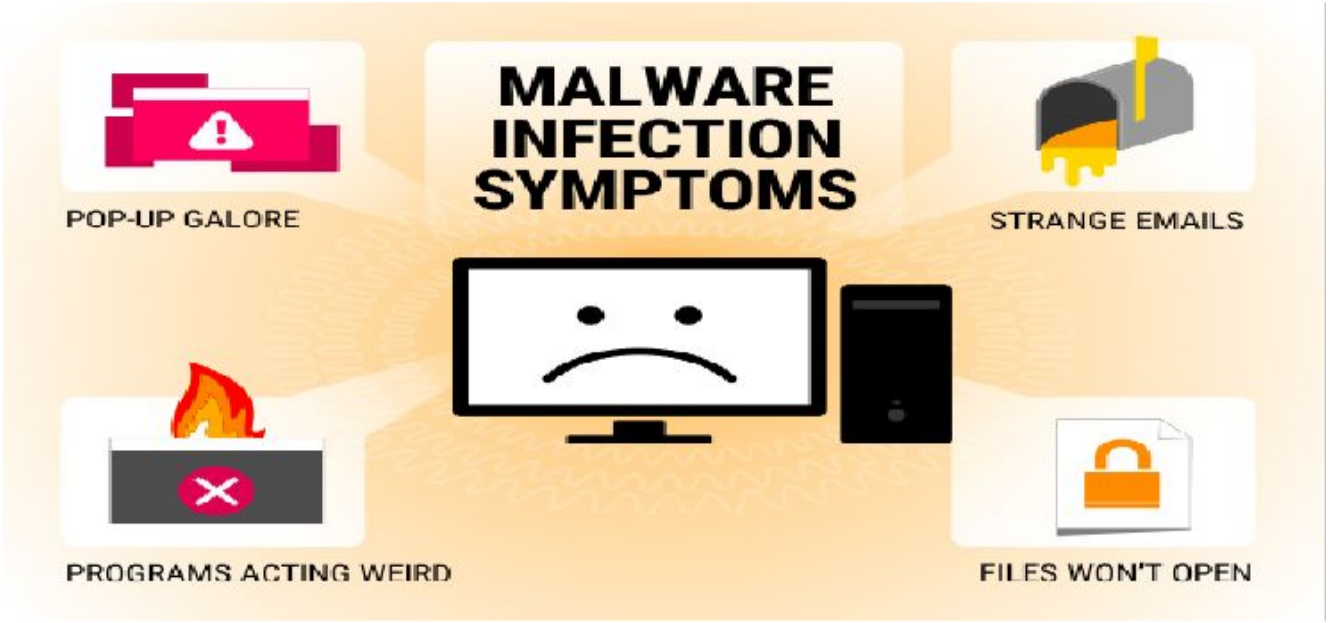
Attacker

- An **attacker** is the individual or organization who performs the malicious activities to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of computer systems.

Types of Cyber Attacks

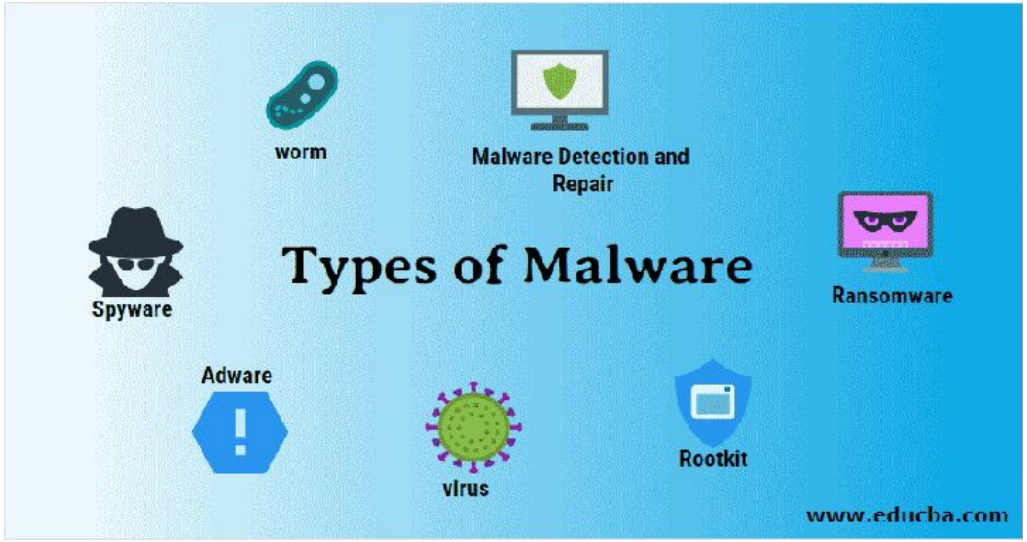
Malware

- Malware, or malicious software, is any program or file that is harmful to a computer user



Types of Malware

- Virus : Execute itself and spread by infecting other programs or files.
- Worm : Can self-replicate without a host program and typically spreads without any human interaction.

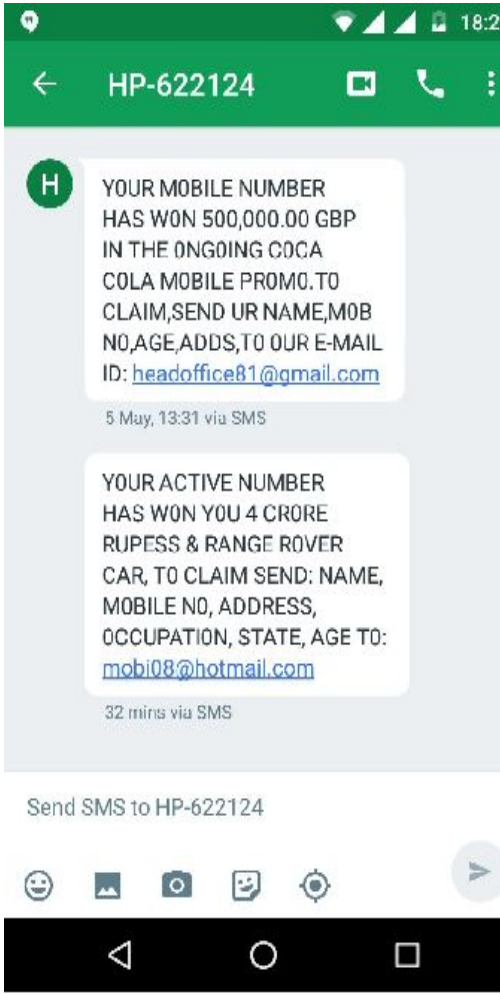


Types of Malware

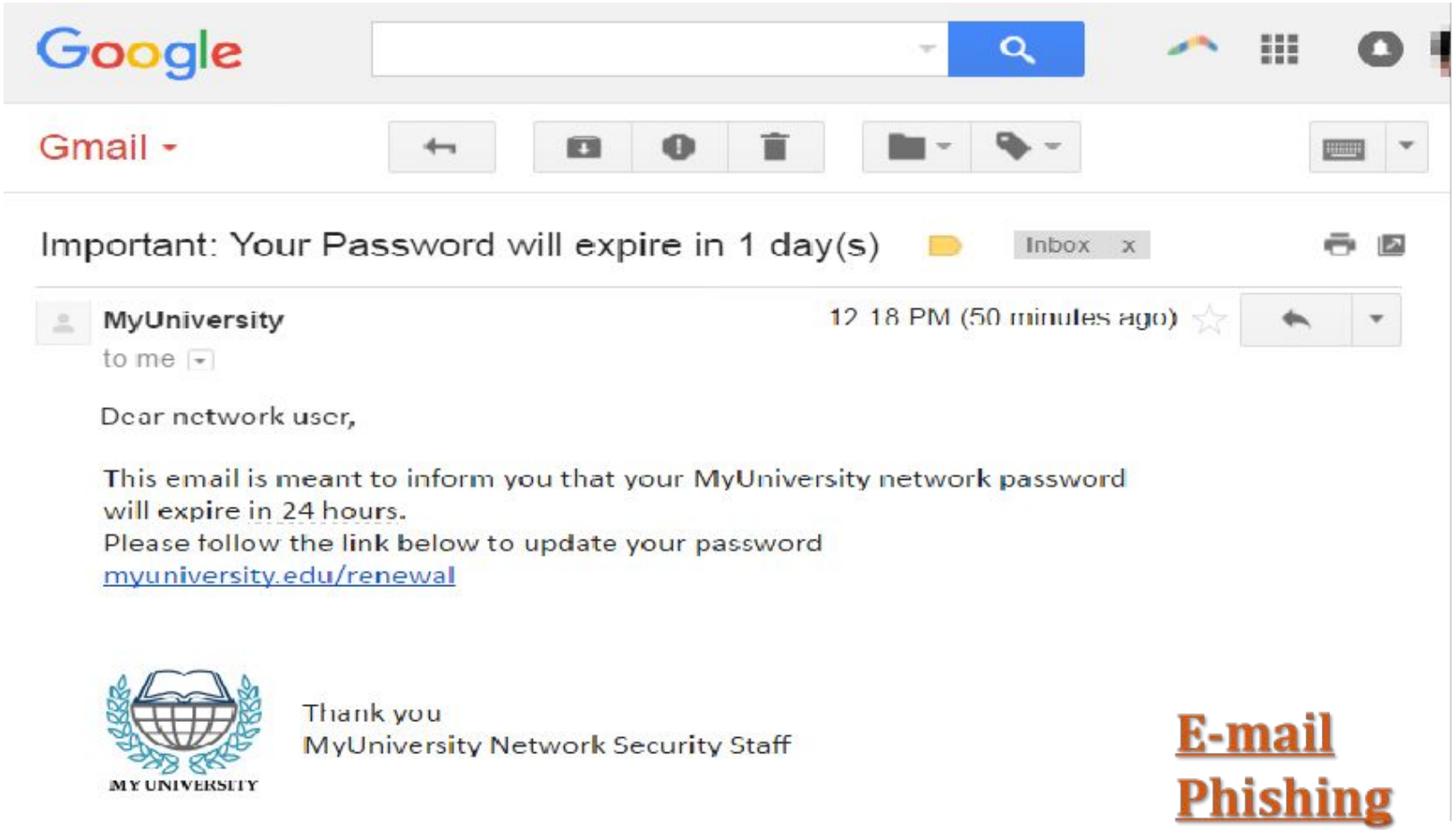
- Trojan Horse : Program that gain access to a system.
- Spyware: Observe the activity without our knowledge.
- Ransomware : Infect a user's system and encrypt the data.
- Rootkit : Obtains administrator-level access
- Adware : Downloads browsing history

Phishing

- **Phishing** is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details via e mail or phone.



E-mail Phishing



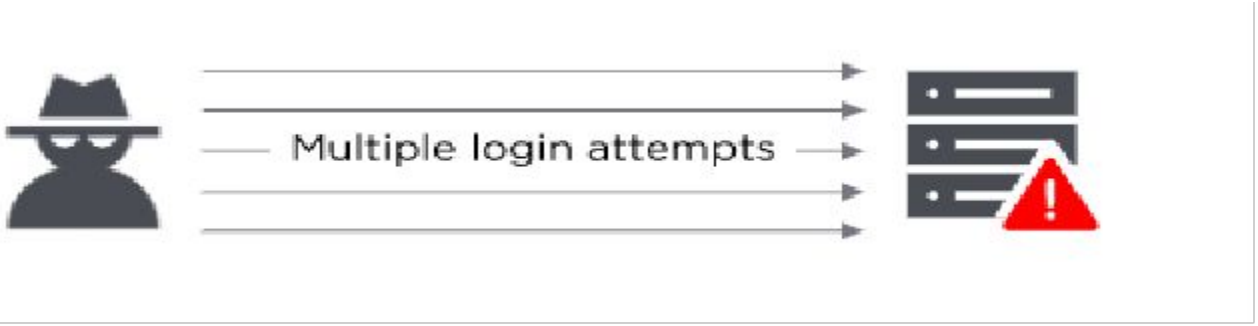
Password Attack

- A **password attack** is exactly what it sounds like: a third party trying to gain access to your systems by cracking a user's password.

Password Attack

Dictionary Attack

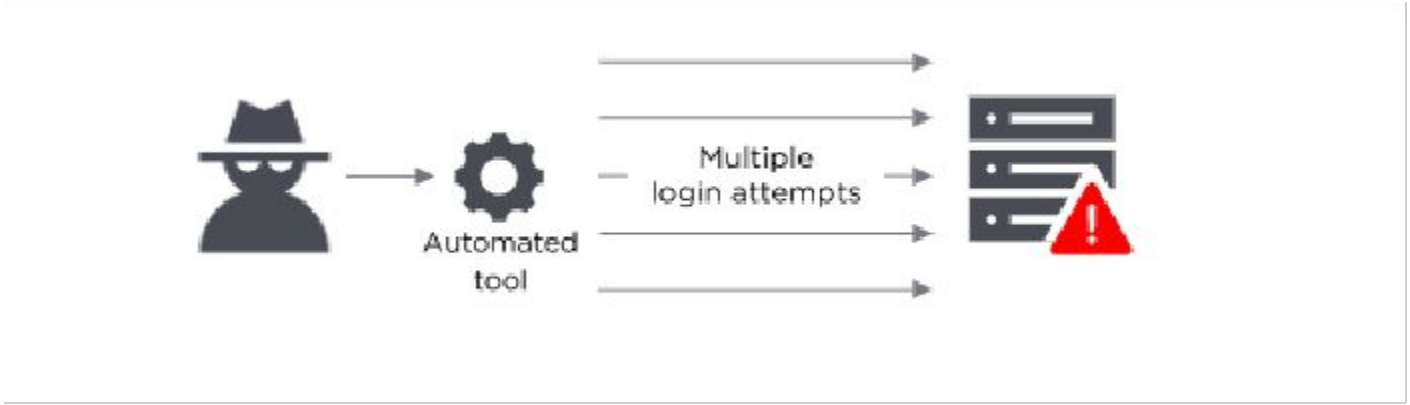
An attack that takes advantage of the fact people tend to use common words and short passwords



Password Attack

Brute force

Using a program to generate likely passwords or even random character sets



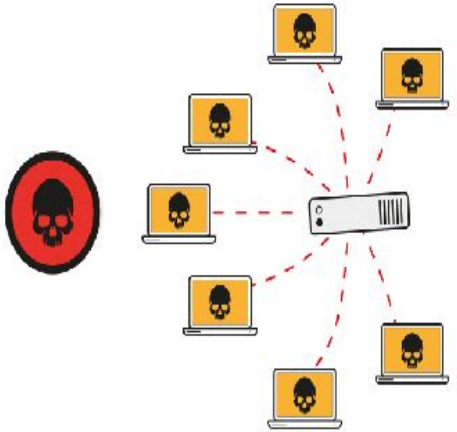
Password Attack

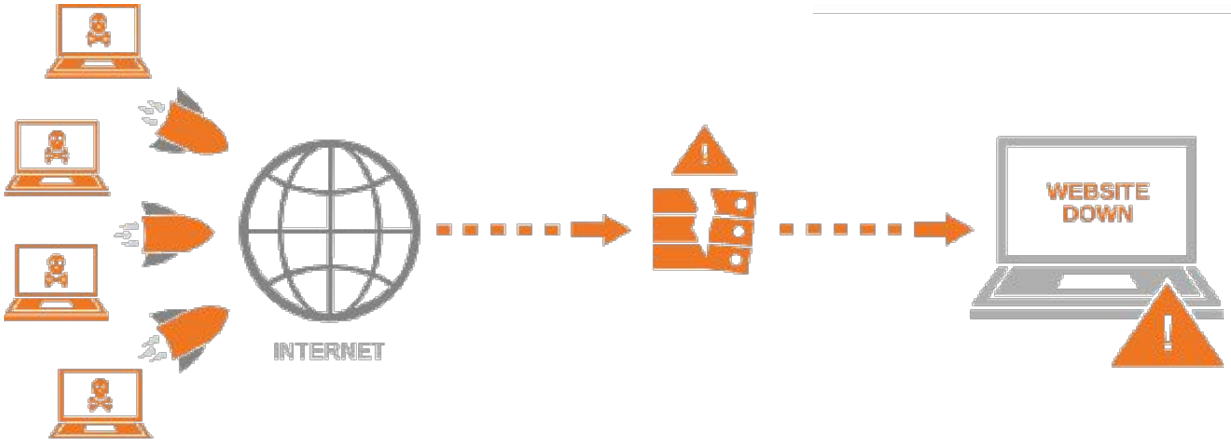
Traffic interception

In this attack, the cyber criminal uses software such as packet sniffers to monitor network traffic and capture passwords as they're passed.

DDoS Attack

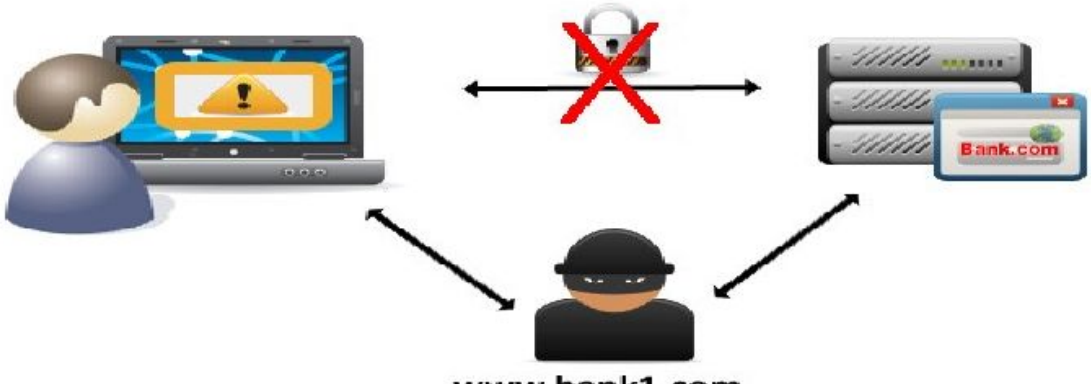
- **Distributed Denial-of Service (DDoS)** attack occurs when multiple systems flood the bandwidth or resources of a targeted system and makes it unavailable.





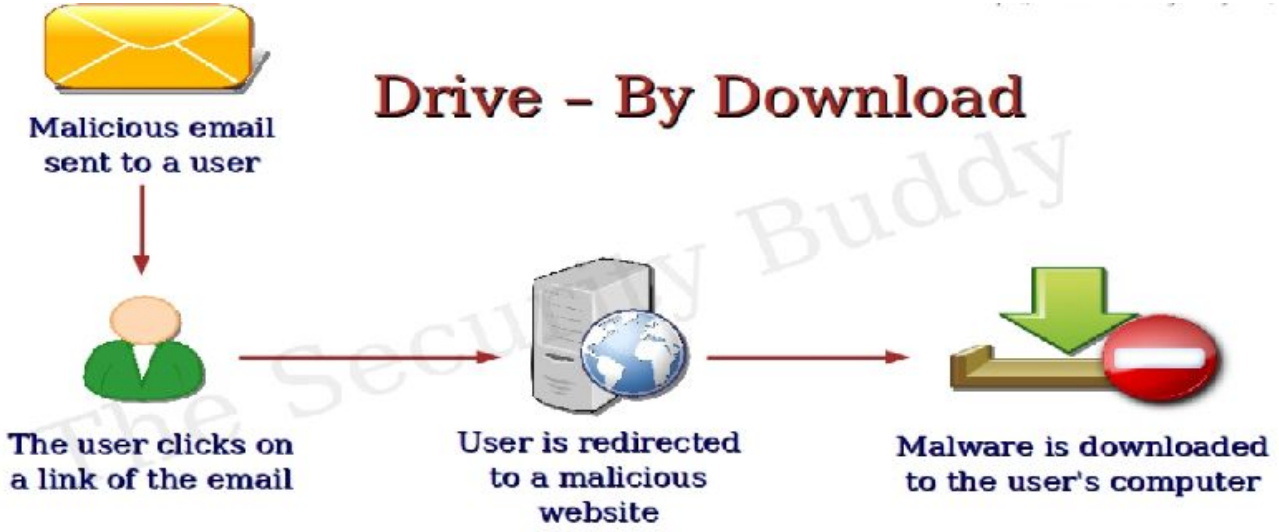
Man in the Middle Attack

- MITM is an **attack** where the attacker secretly relays and alters the communications between two parties who believe that they are directly communicating with each other.



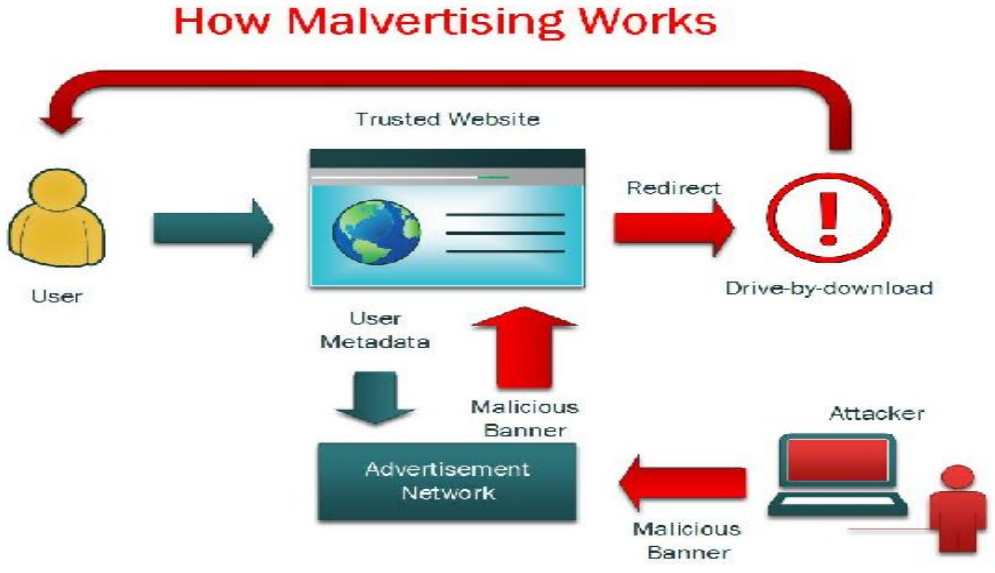
Drive by Downloads

- A drive-by download refers to the unintentional download of malicious code to your computer or mobile device that leaves you open to a cyber attack.



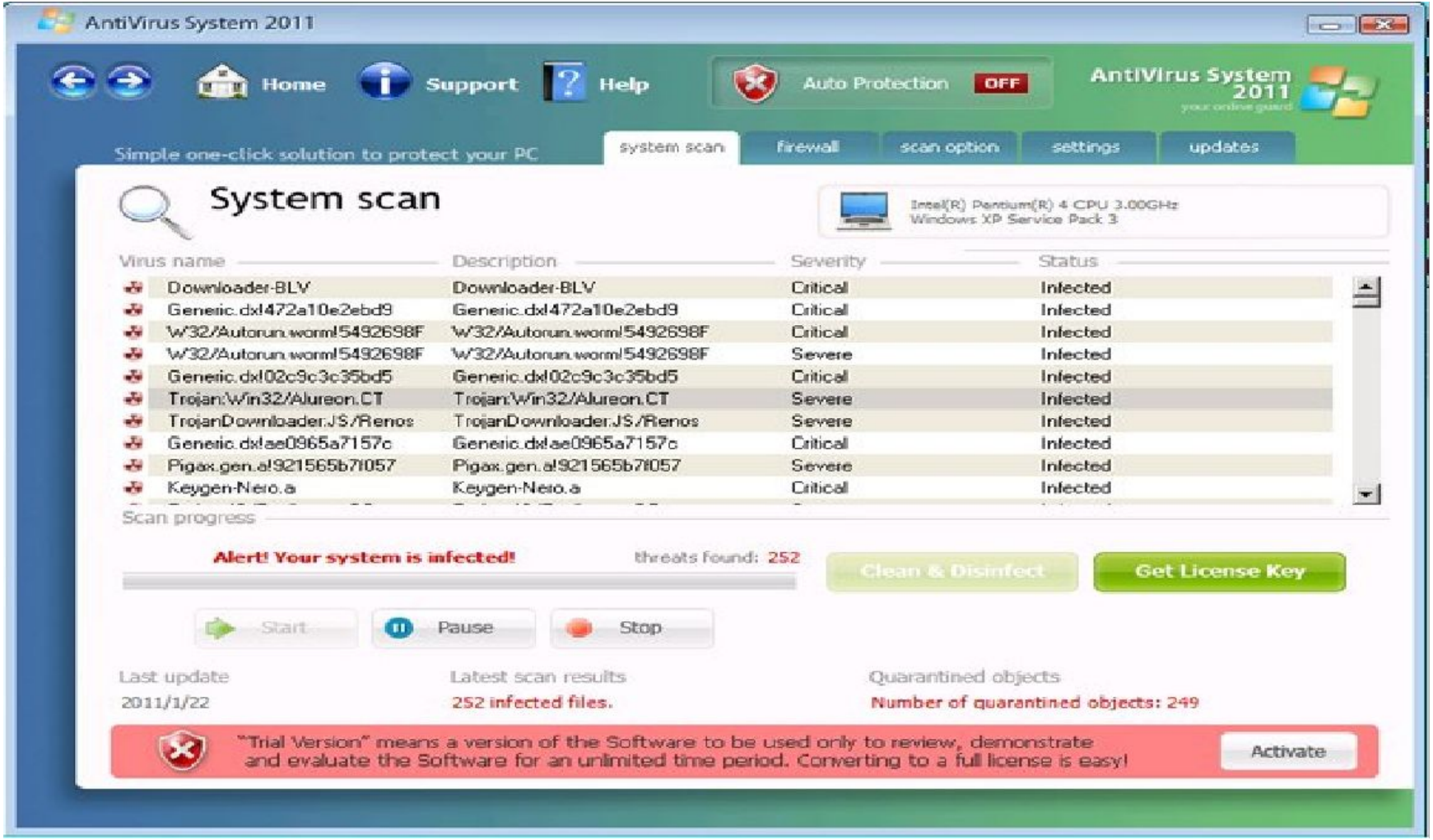
Malvertising Attack

Malvertising is a malicious cyber tactic that attempts to distribute malware through online advertisements.



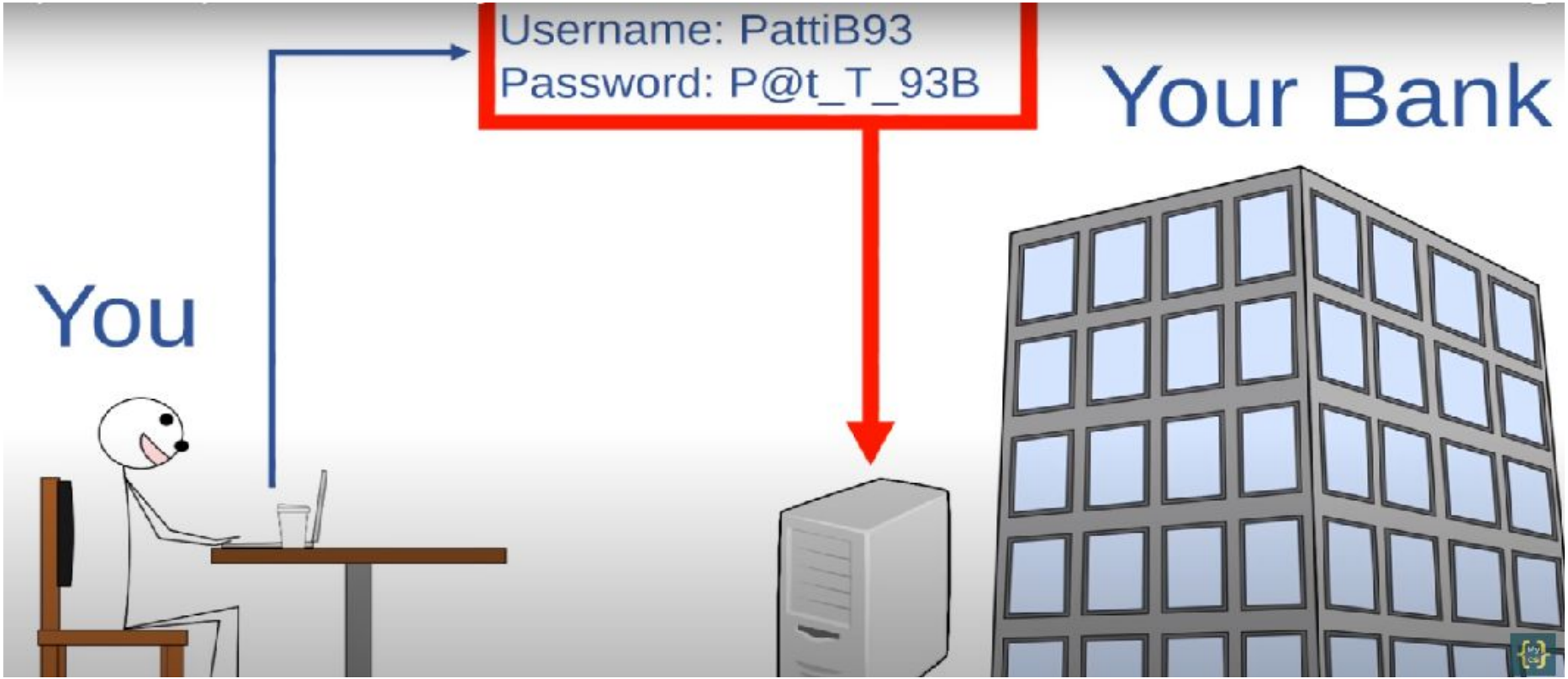
Rogue security software

- **Rogue security software** is a form of malicious software and internet fraud that misleads users into believing there is a virus on their computer and aims to convince them to pay for a fake malware removal tool that actually installs malware on their computer.


AntiVirus System 2011
Home
Support
Help
Auto Protection
OFF
AntiVirus System 2011
your online guard
Simple one-click solution to protect your PC
system scan
firewall
scan option
settings
updates
System scan
Intel(R) Pentium(R) 4 CPU 3.00GHz
Windows XP Service Pack 3
Virus name
Description
Severity
Status
Downloader-BLV
Downloader-BLV
Critical
Infected
Generic.dxl472a10e2ebd9
Generic.dxl472a10e2ebd9
Critical
Infected
W32/Autorun.worm!5492698F
W32/Autorun.worm!5492698F
Critical
Infected
W32/Autorun.worm!5492698F
W32/Autorun.worm!5492698F
Severe
Infected
Generic.dxl02c9c3c35bd5
Generic.dxl02c9c3c35bd5
Critical
Infected
Trojan:Win32/Alureon.CT
Trojan:Win32/Alureon.CT
Severe
Infected
TrojanDownloader:JS/Renos
TrojanDownloader:JS/Renos
Severe
Infected
Generic.dxlae0965a7157c
Generic.dxlae0965a7157c
Critical
Infected
Pigax.gen.a!921565b7f057
Pigax.gen.a!921565b7f057
Severe
Infected
Keygen-Nero.a
Keygen-Nero.a
Critical
Infected
Scan progress
Alert! Your system is infected!
threats found: 252
Clean & Disinfect
Get License Key
Start
Pause
Stop
Last update
2011/1/22
Latest scan results
252 infected files.
Quarantined objects
Number of quarantined objects: 249
"Trial Version" means a version of the Software to be used only to review, demonstrate and evaluate the Software for an unlimited time period. Converting to a full license is easy!
Activate

How many password-protected accounts and devices do you have?

Password-Protected accounts



Introduction-Intrusion Detection System (IDS)

Introduction

- Today in this era of globalization, with the development of information technology as well as ease of access and development of hacking tools, comes the need for security of important data.
- Firewalls may provide this, but they never alert the administrator of any attacks. That's where comes the need for a different system – a sort of detection system.
- An Intrusion Detection System is a required solution to the above problem. It is similar to a burglar alarm system in your home or any organization which detects the presence of any unwanted intervention and alerts the system administrator.

Introduction

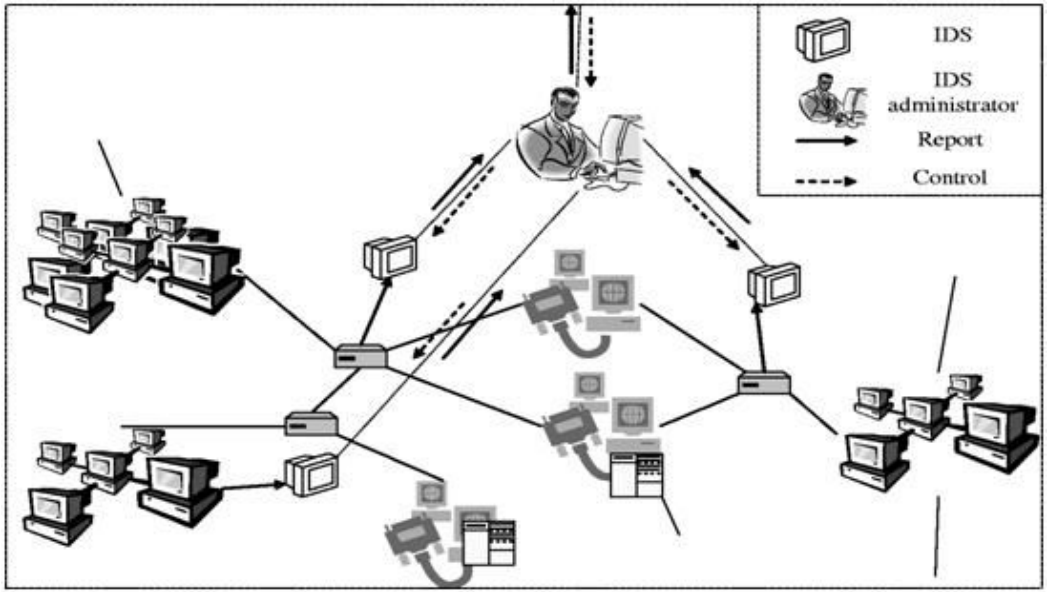
- IDS is a type of software that is designed to automatically caution administrators when anyone is trying to breach through the system using malicious activities.
- Firewalls are software programs or hardware devices which can be used to prevent any malicious attack on the system or on the network. They basically act as filters that block any kind of information which can cause a threat to the system or the network. They can either monitor few contents of the incoming packet or monitor the whole packet.

Classification of Intrusion Detection System

- Network Intrusion Detection System
- Host Intrusion Detection System

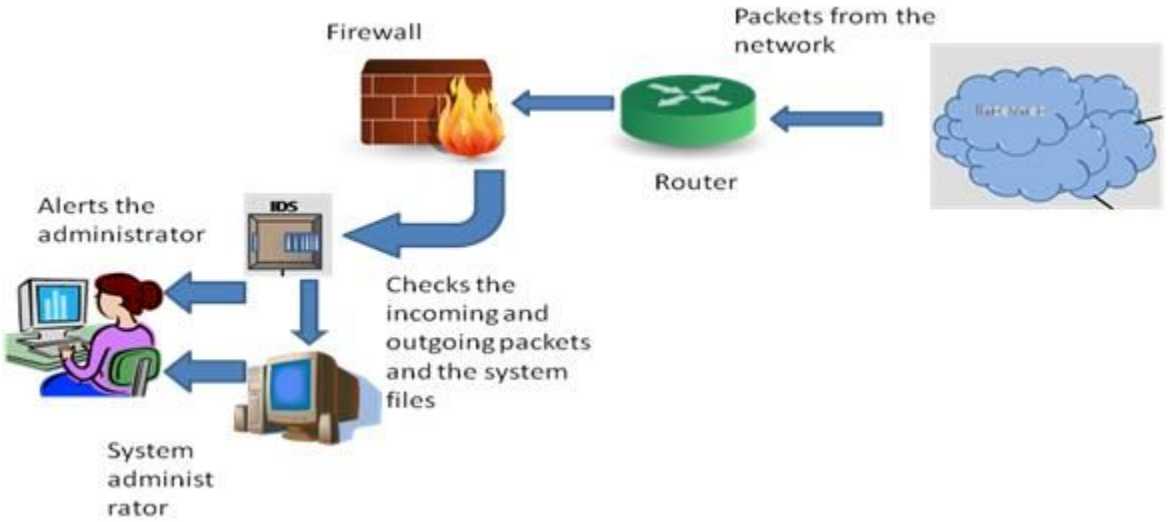
Network Intrusion Detection System

- This system monitors the traffic on individual networks or subnets by continuously analyzing the traffic and comparing it with the known attacks in the library.
- If an attack is detected, an alert is sent to the system administrator.
- It is placed mostly at important points in the network so that it can keep an eye on the traffic traveling to and from the different devices on the network.
- The IDS is placed along the network boundary or between the network and the server. An advantage of this system is that it can be deployed easily and at low cost, without having to be loaded for each system.



Host Intrusion Detection System

- Such a system works on individual systems where the network connection to the system, i.e. incoming and outgoing of packets are constantly monitored and also the auditing of system files is done and in case of any discrepancy, the system administrator is alerted about the same.
- This system monitors the operating system of the computer. The IDS is installed on the computer. The advantage of this system is it can accurately monitor the whole system and does not require installation of any other hardware.

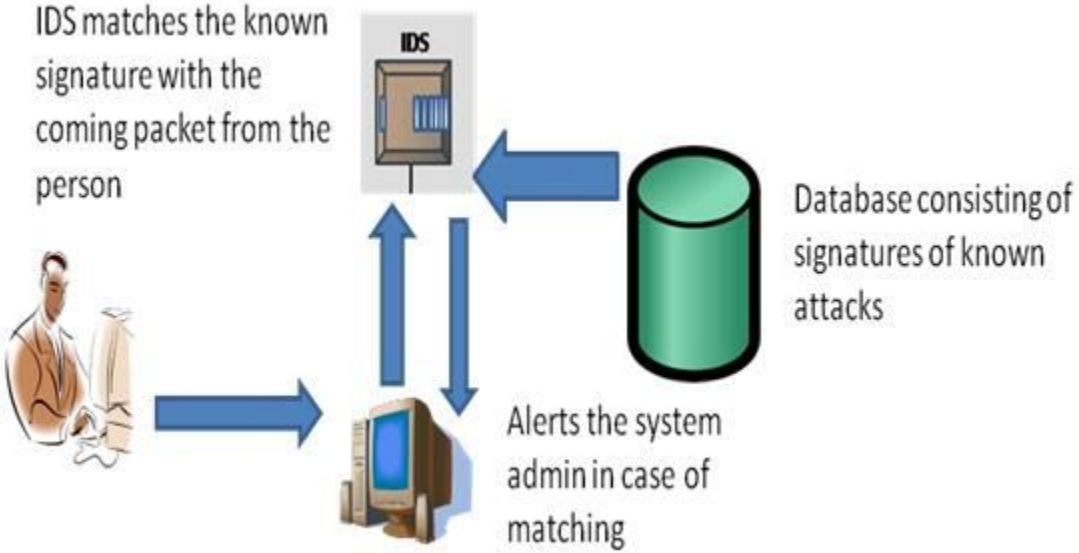


Based on the method of working

- Signature-based Intrusion Detection System
- Anomaly-based Intrusion Detection System

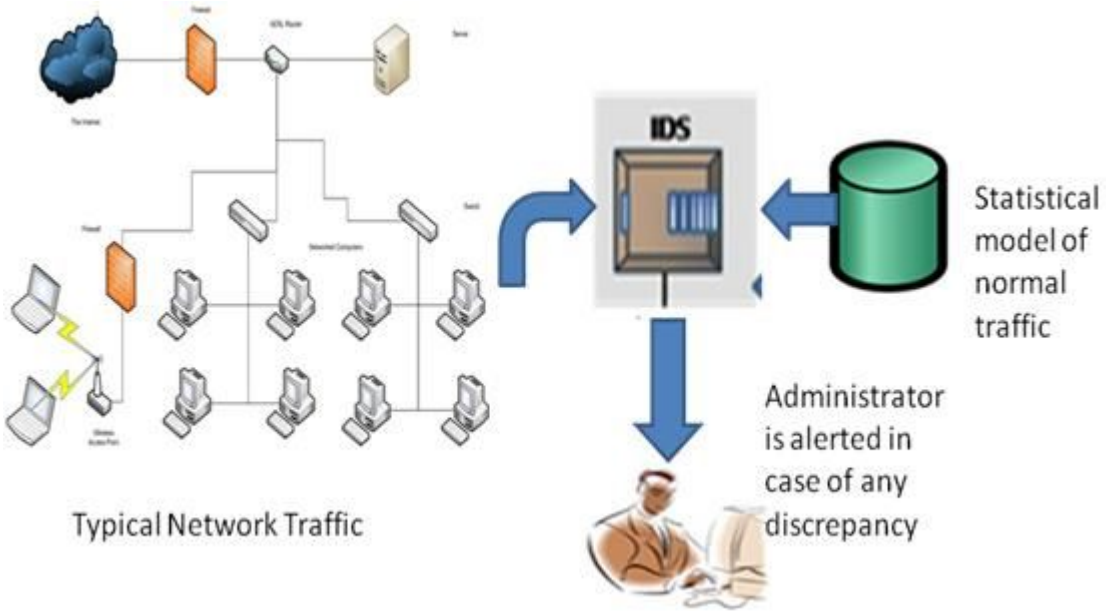
Signature-based Intrusion Detection System

- This system works on the principle of matching. The data is analyzed and compared with the signature of known attacks. In case of any matching, an alert is issued. An advantage of this system is it has more accuracy and standard alarms understood by the user.

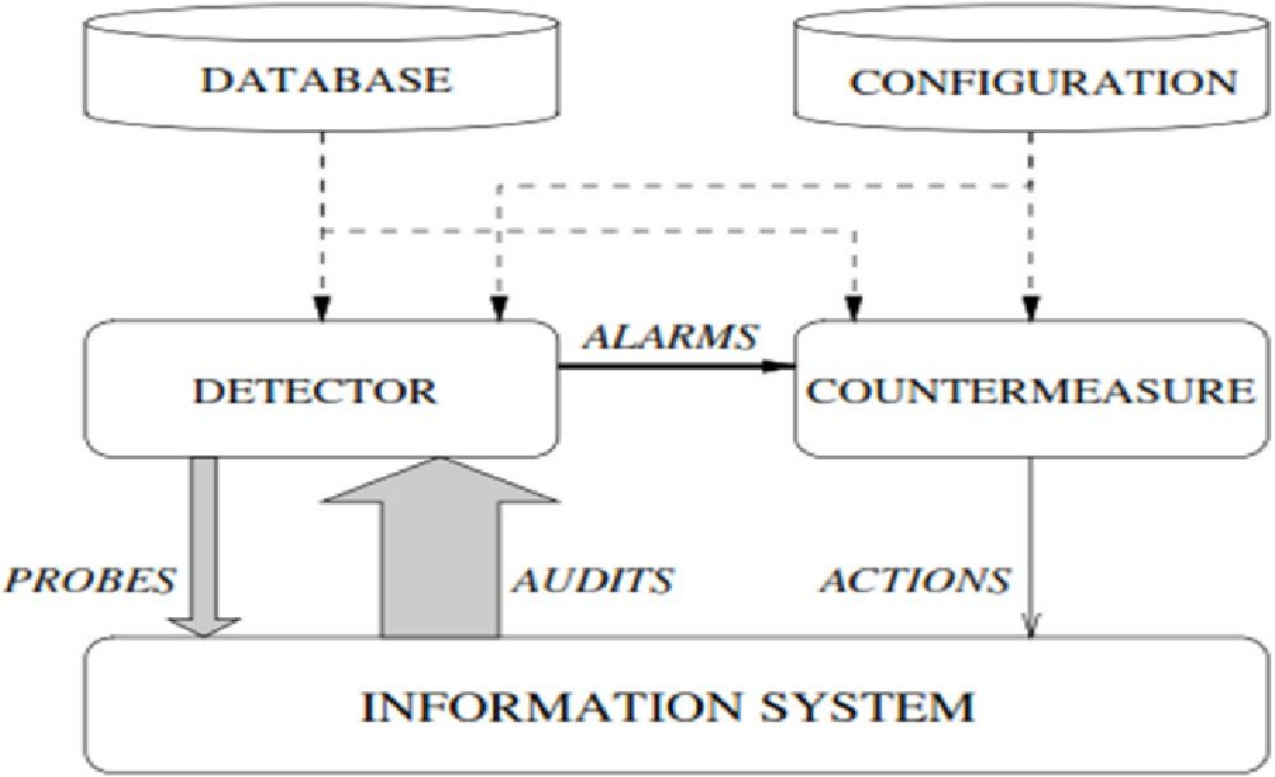


Anomaly-based Intrusion Detection System

- It consists of a statistical model of normal network traffic which consists of the bandwidth used, the protocols defined for the traffic, the ports, and devices that are part of the network.
- It regularly monitors the network traffic and compares it with the statistical model.
- In case of any anomaly or discrepancy, the administrator is alerted. An advantage of this system is it can detect new and unique attacks.



Simple Intrusion Detection System



Threats to information system

Introduction

- Threats to information system can come from a variety of places inside and external to an organizations or companies.
- In order to secure system and information ,each company or organization should analyze the types of threats that will be faced and how the threats affect information system security .
- Examples of threats such as unauthorized access (hacker and cracker) ,computer viruses ,theft.

Unauthorized access (hacker and cracker)

- One of the most common security risks in relation to computerized information systems is the danger of unauthorized access to confidential data .
- The main concern comes from unwanted intruders, or hackers, who use the latest technology and their skills to break into supposedly secure computers or to disable them .
- A person who gains access to information system for malicious reason is often termed of cracker rather than a hacker.
- Example : Spoofing and Sniffing, Denial of Service Attacks (DOS).

Spoofing and Sniffing

- Spoofing is, For example ,if hackers redirect customers to a fake Website that looks almost exactly like the true site ,they can collect and process orders effectively stealing business as well as sensitive customer information from the true site .
- While a sniffer is a type of eavesdropping program that monitors information travelling over a network .When used legitimately ,sniffers can help identify potential network trouble-spots or criminal activity on network ,but when used for criminal purposes ,they can be damaging and very difficult to detect .Sniffer enable hackers to steal proprietary information from anywhere on a network ,including e-mail messages ,company files ,and confidential reports .

Denial of Service Attacks (DOS)

- The main aim of this attack is to bring down the targeted network and make it to deny the service for legitimate users.
- They will install a small program called zombies on some computers those are in intermediate level in the networks ,whenever they want to attack ,they will run those programs remotely and will make the intermediate computers to launch the attacks simultaneously .

Computer Viruses

Worms

- Worms can destroy data and programs as well as disrupt or even halt the operation of computer networks .
- Worm is to modify or destroy the data, but it differs from a virus in that it does not have the ability to duplicate itself.

Trojan horses

- A Trojan appears as a legitimate in order to gain access to computer.
- Typically ,a Trojan will incorporate a key logging facility ,which also called a ‘keystroke recorder’ to capture all keyboard input from a given computer .Capturing keyboard data allows the owner of the Trojan to gather a great deal of information ,such as passwords and the contents of all outgoing e-mail messages .

Theft

Physical Theft

- Physical theft, as the term implies, involves the theft of hardware and software .Components are often targeted by criminals because of their small size and relatively high value .Physical theft results in the loss of confidentiality and availability and make the integrity of the data stored on the disk suspect.

Data Theft

- Data theft normally involves making copies of important files without causing any harm to the originals .This can involve stealing sensitive information and confidential data or making unauthorized changes to computer records .Such data can include passwords activation keys to software, sensitive correspondence, and any other information that is stored on a victim's computer.
- A serious problem related to identity theft is spam .Spam electronic junk mail or junk newsgroup postings, usually for the purpose advertising for some product and / or service .Spammers commonly use zombie computers to send out millions of e-mail messages, unbeknown to the computer users.

Threats to communication networks

Status of Computer Networks

- In February, 2002, the Internet security watch group CERT Coordination Center disclosed that global networks including the Internet, phone systems, and the electrical power grid are vulnerable to attack because of weakness in programming in a small but key network component. The component, an Abstract Syntax Notation One, or ASN.1, is a communication protocol used widely in the Simple Network Management Protocol (SNMP).
- This is one example of what is happening and will continue to happen.
- The number of threats is rising daily, yet the time window to deal with them is rapidly shrinking.
- Hacker tools are becoming more sophisticated and powerful. Currently the average time between the point at which a vulnerability is announced and when it is actually deployed in the wild is getting shorter and shorter.

Common network security threats

1. Computer virus
2. Rogue security software
3. Trojan horse
4. Adware and spyware
5. DOS and DDOS attack
6. Phishing
7. Rootkit
8. SQL Injection attack
9. MIM attacks

Computer virus

Computer viruses are pieces of software that are designed to be spread from one computer to another.

They’re often sent as email attachments or downloaded from specific websites with the intent to infect your computer — and other computers on your contact list — by using systems on your network.

Viruses are known to send spam, disable your security settings, corrupt and steal data from your computer including personal information such as passwords, even going as far as to delete everything on your hard drive.

Rogue security software

Leveraging the fear of computer viruses, scammers have a found a new way to commit Internet fraud.

Rogue security software is malicious software that mislead users to believe that they have network security issues, most commonly a computer virus installed on their computer or that their security measures are not up to date.

Then they offer to install or update users' security settings. They'll either ask you to download their program to remove the alleged viruses, or to pay for a tool. Both cases lead to actual malware being installed on your computer.

Trojan horse

“Trojan horse” refers to tricking someone into inviting an attacker into a securely protected area.

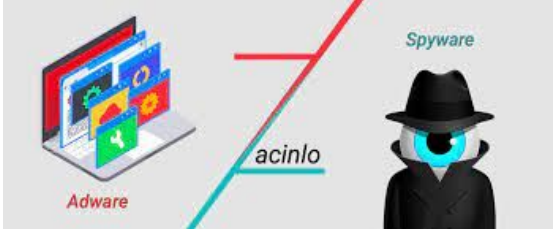
In computing, it holds a very similar meaning — a Trojan horse, or “Trojan,” is a malicious bit of attacking code or software that tricks users into running it willingly, by hiding behind a legitimate program.

They spread often by email; it may appear as an email from someone you know, and when you click on the email and its included attachment, you’ve immediately downloaded malware to your computer.

Trojans also spread when you click on a false advertisement.

Once inside your computer, a Trojan horse can record your passwords by logging keystrokes, hijacking your webcam, and stealing any sensitive data you may have on your computer.

Adware and spyware



By “adware” we consider any software that is designed to track data of your browsing habits and, based on that, show you advertisements and pop-ups. Adware collects data with your consent — and is even a legitimate source of income for companies that allow users to try their software for free, but with advertisements showing while using the software.

The adware clause is often hidden in related User Agreement docs, but it can be checked by carefully reading anything you accept while installing software.

The presence of adware on your computer is noticeable only in those pop-ups, and sometimes it can slow down your computer’s processor and internet connection speed.

When adware is downloaded without consent, it is considered malicious.

Spyware works similarly to adware, but is installed on your computer without your knowledge. It can contain keyloggers that record personal information including email addresses, passwords, even credit card numbers, making it dangerous because of the high risk of identity theft.

DOS and DDOS attack

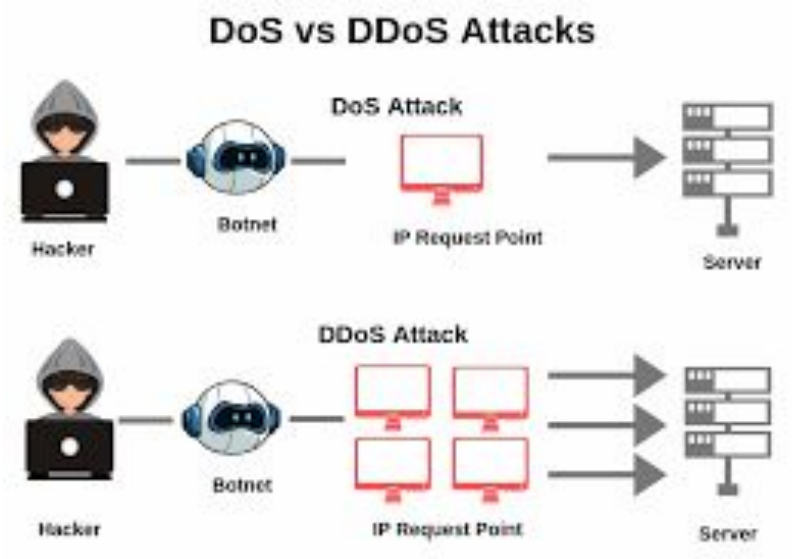
A DoS attack is performed by one machine and its internet connection, by flooding a website with packets and making it impossible for legitimate users to access the content of flooded website.

Fortunately, you can’t really overload a server with a single other server or a PC anymore. In the past years it hasn’t been that common if anything, then by flaws in the protocol.

A DDoS attack, or distributed denial-of-service attack, is similar to DoS, but is more forceful. It’s harder to overcome a DDoS attack. It’s launched from several computers, and the number of computers involved can range from just a couple of them to thousands or even more.

Since the attack comes from so many different IP addresses simultaneously, a DDoS attack is much more difficult for the victim to locate and defend against.


DoS attack
DDoS attack
UpGuard


DoS vs DDoS Attacks
DoS Attack
Hacker
Botnet
IP Request Point
Server
DDoS Attack
Hacker
Botnet
IP Request Point
Server

Phishing

Phishing is a method of a social engineering with the goal of obtaining sensitive data such as passwords, usernames, credit card numbers.

The attacks often come in the form of instant messages or phishing emails designed to appear legitimate. The recipient of the email is then tricked into opening a malicious link, which leads to the installation of malware on the recipient’s computer.

It can also obtain personal information by sending an email that appears to be sent from a bank, asking to verify your identity by giving away your private information.

Rootkit

Rootkit is a collection of software tools that enables remote control and administration-level access over a computer or computer networks.

Once remote access is obtained, the rootkit can perform a number of malicious actions; they come equipped with keyloggers, password stealers and antivirus disablers.

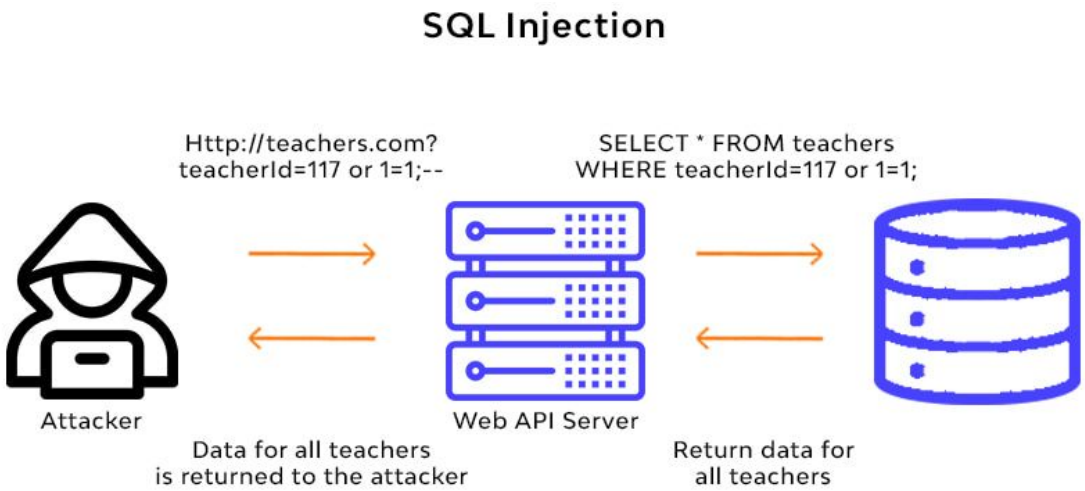
Rootkits are installed by hiding in legitimate software: when you give permission to that software to make changes to your OS, the rootkit installs itself in your computer and waits for the hacker to activate it.

Other ways of rootkit distribution include phishing emails, malicious links, files, and downloading software from suspicious websites.

SQL Injection attack

SQL injection attacks are designed to target data-driven applications by exploiting security vulnerabilities in the application's software.

They use malicious code to obtain private data, change and even destroy that data, and can go as far as to void transactions on websites. It has quickly become one of the most dangerous privacy issues for data confidentiality.



MIM attacks

Man-in-the-middle attacks are cybersecurity attacks that allow the attacker to eavesdrop on communication between two targets. It can listen to a communication which should, in normal settings, be private.

As an example, a man-in-the-middle attack happens when the attacker wants to intercept a communication between person A and person B.

Person A sends their public key to person B, but the attacker intercepts it and sends a forged message to person B, representing themselves as A, but instead it has the attackers public key. B believes that the message comes from person A and encrypts the message with the attackers public key, sends it back to A, but attacker again intercepts this message, opens the message with private key, possibly alters it, and re-encrypts it using the public key that was firstly provided by person A.

Here are just some of the types of MITM attacks:

- DNS spoofing
- HTTPS spoofing
- IP spoofing
- ARP spoofing
- SSL hijacking
- Wi-Fi hacking

5G-based swarm attacks

With the rise of new 5G technologies and networks, higher-speed transfers and large amounts of data can be retrieved and uploaded faster than ever. A new face of cybercrime is emerging.

High bandwidth-based attacks are more usual than ever too, affecting most technologies, but particularly focused on the Internet of Things and mobile devices.

This type of attack also uses AI to discover new victims, switch attack strategy, and correlate and share data with the original attacker.

Wireless Network Components

Wireless Routers

- Like the wired network, wireless router connects directly to a modem through a cable for receiving Internet data packets.
- However, instead of carrying data through cables to computers, wireless routers distribute data packets using one or more antennae.
- It carries binary code data packets or series of 1s and 0s which converted into radio signals and the antennae broadcast wirelessly.
- Computer with a wireless receiver can then receive these radio signals and convert them back into binary code. Unlike a wired router because it establishes a wired local area network (LAN), a wireless router establishes a wireless local area network (Wi-Fi).
- To protect the WLAN, wireless routers commonly engage wireless media access control (MAC) address filtering and Wi-Fi Protected Access (WPA) security.

How to secure your home wireless network router

Wifi systems can reach beyond your home's limits, unlike physical networks

There may be a security risk if you have an open wireless network, as it allows anyone within range of your router to have access to your network.

It is tough to keep track of who has access to your home network once the password is out in the open.

As a result, you should think about making some changes and developing some routines in order to protect yourself against snoopers, intruders, and internet carpetbaggers.

Methods to secure your Router

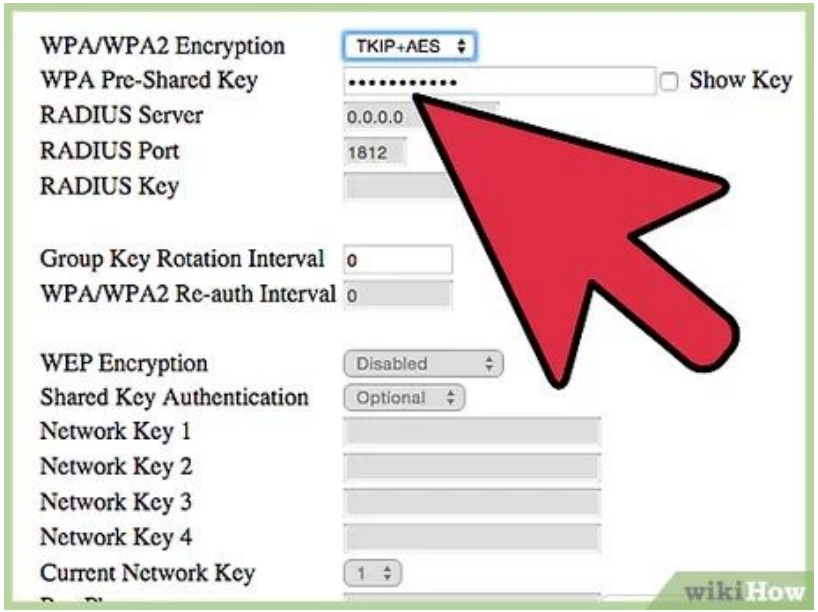
- ### Close the network

(i)Go to your router's configuration page and seek for a Wireless Security option to enable security.

(ii) In the Wireless Security section, you can see an example of a Linksys router configuration.

(iii)Choose from WEP, WPA, or WPA2 as your wireless security method.

(iv)You will need the key for each wireless device that wants to connect to your network once you've activated security on your router.



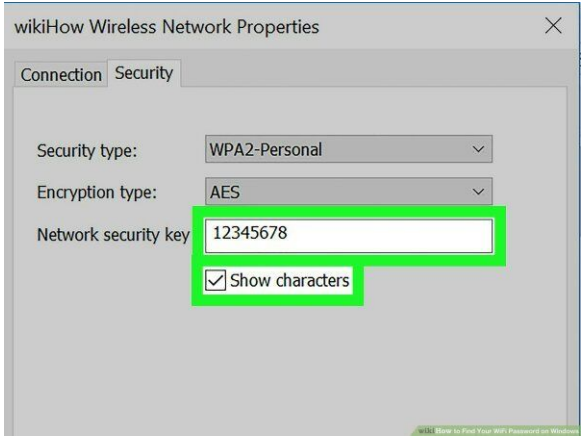
- Make a complicated router password

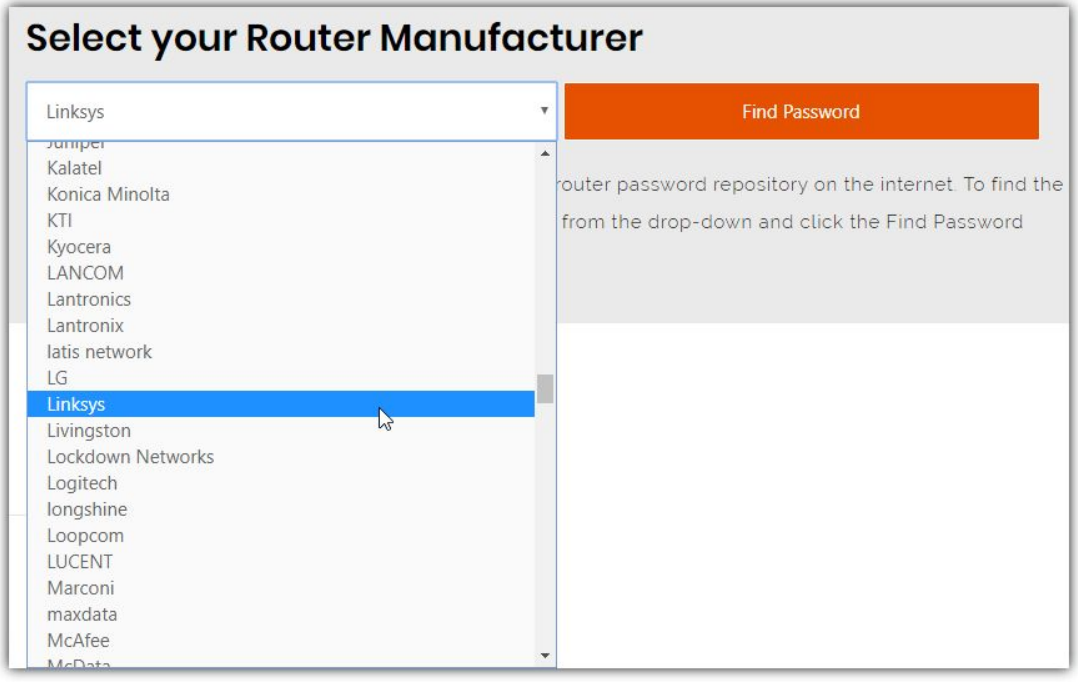
1) Using a string of random characters to make it more difficult for people who attempt to guess your Wifi password and try to gain unauthorized access to your network connection.
2) Use the Comparitech password generator to help you create a strong password, and a Wi-Fi password should be between 12 and 20 characters long.

Change default password

Limit access to the password

Change the password frequently





Wireless access points (WAP), or simply access point (AP)

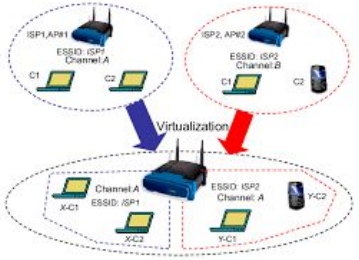
Wireless access point (**WAP**), or more generally just **access point** (**AP**), is a networking hardware device that allows other Wi-Fi devices to connect to a wired network.

As a standalone device, the AP may have a wired connection to a router, but, in a wireless router, it can also be an integral component of the router itself.

An AP is differentiated from a hotspot which is a physical location where Wi-Fi access is available.

Wireless access has special security considerations. Many wired networks base the security on physical access control, trusting all the users on the local network, but if wireless access points are connected to the network, anybody within range of the AP (which typically extends farther than the intended area) can attach to the network.

The most common solution is wireless traffic encryption. Modern access points come with built-in encryption. The first generation encryption scheme, WEP, proved easy to crack; the second and third generation schemes, WPA and WPA2, are considered secure if a strong enough password or passphrase is used.



Network interface cards (NICs)

- A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network.
- It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

Purpose

- NIC allows both wired and wireless communications.
- NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Functions of the Network Interface Card

1. NIC is used to convert data into a digital signal.
2. In the OSI model, NIC uses the physical layer to transmit signals and the network layer to transmit data packets.
3. NIC offers both wired (using cables) and wireless (using Wi-Fi) data communication techniques.
4. NIC is a middleware between a computer/server and a data network.
5. NIC operates on both physical as well as the data link layer of the OSI model.

Types of Network Interface Cards

There are the following two types of NICs -

1. Ethernet NIC

Ethernet NIC was developed by **Robert Metcalf in 1980**. It is made by ethernet cables. This type of NIC is most widely used in the LAN, MAN, and WAN networks.

Example: TP-LINK TG-3468 Gigabit PCI Express Network Adapter.

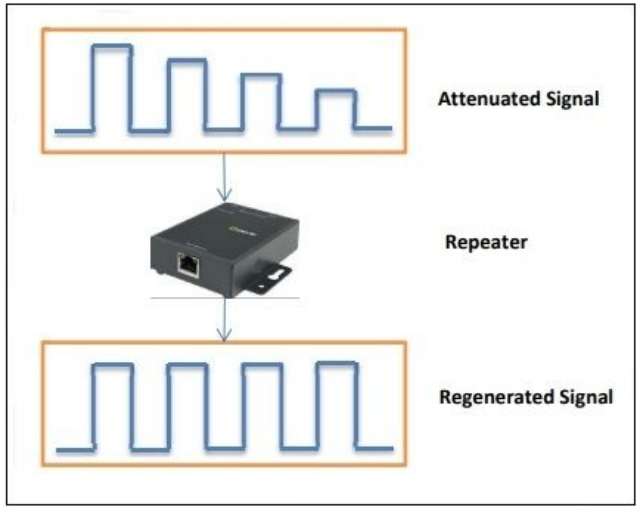
2. Wireless Networks NIC

It is a wireless network that allows us to connect the devices without using the cables. These types of NICs are used to design a Wi-Fi connection.

Example: Intel 3160 Dual-Band Wireless Adapter

Wireless repeater

Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.

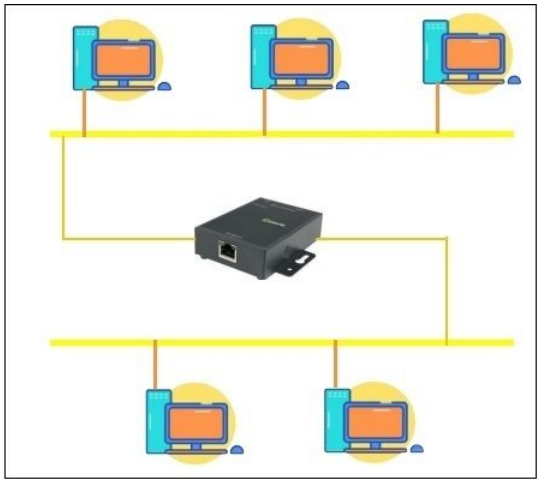


Why are Repeaters needed?

When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals.

Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss.So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN.

- Wireless Repeaters – They are used in wireless LANs and cellular networks.



Advantages of Repeaters

- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- Repeaters don’t require any processing overhead. The only time they need to be investigated is in case of degradation of performance.
- They can connect signals using different types of cables.

Disadvantages of Repeaters

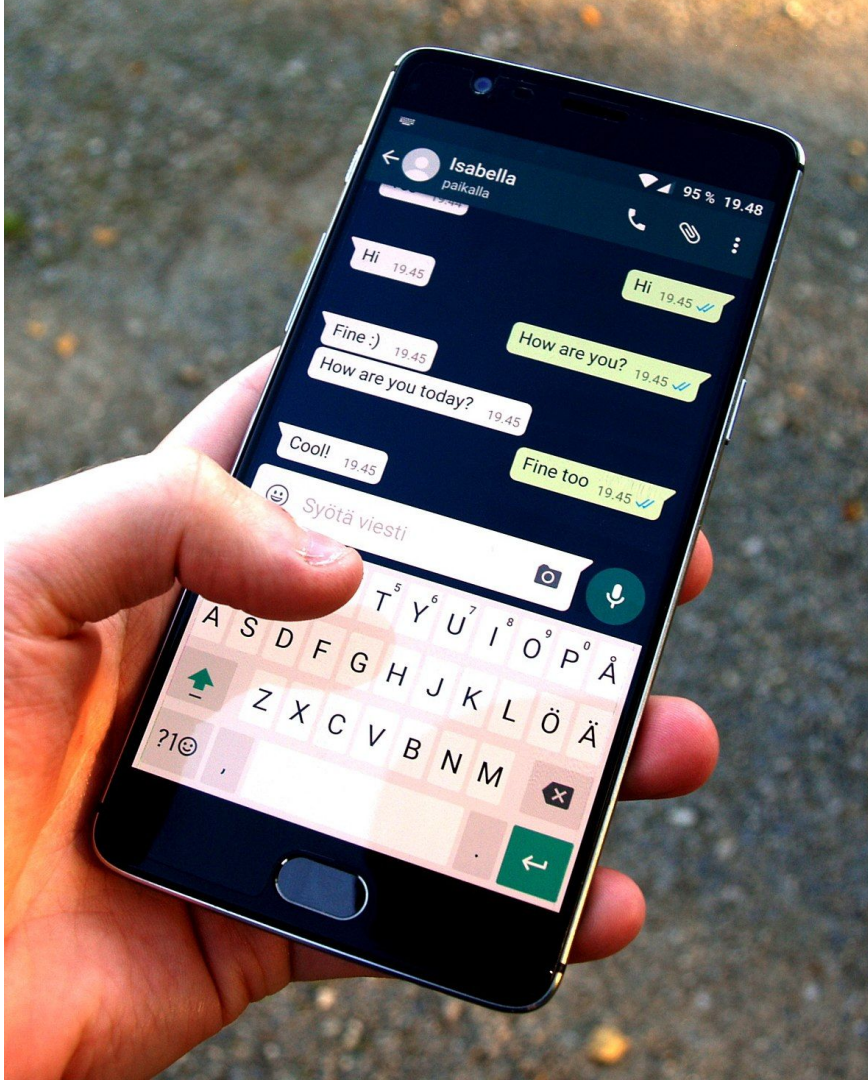
- Repeaters cannot connect dissimilar networks.
- They cannot differentiate between actual signal and noise.
- They cannot reduce network traffic or congestion.
- Most networks have limitations upon the number of repeaters that can be deployed.

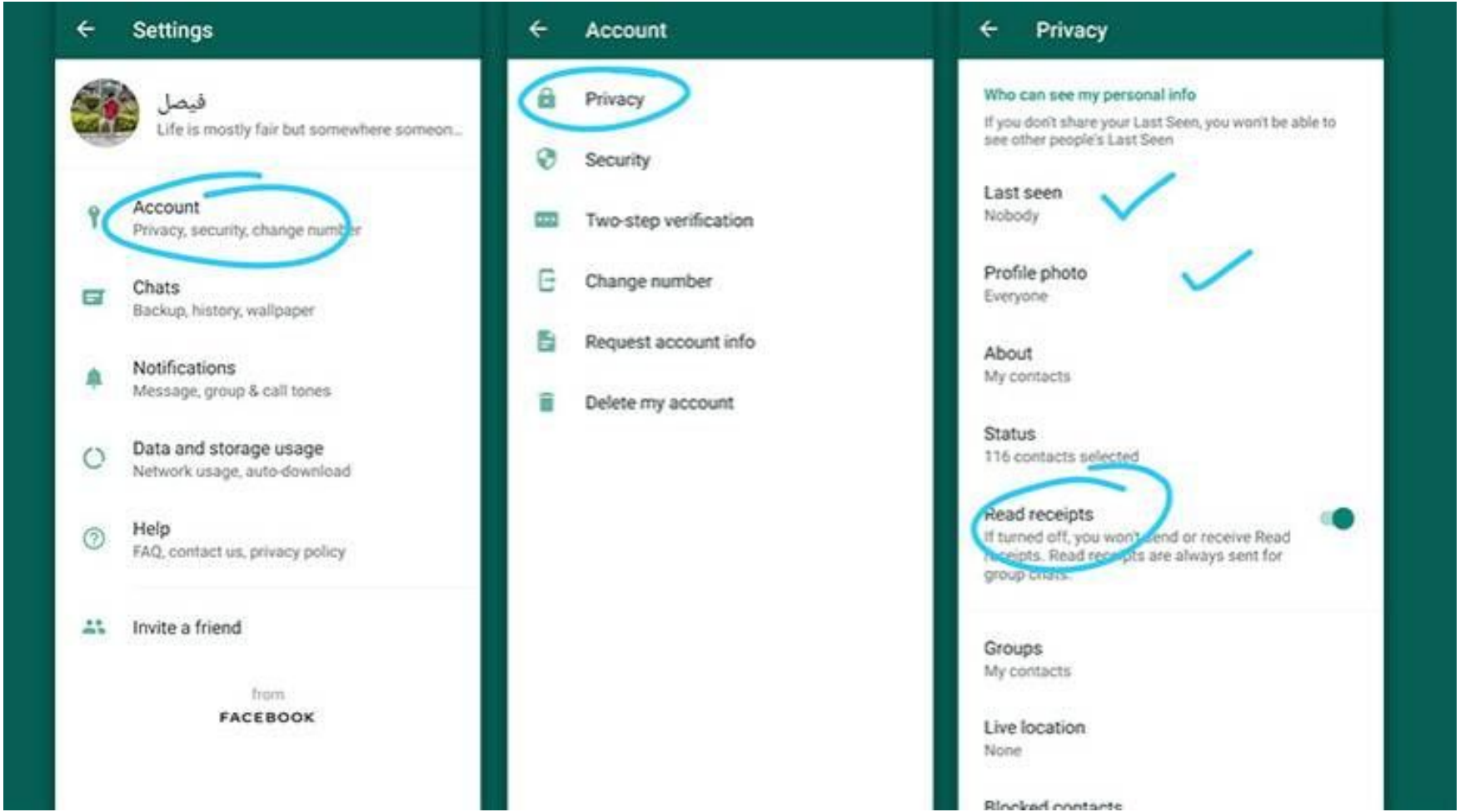
Mobile App Security

Mobile application security

Mobile application security focuses on the software security posture of mobile apps on various platforms like Android, iOS, and Windows Phone.

It involves assessing applications for security issues in the contexts of the platforms that they are designed to run on, the frameworks that they are developed with, and the anticipated set of users (e.g., employees vs. end users).



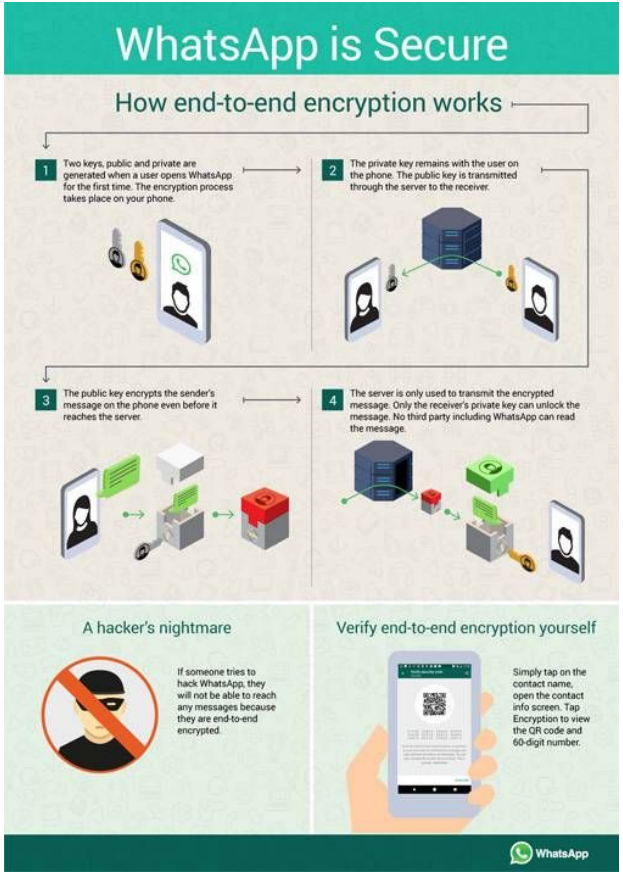

Settings
فيصل
Life is mostly fair but somewhere someon...
Account
Privacy, security, change number
Chats
Backup, history, wallpaper
Notifications
Message, group & call tones
Data and storage usage
Network usage, auto-download
Help
FAQ, contact us, privacy policy
Invite a friend
from
FACEBOOK
Account
Privacy
Security
Two-step verification
Change number
Request account info
Delete my account
Privacy
Who can see my personal info
If you don't share your Last Seen, you won't be able to see other people's Last Seen
Last seen
Nobody
Profile photo
Everyone
About
My contacts
Status
116 contacts selected
Read receipts
If turned off, you won't send or receive Read receipts. Read receipts are always sent for group chats.
Groups
My contacts
Live location
None
Blocked contacts

Common issues that affect mobile apps include:

- Storing or unintentionally leaking sensitive data in ways that it could be read by other applications on the user's phone.

- Implementing poor authentication and authorization checks that could be bypassed by malicious applications or users.

- Using data encryption methods that are known to be vulnerable or can be easily broken.
- Transmitting sensitive data without encryption over the Internet.

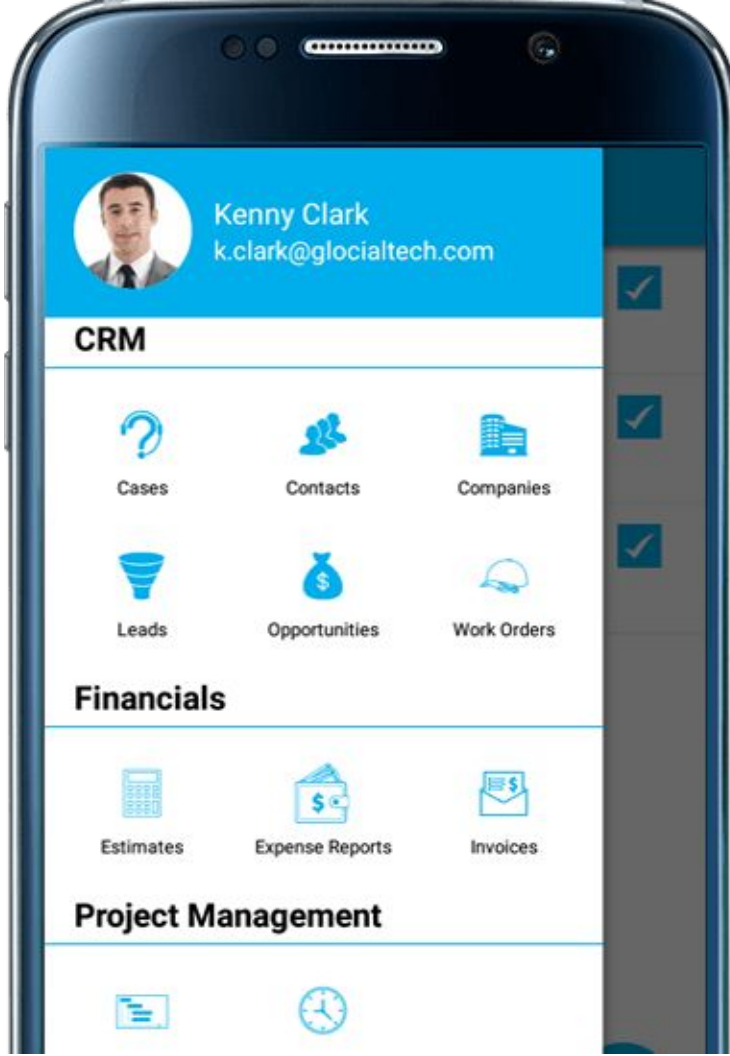


Impact of Weak Mobile A

Consumers are often dependent and trust organizations to test their applications for security measures before making them available to them.Studies conducted by IBM revealed shocking facts.

Customer Information

- Hackers gain login credentials of any website or device; for example, email, banking, social networking websites, etc.
- Anubis banking Trojan is a notorious example in this category, which enters the user's device by downloading compromised apps, some of which are even hosted on the official app stores of Android.
- Once a device is infected, the Trojan forces it to send and receive SMSes, read contact lists, request permission to access device location, allow push notifications, and determine the IP address of the mobile connection along with access to personal files on the mobile device.
- In May 2019, WhatsApp acknowledged that its app was vulnerable to spyware from an Israeli firm NSO group that could infect a mobile device simply by calling a user on WhatsApp from an unknown number.
- Once infected, the spyware could send almost all data - including contact lists, GPS information, media files, etc from the device to the hacker's server.

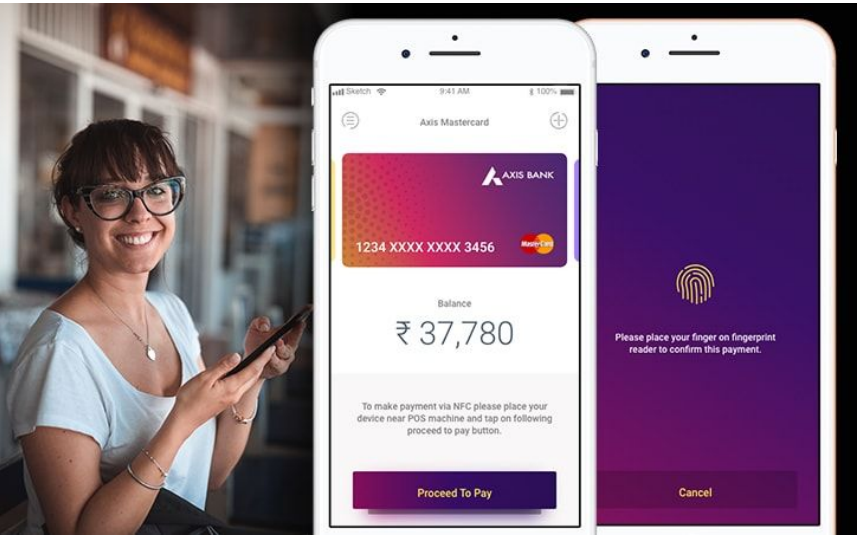


Financial Information

Hackers can gain credit and debit card numbers to make bank transactions, particularly in cases where a one-time password is not required.

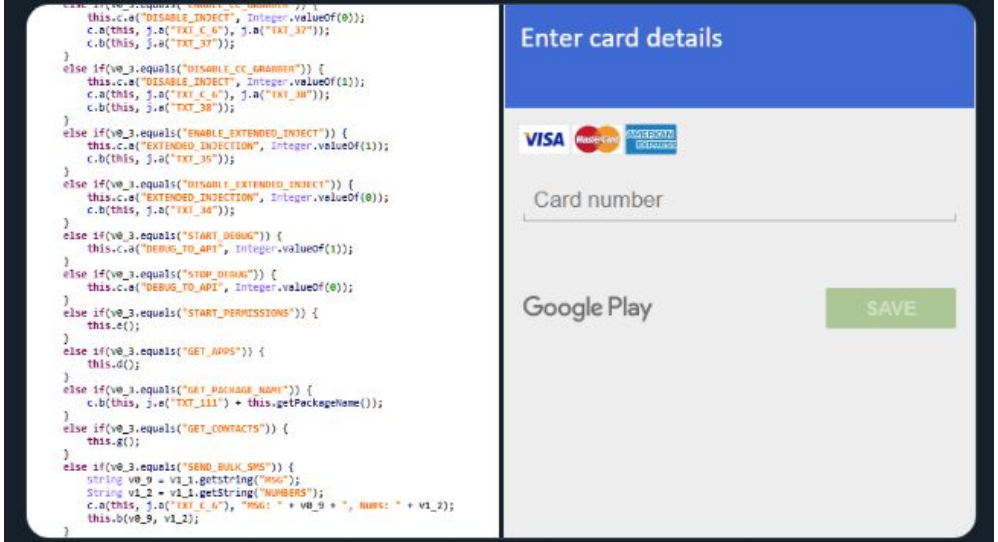
Researchers from Kaspersky discovered a new version of the banking Trojan called Ginp, which could steal user credentials and credit card information from a user's device.

Its ability to take control of the SMS feature of the device allows it to manipulate banking functions. Its code was found to be manipulating 24 apps of Spanish banks.



Tatyana Shishkova
@sh1shk0va

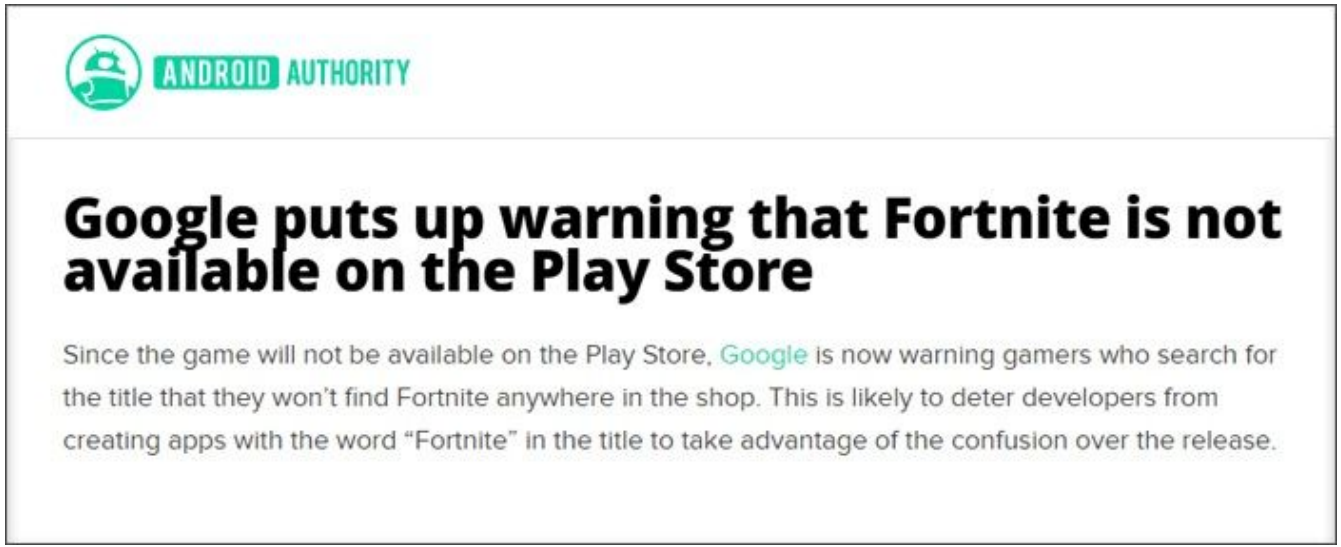
New Android banking Trojan family #Ginp targeting Spain 🇪🇸 and UK 🇬🇧. Latest versions imitate Adobe Flash Player and decrypt payload from assets. Abuses Accessibility Service, sets itself as default SMS app, gets phishing injects from C&C server. (1/2)



IP Theft

Hackers gain the code base of the app to illegally create their clones or simply steal the intellectual property of the company that owns the app.

The more successful an app is, the more number of clones it is likely to attract on app stores. For example, Fortnite and PUBG Mobile became popular and were not available on Google Play store, but many cloning soon became available because of their high popularity, so much so that at one point Google had to warn its users that the official Fortnite was not available at Google Play.



Malicious code injection

User forms can be easily used to inject malicious code and access the server data. For example, certain apps do not restrict the characters a user can input in a field. This allows hackers to inject a line of Javascript in to the login form and gain access to private information.

Mobile botnets

They are a type of bots that run on IRC networks created with the help of Trojans. When an infected device connects to the internet, it starts to work as a client and sends information to a server.

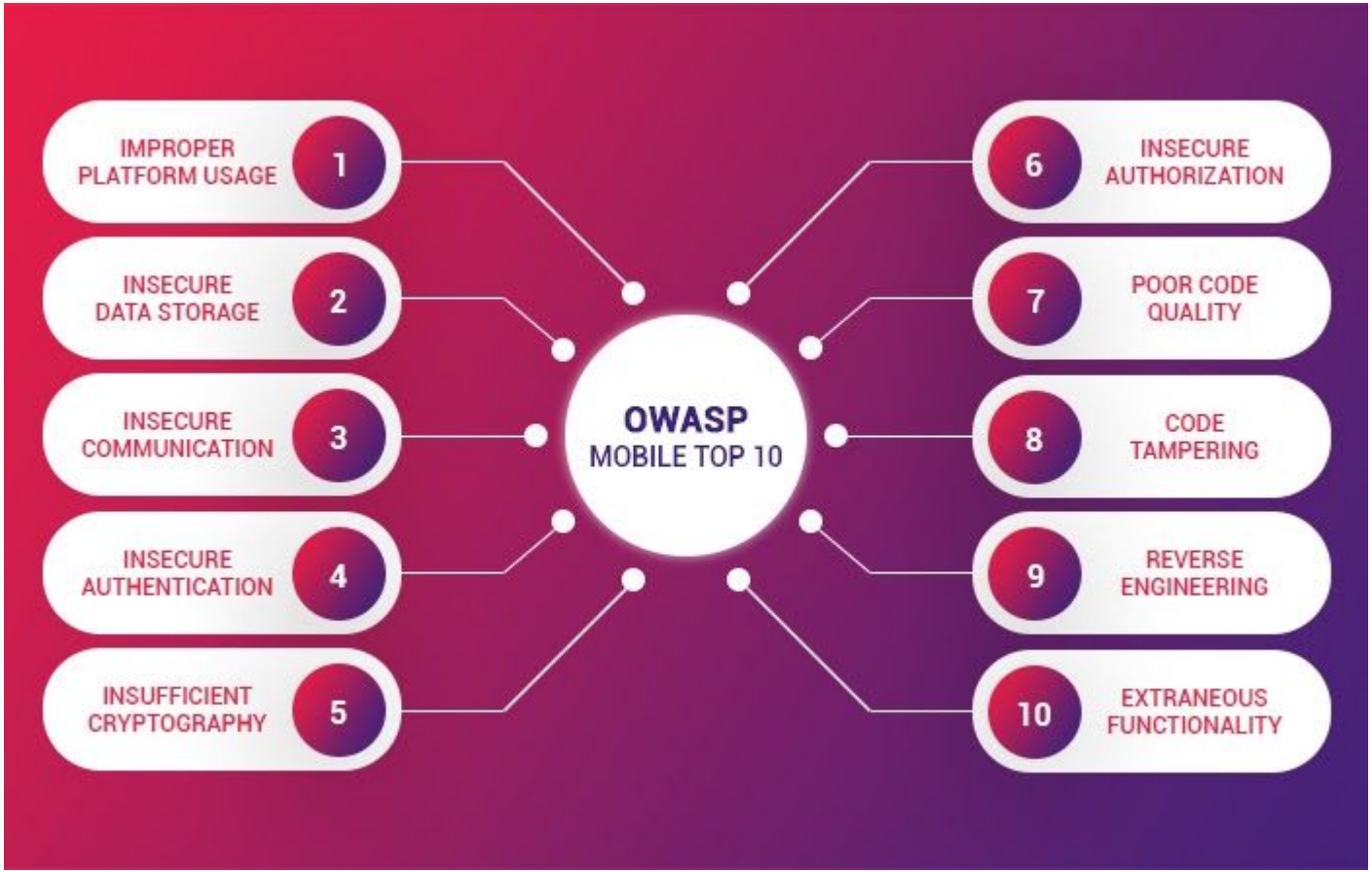
Mobile botnets aim to gain complete control over the device and can be used to send emails and text messages, make phone calls, and access personal data, like photos and contact lists.

Loopholes in Mobile App Security

Mobile apps are not designed to serve as anti-viruses or to transmit data securely over the internet. Rather they focus on a smooth interface and provide the best functionality to users.

Similarly installing an antivirus app may secure the network and prevent attacks on a device, but it cannot provide protection against weak passwords or a poorly designed app.

Most of the common security lapses are documented by industry experts under the aegis of The Open Web Application Security Project (OWASP) for reference for developers


OWASP
MOBILE TOP 10
1
IMPROPER PLATFORM USAGE
2
INSECURE DATA STORAGE
3
INSECURE COMMUNICATION
4
INSECURE AUTHENTICATION
5
INSUFFICIENT CRYPTOGRAPHY
6
INSECURE AUTHORIZATION
7
POOR CODE QUALITY
8
CODE TAMPERING
9
REVERSE ENGINEERING
10
EXTRANEOUS FUNCTIONALITY

Android App Security Risks

Reverse Engineering

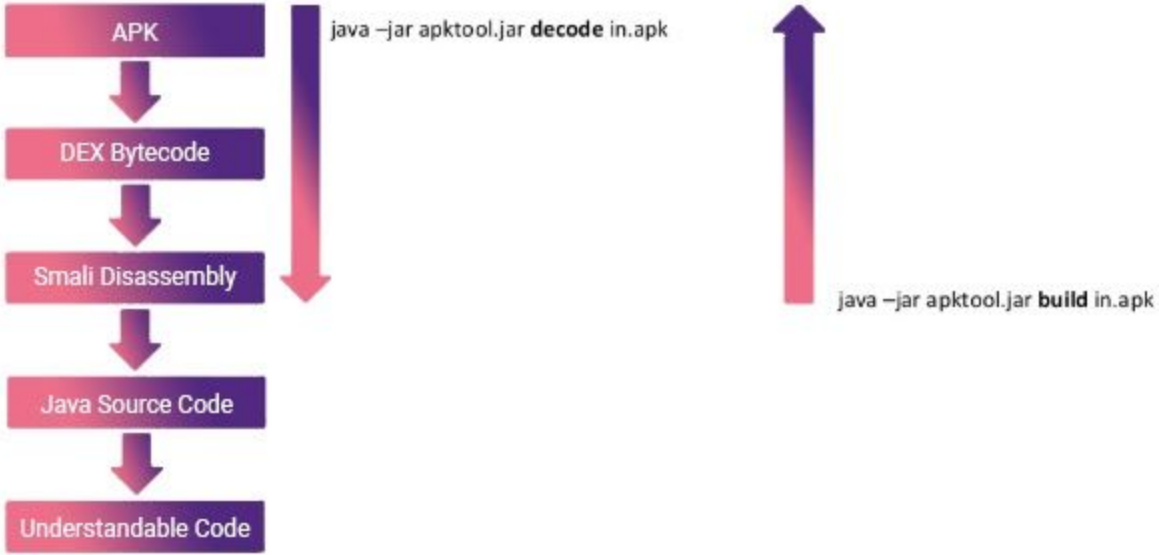
Android apps are developed in Java with an integrated development environment (IDE) like Eclipse. These Java apps can be reversed with various tools available on the internet.

With Android, the bytecode can be altered and packed again in the form of APK files.

Reversing Android apps can easily provide test login credentials, insights into bad design, details about the libraries and classes used.

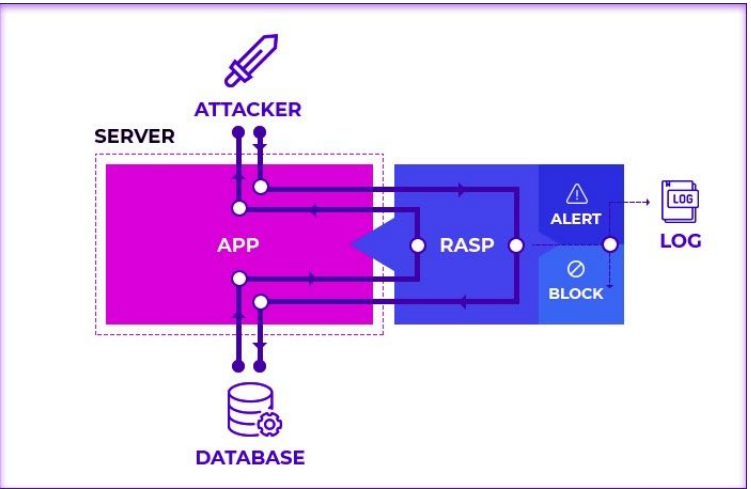
It can also provide details about the type of encryption used in the app. This can help the attacker is not only hacking one device but multiple devices using the same decryption method.

Reversing an APK



Right Steps for Installing APP.

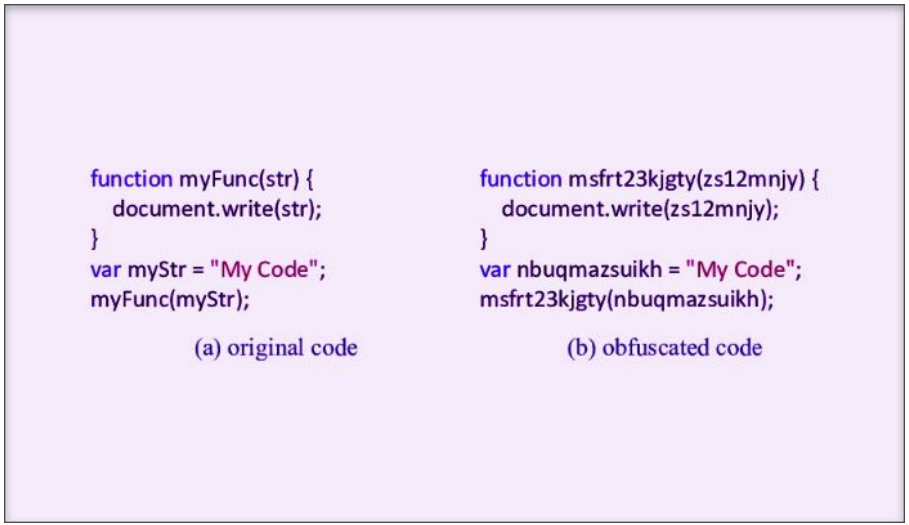
- **Minimal Application Permissions-**No application should seek permission requests beyond its functional area.
- **Guarding sensitive information**- If possible, the volume of data stored on the device should be cut down to minimize the risk.
- **Enhance Data Security**
- **Not Saving Passwords**
- **Enforce Session Logout**
- **Consult Security Experts**
- **Apply Multi-Factor Authentication**
- **Ensure HTTPS Communication**
- **Apply RASP Security-**Runtime application self-protection



Code Obfuscation

One of the best ways to protect an app from hackers is to employ code obfuscation techniques. It is an act of creating a code that is difficult for hackers to understand. This technique has become popular and is used to conceal code from attacks. Obfuscators are used to automatically convert programming code into a format that cannot be understood by humans. Code obfuscation includes:

- Encrypting some or the entire code
- Removing metadata which may reveal information about the libraries or APIs used
- Renaming classes and variables so they cannot be guessed



```
function myFunc(str) {
  document.write(str);
}
var myStr = "My Code";
myFunc(myStr);
```

(a) original code

```
function msfrt23kjgty(zs12mnjy) {
  document.write(zs12mnjy);
}
var nbuqmazsuikh = "My Code";
msfrt23kjgty(nbuqmazsuikh);
```

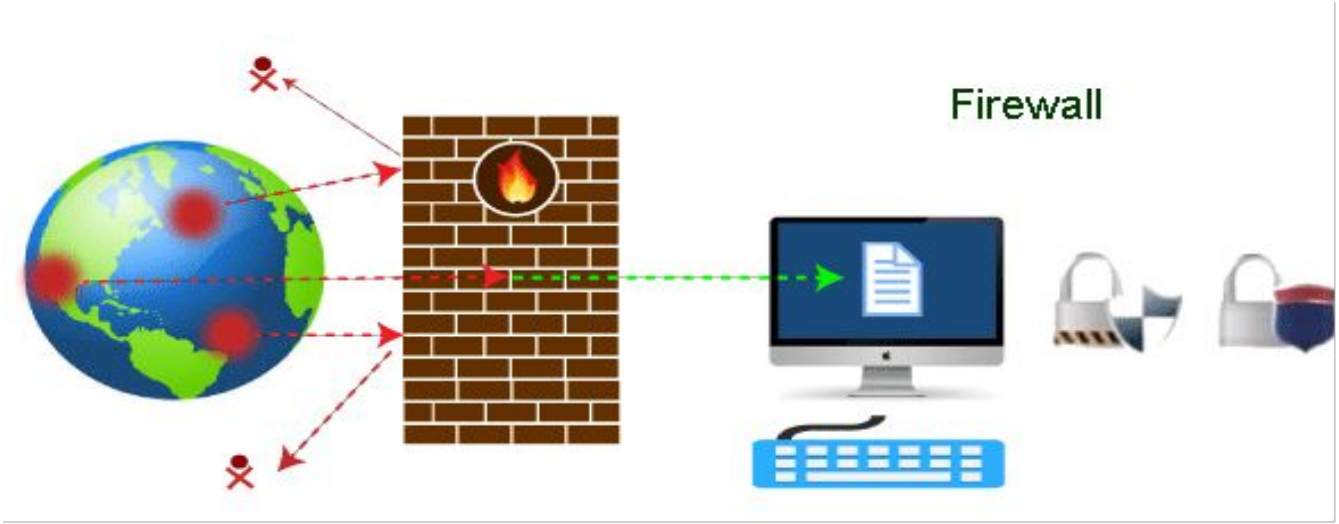
(b) obfuscated code

Firewall

Firewall

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.



Firewall: Hardware or Software

- This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., hardware and software.
- A hardware firewall is a physical device that attaches between a computer network and a gateway. For example, a broadband router.
- A software firewall is a simple program installed on a computer that works through port numbers and other installed software.

Why Firewall

- Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network. They do not allow data packets to be transferred through them unless the data is coming or going from a user-specified trusted source.
- Firewalls are designed in such a way that they can react quickly to detect and counter-attacks throughout the network. They can work with rules configured to protect the network and perform quick assessments to find any suspicious activity. In short, we can point to the firewall as a traffic controller.

Some of the important risks of not having a firewall are:

Open Access

- If a computer is running without a firewall, it is giving open access to other networks. This means that it is accepting every kind of connection that comes through someone. In this case, it is not possible to detect threats or attacks coming through our network. Without a firewall, we make our devices vulnerable to malicious users and other unwanted sources.

Lost or Comprised Data

- Without a firewall, we are leaving our devices accessible to everyone. This means that anyone can access our device and have complete control over it, including the network. In this case, cybercriminals can easily delete our data or use our personal information for their benefit.

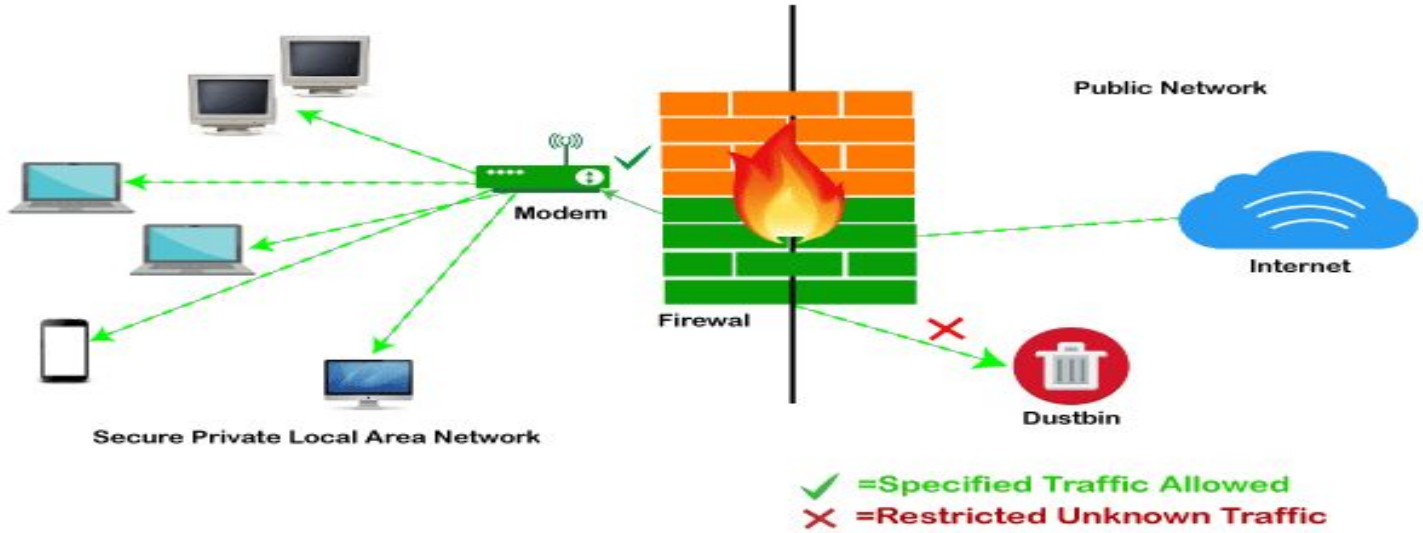
Network Crashes

- In the absence of a firewall, anyone could access our network and shut it down. It may lead us to invest our valuable time and money to get our network working again.
- Therefore, it is essential to use firewalls and keep our network, computer, and data safe and secure from unwanted sources.

How does a firewall work?

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.



Functions of Firewall

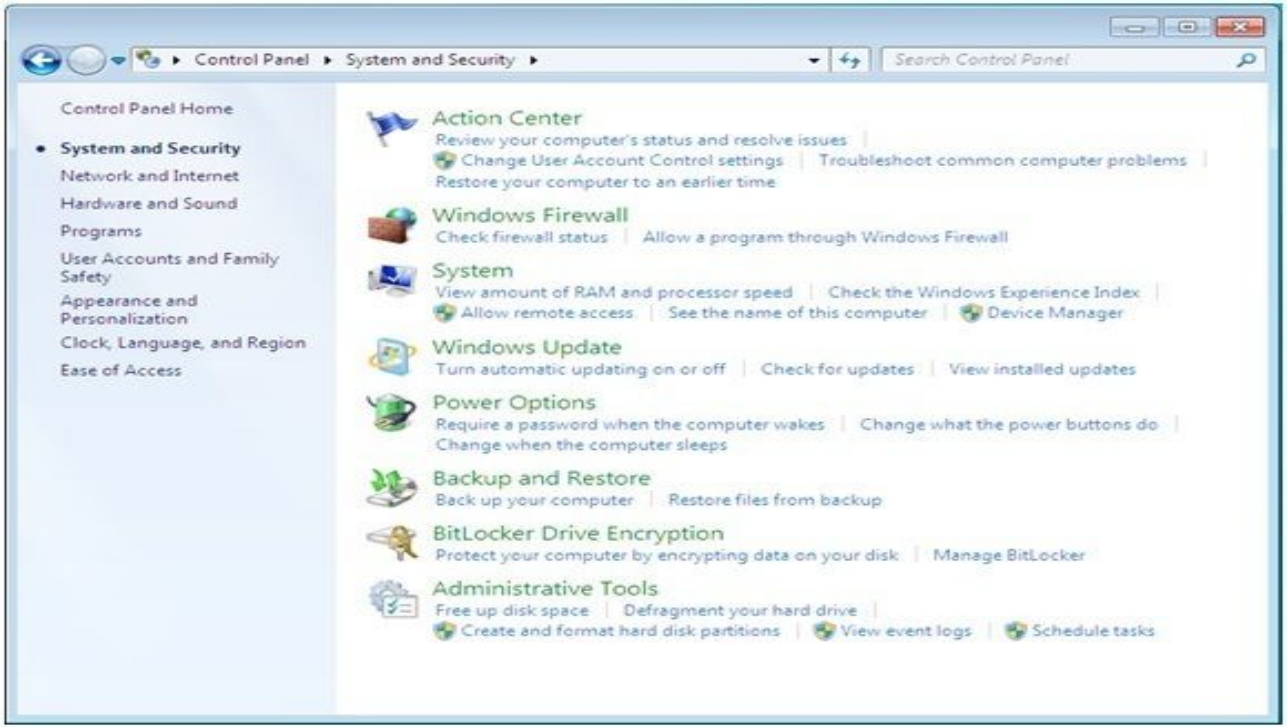
- The firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources.
- Since the firewall acts as a barrier or filter between the computer system and other networks (i.e., the public Internet), we can consider it as a traffic controller. Therefore, a firewall's primary function is to secure our network and information by controlling network traffic, preventing unwanted incoming network traffic, and validating access by assessing network traffic for malicious things such as hackers and malware.
- Generally, most operating systems (for example - Windows OS) and security software come with built-in firewall support. Therefore, it is a good idea to ensure that those options are turned on. Additionally, we can configure the security settings of the system to be automatically updated whenever available.

Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events

Setting Up a Firewall: Windows

- Setup system and security settings
- From the Start menu, click **Control Panel**, then click **System and Security**
- Under Windows Firewall, select either **Check firewall status** to determine whether the firewall is turned on or off, or **Allow a program through Windows Firewall** to allow a blocked program through the firewall

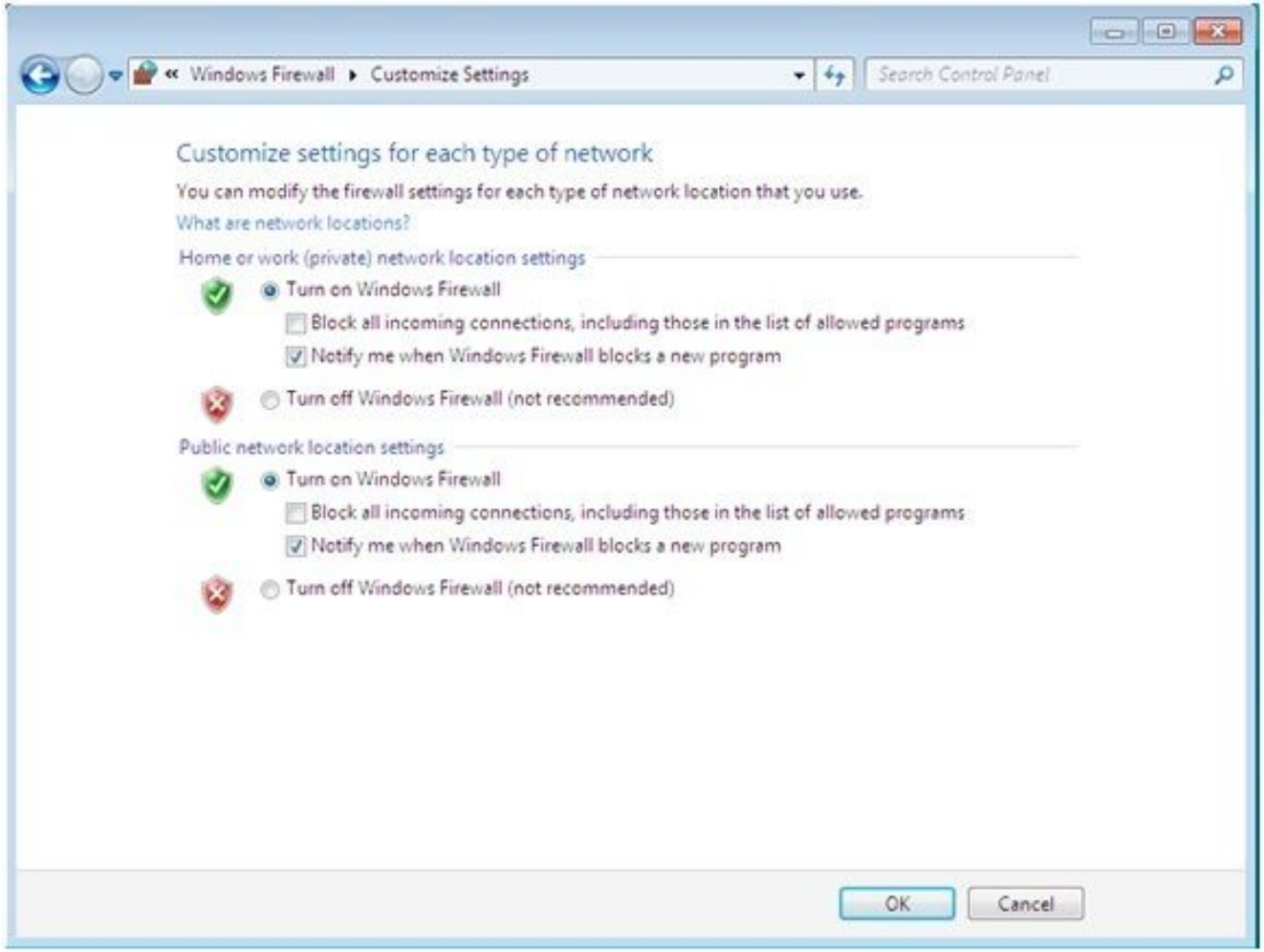


2. Select program features

- Click **Turn Windows Firewall on or off** from the left side menu
- Configure the settings for your home/work (private) or public network
- Click **OK** to save your changes

3. Choose firewall settings for different network location types

- Turn on Windows Firewall for each network location you use - **Home or work (private)** or **Public**
    - Click **What are network locations?** for more information on network types
    - Domain network locations are controlled by your network administrator and can't be selected or changed
- Select **Turn on Windows Firewall** under the applicable network location type (in image below, both locations are selected)
- Select **Notify me when Windows Firewall blocks a new program** for each network type, if the box is not already checked
- Click **OK** to save your changes


« Windows Firewall ▸ Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network location that you use.
What are network locations?
Home or work (private) network location settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed programs
Notify me when Windows Firewall blocks a new program
Turn off Windows Firewall (not recommended)
Public network location settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed programs
Notify me when Windows Firewall blocks a new program
Turn off Windows Firewall (not recommended)
OK
Cancel

Web Browser Security

- Web browser security consists of all measures, procedures, and policies necessary to protect users accessing the Internet from a web browser application.
- Almost everyone who is online has a web browser available on their computer or mobile device. Since it is so common, hackers and other cybercriminals prefer to launch compromising attacks on this client-side application.
- A web browser can store information for your convenience, but others may eventually access the information.
- Therefore, it provides a large surface area for exposure to email accounts, usernames, all sorts of passwords, and personal or corporate information.
- Attackers often target the web browser to hijack or sniff on the web traffic from it. They may also use it as a means to access the device itself or any files available on it.

1. How Attackers Target the Browser

- The web browser can display text documents, play multimedia files, and allow users to play games or interact with forms and all other content on the Internet.
- The versatility of the web browser is good, but this also makes it more challenging to secure since there are more “weak points” an attacker could exploit. The most vulnerable parts of a web browser are as follows:
- Connections to DNS servers, websites, and other online resources
- A DNS server is the bridge between the browser and the content from any site. It points the browser to the correct website, and the site makes the appropriate content available to the browser.
- Many attacks compromise and intercept this communication, and it can occur at one of several points. The goal is often to redirect the browser to a malicious website, where the browser (and by implication, the user) encounters driveby downloads, exploit kits, and unwanted content.

2. Browser plugins

- Browsers are frameworks on which users can install third-party tools to be more comprehensive. However, such plugins may contain vulnerabilities that cyberattacks can exploit to snoop on the browser's web traffic, hijack it, and install malware or carry out harmful actions on the device. Finance-related data is lucrative for such browser attacks.

3. Browser-specific vulnerabilities

- Flaws in a browser can enable attackers to sniff sensitive data passing through the web browser, such as when the user fills web forms. These flaws may also give criminal elements unwarranted access to devices.

How to Improve Web Browser Security

In computing circles, this is also called “hardening the browser” by taking measures to improve security and prevent attacks. Note that it’s nearly impossible to achieve 100% impenetrability, but attackers will have a much harder time succeeding.

1. Use the latest web browser version

Users should get the latest updates of their web browser software. Vendors often release updates of their browsers, adding new functionality or improving existing features. The most critical security features include:

- **Anti-phishing**: Assess and filter suspicious links in search results or on a webpage.
- **Anti-malware**: Scan and block downloading of suspicious files.
- **Plugin security**: Analyse and block insecure plugins.
- **Sandbox**: Build a fence around web browser processes to prevent access to the operating system.

A few browsers include an auto-update function, notifying the user of updates.

2. Restrict user access

- It is advisable to use the web browser from a limited user account without administrator privileges. It limits the ability of any malware that succeeds in infecting the machine to have little to no room to operate within the machine.

3. Use custom security settings

- Even though the controls differ, modern browsers often allow some customisation of security-related settings. The recommendation is to set the following settings as high as possible:
- **Block fake sites**: Always enable this feature to prevent unplanned visits to malicious websites.
- **Camera & Microphone**: These should never run automatically. The browser should confirm if the user wants to use the camera or microphone at any time.
- **Cookies**: Completely disable cookies. Users should only enable cookies if a trusted site needs them.
- **JavaScript**: Same rule as for cookies.
- **Plugins/Add-ons**: Same rule as for cookies and JavaScript
- **Pop-up windows**: Same rule as for cookies, JavaScript, and Plugins/Add-ons.
- Only include plugins that improve security or those you will use

Some plugins improve web browser security. Security professionals recommend the following for all browsers:

- **Flashblock**: This add-on will prevent Flash ads from playing until the user opts to allow them.
- **HTTPS Everywhere**: This plugin encrypts a user's web browsing traffic. It is the result of a joint effort by the **Electronic Frontier Foundation** and **The Tor Project**.
- **NoScript** or **ScriptSafe**: These programs are popular and block scripts on websites unless the user explicitly accepts to run them. The US-CERT specifically recommends NoScript.

Using Multiple Browsers

- A user may install multiple web browsers as a way to improve security. Document viewers and email clients may use another browser or offer various functionalities depending on the browser in use. Specific browsers may be necessary to open certain file types. The point is that one web browser will not necessarily fit all of a user's applications and purposes.

- It is therefore essential to securely configure each web browser available on a computer. There is a distinctive advantage in dedicating one web browser for sensitive activities such as online banking while dedicating another for general-purpose web browsing.
- The use of multiple browsers greatly minimises the probability of compromising sensitive information in a specific browser, website, or software.
- Improving internet security for web browsers will protect networked data and computer devices from malware or privacy breaches.

Implementing security measures in web browser

Implementing security measures in web browse

- Browser security is the application of Internet security to web browsers in order to protect networked data and computer systems from breaches of privacy or malware.

- Web browser security consists of all measures, procedures, and policies necessary to protect users accessing the Internet from a web browser application.

Implementing security measures in web browse

- Almost everyone who is online has a web browser available on their computer or mobile device.
- A web browser can store information for your convenience, but others may eventually access the information.
- Therefore, it provides a large surface area for exposure to email accounts, usernames, all sorts of passwords, and personal or corporate information. Attackers often target the web browser to hijack or sniff on the web traffic from it.

Implementing security measures in web browse

- **Browser Security Best Practices**
  - Keep Browsers Up-to-Date
  - Use HTTPS
  - Use Unique Passwords
  - Disable Auto-Complete for Forms
  - Block Pop-ups and Ads
  - Limit the Use of Cookies

Browser Security Best Practices

1. Keep Browsers Up-to-Date

- Keeping your browser software updated is an essential part of browser security and must never be overlooked.

- Hackers are constantly hunting for flaws in browsers that they can exploit, with new vulnerabilities being exposed every day.

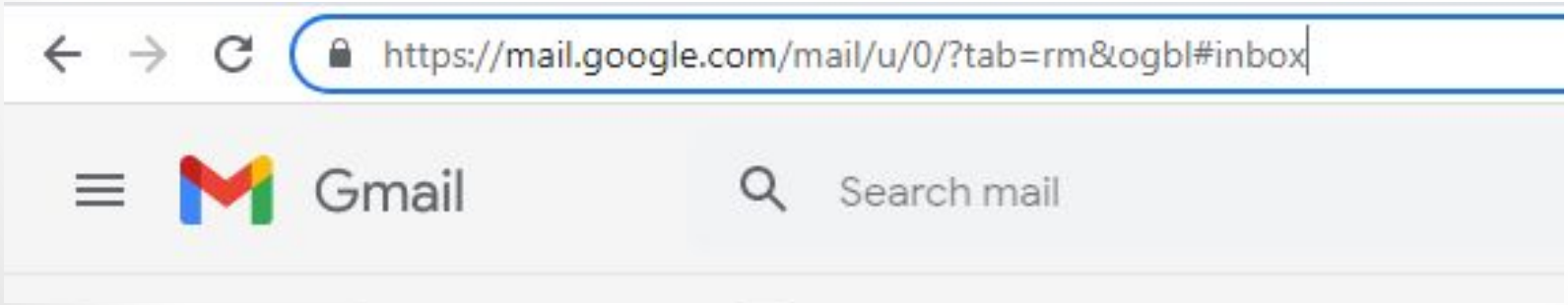
Browser Security Best Practices

- On company-owned devices, ensure you have an automated patching mechanism to update browsers to the latest version.
- On user-owned devices, educate users to always run the most up-to-date version of the web browser to protect themselves and the network from browser attacks.

Browser Security Best Practices

2. Use HTTPS

- When visiting a website, users should make sure the site uses HTTPS, which is a secure, encrypted communication protocol.
- Users should look for the padlock in the URL bar of the browser, and if it isn't there (a warning will typically be displayed), avoid using the website.



Browser Security Best Practices

3. Use Unique Passwords

- Reusing the same password across multiple sites means attackers can compromise a user's sensitive information more easily, as they can access multiple resources once they have cracked a single password.

- Users need to understand that billions of cracked passwords are freely available on the dark web, probably including their own weak, reused passwords.

Browser Security Best Practices

- Give simple technique to generate strong, unique passwords they can remember. Alternatively, provide an automated mechanism to generate strong passwords.

- Ensure that users change their passwords frequently, at least every 90 days.

Browser Security Best Practices

4. Disable Auto-Complete for Forms

- Most browsers, as well as many websites, provide the option of remembering passwords and personal details entered into forms.

- This information, intended to make it easier to revisit websites and fill out forms in future, provides a reservoir of data that attackers can exploit. Hidden fields allow websites to steal form data.

Browser Security Best Practices

- Need awareness that an attacker can more easily detect if they have enabled auto-complete for forms.
- If Users remain logged into a site, attackers can hijack their browsing session and steal their data.
- Users must disable auto-complete features on the browser are disabled and clear any stored passwords.

Browser Security Best Practices

5. Block Pop-ups and Ads

- Pop-up windows are usually a form of online advertisement designed to drive web traffic or obtain the user's email address.

- A pop-up window typically opens a new web browser window displaying an advertisement.

Browser Security Best Practices

- Ads can also be malicious—there have been many cases of advertisements shown on legitimate publisher websites, which contained malicious scripts that could do damage to visitors.

- Modern browsers have a built-in ability to block popups, and users should enable this option. It is preferable for users to install a browser extension from a known, safe software provider to block popups and ads.

Browser Security Best Practices

- **Limit the Use of Cookies**
- Cookies are small text files that are stored in the browser cache when a user visits certain websites. There are two main types of cookies:

  - First party cookies
  - Third party cookies

Browser Security Best Practices

- **First party cookies** are stored directly by the websites you visit and may contain information such as username and login credentials.
- This allows users to quickly login on subsequent visits, and remembers their session data.
- However, these cookies are an attractive target for cybercriminals, who can use them to steal user credentials or sensitive data.

Browser Security Best Practices

- **Third party cookies** are served by the website the user is visiting, on behalf of an external website or advertiser.

- They may be used to track the user's activities for marketing purposes, but may also be used for malicious purposes.