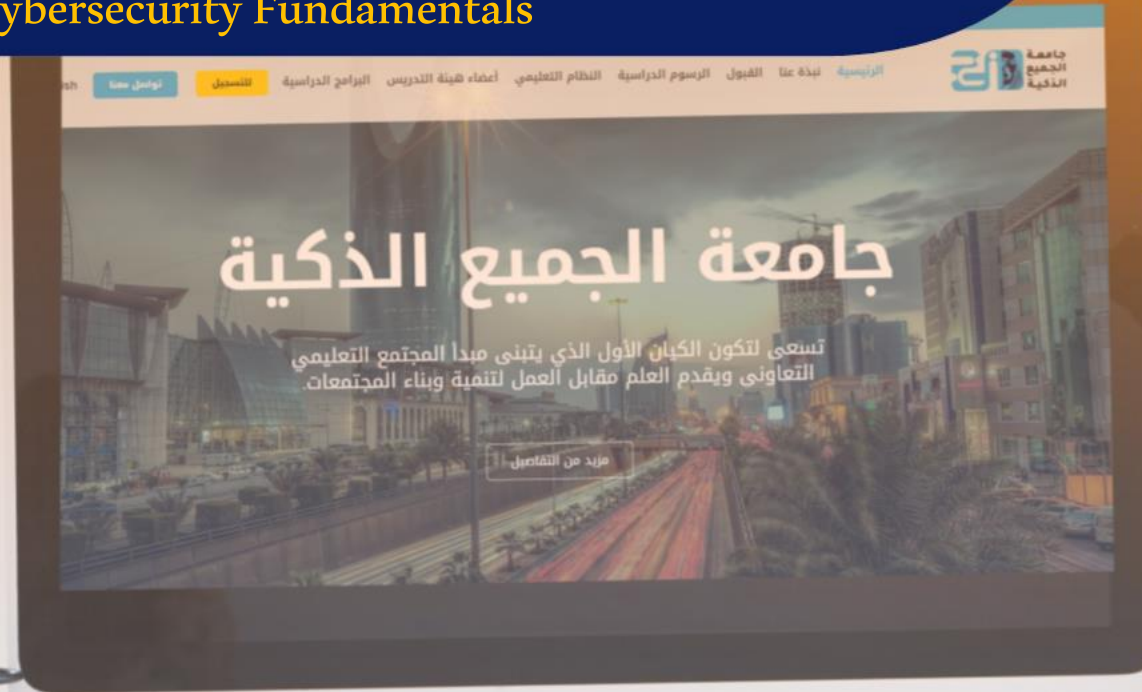


CYB670

Prevention from Cyberattacks

Cybersecurity Fundamentals



Prepared by Dr. Redhwan M. A. Saad

Lecture # 8



جامعة الكوفة
EVERYONE'S SMART UNIVERSITY

Prevention from Cyberattacks

Introduction

Algorithms and
Techniques

Firewalls

Intrusion
Detection/Preventi
on Systems

Authentication
Using Hash

Secure Socket Layer

Virtual Private
Network

Mac Computer
Firewall
Configuration

Choosing the Right
Browser

Multifactor
Authentication



Introduction

- **Cyberattacks cost** billions of dollars to the businesses, government organizations, defense institutes, and many other sectors that directly impact on our day to day lives.
- The cyberattacks are becoming more and more sophisticated and advanced in technology and ideology.
- New techniques and patterns are being utilized to **launch cyber-attacks** on the networks, data, services to disrupt the genuine processes and systems of our peaceful loving people all around the world.
- The **prevention from the cyberattacks** also need to a step ahead of the thinking of the cyber criminals to counter them, but normally conditions, it happens very rarely.
- The cyber criminals are more creative and also diverse in thinking.
- But the main components that they use for launching the cyberattacks include the **exploitations of the weaknesses** in your computers, web pages, networks, databases, and lack of awareness about the security threats in the users of the internet, and computer technologies.



Introduction

- **Cyber security** to prevent or reduce the impact of cyberattacks is the name of continuous practice of security measures and standards.
- So, the fundamental component to prevent your IT system from cyber-attacks is the security awareness of the users of the IT systems.
- The **awareness of the cyber security** will include the following important factors.
 - Continuously educate the people about cyber security
 - Make the users realize the importance of password security
 - Train about keeping the software updated
 - Provide guidelines on how to deal with unknown emails
 - Train for the potential social engineering ways that exploit the innocence of people
 - Implement proper system logout and monitoring mechanism



Introduction

- The awareness and implementation of the standard guidelines in the people **creates a strong shield against the cyber attacks.**
- According to the Small Biz Trends research, more than 52% of the cyber attacks on small businesses take place due to the human errors, system failures and other factors, while 48% of the attacks are done deliberately for fulfilling the malicious intentions.
- **Small businesses** are normally *short of money to purchase and train the staff for cyber security*. That's why some of the serious attacks take place on the small businesses on a regular basis.
- The **cyber attacks prevention measures** can be classified into **two major categories**:
 - Cyber attack **preventive** measures
 - Cyber attack **corrective** measures



Introduction

The **cyberattacks preventive measures** include the following **major activities**:

- Stick to the company security guidelines
- Never underestimate the hackers
- Keep all software and tools updated
- Always back up your data
- Keep your backup data encrypted and protected
- Follow the password management policies strictly
- Follow email use policy strictly
- Use intrusion detection and intrusion prevention systems (IDS/IPS)
- Implement and antivirus software and firewalls



Introduction

- On the other hand, the **corrective measures** are normally taken, when some cyber-attacks have broken into the systems and need the immediate and befitting response to reduce the impact of the cyber-attack.
 - Block the suspected IDs and IPs
 - Isolate the affected or targeted system from the other network
 - Rerouting of the traffic should be done
 - Block the malicious and suspected traffic
 - Implement the disaster recovery mechanism
 - Assess the depth of the attack and consequent damages
 - Inform the concerned security and law enforcement agencies
 - Use the backed-up data to restore the services



Introduction

Let's discuss about the **main techniques, systems, guidelines** used for the **prevention of cyberattacks** in the present modern marketplace:

- Algorithms and Techniques
- Firewalls
- Intrusion detection/prevention systems
- Authentication Using Hash
- Multi-factor Authentication
- Mac Computer Firewall Configuration
- Choosing the Right Browser (Mozilla Firefox)
- Secure Socket Layer
- Virtual Private Network.

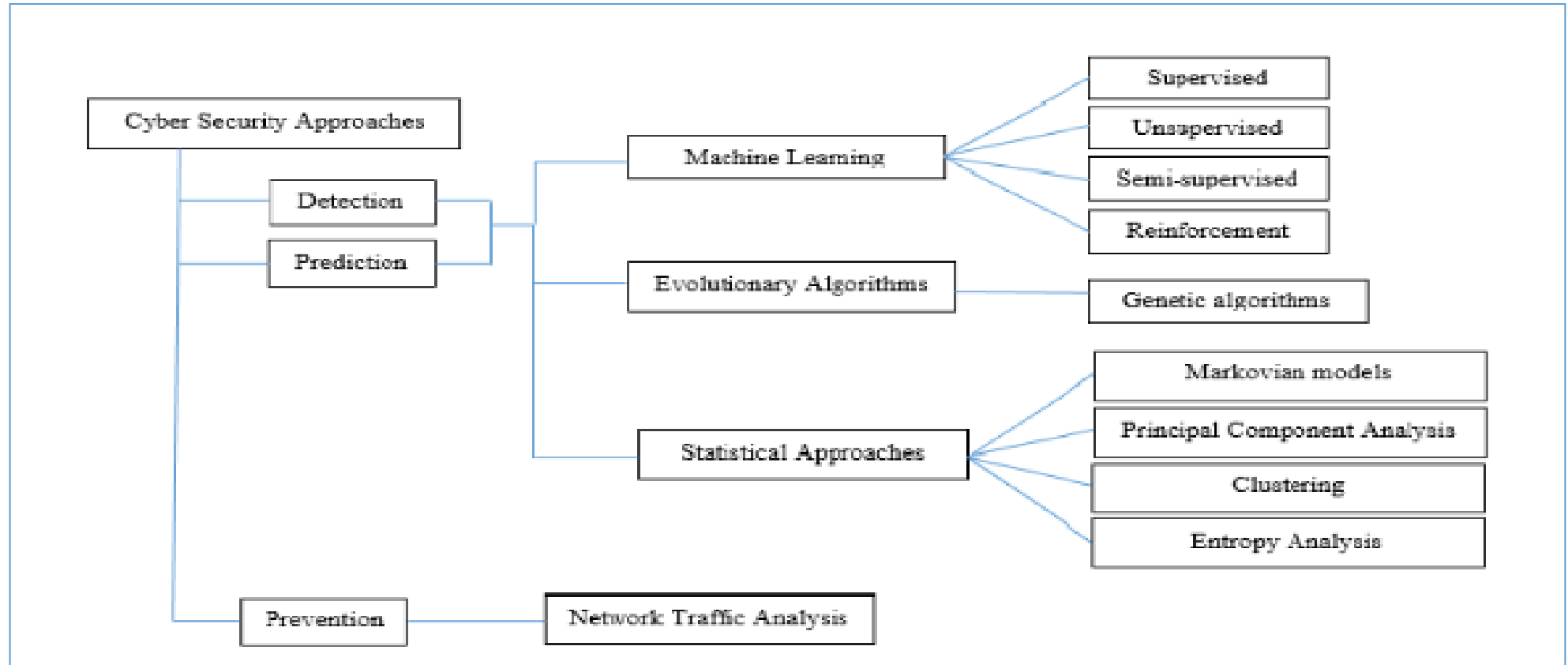


Algorithms and Techniques



- This is very important to know that our online as well as offline **digital resources are not 100% safe at all**, though many great security methods, policies, techniques, and modern algorithms have designed and implemented in the cyber security field.
- The **approach of prevention of cyberattacks** fall in the three major activities as listed below:
 - Detection of cyberattacks
 - Prediction of cyberattacks
 - Prevention of cyberattacks

Algorithms and Techniques



Algorithms and Techniques



- Two approaches mentioned in the above diagram – cyberattack detection and predictions – use commonly similar types of algorithms.
- Those algorithms include the evolutionary, statistical and machine learning, while the cyberattack prevention approach uses the network traffic analysis algorithms to achieve the desired objectives.
- **Cyberattack Detection**
- **Cyberattack Prediction**
- **Cyberattack Prevention**

Algorithms and Techniques

❖ Cyberattack Detection...

- Cyberattack detection approach is very fundamental in ensuring the security of the IT resources including the computers, servers, networks, and databases.
- The cyberattack detection uses three types of major algorithms as given below:
 - Machine learning algorithms
 - Evolutionary algorithms
 - Statistical algorithms



Algorithms and Techniques

❖ Cyberattack Prediction...

- The **main objective of the cyberattack prediction** approach is to improve the security system and enhance the security preemptive power of the cyber systems.
- This approach is based on different approaches as used in the cyberattack detection system.
- The **major algorithms** used in the **security prediction system** include the following:
 - Machine learning based algorithms
 - Genetic algorithms
 - Data analysis statistics algorithms



Algorithms and Techniques

❖ Cyberattack Prevention...

- The prevention of cyberattacks is the most critical aspect of the cyber security, which includes the detection, prediction and disaster recovery activities. But, the most important of all is the cyberattack prevention.
- This is a proactive process in which the security system.
- In the modern cyber security field, many cyber prevention systems have already been introduced in the marketplace.
- The **intrusion prevention system (IPS)** is one of the most important to name among such cyberattack prevention mechanisms.
- The security professionals and the organizations should also take their proactive responsibilities and implement the standard cyberattack prevention measures effectively.



Algorithms and Techniques

▪ Cyberattack Prevention...

- Among such **preemptive measures** the important ones are listed below:
 - Follow security guidelines strictly
 - Update all software applications and tools
 - Keep a close eye on the internal and external threats
 - Always backup the critical data and store safely
 - Make an emergency plan to cope with any disastrous situation
 - The **most important algorithm** used in the **cyberattack prevention** approach is the sniffing and analysis of the incoming traffic from different sources.
 - The close monitoring of the traffic patterns, traffic type, and other characteristics of the traffic will help you detect the intention of the traffic.
 - Once the traffic nature is known, the system can take the predefined actions to prevent the attackers to succeed in their malicious activities.

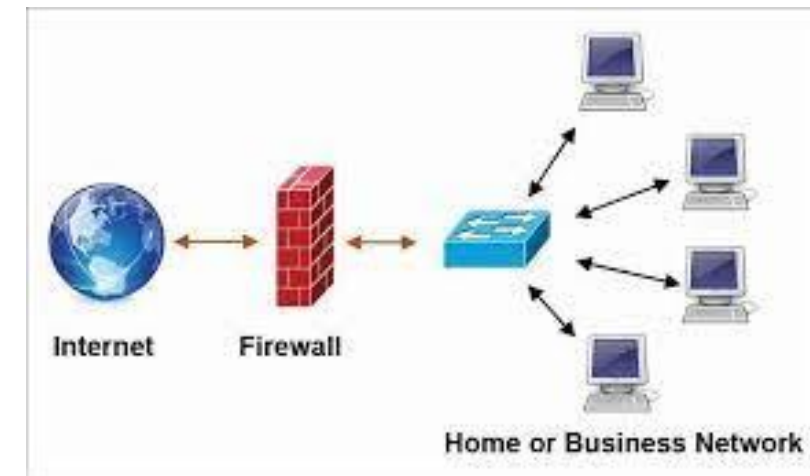


Firewalls



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- **Firewall** is the most important and first layer of defense for any online network. Firewall has been used extensively in the cyber security field for over 25 years now.
- A **firewall** acts as the filter for the traffic both incoming and outgoing.
- Firewall checks, and monitors the traffic continuously before the traffic enters into the network.
- It monitors and analyzes the incoming traffic to avoid any attack originating from the external un-trusted sources. Similarly, it monitors the patterns and parameters of the traffic originating from the internal networks and going out to certain networks.
- **Firewalls** can be either a **software program** installed on the servers, computers, or routers to safeguard any computer, server or even the entire system **or** it can be a dedicated **hardware device** loaded with the dedicated firewall software on it.



Firewalls



- In our daily use PC, computers, and mobile devices, we use the software firewalls installed on those devices to protect us from external deliberate attacks by the hackers.
- In big networks, such as enterprise networks, corporate networks, service providers, data centers, and government departments normally use the dedicated firewall devices with specialized firewall programs running on those devices. The terminating traffic enters the network through firewall.
- The firewall checks the traffic as per its configurations that were set earlier. If the firewall finds any kinds of problem or threat in the incoming traffic, it will not allow entering the network by either redirecting or blocking the traffic.
- Normally, there are many advanced settings and features in the firewalls, which can be activated, customized, configured so that the high-level of network security can be achieved.
- But, **using all features and capabilities** creates communication delays and performance issue due to heavy use of resources for detailed analysis of the traffic.
- So, the main and very important features are configured so that the performance of the communication services can be maintained.

Firewalls

Let's have a look at how to activate and configure software firewalls on different computers.

❖ **Activating Windows Firewall**

- **Windows 10 firewall**
- **What Are Traffic Rules?**
- **What is Monitoring Feature on Advanced Firewall Settings?**
- All latest Windows operating systems come with integrated software of firewalls. You can easily turn on the Windows firewall software and configure as per your requirements.
- The newer versions like Windows 10, Windows 8, and Windows 7 have two types of firewalls installed on the systems. So, you need to enable both of them as per your required security level.
- **Windows 10 Firewall**

Windows 10 comes with two types of firewalls. They are listed below:

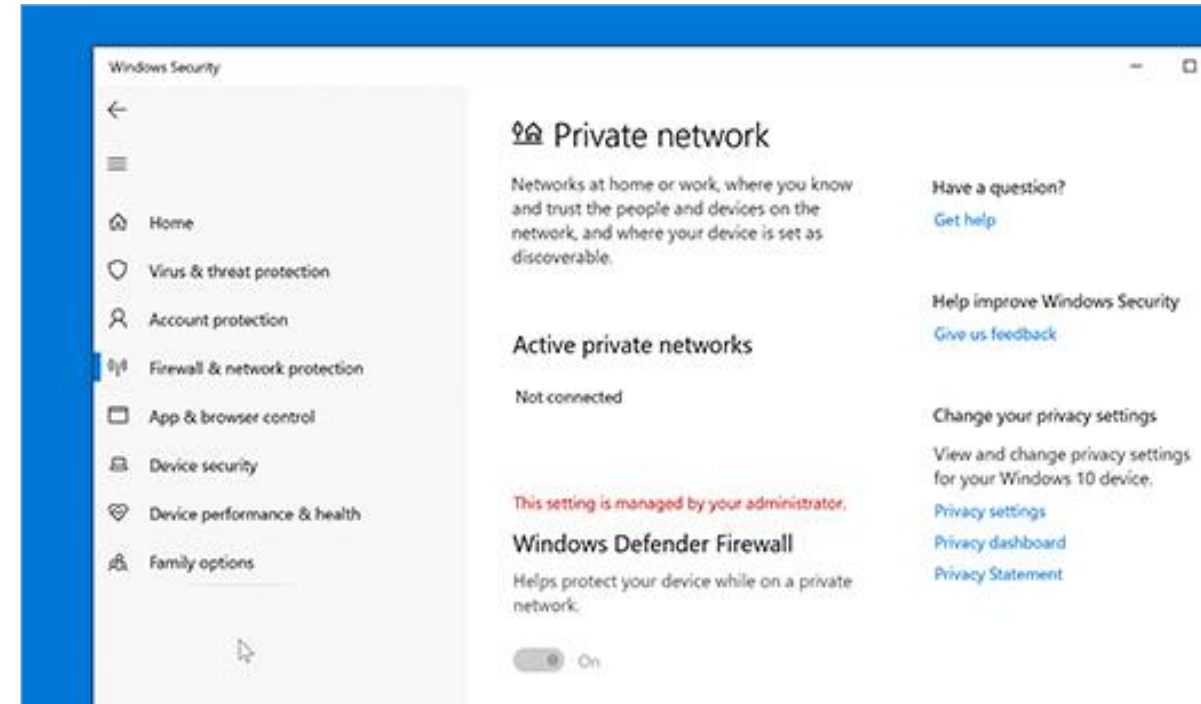
- Windows Firewall
- Windows Defender Firewall



Firewalls

❖ Activating Windows Firewall...

- It is highly recommended to configure both of the firewalls so that your computer and any network lying behind your computer remains safe from any malicious attack originated from the un-trusted resources.
- Windows firewall should be enabled by default to protect your computer on Windows 10, and you should also configure the Windows Defender Firewall by taking the following steps:
 - Click the **Start**  button
 - Choose the **Settings**  option
 - Choose **Update and Security** option
 - Select **Windows Security**. Windows security page appears
 - Finally choose **Firewall & Network Protection** option.
 - Turn the button to “**On**” position.



You can configure other parameters by just clicking the links shown in the above figure and then set the required parameters of the traffic or internal device.

Firewalls



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Activating Windows Firewall...

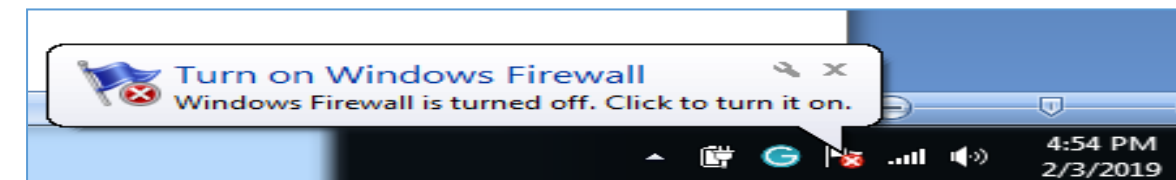
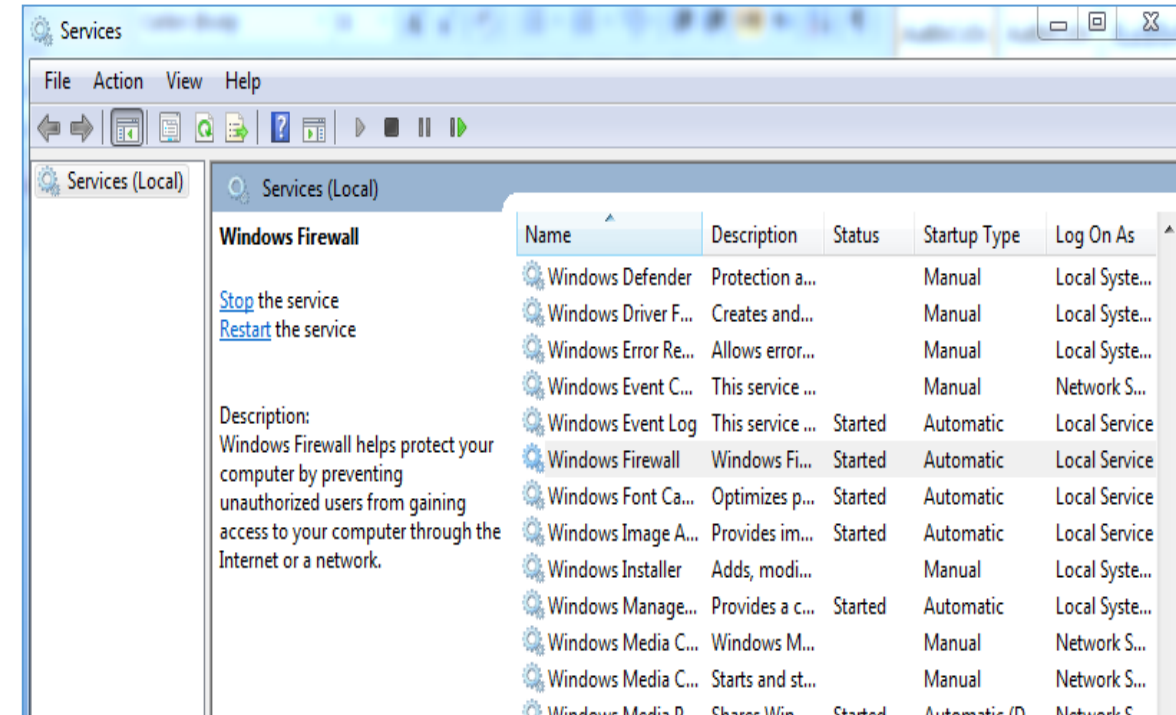
◦ Enabling Windows Firewall Service

In windows operating system, windows firewall is embedded in the system as a service. You can enable it as an automatic or manual service. You can also disable it directly in the windows services panel.

Take the following steps to enable the windows firewall service:

- Click the **Start**  button
- Search for services in the search bar, and click the **Services** link
- Locate the **Windows Firewall** service from the list
- Right click on the firewall service and choose the desired option that include start, stop, properties and other options

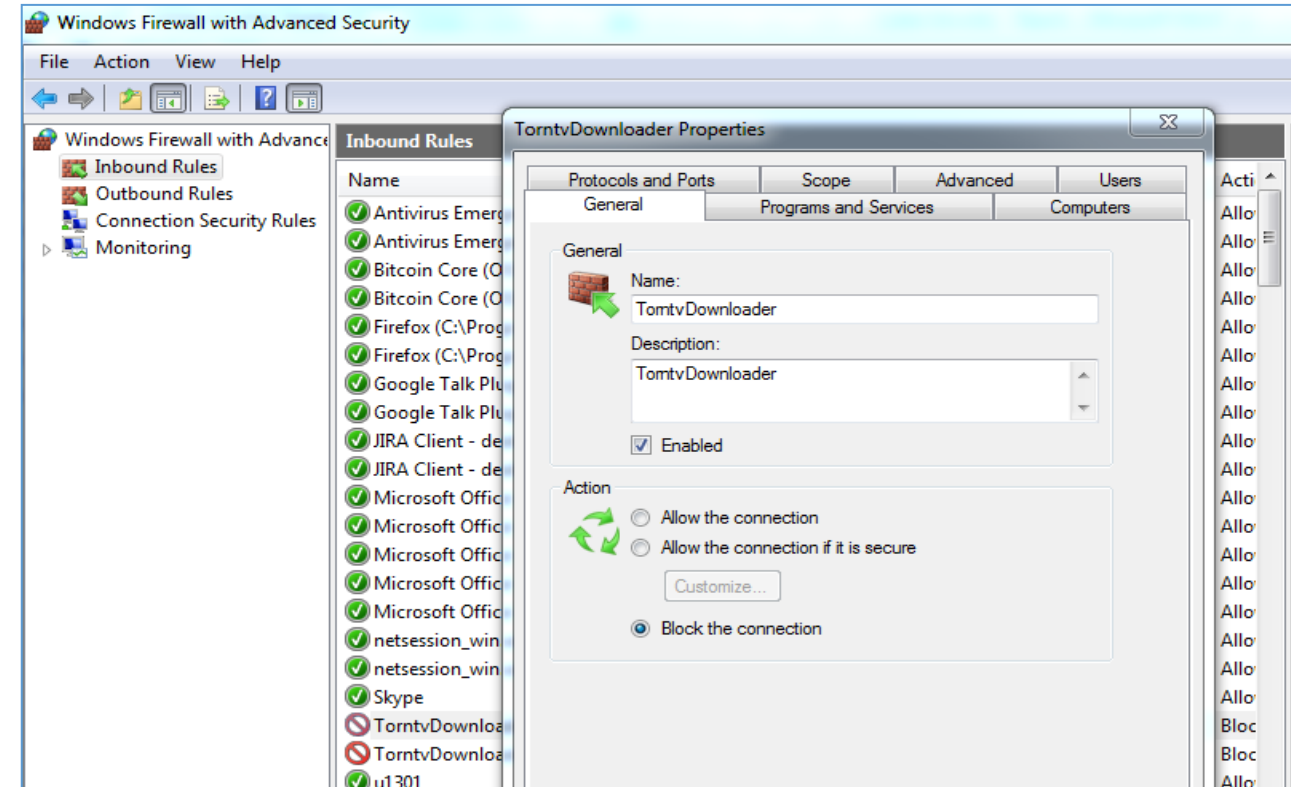
Note: If you turn off the Windows firewall, computer will warn you that firewall is turned off and your computer might be at risk.



Activating Windows Firewall...

• What Are Traffic Rules?

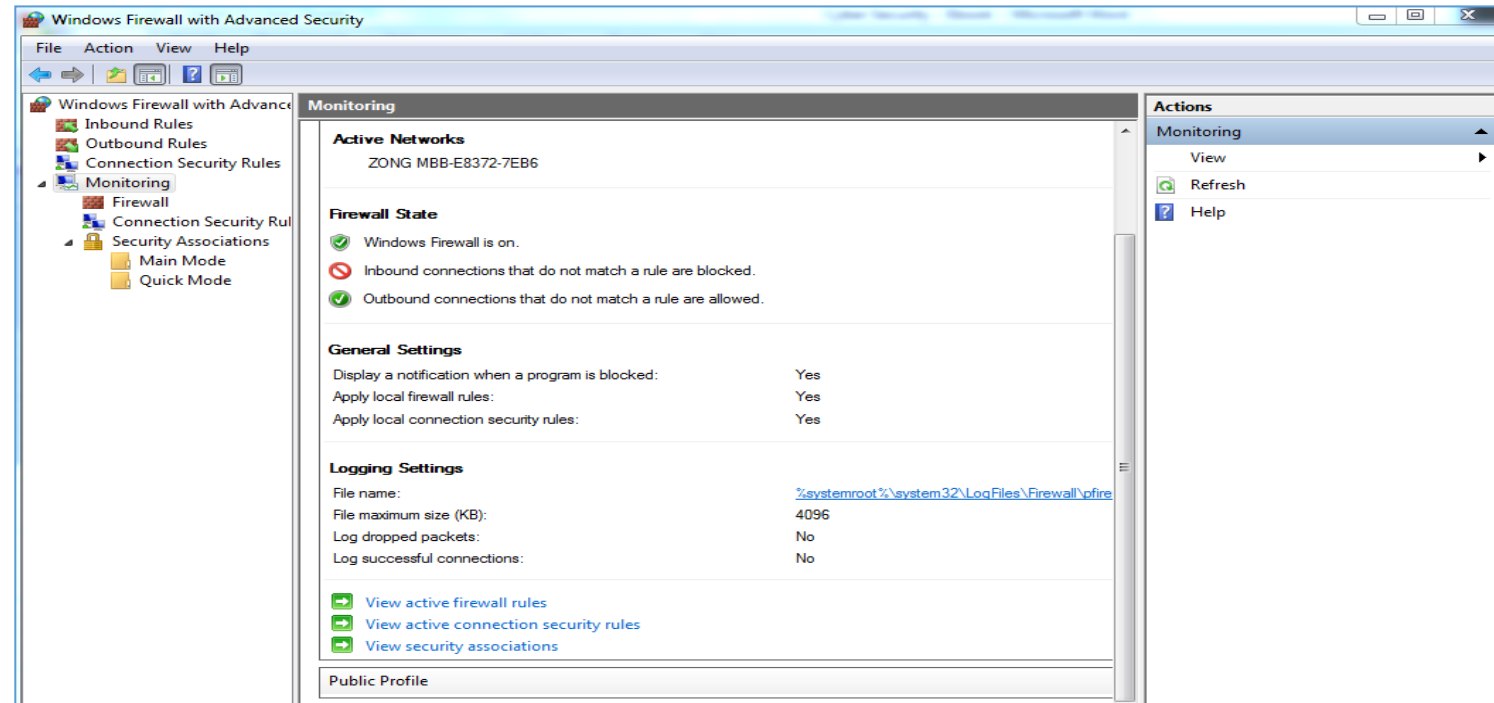
- Traffic rules define the criteria for the traffic , both inbound and outbound , to pass through the firewall.
- In the traffic rules different parameters are used to define the authorization of the traffic either to pass through or to stop at the security firewall.
- The traffic rules are classified into two types:
 - Inbound traffic rules
 - Outbound traffic rules
- You can change the status of the rules whenever you like to do so.
- To know about the rules, you need to right-click the **rule** >> click the **properties** option. The details of the rules appear as shown below.
- Click **Protocol and Ports** tab to know about the port and protocol details
- Similarly, for services and program traffic profile click **Program and Services** tab....and so on...



Activating Windows Firewall...

What is Monitoring Feature on Advanced Firewall Settings?

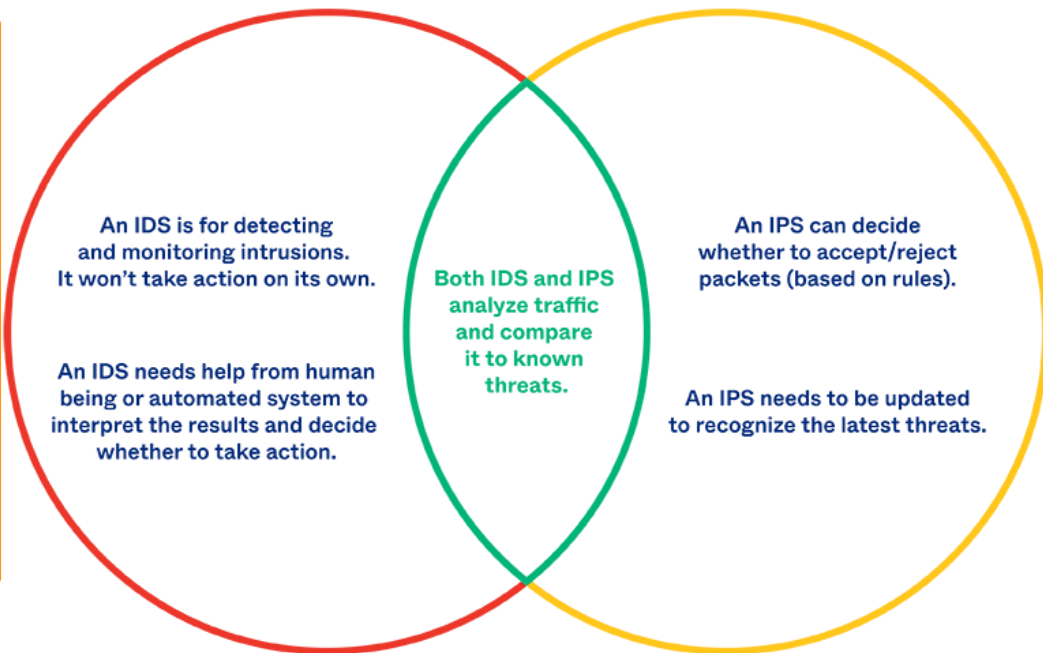
- Windows Firewall offers the capabilities of monitoring of the security rules on any particular profile.
- You can see security monitoring on different active connections, rules, and other security associations active on your computer.
- Monitoring displays only active inbound, outbound, and firewall rules. So, you cannot see any other rules and security features enabled on the any other network profile, if that is not active at the time of viewing the monitoring status of the firewall.



The pictorial view of the monitoring features on an active network connection is shown in the figure.

Intrusion Detection/Prevention Systems

IDS vs IPS



- Intrusion detection system IDS and intrusion prevention systems IPS are the most effective ways of the modern security systems on the networks as well as on computer host.
- Let's dive a bit deeper in both of these systems individually.
 - **Intrusion Detection System IDS**
 - **Intrusion Prevention System IPS**

Intrusion Detection/Prevention Systems

❖ Intrusion Detection System IDS...

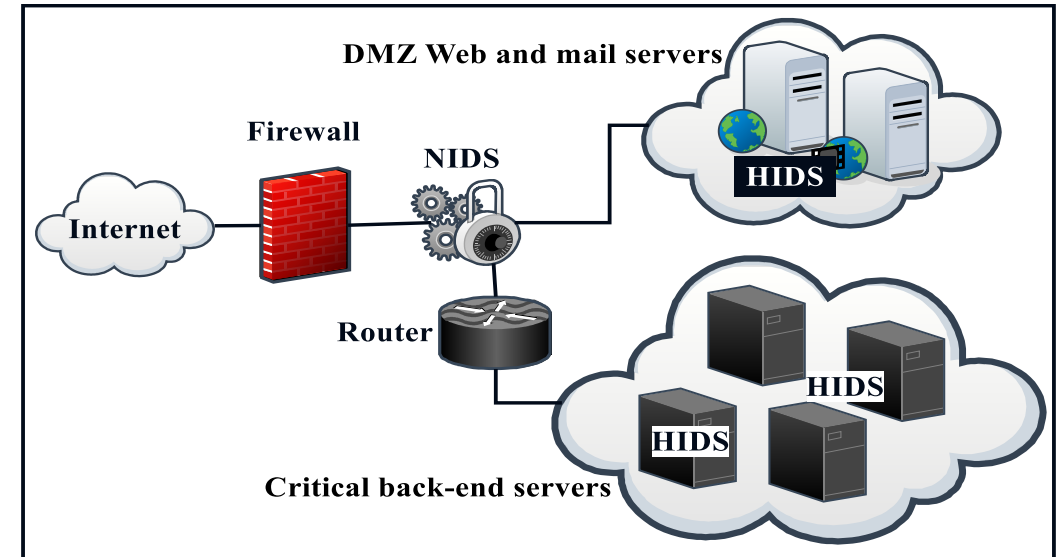
- **Intrusion detection system** is a combined system of a device or sensor and the software application. Intrusion detection system device is also known as IDS sensor.
- An **IDS system** monitors the malicious activities and events on the network as well as on the host operating system and its major registry files. It works on the basis of certain algorithms defined for detecting the malicious activities.
- The machine learning is used as one of the most important part of this entire system for detecting the malicious activities. And many other algorithms and approaches are also used in determining the malicious activities.

Intrusion Detection/Prevention Systems

❖ Intrusion Detection System IDS...

- There are three major IDS systems:

- Network intrusion detection system NIDS
- Host intrusion detection system HIDS
- Application-based detection system



- The network-based intrusion detection system monitors and analyzes the traffic patterns and other parameters on the network traffic. If any anomaly in the traffic is found, it immediately alerts the network administrator or the security information and event management systems (SIEM) for the corrective measures to safeguard the data and take the effective measures to avert any cyberattack.
- The position of the intrusion detection system for the internal as well as external traffic is shown in the following figure.

Intrusion Detection/Prevention Systems

■ Intrusion Detection System IDS...

- The host-based IDS system monitors and analyzes the files and events on the operating system for detecting any malicious activity. **Two major detection methods are commonly used in the IDS systems;** they are listed below:
 - Anomaly-based detection
 - Signature-based detection
- It is very important to note that IDS is also capable of identifying and detecting the hacking attacks from within the system along with the external intrusion detection.



Intrusion Detection/Prevention Systems

▪ Intrusion Detection System IDS...

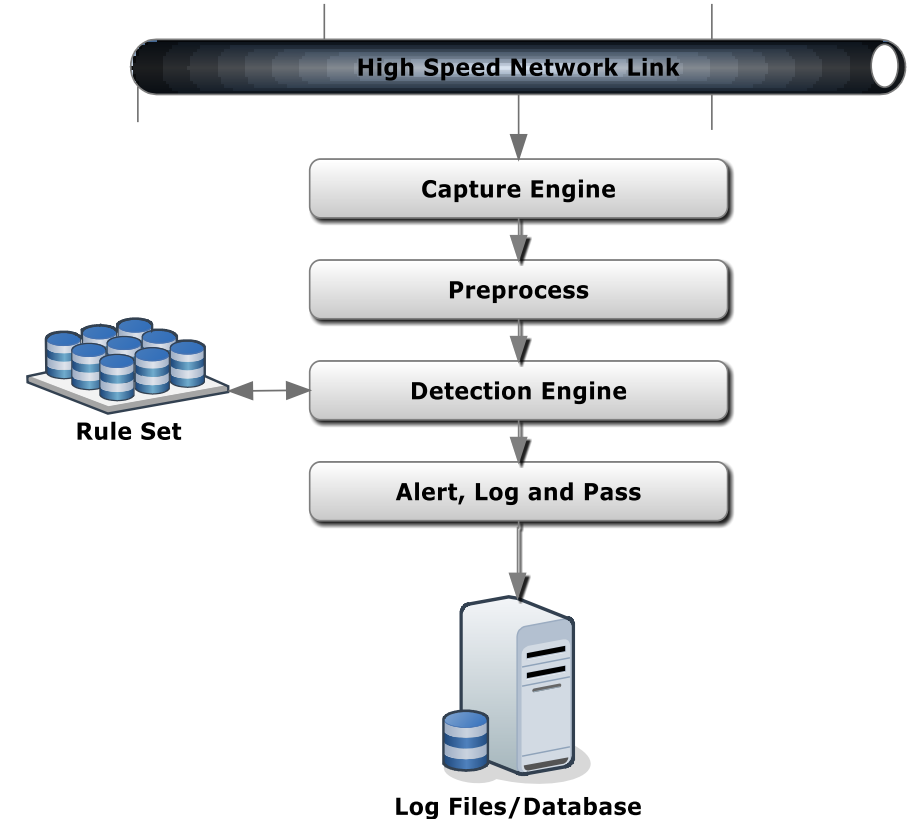
- Host-based IDS takes images of the file frequently and compares them with the previous one. If any anomaly is found, it alerts the network administration or centralized security system for the subsequent actions.
- The network-based IDS systems monitor and analyze the data packets passing through the network. You can install the data sensor at any point in the network – internal or external network sides. Application-based intrusion detection system precisely referred to as AppIDS. This is developed for a particular application that may include content management system, database system, or accounting system.



Intrusion Detection/Prevention Systems

■ Intrusion Detection System IDS...

- The major functions of a good intrusion detection system IDS include the following in the real-world sequential order:
 - Data collection
 - Feature selection
 - Analysis of data
 - Action
- The security of networks and servers is becoming a big challenge not only for the security professionals, but also for the enterprises and corporations. The newer security technologies are emerging, the intrusion detection system IPS is the advance system for detecting and preventing the cyber threats on the network.



Intrusion Detection/Prevention Systems

▪ Intrusion Prevention System IPS...

Firewall and intrusion detection are two major components of a security system in a network or on a host. But they have their own shortcomings that don't make them a perfect security tool. For example, firewall is only able to block the traffic that uses the port numbers that are not configured for the authorized traffic in the system that means it is able to block any port that is not in use for the genuine traffic. But a security firewall is unable to stop the malicious traffic that is passing through the allowed port. If hackers exploit the vulnerabilities of the allowed ports, firewall can easily be deceived.

Intrusion Detection/Prevention Systems

▪ Intrusion Prevention System IPS...

On the other hand, the intrusion detection system is capable enough to analyze and detect the malicious traffic passing through the allowed ports, but still not able to take any appropriate action against that breach. So, the security people needed an advanced system that could automatically take actions against the intrusion into the system. So, intrusion detection system was introduced that has advanced capabilities to detect, analyze, and prompt an appropriate action against any intrusion.



(Image of Cisco IPS 4240 Sensor is shown on Right of the slide)

Intrusion Detection/Prevention Systems



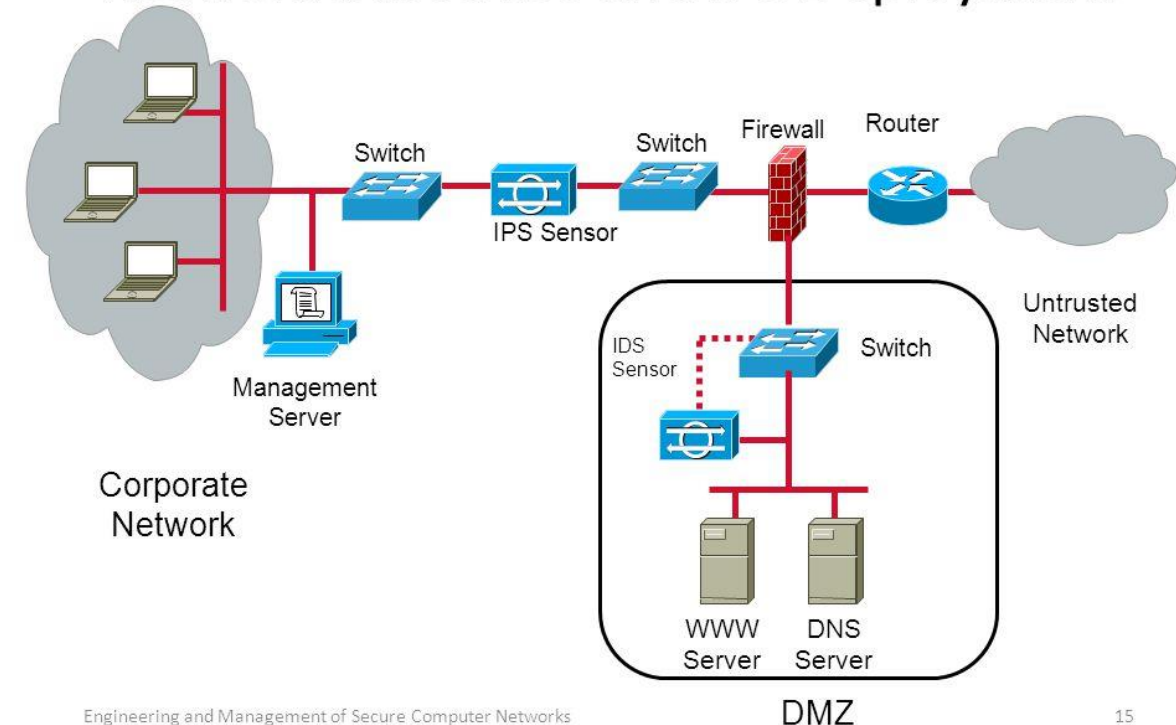
جامعة القادسية

■ Intrusion Prevention System IPS...

The main advantages of the IPS system include:

- Offers a comprehensive network security
- Offers robust protection against viruses or even any other traffic designed for attacking any network or web service
- Offers details of the origination of the cyberattack
- Automated response to the attacks and proper event recording
- Provides instant alerts and preemptive actions
- Stops access to email contacts
- Prevents reversal of the system directories
- Protects all resources of the system and network

Network based IDS and IPS Deployment



Engineering and Management of Secure Computer Networks

15

Intrusion Detection/Prevention Systems

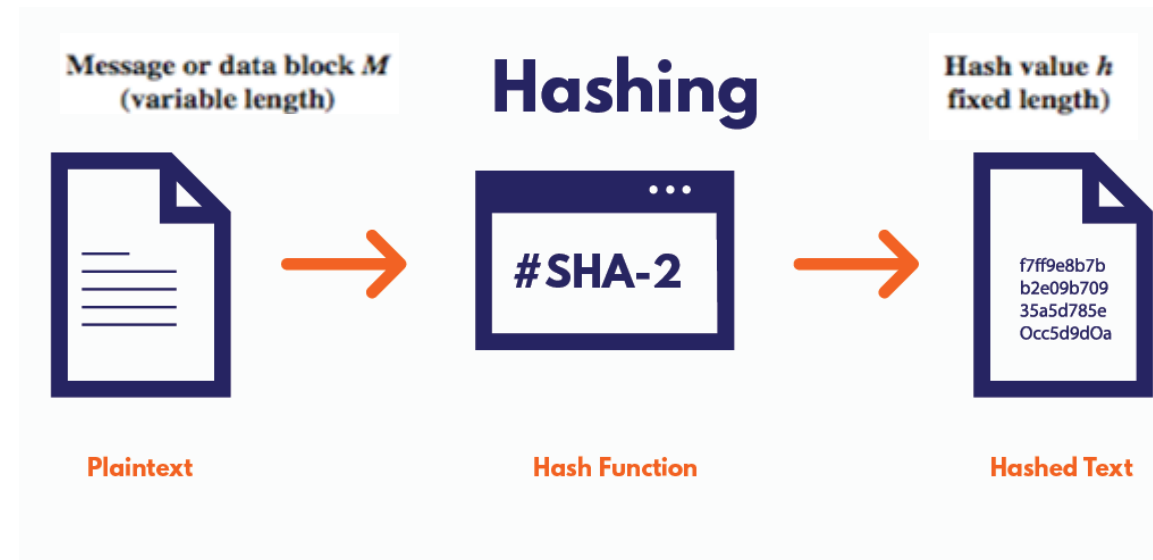


▪ Intrusion Prevention System IPS...

- Like IDS systems, **there are two main types of IPS systems, which are given below:**
 - Host-based Intrusion Prevention System (HIPS)
 - Network-based Intrusion Prevention System (NIPS)
- The host-based IPS systems are normally software based IPS systems, but not all the times. Similarly, the network-based IPS systems are normally appliance-based systems, but not every time.
- **The main approaches and algorithms used by the both the host-based and network-based IPS systems are listed below.**
 - Protocol anomaly detection approach
 - Detection of state-full signature approach
 - Kernel-based approach
 - Sandbox analysis approach
 - Software-based heuristic approach
 - Combined or hybrid approach

Authentication Using Hash

- Hashing is a type of computer process in which certain information in plain language is transformed into fixed length short codes that are not understandable for a normal reader without any help of computer and processing through the hashing function. The hashing is used for the security and integrity of the messages transported over the internet.



- The Schematic diagram of hashing process is shown in the figure.



Authentication Using Hash

- Authentication using hash is a type of authentication of the message to make sure that the data has not been altered and the sender is the person that the receiver wants to receive data from. Hashing is also extensively used in the databases for indexing and retrieving the data strings fast.
- The major hashing techniques include:
 - Cryptographic Hash Functions (CHF)
 - Message Authentication Code (MAC)
 - Digital Signature (DS)
- Many kinds of authentication methods based on hashing functions are used for integrity and security of the messages sent over the internet.

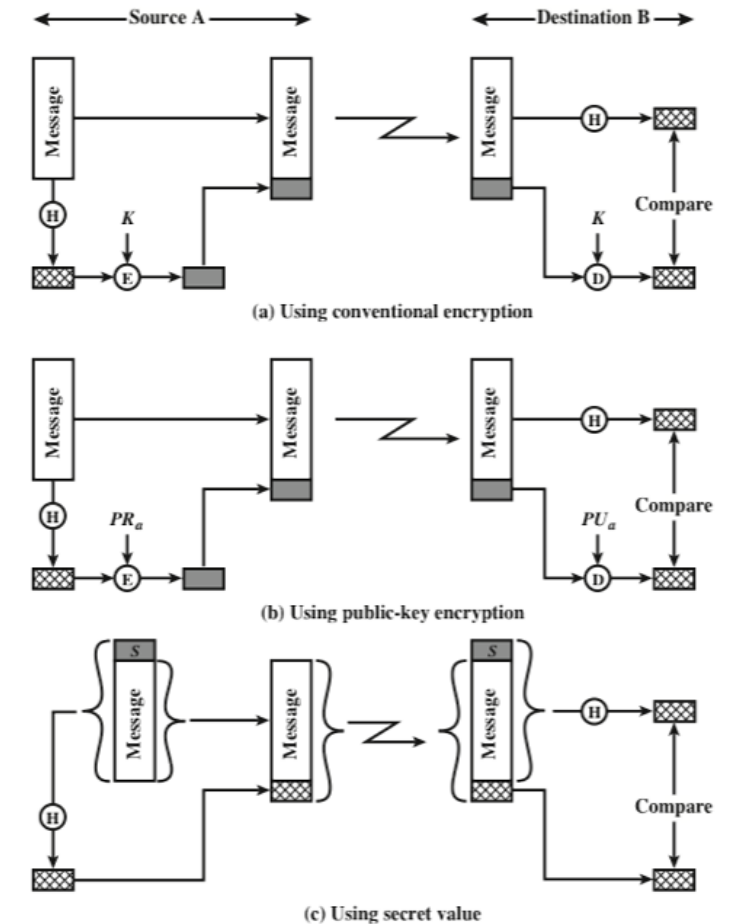


Figure 3.2 Message Authentication Using a One-Way Hash Function



Authentication Using Hash

- A few authentication methods are listed below.
 - Message Digest 2 (MD2)
 - Message Digest 4 (MD4)
 - Message Digest 5 (MD5)
 - Secure Hash Algorithm SHA
- In the above hashing methods, the message authentication code (MAC) and digital signatures (DS) use the private key for the authentication of the message at the receiving end. But, the cryptographic hash functions does not require private or secret key for the authentication of messages.
- Cryptographic functions that don't use the secret key over the Secure Socket Layer (SSL) encrypted connection for the transportation of the information or messages. The most commonly used cryptographic functions on SSL are presently are message digest 5 (MD5) and secure hash algorithm (SHA).



Authentication Using Hash

- **Message Digest 5**

- Message Digest 5 (MD5) is a hashing algorithm most extensively used in the secure socket layer encryption protocol. It is a one-way hashing function that takes the message of any length as an input and returns a fixed length of encrypted code, which is fixed in length. This code is used for the authentication of the message to check its originality and integrity of the content.
- The MD5 algorithm is governed by the Internet Engineering Task Force via RFC 1321. The fixed output of generated by the MD5 encryption algorithm is 128-bits message digest. In the present high-tech cyber security field, 128-bit encryption is not considered as the high level of security.
- It is recommended to use at least 256-bit or higher level of security encryption methods. This series of encryption functions starting from MD2, MD4, and MD5 have been designed by Ronald Rivest. The latest version in the market is MD6, which is 256-bit based encryption.



Authentication Using Hash

- **Secure Hash Algorithm**

- Secure hash algorithm (SHA) is a hashing algorithm. It has multiple versions in the series, such as SHA0, SHA1, SHA2, and SHA3 with different capabilities and features. This algorithm was developed by the US National Security Agency (NSA).
- SHA hashing algorithms are published and governed by the National Institute of Standards and Technology precisely referred to as NIST, which is a US standard organization. The latest standard SHA 3 is capable of encrypting the data with 224-bit, 256-bit, 384-bit, and 512-bit encryption. But the most commonly used SHA algorithm is SHA 3 with 256-bit encryption.

Secure Socket Layer

- Secure socket layer (SSL) is a type of security protocol for secure data transfer from web server to the browser and vice versa. The SSL is a recognized and standard security protocol that establishes a secure and encrypted link between the web server and the browser so that the transactions of data between the client and server are fully secure and reliable.
- There are two most commonly used types of data encryption methods. They are given below:

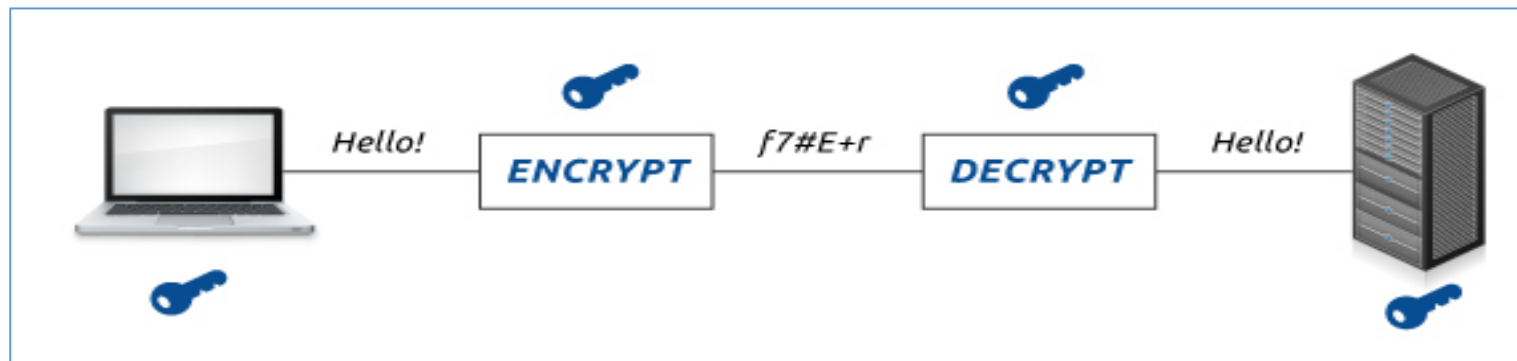
- Symmetric encryption
- Asymmetric encryption

Secure
Socket
Layer



Secure Socket Layer

- **Symmetric encryption** uses the same key for the encryption and decryption of the data as shown in the following figure.

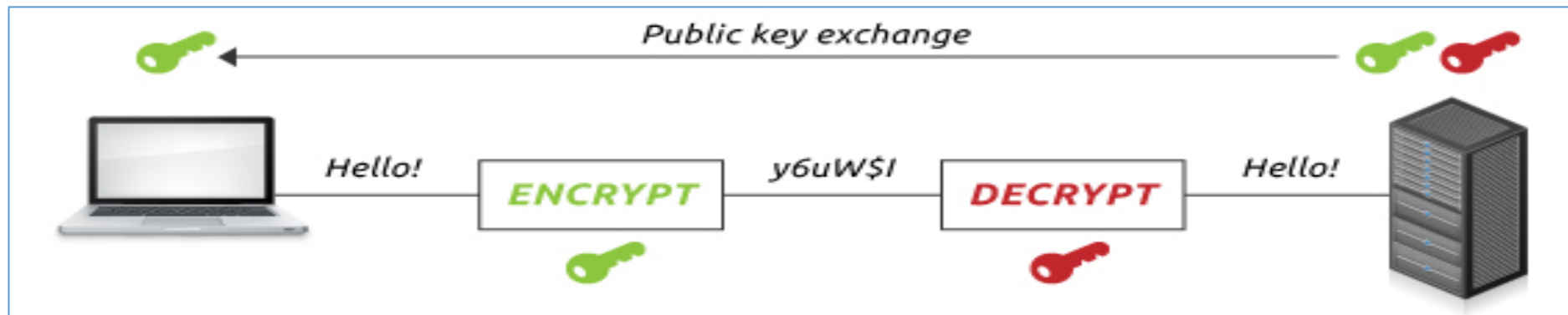


- While the asymmetric encryption uses two separate keys for encryption and decryption respectively. Asymmetric encryption uses 2048-bit keys nowadays. Previously it also used the 1024 bit key, but now it is not considered as very safe encryption.



Secure Socket Layer

- The following figure shows the **asymmetric encryption**, which uses two separate keys for encryption and decryption.



- SSL protocol works on certain data encryption algorithms. The most commonly used public and private key based encryption uses the following encryption algorithms:
 - Rivest, Shamir Adleman (RSA) algorithm
 - Elliptic Curve Cryptography (ECC) algorithm



Secure Socket Layer

- The SSL encryption is based on the SSL certificate, which is normally installed on the web server. The SSL certificate is purchased from the issuing authorities commonly known as Certificate Authority (CA) after proper verification of the business and websites.
- First of all, you need to generate a certificate signing request (CSR) via local browser on the web server. This report is a file of data, which includes web server information and private key. This CSR is submitted to the certificate authorities for issuance of certificate. The web administrator and developer request for SSL certificate. When it is received from the issuing authorities, it is installed on the web server.



Secure Socket Layer

- When the SSL certificate is installed, now the communication between browser and the server will take place on a secure and encrypted link. On that link the data travels in the encrypted form and hackers will not be able to breach the integrity of the data while in traveling over the secure link.
- To establish a secure socket connection between server and web browser the following steps takes place.
 - Browser sends the secure connection request through the 'HTTPS' request through the <https://websiteURL>
 - The web server receives the request and responds with the SSL certificate to the browser that requested for the certificate



Secure Socket Layer

- The web browser authenticates and verifies that the SSL certificate is valid. This process is referred to as 'SSL handshake'
- When the browser verifies the SSL certificate a padlock icon appears in the address bar of the browser as shown below.



- A secure connection is established between browser and web server. Now the communication over the link is fully encrypted and secure



Secure Socket Layer

- The working flow of the SSL link establishment is given in the following figure:



Secure Socket Layer

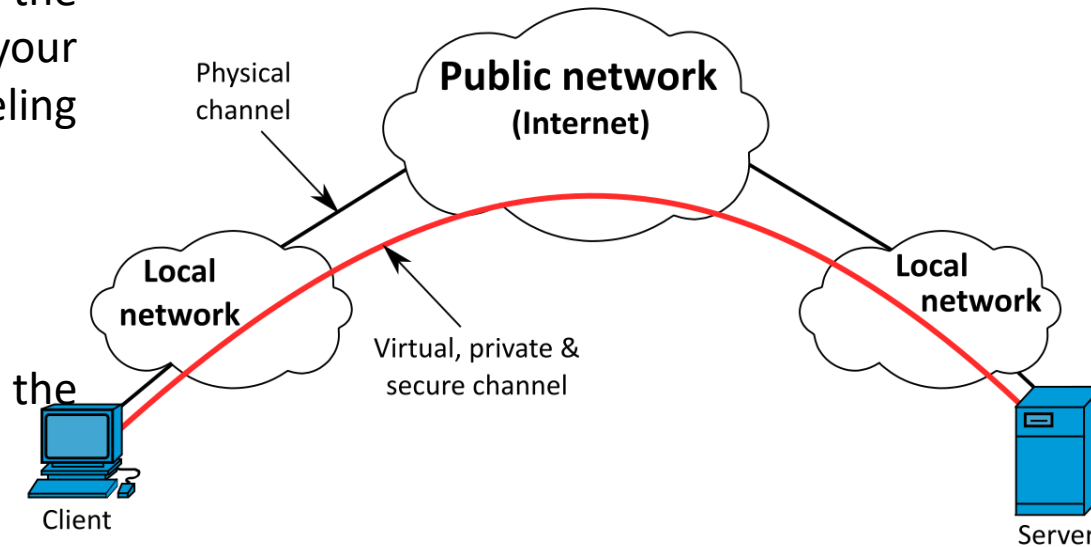
- A secure website is the new security standard of safe browsing. It is highly recommended that don't visit the websites that are not SSL enabled. The secure websites increase the trust of the visitors and subsequently increase the conversion rate.
- The increase in traffic to your website is another important effect of having your website a digital certificate for SSL communication link.

Virtual Private Network

Virtual Private Network or VPN is a type of communication tunnel that is highly secure for private services and communication over the internet. As we know the internet is a public network in which your data travels from one point to another. It is also known as tunneling protocol on the public networks.

The main characteristics of a VPN connection include:

- Secure, private, and anonymous routing through tunnel
- Encapsulation of one protocol over the other is done to hide the details of the origination and termination of the communication
- Routing of your communication through a proxy server
- It hides your internet activities from other external interceptions
- Your IP address is masked with the VPN number/address
- Browsing history is fully hidden from even service providers
- Hides your location
- Hides your device identity
- It is complete connection from device to network



Virtual Private Network

- In the normal communication over the internet, hackers can intercept your data packets and decrypt to know about your communication. But, the communication over VPN is completely hidden, private, and secure passing through a private tunnel, which is created on the public network. The communication over the VPN connection is near to impossible to intercept and interpret.
- VPN service is extensively used by the corporations and government organizations for remote work so that the communication remains private and secure from the external interceptions. Two major types of VPN connections are commonly used in our modern internet services; they are:
 - Site-to-Site VPN connections
 - Remote access VPN connection
- The site-to-site connections are normally used to connect multiple sites and locations of a corporation or governmental organization through VPN connections. These connections are created over the public internet via private proxy servers or the proxy servers of the service providers.



Virtual Private Network

- The remote access VPN connections are normally used for remote work. Any employ that is travelling can access the corporate or other private networks through a VPN connection over the internet. His/her communication with the corporate network remains private for the other internet users.
- VPN uses encryption to encrypt the data before transporting over the private tunnel. It also uses other techniques and mechanism to hide the data from any breach. Then the original communication protocol is masked with the VPN protocol and then transported over the secure tunnel created between proxy server and the VPN enabled device.
- The original packet of information is encrypted at the network layer to disguise it from being identified and then the entire encrypted packet is repacked into an IP envelop to travel over the internet. Thus, the packet data and the message attributes are disguised in the tunneling process.



Virtual Private Network

- The main advantages of VPN connection include the following:
 - Higher level of privacy
 - Greater data security
 - Better reliability
 - Anonymity
 - Reduced cost of connection
- All of the above-mentioned features help you maintain high level of cyber security that helps you prevent any kinds of cyberattack on your data and communication.

The Next Slides are to Practice by Self Study

The END 😊



Mac Computer Firewall Configuration



Mac computers are brand names of Apple Inc. Mac computer runs on operating systems called OS X and macOS. The Apple computers' operating system evolved from its OS X 10 beta release in 2000. From there on, the OS X 10 releases continued till OS X 10.11 commonly known as El Capitan (Gala), which was released in the month of September, 2015.

Mac computers are very well-known brands for the middle and higher-class people in the world. Most of the people in the USA like the Apple's Mac books and computers due to their performance, class, reliability and attraction in the society.

Mac Computer Firewall Configuration



Afterwards, the OS X name was changed to macOS. The first version was named as macOS 10.12 Sierra. The latest version of Apple computer operating system is macOS 10.14 released in September 2018.

The firewall functionalities are inbuilt in the macOS operating systems. By default, the firewall blocks any traffic terminating on the unused ports. The open ports are normally exploited to scan the security and other settings of your computer by the hackers. So, you should enable the firewall on your Apple computer to keep the hackers at bay.

Mac Computer Firewall Configuration

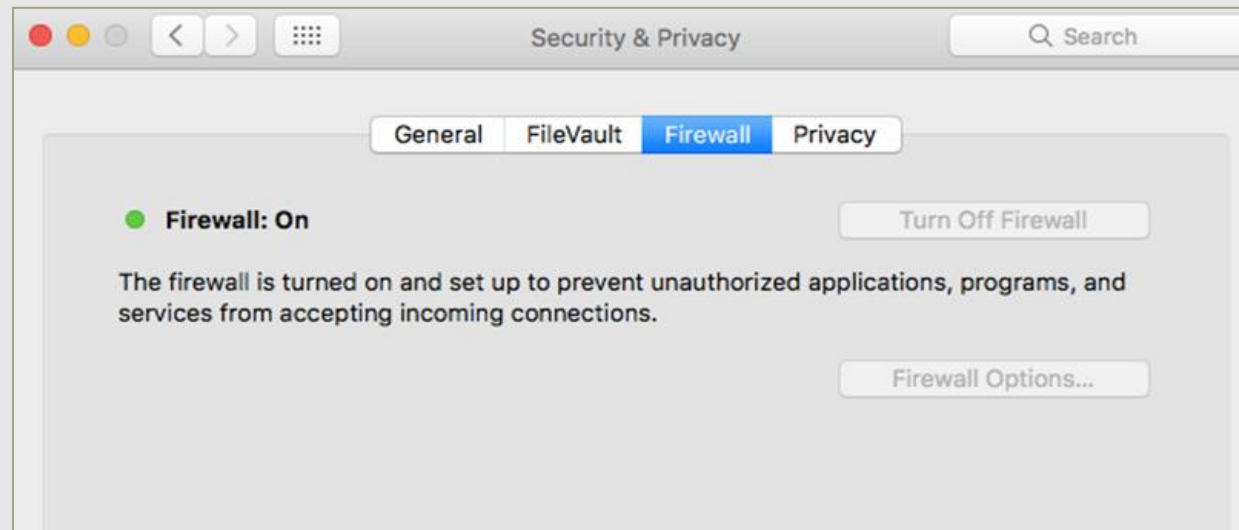
You can configure and activate the exceptions on the enabled ports by taking the following step by step procedure.

- Open the **Apple Menu** and choose the **System Preference** option. The system preference window will open as shown below



Mac Computer Firewall Configuration

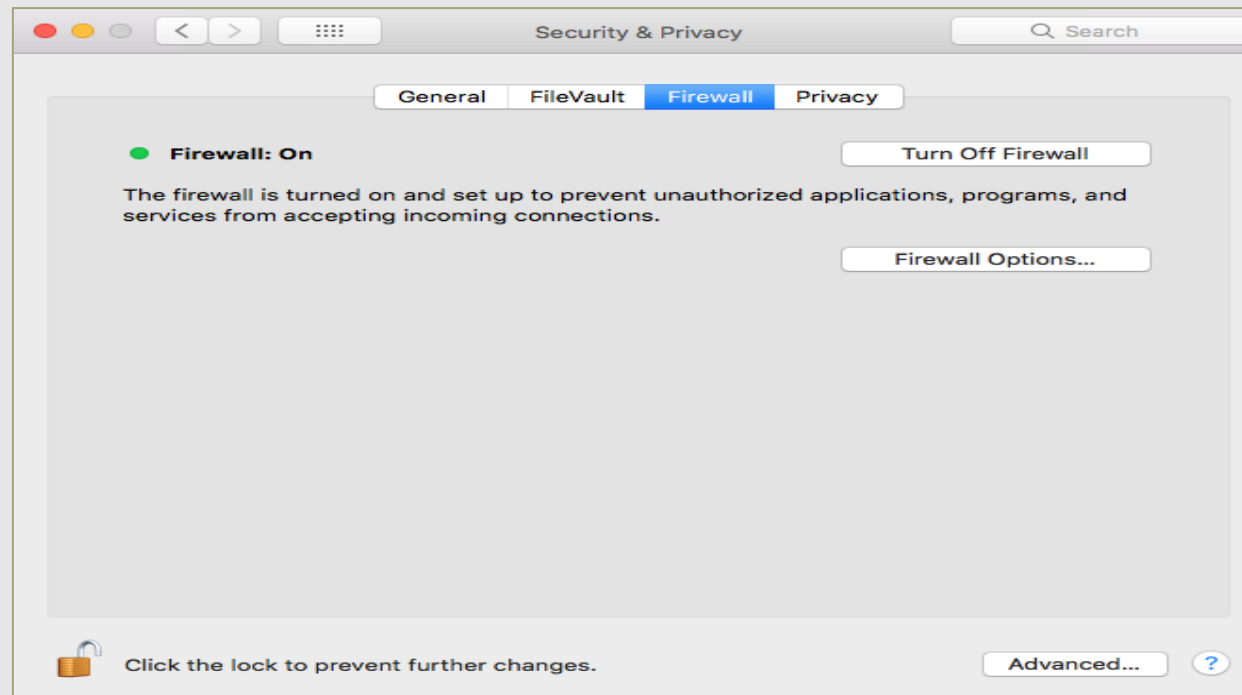
- Click the **Security & Privacy** icon. The security and privacy window appears as shown below.



- Choose the **Firewall** tab on the security and privacy window. The details of firewall will appear.

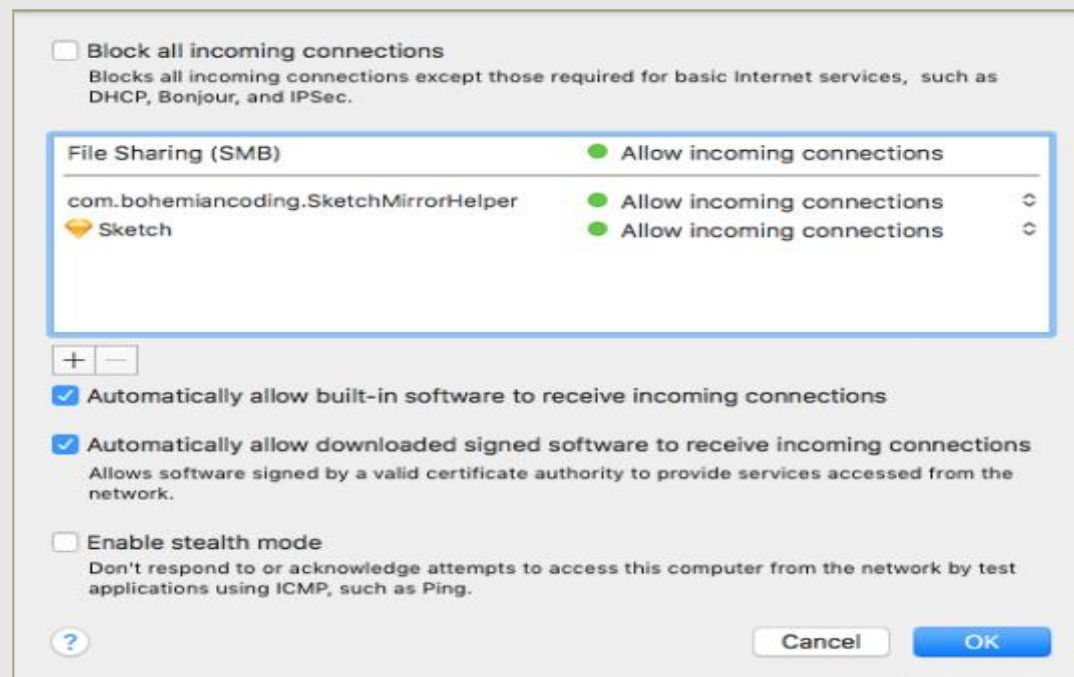
Mac Computer Firewall Configuration

- Click the **Lock** icon at the bottom of the window. Enter the valid administrator password. You are now logged in as administrator to make the desired changes in the Firewall and other security settings. All inactive buttons will activate.



Mac Computer Firewall Configuration

- Click the **Turn Off Firewall** button, if you want to disable the firewall. The '**Start**' option to turn on the firewall appears, if you turn off the firewall.
- Click the Firewall Options... button. The list of applications will appear as shown in the below screenshot image.



Mac Computer Firewall Configuration

- Select any application shown in the list and then click the (-) sign, if you want to remove from the list.
- Click on the (+) sign and choose the desired application that you want add into the list.
- Click the **Enable Stealth Mode** checkbox to enable the stealth mode for the hacker to respond to the probing activities on the computer.
- Choose the **Block all incoming connections** checkbox to stop traffic to any port on your computer.
- Similarly, select/deselect the Automatically allow built-in software to receive incoming connections checkbox to activate and deactivate this option on the firewall of Apple macOS computers
- Click the **OK** button to enable the desired firewall settings

Mac Computer Firewall Configuration

- Close the firewall, privacy & security window to take effect the newly configured settings of the firewall

- **Important Note:**

The firewall is designed to block the internet based incoming connections so some connections that use different protocols at the transport layer may not be affected by the firewall settings on Apple computers. This is the downside of the Apple firewall. The connection like AppleTalk, which uses a proprietary protocol, is not affected by the firewall settings on the Apple computers.

And, ICMP pings are blocked by enabling the stealth mode, which does not allow the external probing that mostly use the ping command to check the status of the ports and applications.

Choosing the Right Browser

A secure, reliable, and fast browser makes your internet experience great. Any old version or bad browser can expose you to the security threats because the browser is the basic component that you sail on to surf the world of internet. So always choose the right browser that is 100% fit for your requirements, system configuration, and security level.

For choosing the right browser for your computer, you should have clear knowledge about the following things:

- Your system information
- Your browsing activities on internet
- Level of security you need

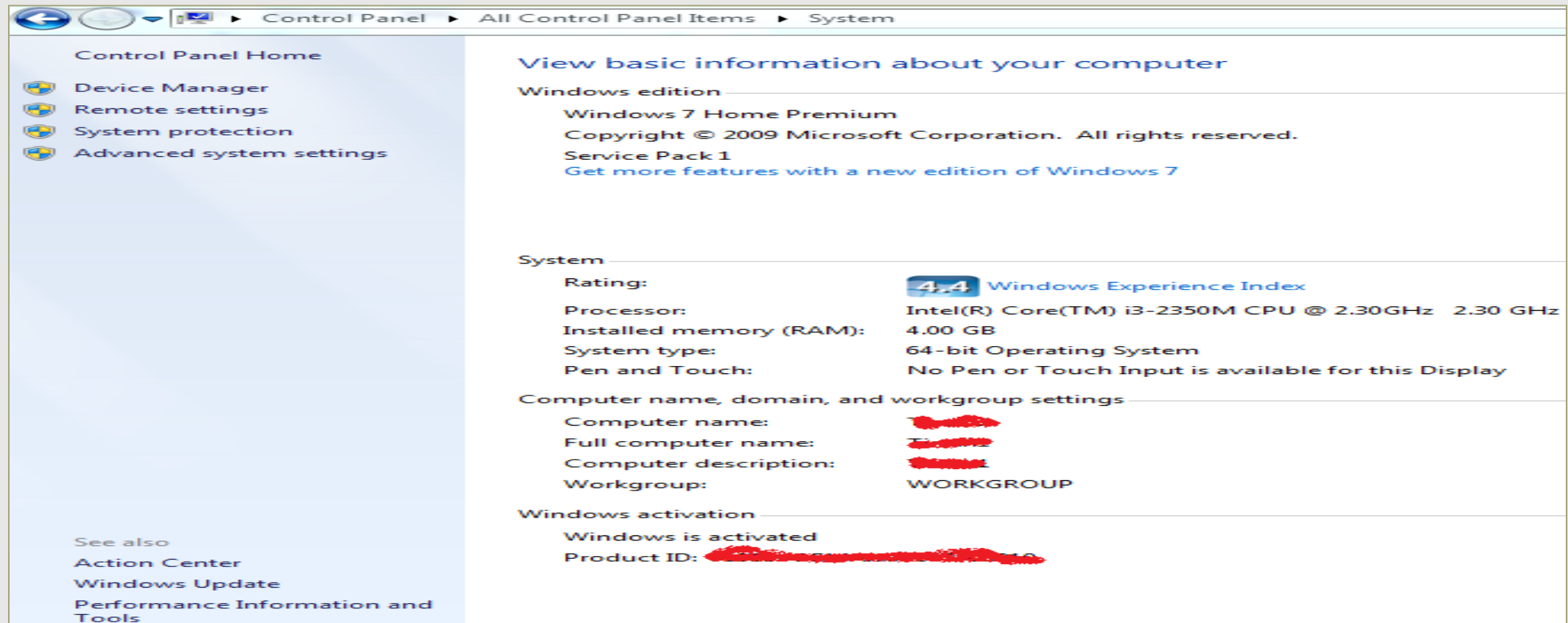
Choosing the Right Browser

Once you have this information on paper, you can easily take the following steps to choose the right browser for you and your computer.

- First of all, check the configuration of your computer so that you can find the most suitable browser that is fully fit with the computer resources
- Click  button and choose the **Control Panel** option. The control panel window appears
- Click the **System** option on the control panel. The details of your computer system appear

(Image on the next slide)

Choosing the Right Browser



Choosing the Right Browser

- Write down the information regarding operating system, service pack, RAM, system type, and processor information
- You need to search for the best browsers suitable for your computer operating system. This is important to note that there are many browsers for different operating systems available in the market.
- Go to internet and Google the best internet browsers as shown in the following figure.

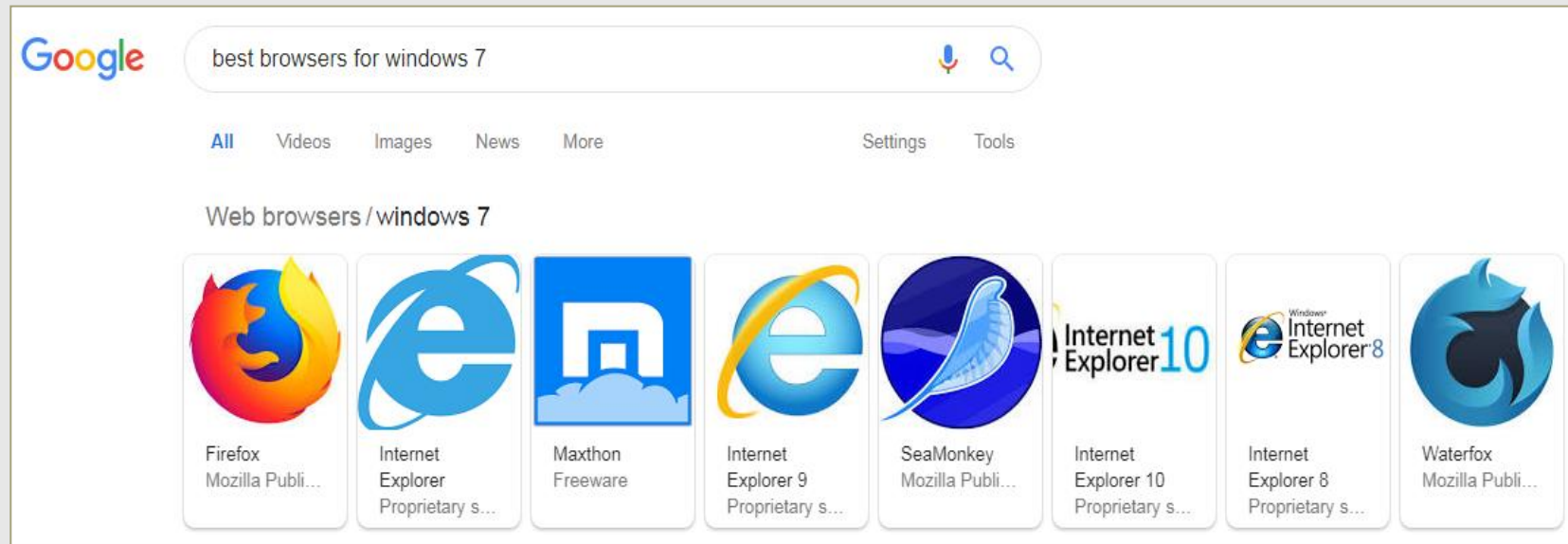
(Figure on the next slide)

Choosing the Right Browser



- Google will return you with the top-rated browsers suitable for the operating system you are using on your computer

Choosing the Right Browser



- Search for the top ten reviews in the Google
- Click the toptenreviews.com website to research about the features and capabilities of the browsers

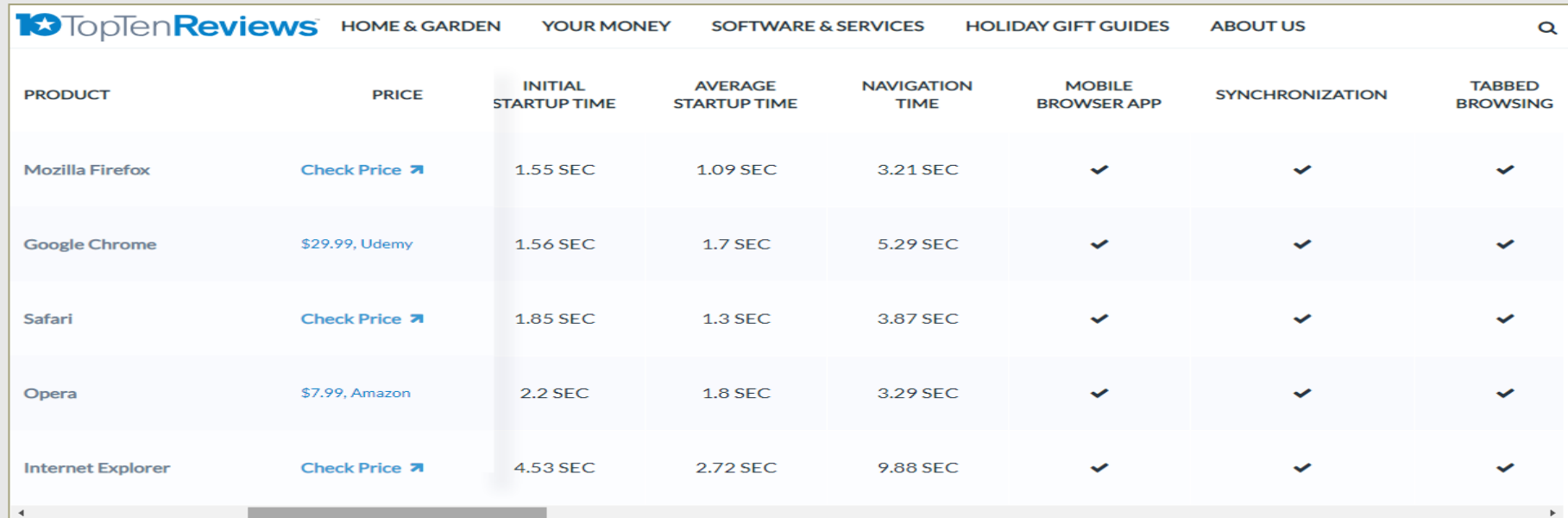
Choosing the Right Browser

— Scroll down to the comparative properties on this website as shown below:

10TopTenReviews™ HOME & GARDEN YOUR MONEY SOFTWARE & SERVICES HOLIDAY GIFT GUIDES ABOUT US							
PRODUCT	PRICE	OVERALL RATING	SPEED & COMPATIBILITY	FEATURES	SECURITY	HELP & SUPPORT	EASE OF USE
Mozilla Firefox	Check Price ↗	9.8	10	10	10	8.5	95%
Google Chrome	\$29.99, Udemy	9.8	9.8	10	10	8.5	95%
Safari	Check Price ↗	9.6	9.8	9	10	10	85%
Opera	\$7.99, Amazon	9.5	9.5	9	10	10	85%
Internet Explorer	Check Price ↗	9.1	8.8	8.3	10	10	80%

Choosing the Right Browser

- Scroll the comparison table to the right to see more features. This compares many features, performance factors, required system configuration, prices and much more. To know about more scroll to the right for information as in the below screenshot image.



TopTenReviews							
HOME & GARDEN YOUR MONEY SOFTWARE & SERVICES HOLIDAY GIFT GUIDES ABOUT US							
PRODUCT	PRICE	INITIAL STARTUP TIME	AVERAGE STARTUP TIME	NAVIGATION TIME	MOBILE BROWSER APP	SYNCHRONIZATION	TABBED BROWSING
Mozilla Firefox	Check Price ↗	1.55 SEC	1.09 SEC	3.21 SEC	✓	✓	✓
Google Chrome	\$29.99, Udemy	1.56 SEC	1.7 SEC	5.29 SEC	✓	✓	✓
Safari	Check Price ↗	1.85 SEC	1.3 SEC	3.87 SEC	✓	✓	✓
Opera	\$7.99, Amazon	2.2 SEC	1.8 SEC	3.29 SEC	✓	✓	✓
Internet Explorer	Check Price ↗	4.53 SEC	2.72 SEC	9.88 SEC	✓	✓	✓

Choosing the Right Browser

- If you are looking for fast performance with the basic features of bookmarks and search bars, you would like to use browsers Midori, Vivaldi, Torch, and similar
- For the performance, reliability and features you can choose Google chrome or Mozilla Firefox for your windows 7 OS system
- If you have a slow internet connection and want to use the faster than fastest browsers, then use the text-based browsers
- The top examples of text-based browsers include Elinks, WebIE, Lynx, Labnol and others
- If you want to use different types of plugins and other third-party apps, then choose either Mozilla Firefox or Google Chrome browsers. They are easy to use with a wide range of plugins.
- Download the browser of your choice once you decided the best fit for you.
- Install the browser and go surfing the internet

Multi-factor Authentication

Multifactor authentication is another very useful and effective way to prevent the threats of cyberattacks. It is highly recommended in the modern field of cyber security that your passwords should be not only strong, but should also be powered by the multifactor authentication process so that the malicious activities to steal your passwords can be averted easily.

In multi-factor authentication, the access to the digital resources such as computer system, web account, cloud service, or any other digital access is not granted through just one credential like password. But you have to provide more credential other than password.

Multi-factor Authentication

The additional factors other than username/password can be generalized in three categories as shown in the above figure.

One factor should be the knowledge question, which relates to some knowledge that only you know, and the other factor is referred to as biometric, which is unique and only you can be that. The third category of multi-factor authentication is referred to as one-time password, which only you can have it through email, mobile, or even you already have it as a hard key.



Multi-factor Authentication

Those credentials are normally one-time-use code to access the digital resources.

Among such second factor for the authentication may include the following factors:

- Short code sent through mobile phone
- A user generated pin on the system
- One time password (OTP)
- Digital signature
- Fingerprints
- Key fobs or
- Digital card swiping

Multi-factor Authentication

The computer processors have become very fast with the advent of advanced computing systems like general purpose graphics processing unit or GPGPU and other techniques of processing. It has become comparatively easy to break the password through brute attacks. So, you need multiple factors to make your digital resources secure.

For example, some hacker has succeeded in breaking your password through super processing devices, and he wants to access your resources. He can easily access your account and hack your account, if you don't have the multi-factor authentication activated.

Multi-factor Authentication

If you have activated the multi-factor authentication on your digital account, the hacker will be asked to enter the other authentication factors that you have enabled on your account like fingerprints, card swipe, OTP, or mobile code.

The hacker has no control over your phone number or other data. Thus, he/she will not be able to get access to your account despite the fact that he has stolen your legitimate password.

The multi-factor authentication will also alert you that someone has attempted to sign into your account by sending you the second factor code to enter. Thus, will also be your alert to change the password again.

Multi-factor Authentication

So, the multi-factor authentication is very useful tool in maintaining high-level of security of your digital accounts and resources. The most commonly used multi-factor authentication method in the present days is the two-factor authentication through mobile or email.

This method uses your mobile phone or your email to send you a one-time use code to enter whenever you login to your account. Thus, your accounts remain safe and your password becomes a strong factor of your digital account security.

- **Activating Two-Factor Authentication**
- **Creating Application Specific Passwords**
- **What if your phone with all apps enabled is lost?**

Multi-factor Authentication

- **Activating Two-Factor Authentication...**

Two-factor authentication is one of the most popular methods of multi-factor authentication system. It is extensively used by the private as well as public companies for the security of the passwords. The major cloud-based services offer the capabilities of two-factor authentication; among such services, Google, Yahoo, Hotmail, Facebook, YouTube and many others are a few to name.

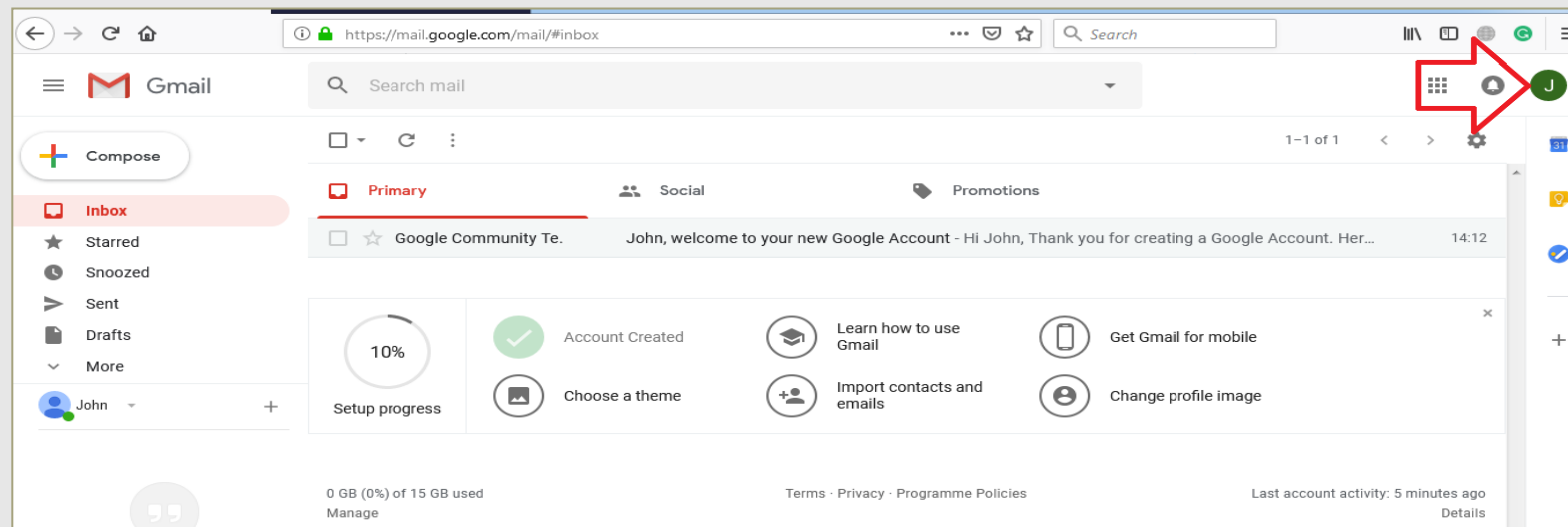
Many private organizations either install a two-factor authentication service or purchase the two-factor authentication service for their employees to use the higher level of security. Let's have a look at the step-by-step procedure to enable a two-factor authentication on the mostly commonly used cloud service by Google.

Multi-factor Authentication

■ Activating Two-Factor Authentication...

Take the following steps, to activate the two-factor authentication on Google account:

Step #1: Login to your Google account by entering your username and password. Or click on the thumbnail image of your account located at the right corner of your Gmail account.



Multi-factor Authentication

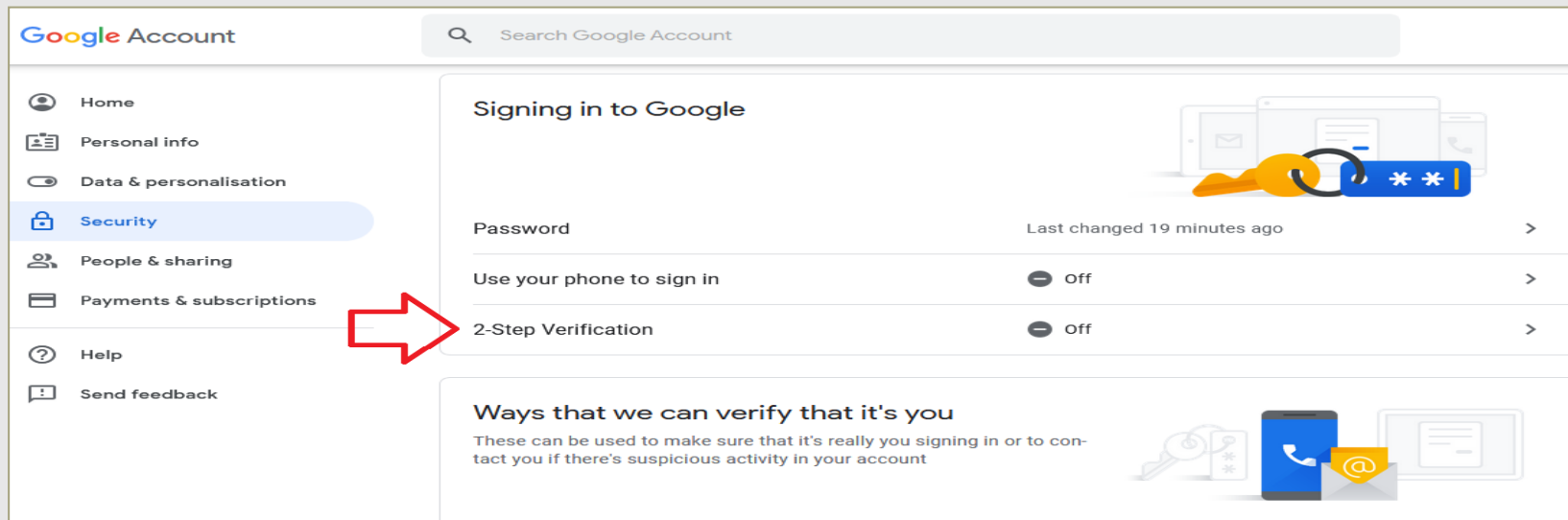
- **Activating Two-Factor Authentication...**

- **Step #2:** Click the **Google Account** button. The Google account setting page appears as shown in the following figure. Here on this page, you can configure activate and configure different features and capabilities along with enabling the two-factor authentication service offered by the Google.
- **Step #3:** Click the **Security** link on the left-page of the Google account settings page. The **Signing in to Google** option appears on the page.

(snapshot on the next slide)

Multi-factor Authentication

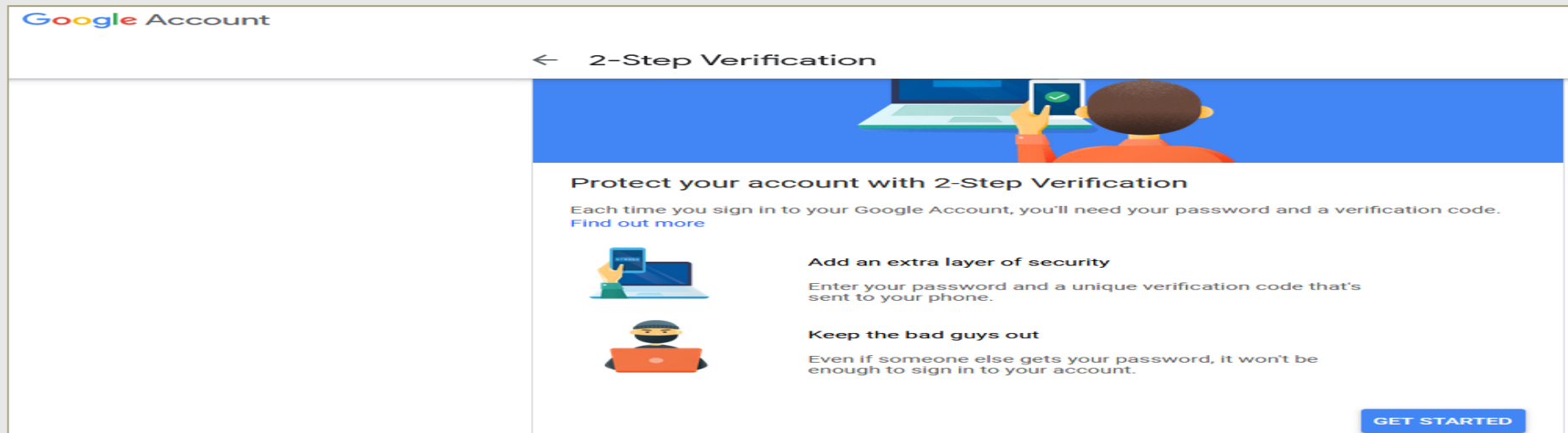
■ Activating Two-Factor Authentication...



- **Step #4:** Click the **2-Step Verification** link located in the signing in to Google block as shown in the above figure. The 2-Step Verification page appears.

Multi-factor Authentication

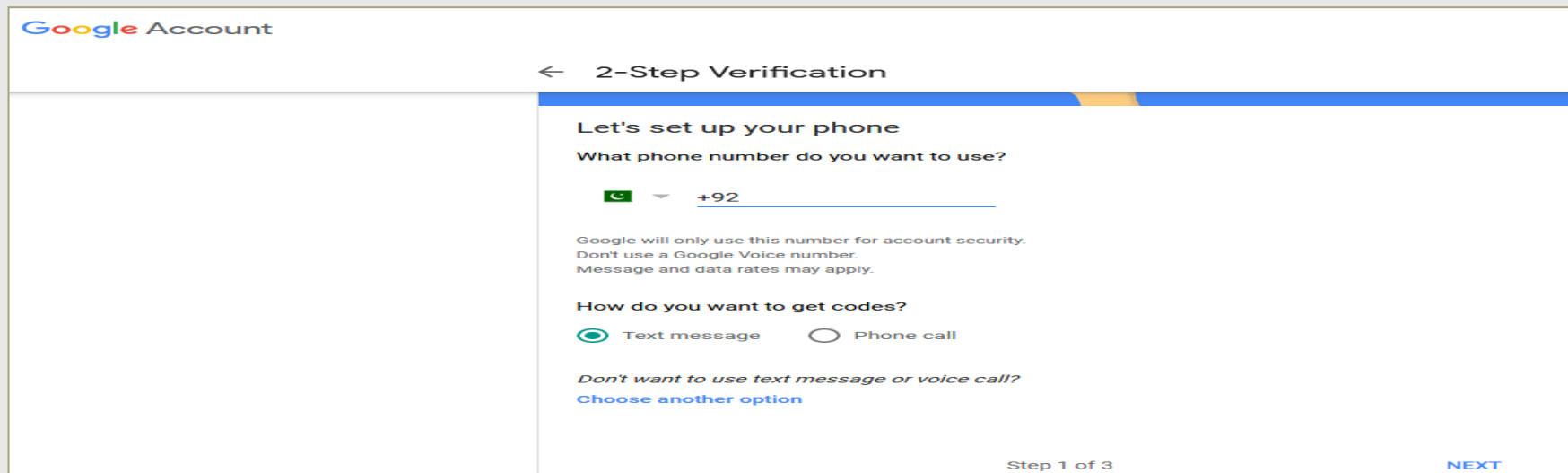
■ Activating Two-Factor Authentication...



Step #5: Click the **Get Started** button as shown in the above figure. The account login verification page appears requiring you to enter your active and valid password of the account. Enter the password to proceed. The 2-step verification wizard appears as shown in the below figure.

Multi-factor Authentication

■ Activating Two-Factor Authentication...

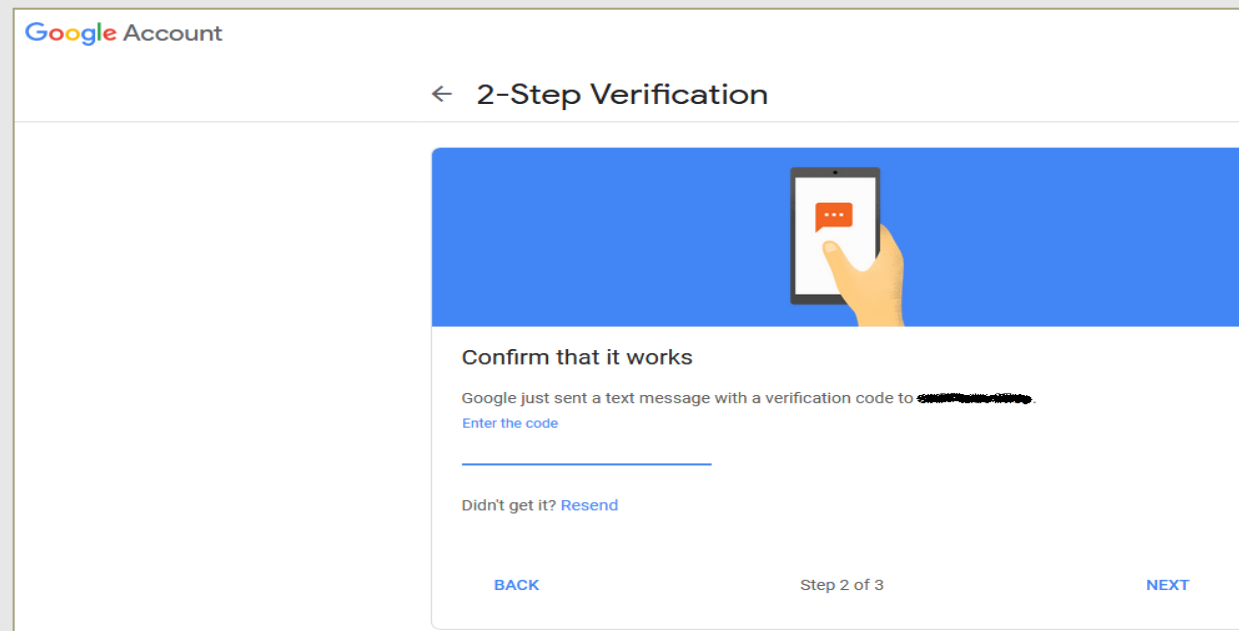


The screenshot shows the Google Account '2-Step Verification' setup page. The header includes the Google Account logo and a back arrow. The main heading is '2-Step Verification'. Below this, a progress bar shows the first step is active. The content area is titled 'Let's set up your phone' and asks 'What phone number do you want to use?'. It features a country selector (currently set to '+92') and a text input field. Below the input field, a note states: 'Google will only use this number for account security. Don't use a Google Voice number. Message and data rates may apply.' The next section, 'How do you want to get codes?', has two radio button options: 'Text message' (which is selected) and 'Phone call'. At the bottom of this section, there is a link that says 'Don't want to use text message or voice call? Choose another option'. The footer of the form indicates 'Step 1 of 3' and a 'NEXT' link.

Step #6: Select the country and enter the valid phone number that you want to use to receive the text message from Google server. Also select the way you want to be contacted for the second factor security code. Google offers two options – text message and phone call. Click the **NEXT** link.

Multi-factor Authentication

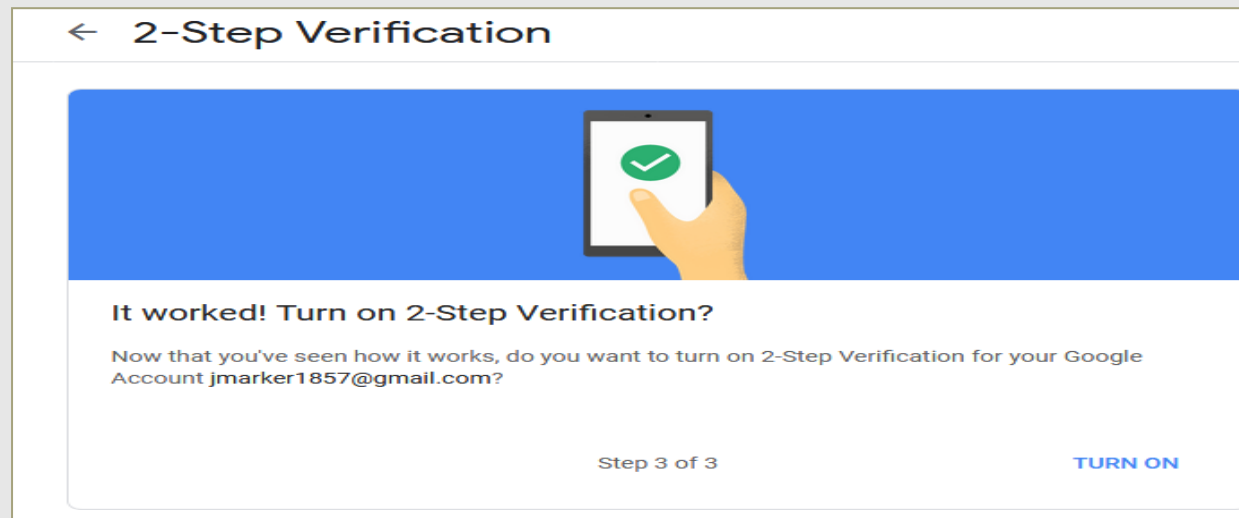
■ Activating Two-Factor Authentication...

The screenshot shows the Google Account '2-Step Verification' setup page. At the top, it says 'Google Account' and '← 2-Step Verification'. Below this is a blue header with an illustration of a hand holding a smartphone displaying a red verification code. The main content area is white and contains the text 'Confirm that it works'. Below this, it says 'Google just sent a text message with a verification code to [redacted]' and 'Enter the code' with a blue link. There is a text input field with a blue underline. Below the input field, it says 'Didn't get it? Resend' with a blue link. At the bottom, there are three links: 'BACK', 'Step 2 of 3', and 'NEXT'.

Step #7: A 5 digit random code will be sent to your mobile for one time use. You need to enter that code in **Enter the Code** field as shown in the above figure, and click the **NEXT** link. The confirmation page will appear as shown in the following figure.

Multi-factor Authentication

- **Activating Two-Factor Authentication...**



- **Step #8:** Click the **TURN ON** link to confirm your selections. The desired two-factor authentication on your Google account has been succeeded. You can modify your information or turn off the 2-factor authentication, if you want as shown in the below figure.

Multi-factor Authentication

- Activating Two-Factor Authentication...

← 2-Step Verification

2-Step Verification is ON since 6 Feb 2019

TURN OFF

Your second step

After entering your password, you'll be asked for a second verification step. [Find out more](#)



Tired of typing verification codes?

Get a Google prompt on your phone and just tap **Yes** to sign in.

[ADD GOOGLE PROMPT](#)



Voice or text message (Default) 

██████████

Verified

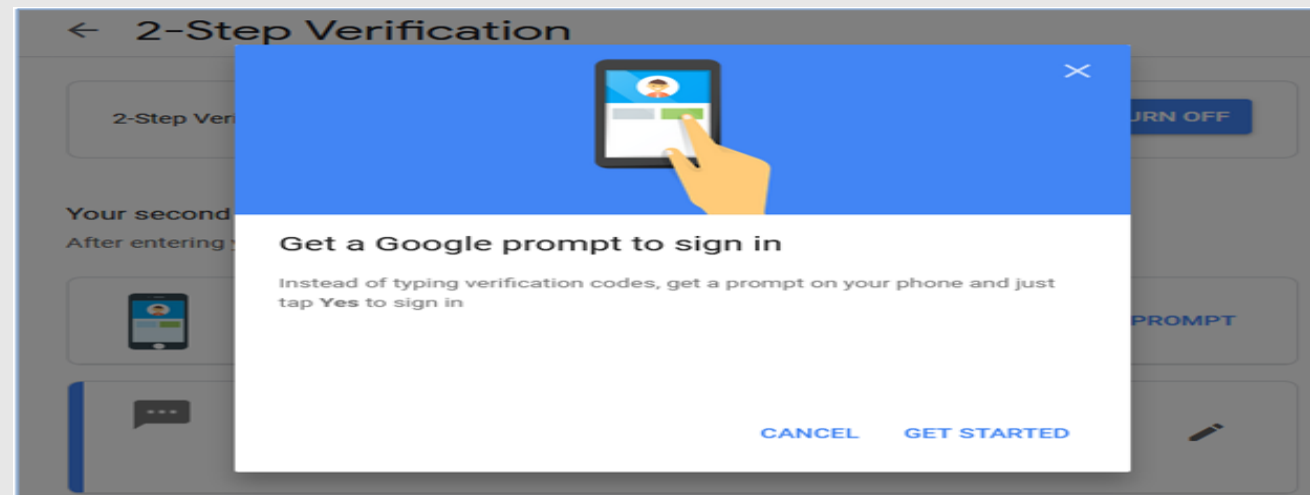
Verification codes are sent by text message.



Multi-factor Authentication

- **Activating Two-Factor Authentication...**

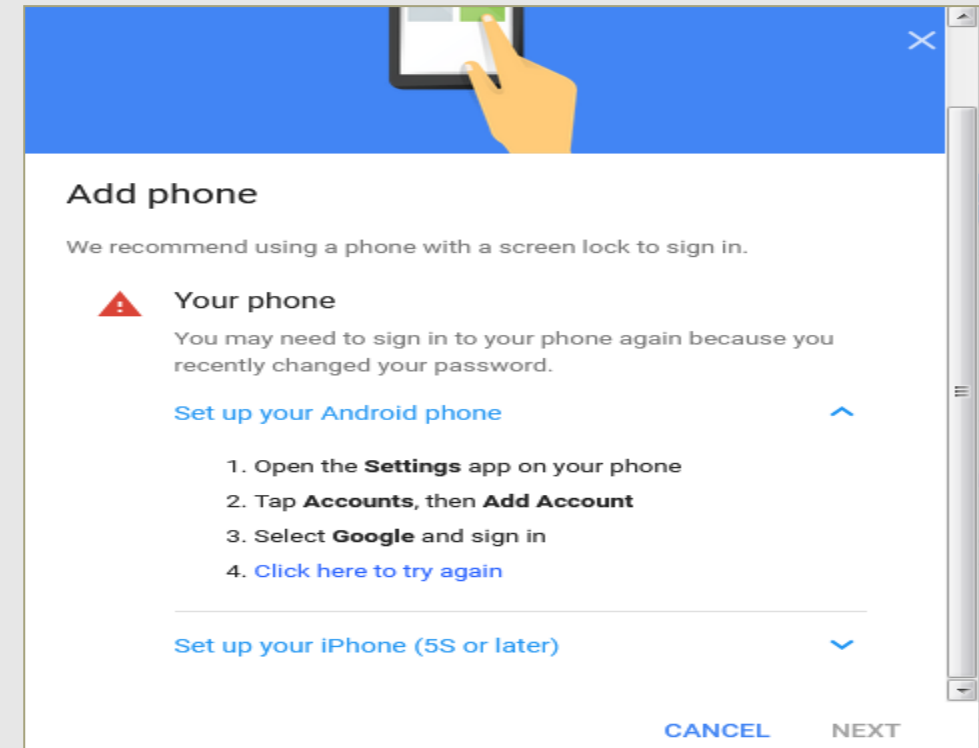
Step #9: You can also choose to inform the Google to login to your account without typing in the code by adding the **ADD GOOGLE PROMPT** option. The popup window appears as shown below.



Multi-factor Authentication

■ Activating Two-Factor Authentication...

- **Step #10:** Click the **GET STARTED** link on the popup message. The Add Phone option appears. Google support adding Android and iPhone for this service. Go to your desired phone and set your phone for the Google **Yes** to login option. The phone that you added will automatically appear, if not you need to click the “**Click here to try again**” link.



Multi-factor Authentication

- **Activating Two-Factor Authentication**

- **Step #11:** Click the **NEXT** link. And you will be asked to enter the code you received on your mobile. Go to the mobile phone and click the 'Yes' push notification that you received from the Google server. You will be automatically logged into your account without typing the code in your Google account.

Multi-factor Authentication

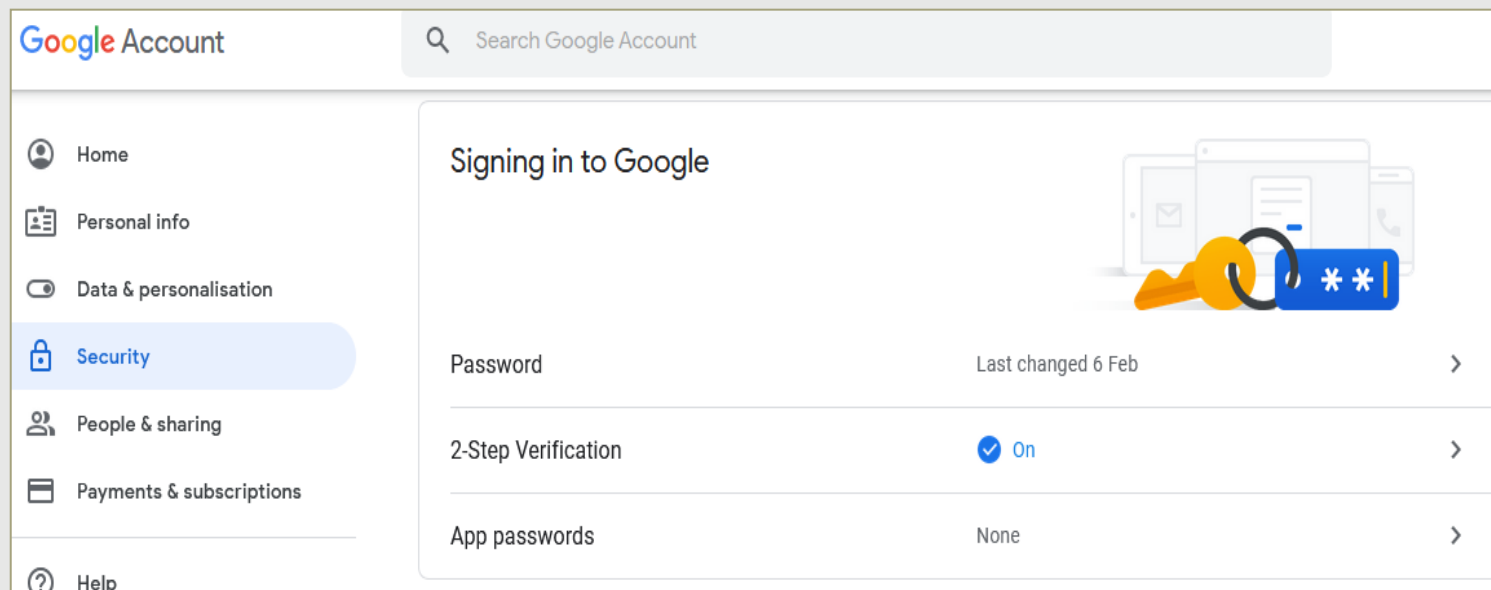
■ Creating Application Specific Passwords...

Google offers great security with 2-factor authentication on your devices. Google also offers the high security on using third party applications on your mobiles. When you use any third-party application on your mobile device with your Google account, then you will need to generate an application specific password from the Google account.

- To generate an application specific password, take the following steps.
 - Login to your Google account
 - Click the **Avatar** button and then choose the **Google Account** option. The account setting page appears
 - Click the **Security** link on the left-pane of the page. The security settings appear

Multi-factor Authentication

■ Creating Application Specific Passwords...

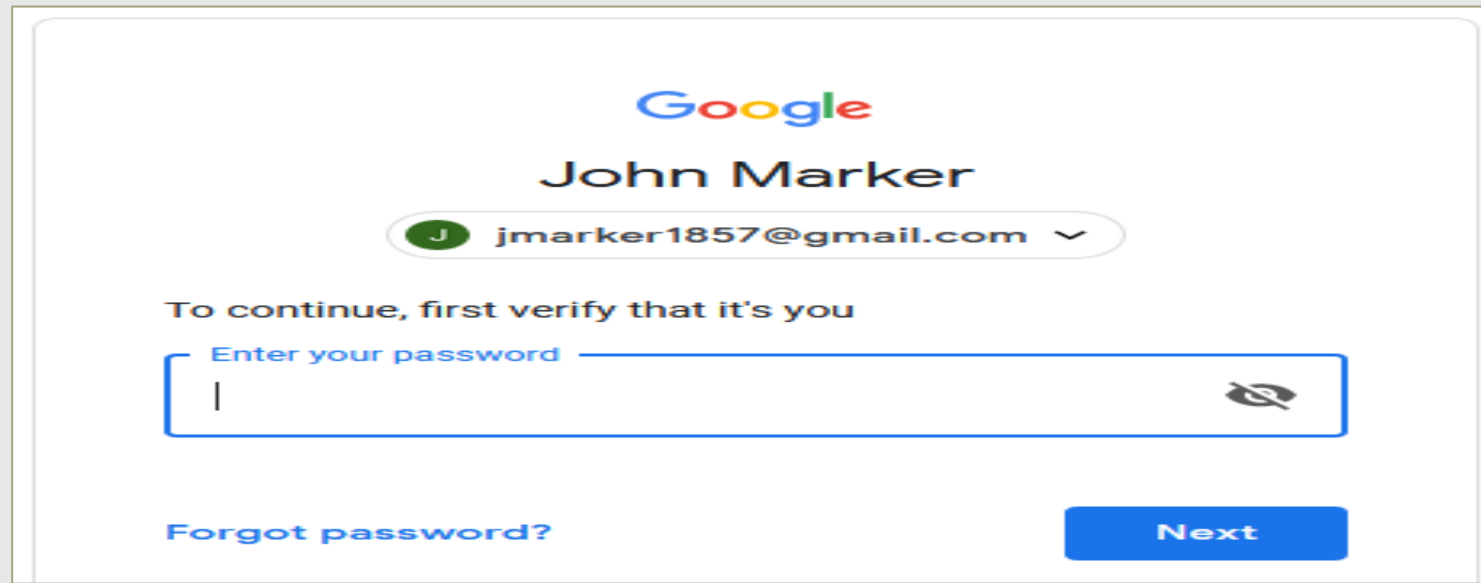


- Click the **App Passwords** link. Google asks to verify your password.

Multi-factor Authentication

- **Creating Application Specific Passwords...**

- Enter your valid password and click the **Next** button. The **App Password** page appears as shown in the following figure.

A screenshot of a Google account verification page. At the top is the Google logo. Below it is the name "John Marker". Under the name is a profile picture placeholder (a green circle with a white 'J') and the email address "jmarker1857@gmail.com" with a dropdown arrow. Below this is the text "To continue, first verify that it's you". Underneath is a password input field with the placeholder text "Enter your password" and a single character 'l' entered. To the right of the input field is an eye icon. At the bottom left is a link "Forgot password?". At the bottom right is a blue button labeled "Next".

Google

John Marker

J jmarker1857@gmail.com ▼

To continue, first verify that it's you

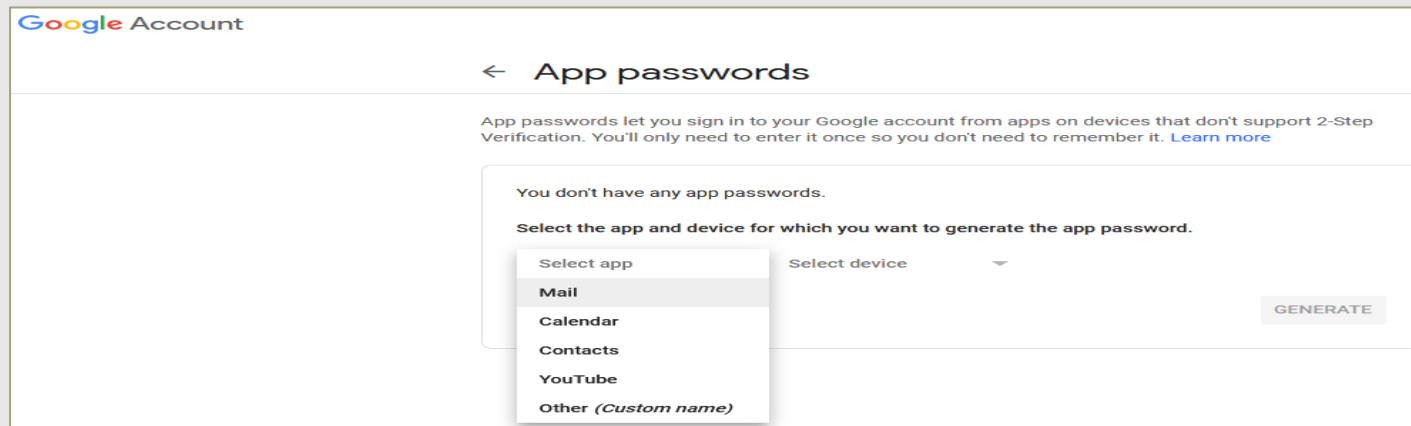
Enter your password |

Forgot password? Next

Multi-factor Authentication

■ Creating Application Specific Passwords...

- Enter your valid password and click the **Next** button. The **App Password** page appears.
- Select the desired app and the device type that you use from the drop-down arrows as shown in the following figure.



The screenshot shows the 'App passwords' page in a Google Account interface. At the top, it says 'Google Account' and '← App passwords'. Below this, a message states: 'App passwords let you sign in to your Google account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)'. A box in the center says 'You don't have any app passwords.' and 'Select the app and device for which you want to generate the app password.' There are two dropdown menus: 'Select app' and 'Select device'. The 'Select app' dropdown is open, showing options: 'Mail', 'Calendar', 'Contacts', 'YouTube', and 'Other (Custom name)'. A 'GENERATE' button is located to the right of the 'Select device' dropdown.

Multi-factor Authentication

■ Creating Application Specific Passwords...

- Click the **GENERATE** button. The app password will be generated as shown in the following figure.
- A full detail of how to use the application specific password is also described.
- Copy this application specific password
- Open the application on the selected device that you want to link with your Google account for using the applications.

Generated app password

Your app password for Windows Computer

dshl rcac ecyz efry

How to use it

1. Open the "Mail" app.
2. Open the "Settings" menu.
3. Select "Accounts" and then select your Google Account.
4. Replace your password with the 16-character password shown above.

Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

[Learn more](#)

DONE

Add your Google account

Enter the information below to connect to your Google account.

Email address
securesally@gmail.com

Password

☐ Include your Google contacts and calendars

Multi-factor Authentication

- **Creating Application Specific Passwords...**

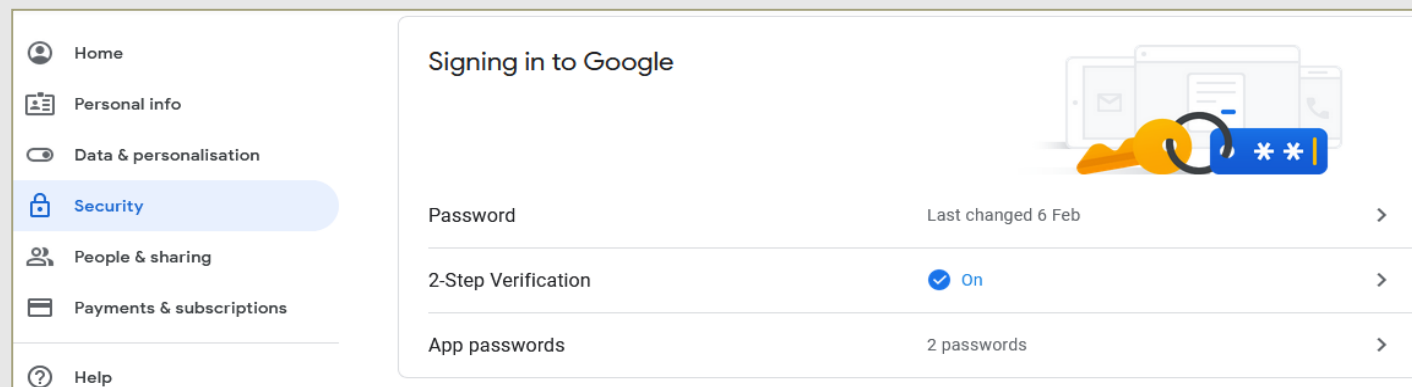
- Enter the application specific password in the application and click the login button to login to that particular application.
- All these app specific passwords are saved for future use of that password on that particular application
- You can create passwords for other applications by following the same procedure

Multi-factor Authentication

- **What if your phone with all apps enabled is lost?...**

Google offers a robust security for your all devices, but you have to be proactive enough to follow the security measures in case you lose your mobile. First of all, you should revoke the application specific passwords on any of your device. To do so, take the following steps:

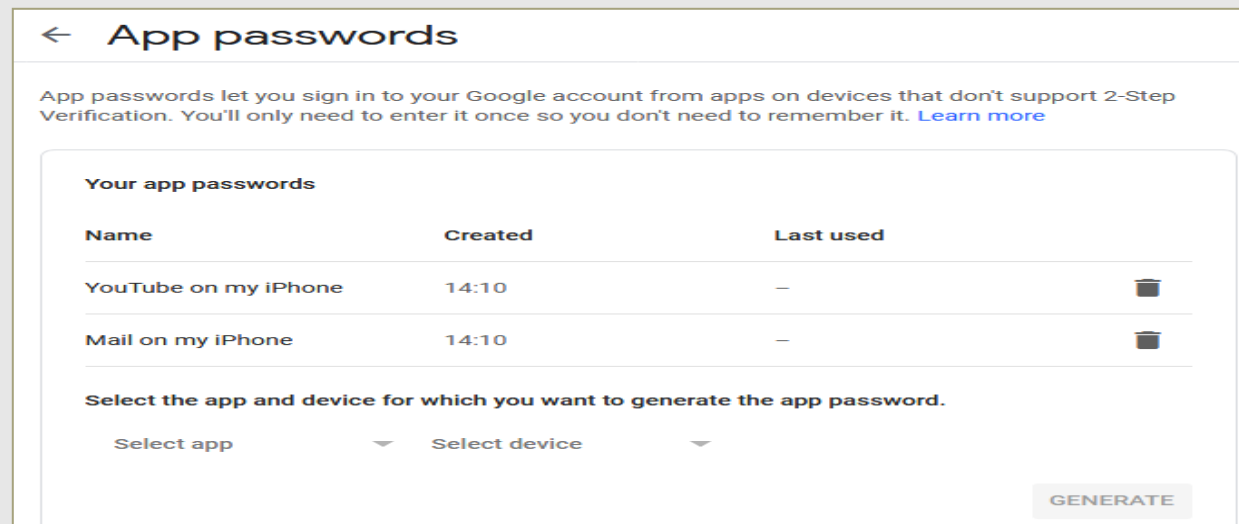
- Go to your account settings and click the Security link on the left-pane



Multi-factor Authentication

- What if your phone with all apps enabled is lost?

- Click the App Passwords link. The existing application specific passwords will appear.



The screenshot shows the 'App passwords' management page in a web browser. At the top, there is a back arrow and the title 'App passwords'. Below this is a descriptive paragraph: 'App passwords let you sign in to your Google account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)'. The main section is titled 'Your app passwords' and contains a table with three columns: 'Name', 'Created', and 'Last used'. There are two rows of app passwords listed: 'YouTube on my iPhone' and 'Mail on my iPhone', both created at '14:10' and with a trash can icon for deletion. Below the table, there is a section titled 'Select the app and device for which you want to generate the app password.' with two dropdown menus labeled 'Select app' and 'Select device'. A 'GENERATE' button is located at the bottom right of the form.

Name	Created	Last used
YouTube on my iPhone	14:10	—
Mail on my iPhone	14:10	—

- Click the  icon to delete the application specific passwords

Multi-factor Authentication

- **What if your phone with all apps enabled is lost?**
 - Your applications will logout on your mobile device that you lost. You can create new application specific password on your new device.
 - Change the password of your Google account and its backup numbers
 - It is always recommended to add backup phone number so that you can recover your Google account in case of losing mobile device with the primary phone number.
 - Another option is to save the codes that you generated on your computer

The End 😊



جامعة زايد الذكية
EVERYONE'S SMART UNIVERSITY

