



# COMPUTER SECURITY



**tutorialspoint**

SIMPLY EASY LEARNING

[www.tutorialspoint.com](http://www.tutorialspoint.com)



<https://www.facebook.com/tutorialspointindia>



<https://twitter.com/tutorialspoint>

## About the Tutorial

---

Computer Security is the process of detecting and preventing any unauthorized use of your laptop/computer. It involves the process of safeguarding against trespassers from using your personal or office based computer resources with malicious intent or for their own gains, or even for gaining any access to them accidentally.

In this tutorial, we will treat the concept of computer security which can be a laptop, a workstation, a server or even a network device. This is an introductory tutorial that covers the basics of Computer Security and how to deal with its various components and sub-components.

## Audience

---

This tutorial has been prepared mainly for those professionals who are within the IT industry, working as IT specialists, System administrators, and Security administrators.

This tutorial is intended to make you comfortable in getting started with Computer Security and its various functions.

## Prerequisites

---

It is an elementary tutorial and you can easily understand the concepts explained here with a basic knowledge of how a company or an organization deals with its Computer Security. However, it will help if you have some prior exposure on how to carry out computer updates regularly, setting up firewalls, antiviruses, etc.

## Copyright and Disclaimer

---

© Copyright 2016 by Tutorials Point (I) Pvt. Ltd.

All the content and graphics published in this e-book are the property of Tutorials Point (I) Pvt. Ltd. The user of this e-book is prohibited to reuse, retain, copy, distribute or republish any contents or a part of contents of this e-book in any manner without written consent of the publisher.

We strive to update the contents of our website and tutorials as timely and as precisely as possible, however, the contents may contain inaccuracies or errors. Tutorials Point (I) Pvt. Ltd. provides no guarantee regarding the accuracy, timeliness or completeness of our website or its contents including this tutorial. If you discover any errors on our website or in this tutorial, please notify us at [contact@tutorialspoint.com](mailto:contact@tutorialspoint.com)

## Table of Contents

---

About the Tutorial.....	i
Audience .....	i
Prerequisites .....	i
Copyright and Disclaimer .....	i
Table of Contents .....	ii
<b>1. COMPUTER SECURITY – OVERVIEW.....</b>	<b>1</b>
Why Security? .....	1
What to Secure?.....	2
Benefits of Computer Security Awareness .....	4
Potential Losses due to Security Attacks .....	5
Basic Computer Security Checklist.....	6
<b>2. COMPUTER SECURITY – ELEMENTS .....</b>	<b>9</b>
Different Elements in Computer Security .....	9
Confidentiality .....	10
Integrity .....	10
Availability .....	11
<b>3. COMPUTER SECURITY – TERMINOLOGIES .....</b>	<b>12</b>
<b>4. COMPUTER SECURITY – LAYERS .....</b>	<b>13</b>
<b>5. COMPUTER SECURITY – SECURING OS .....</b>	<b>15</b>
Guidelines for Windows OS Security .....	15
Guidelines for Mac OS X Security .....	22
<b>6. COMPUTER SECURITY – ANTIVIRUSES .....</b>	<b>31</b>
Basic Functions of Antivirus Engines.....	31

Online Virus Testing .....	32
Free Antivirus Software.....	33
Avast Antivirus.....	34
AVG Antivirus.....	35
Panda Antivirus 2016 .....	35
Bitdefender Antivirus .....	36
Microsoft Security Essentials.....	37
Commercial Antivirus .....	37
Kaspersky Antivirus.....	37
McAfee AntiVirus Plus.....	38
Webroot SecureAnywhere Antivirus .....	40
<b>7. COMPUTER SECURITY – MALWARES .....</b>	<b>41</b>
Characteristics of a Virus .....	41
Working Process of Malwares and how to Clean it.....	43
Detecting a Computer Error from a Virus Infection .....	45
Virus Information .....	46
<b>8. COMPUTER SECURITY – ENCRYPTION.....</b>	<b>47</b>
What is Encryption? .....	47
Tools Used to Encrypt Documents.....	47
Encryption Ways of Communication .....	48
<b>9. COMPUTER SECURITY – DATA BACKUP .....</b>	<b>50</b>
Why is Backup Needed? .....	50
Backup Devices .....	50
Types of Backups Based on Location .....	52
<b>10. COMPUTER SECURITY – DISASTER RECOVERY .....</b>	<b>57</b>
Requirements to Have a Disaster Recovery Plan .....	57

11. COMPUTER SECURITY – NETWORK .....	59
<b>Devices that Help us with Network Security</b> .....	59
<b>Intrusion Detection Systems</b> .....	60
<b>Intrusion Detection Tools</b> .....	60
<b>Virtual Private Network</b> .....	62
12. COMPUTER SECURITY – POLICIES .....	63
<b>Role of the Security Policy in Setting up Protocols</b> .....	63
<b>Structure of a Security Policy</b> .....	64
<b>Types of Policies</b> .....	64
13. COMPUTER SECURITY – CHECKLIST .....	66
14. COMPUTER SECURITY - LEGAL COMPLIANCE.....	70
<b>What are the Main Compliances?</b> .....	70

# 1. Computer Security – Overview

In this tutorial, we will treat the concept of Computer Security which can be a laptop, a workstation, a server or a network device. This tutorial is done mainly for people that are within the IT industry who are IT specialists, System administrators, Security administrators.

## Why Security?

---

Cyberspace (internet, work environment, intranet) is becoming a dangerous place for all organizations and individuals to protect their sensitive data or reputation. This is because of the numerous people and machines accessing it. It is important to mention that the recent studies have shown a big danger is coming from internal threats or from disappointed employees like the Edward Snowden case, another internal threat is that information material can be easy accessible over the intranet.

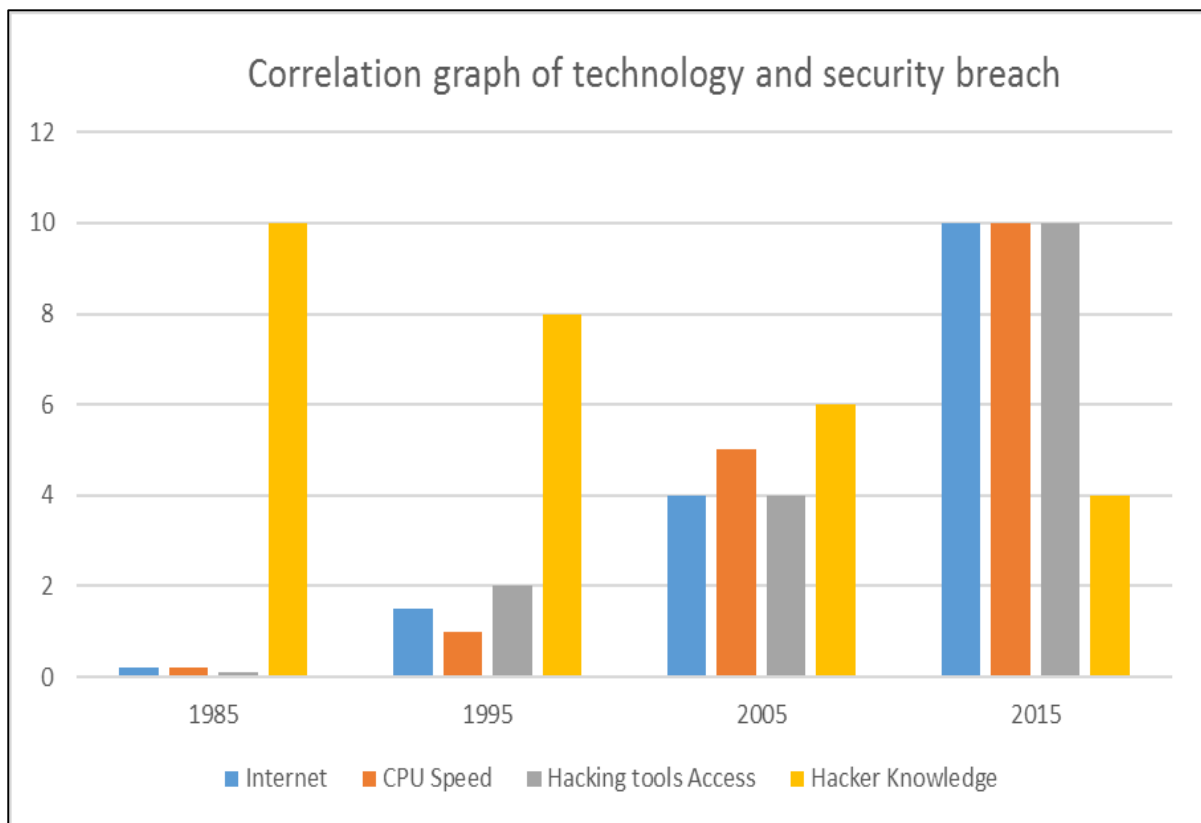
One important indicator is the IT skills of a person that wants to hack or to breach your security has decreased but the success rate of it has increased, this is because of three main factors:

1. Hacking tools that can be found very easily by everyone just by googling and they are endless.
2. Technology with the end-users has increased rapidly within these years, like internet bandwidth and computer processing speeds.
3. Access to hacking information manuals.

All this can make even a school boy with the curiosity, a potential hacker for your organization.

Since locking down all networks is not an available option, the only response the security managers can give is to harden their networks, applications and operating systems to a reasonable level of safety, and conducting a business disaster recovery plan.

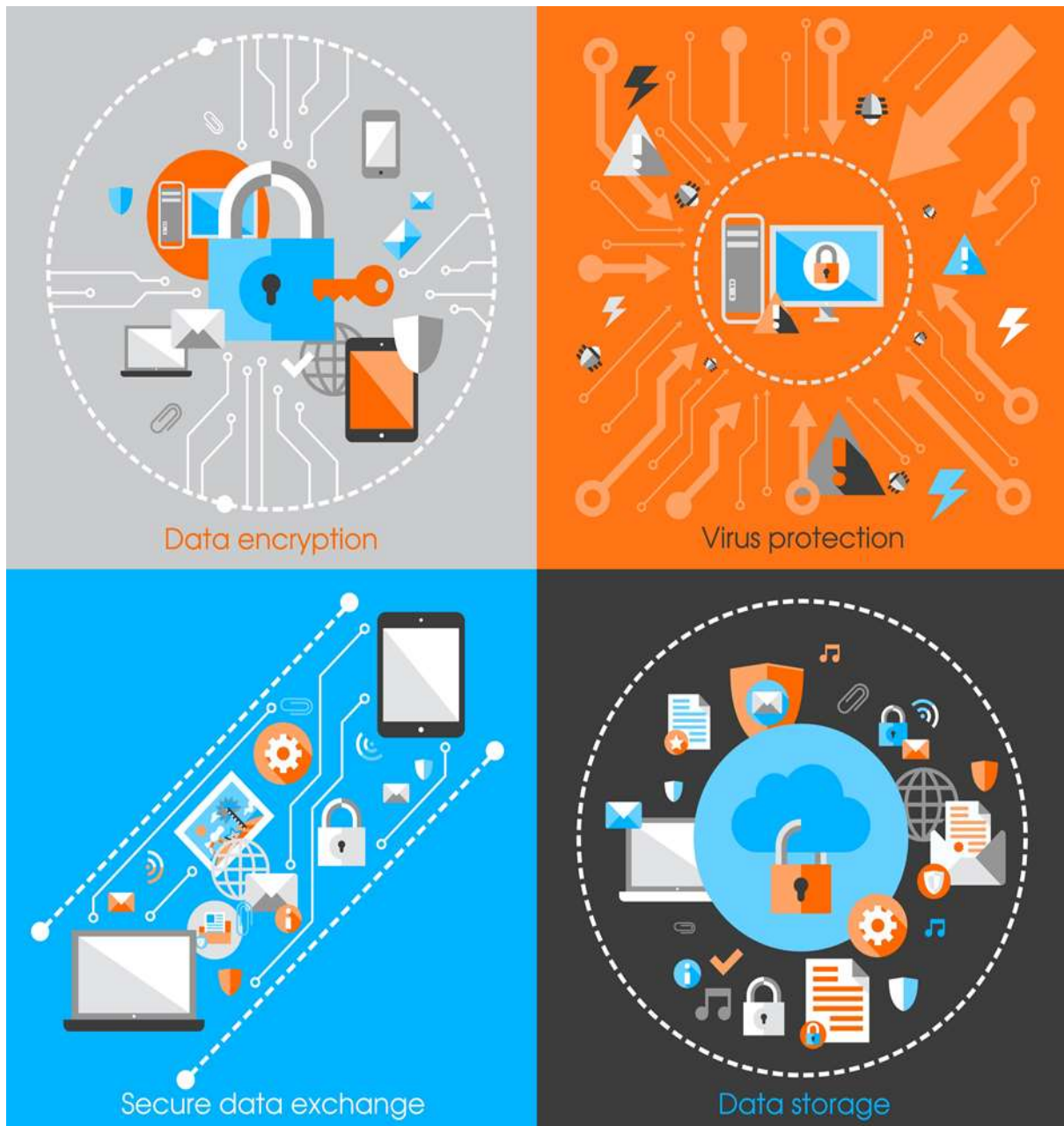
The following graph gives us a basic idea.



## What to Secure?

Let's see this case, you are an IT administrator in a small company having two small servers staying in a corner and you are very good at your job. You are doing updates regularly, setting up firewalls, antiviruses, etc. One day, you see that the organization employees are not accessing the systems anymore. When you go and check, you see the cleaning lady doing her job and by mistake, she had removed the power cable and unplugged the server.

What I mean by this case is that even physical security is important in computer security, as most of us think it is the last thing to take care of.



Now let's go directly to the point of what all to secure in a computer environment:

- First of all, is to check the physical security by setting control systems like motion alarms, door accessing systems, humidity sensors, temperature sensors. All these components decrease the possibility of a computer to be stolen or damaged by humans and environment itself.
- People having access to computer systems should have their own user id with password protection.
- Monitors should be screen saver protected to hide the information from being displayed when the user is away or inactive.
- Secure your network especially wireless, passwords should be used.
- Internet equipment as routers to be protected with password.



- Data that you use to store information which can be financial, or non-financial by encryption.
- Information should be protected in all types of its representation in transmission by encrypting it.

## Benefits of Computer Security Awareness

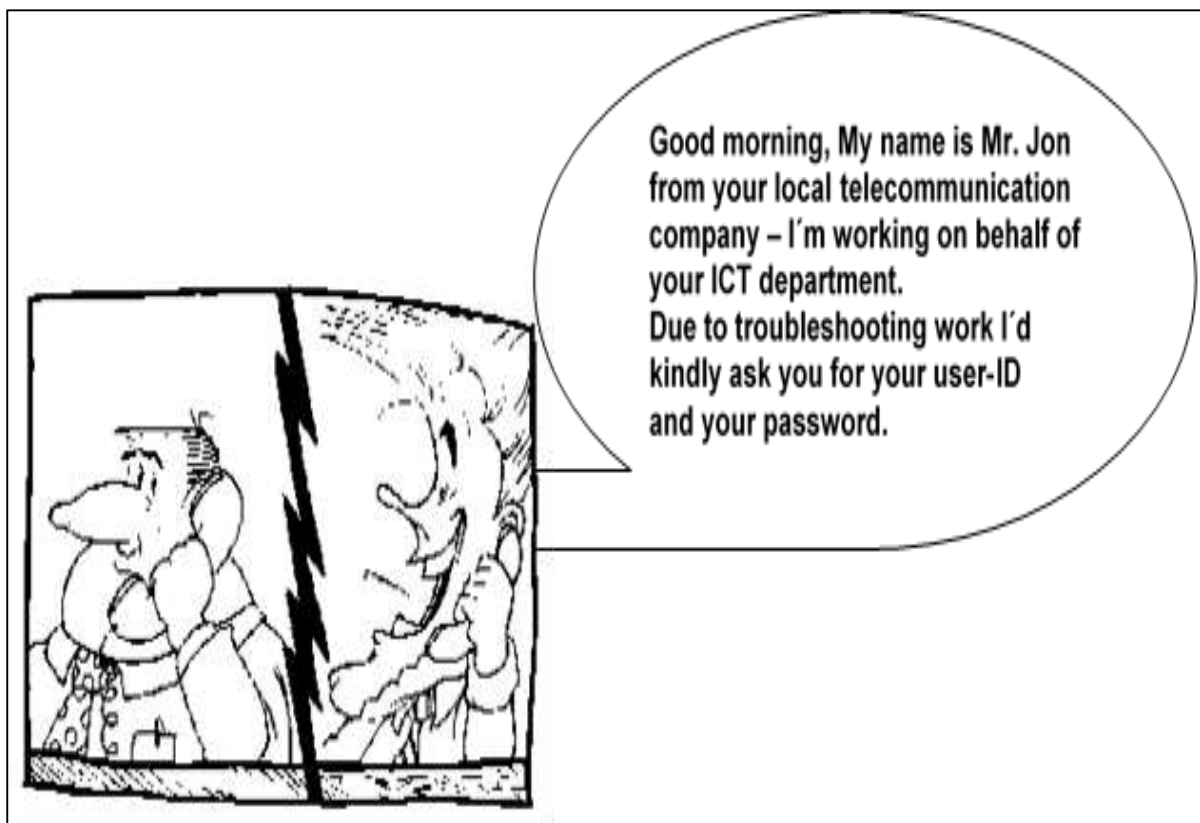
---

*Do you know in all this digital world, what is the biggest hole or the weakest point of the security?*

*Answer. It is us, humans.*

Most of the security breaches come from uninformed and untrained persons which give information to a third party or publish data in Internet without knowing the consequences.

See the following scenario which tells us what employees might end up doing without computer security awareness:



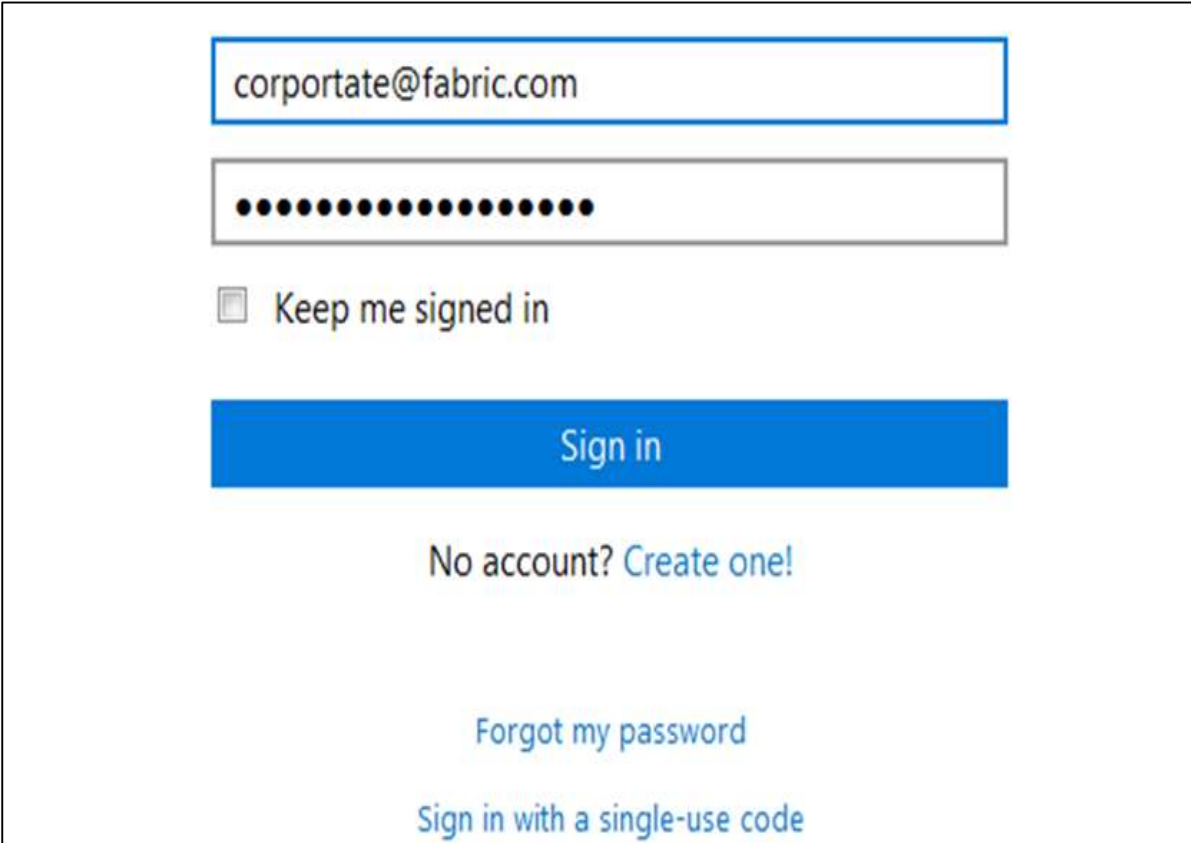
So the benefits of computer security awareness are obvious as it directly minimizes the potential of you being hacked off your identity, your computer, your organization.

## Potential Losses due to Security Attacks

---

The potential losses in this cyberspace are many even if you are using a single computer in your room. Here, I will be listing some examples that have a direct impact on you and on others:

- **Losing you data** – If your computer has been hacked or infected, there is a big chance that all your stored data might be taken by the attacker.
- **Bad usage of your computer resources** – This means that your network or computer can go in overload so you cannot access your genuine services or in a worst case scenario, it can be used by the hacker to attack another machine or network.
- **Reputation loss** – Just think if your Facebook account or business email has been owned by a social engineering attack and it sends fake information to your friends, business partners. You will need time to gain back your reputation.
- **Identity theft** – This is a case where your identity is stolen (photo, name surname, address, and credit card) and can be used for a crime like making false identity documents.



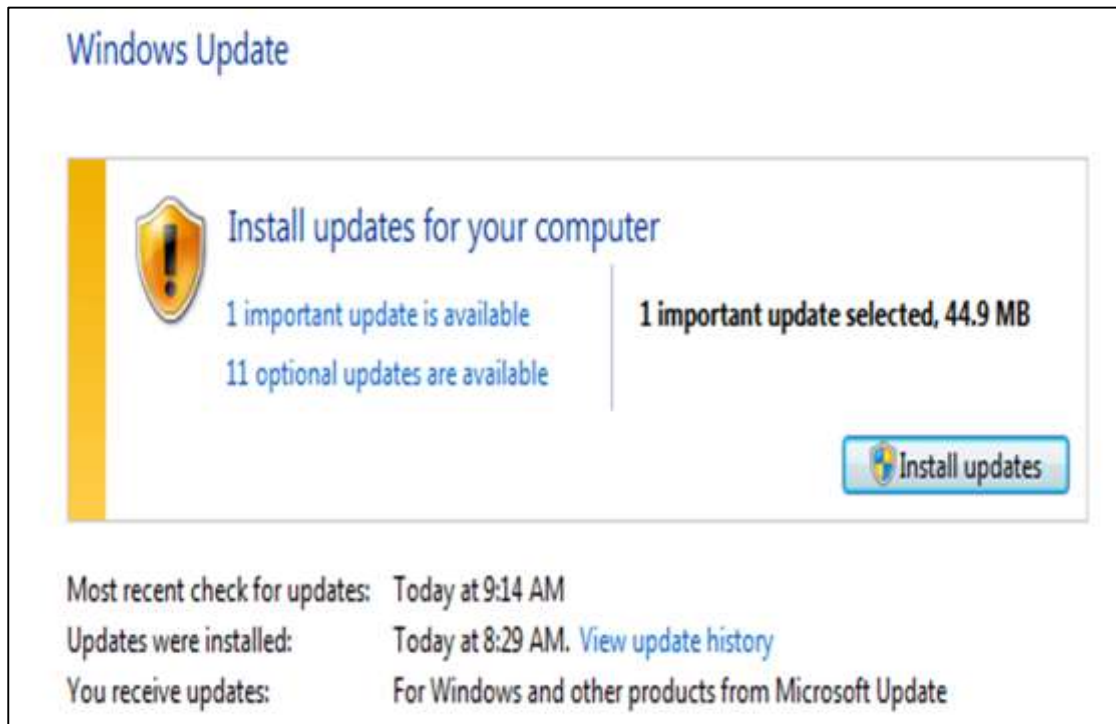
The image shows a login form for fabric.com. It features a text input field containing the email address 'corportate@fabric.com'. Below it is a password input field with 12 black dots. There is a checkbox labeled 'Keep me signed in' which is currently unchecked. A prominent blue button labeled 'Sign in' is positioned below the password field. At the bottom of the form, there are three links: 'No account? Create one!', 'Forgot my password', and 'Sign in with a single-use code'.

## Basic Computer Security Checklist

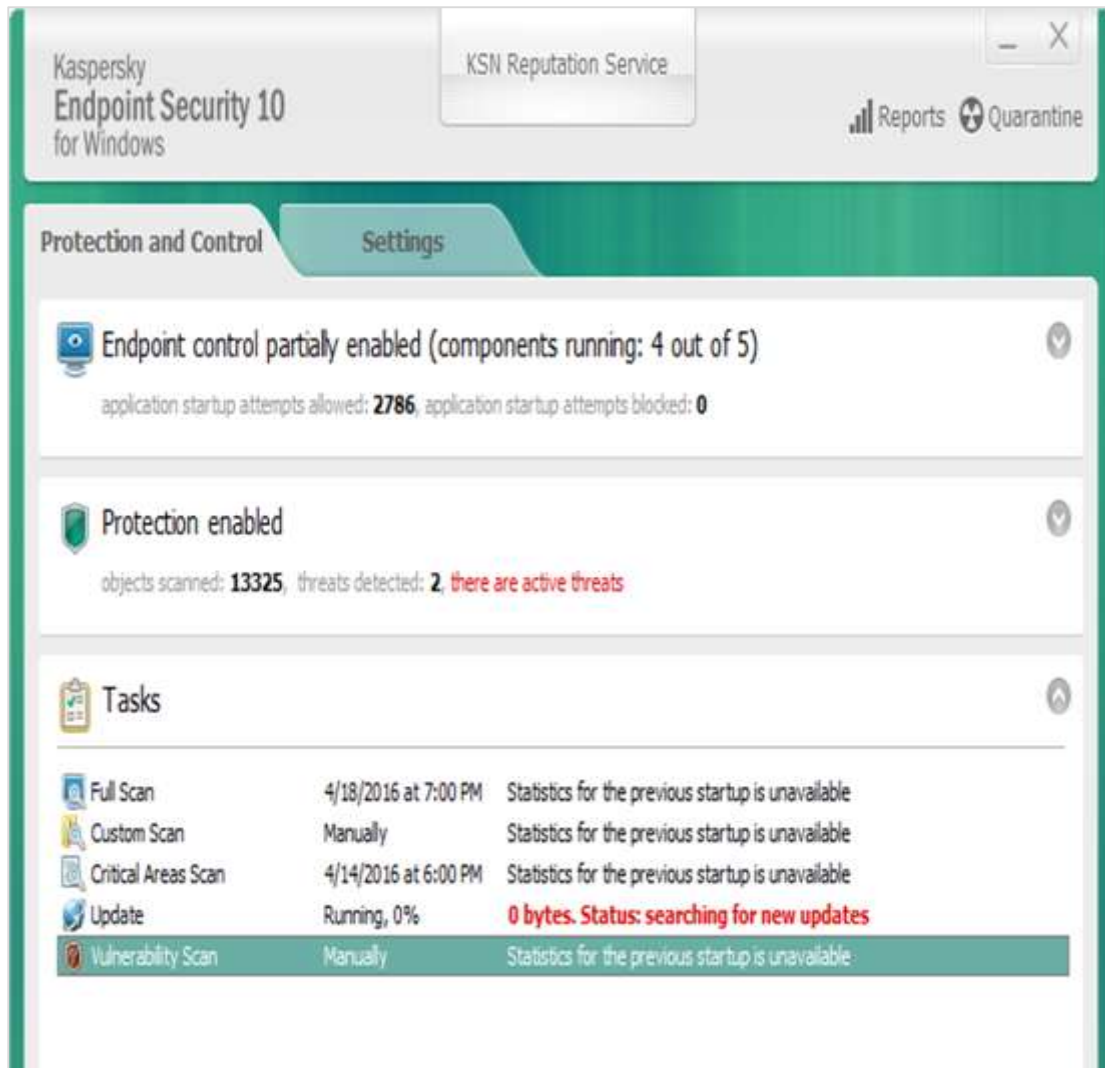
---

There are some basic things that everyone of us in every operating system need to do:

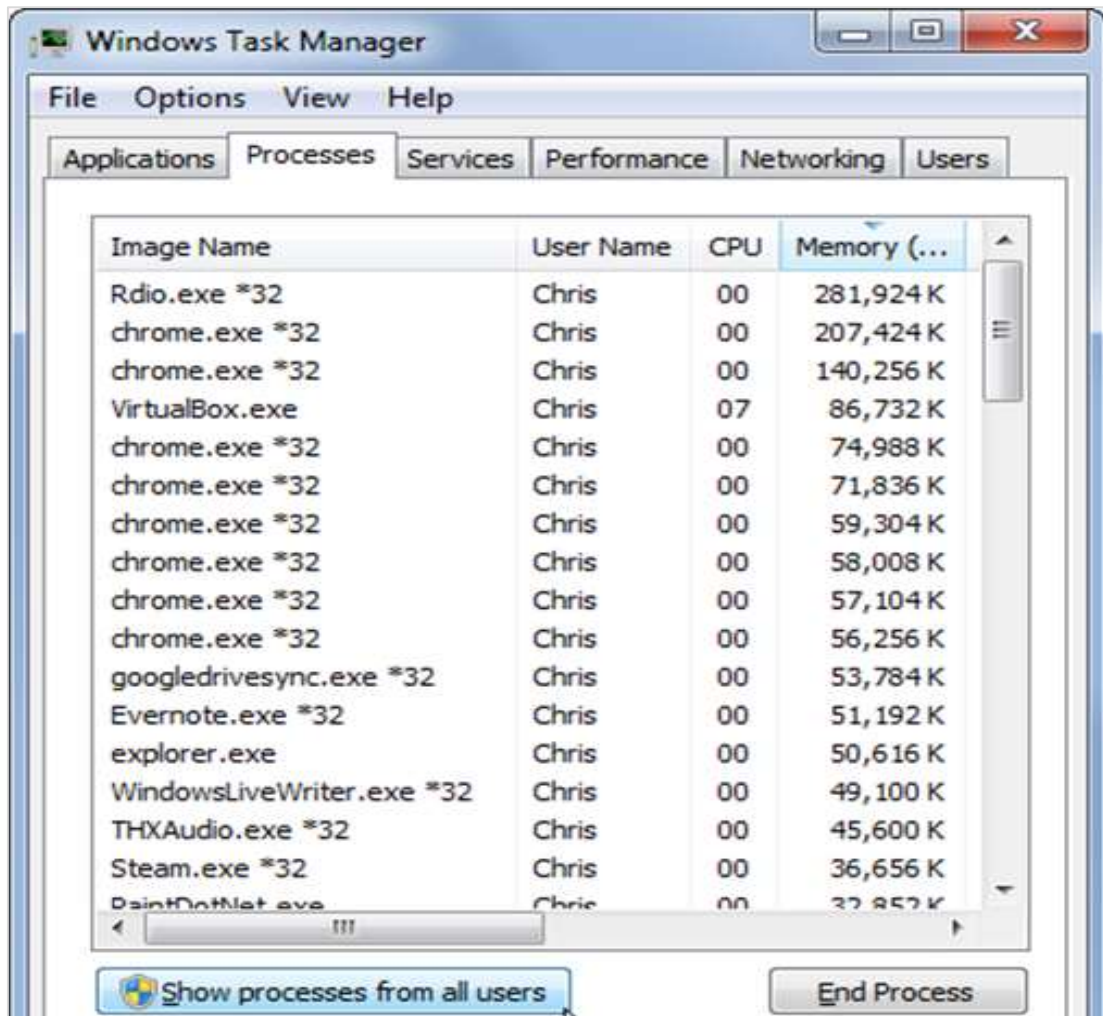
- Check if the user is password protected.
- Check if the operating system is being updated. In my case, I did a screenshot of my laptop which is a Windows 7.



- Check if the antivirus or antimalware is installed and updated. In my case, I have a Kaspersky antivirus being updated.



- Check for the unusual services running that consumes resources.



- Check if your monitor is using a screen saver.
- Check if the computer firewall is on or not.
- Check if you are doing backups regularly.
- Check if there are shares that are not useful.
- Check if your account has full rights or is restricted.
- Update other third party software's.

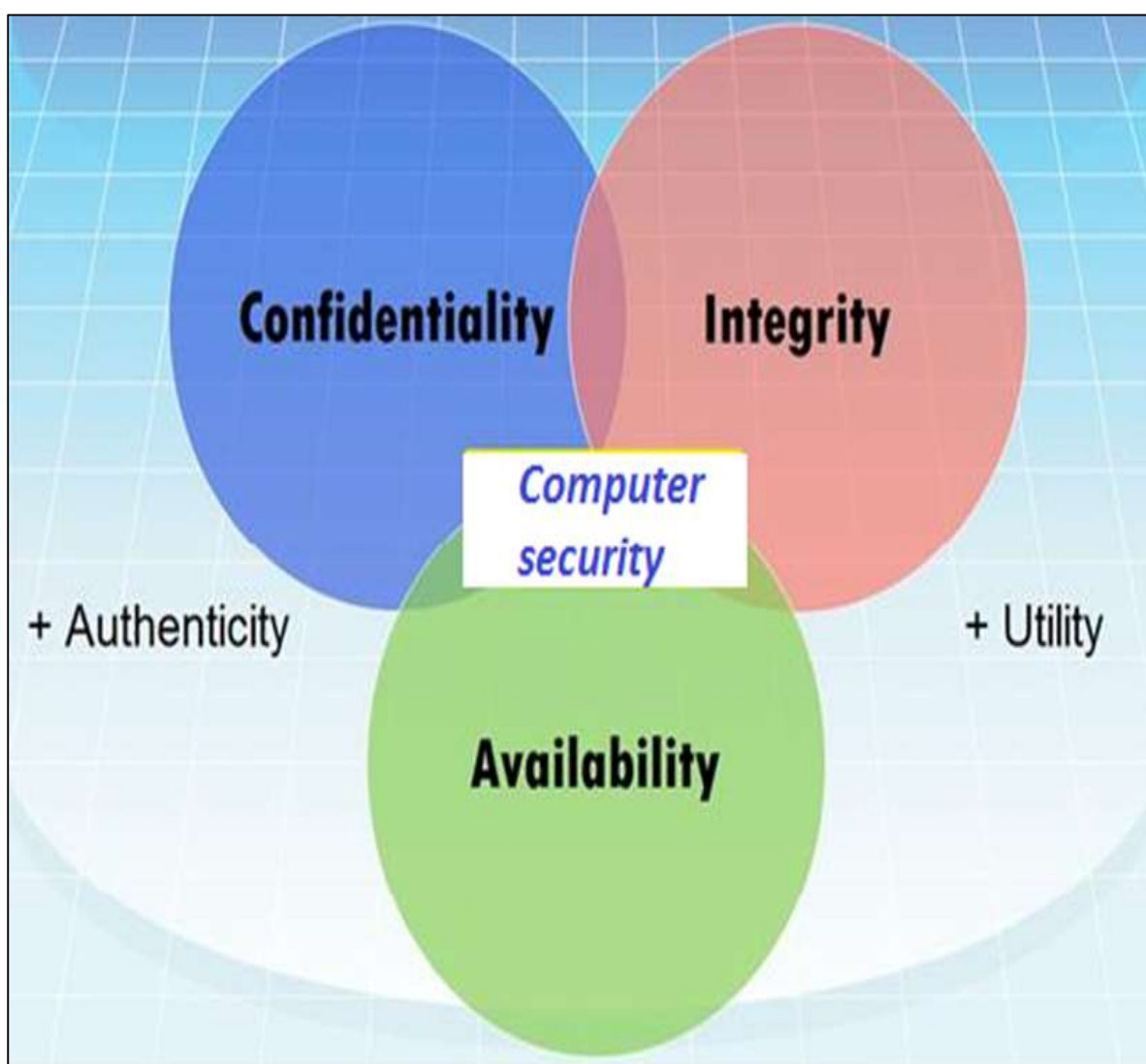
## 2. Computer Security – Elements

The general state in Computer Security has the ability to detect and prevent attacks and to be able to recover. If these attacks are successful as such then it has to contain the disruption of information and services and check if they are kept low or tolerable.

### Different Elements in Computer Security

---

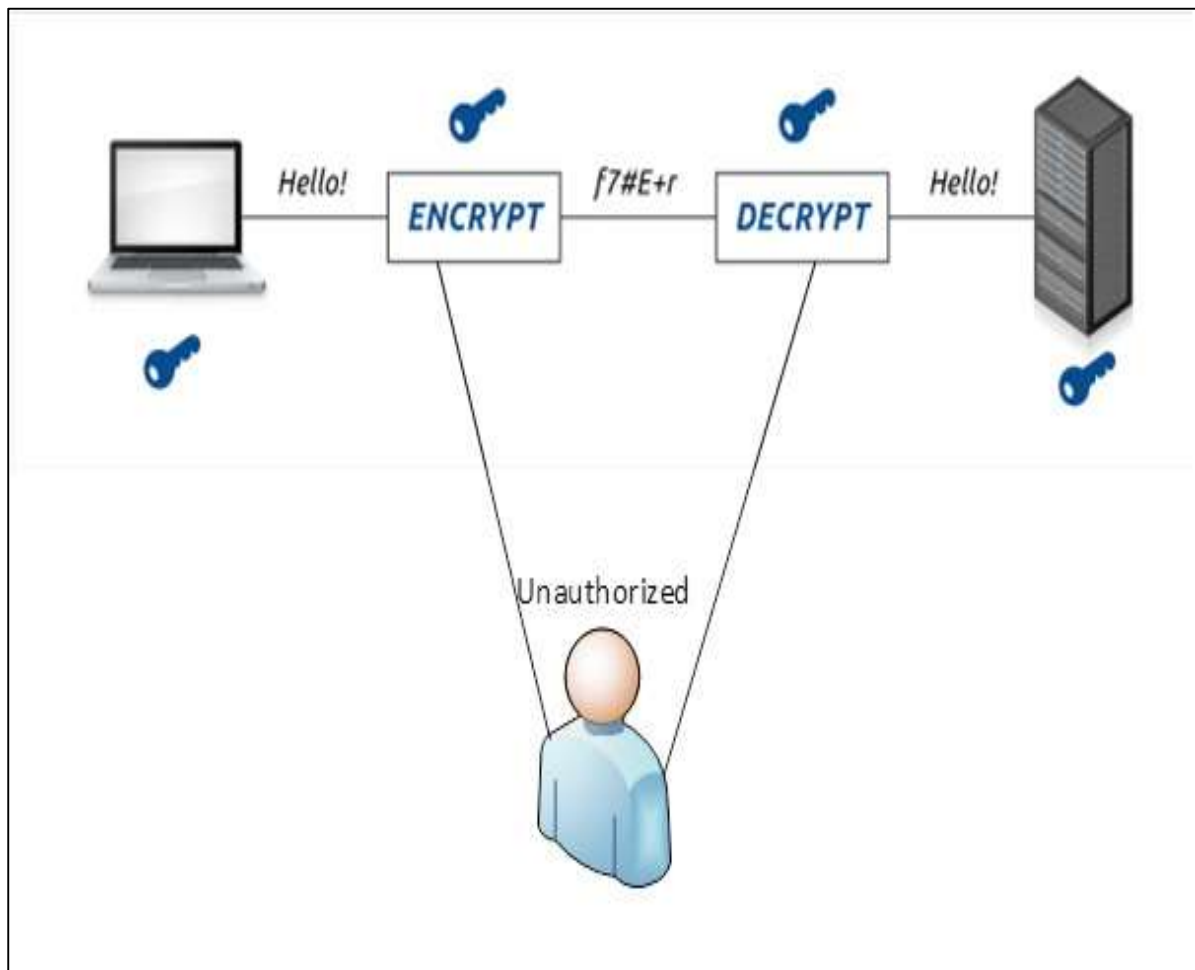
In order to fulfil these requirements, we come to the three main elements which are **confidentiality**, **integrity**, and **availability** and the recently added **authenticity and utility**.



## Confidentiality

Confidentiality is the concealment of information or resources. Also, there is a need to keep information secret from other third parties that want to have access to it, so just the right people can access it.

**Example in real life:** Let's say there are two people communicating via an encrypted email they know the decryption keys of each other and they read the email by entering these keys into the email program. If someone else can read these decryption keys when they are entered into the program, then the confidentiality of that email is compromised.



## Integrity

Integrity is the trustworthiness of data in the systems or resources by the point of view of preventing unauthorized and improper changes. Generally, Integrity is composed of two sub-elements – data-integrity, which it has to do with the content of the data and authentication which has to do with the origin of the data as such information has values only if it is correct.

**Example in real life:** Let's say you are doing an online payment of 5 USD, but your information is tampered without your knowledge in a way by sending to the seller 500 USD, this would cost you too much.

In this case cryptography plays a very major role in ensuring data integrity. Commonly used methods to protect data integrity includes hashing the data you receive and

comparing it with the hash of the original message. However, this means that the hash of the original data must be provided in a secure way.

## Availability

---

Availability refers to the ability to access data of a resource when it is needed, as such the information has value only if the authorized people can access at right time. Denying access to data nowadays has become a common attack. Imagine a downtime of a live server how costly it can be.

**Example in real life:** Let's say a hacker has compromised a webserver of a bank and put it down. You as an authenticated user want to do an e-banking transfer but it is impossible to access it, the undone transfer is a money lost for the bank.



# 3. Computer Security – Terminologies

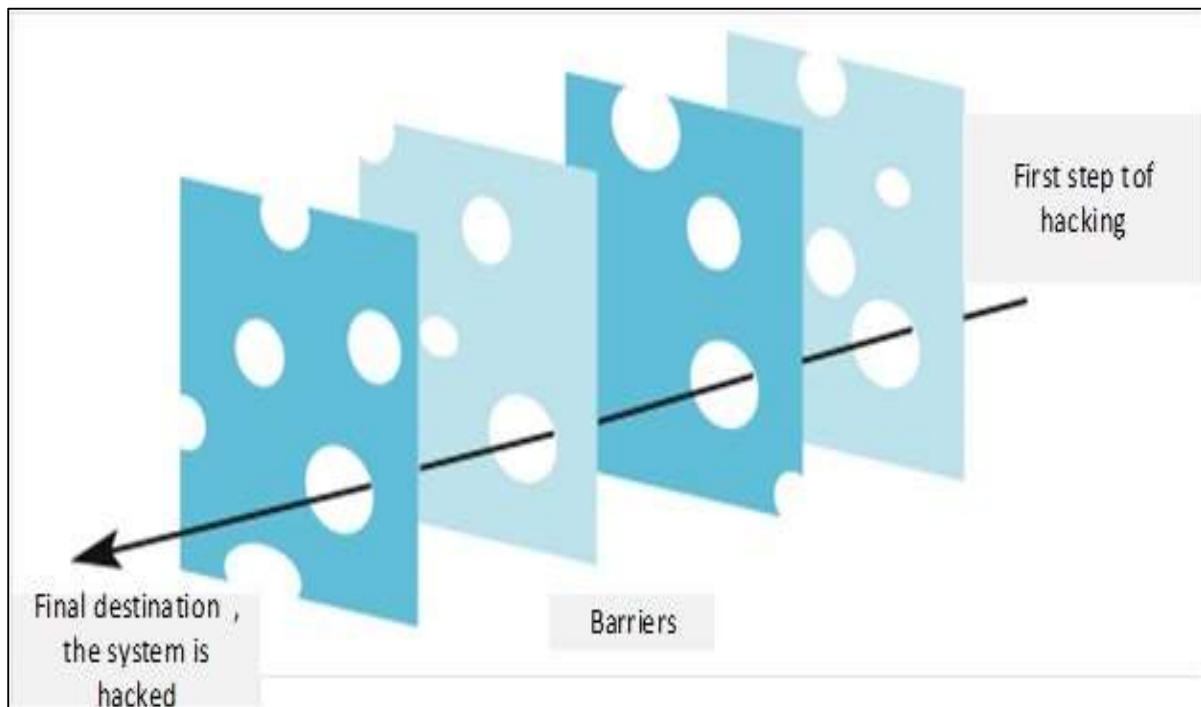
In this chapter, we will discuss about the different terminology used in Computer Security.

- **Unauthorized access** – An unauthorized access is when someone gains access to a server, website, or other sensitive data using someone else's account details.
- **Hacker** – Is a Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.
- **Threat** – Is an action or event that might compromise the security.
- **Vulnerability** – It is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system.
- **Attack** – Is an assault on the system security that is delivered by a person or a machine to a system. It violates security.
- **Antivirus or Antimalware** – Is a software that operates on different OS which is used to prevent from malicious software.
- **Social Engineering** – Is a technique that a hacker uses to stole data by a person for different for purposes by psychological manipulation combined with social scenes.
- **Virus** – It is a malicious software that installs on your computer without your consent for a bad purpose.
- **Firewall** – It is a software or hardware which is used to filter network traffic based on rules.

## 4. Computer Security – Layers

In Computer Security, layers is a well-known practice which was taken from military techniques. The aim of this is to exhaust the attacker when he succeeds to penetrate the first layer of security by finding a hole, then he has to find a hole in the second layer and so on, until he arrives at the destination if he succeeds.

Following is an image which explains about Layer Security.



Let's see the best practices in a Layer type of Security:

- **Computer Application Whitelisting:** The idea is to install just a restricted number of applications in your computers, which are useful as well as are genuine.
- **Computer System Restore Solution:** In case your computer is hacked and your files are damaged, you should have the possibility to again have access to your files. An example is Windows System Restore or Backup.
- **Computer and Network Authentication:** The data that is accessed over the network is best to be provided only to the authorized users. Use usernames and passwords!!!
- **File, Disk and Removable Media Encryption:** Generally a good practice is to encrypt hard disks or removable devices, the idea behind this is in case your laptop or your removable USB is stolen and it is plugged in another machine it cannot be read. A good tool for this is **Truecrypt**.

- **Remote Access Authentication:** Systems which are accessed over the network is best to be provided only to the authorized users. Use usernames and passwords!!!
- **Network Folder Encryption:** Again like the case of Network Authentication, if you have a network storage or a network folder shared, it is good to be encrypted to prevent any unauthorized user who is listening to the network to read the information.
- **Secure Boundary and End-To-End Messaging:** Nowadays email or instant messaging is widely spread and it is the number one tool to communicate. It is better that the communication to be encrypted between the end users, a good tool for this is **PGP Encryption Tool**.

## 5. Computer Security – Securing OS

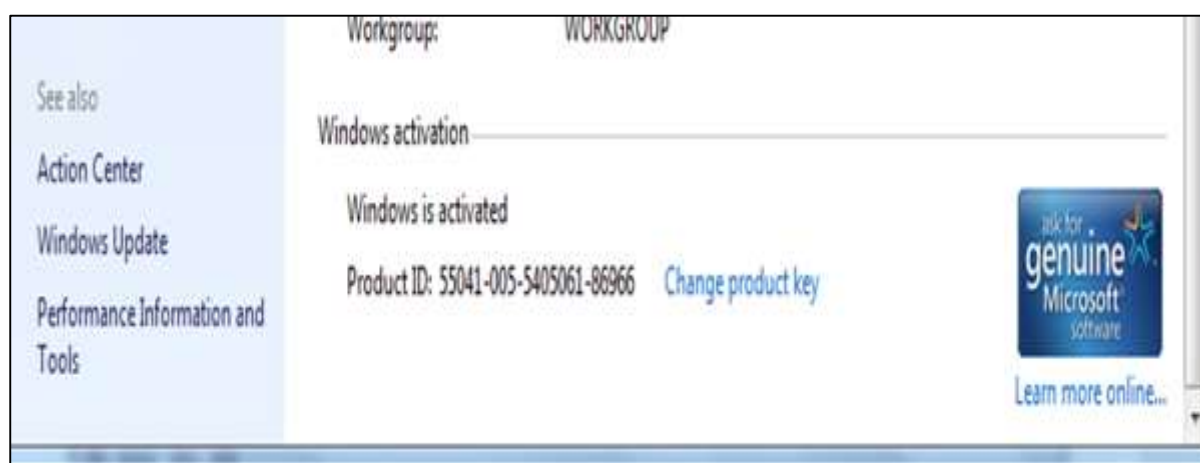
In this section we will treat how to secure or harden (harden is another word used for securing OS) a workstation from the practical point of view and what are the steps to follow. We will treat the **Windows OS** and **Mac OS X** because most of the computers have this two operating systems, but the logic of securing is same for all the other operating systems like **Linux or Android**.

### Guidelines for Windows OS Security

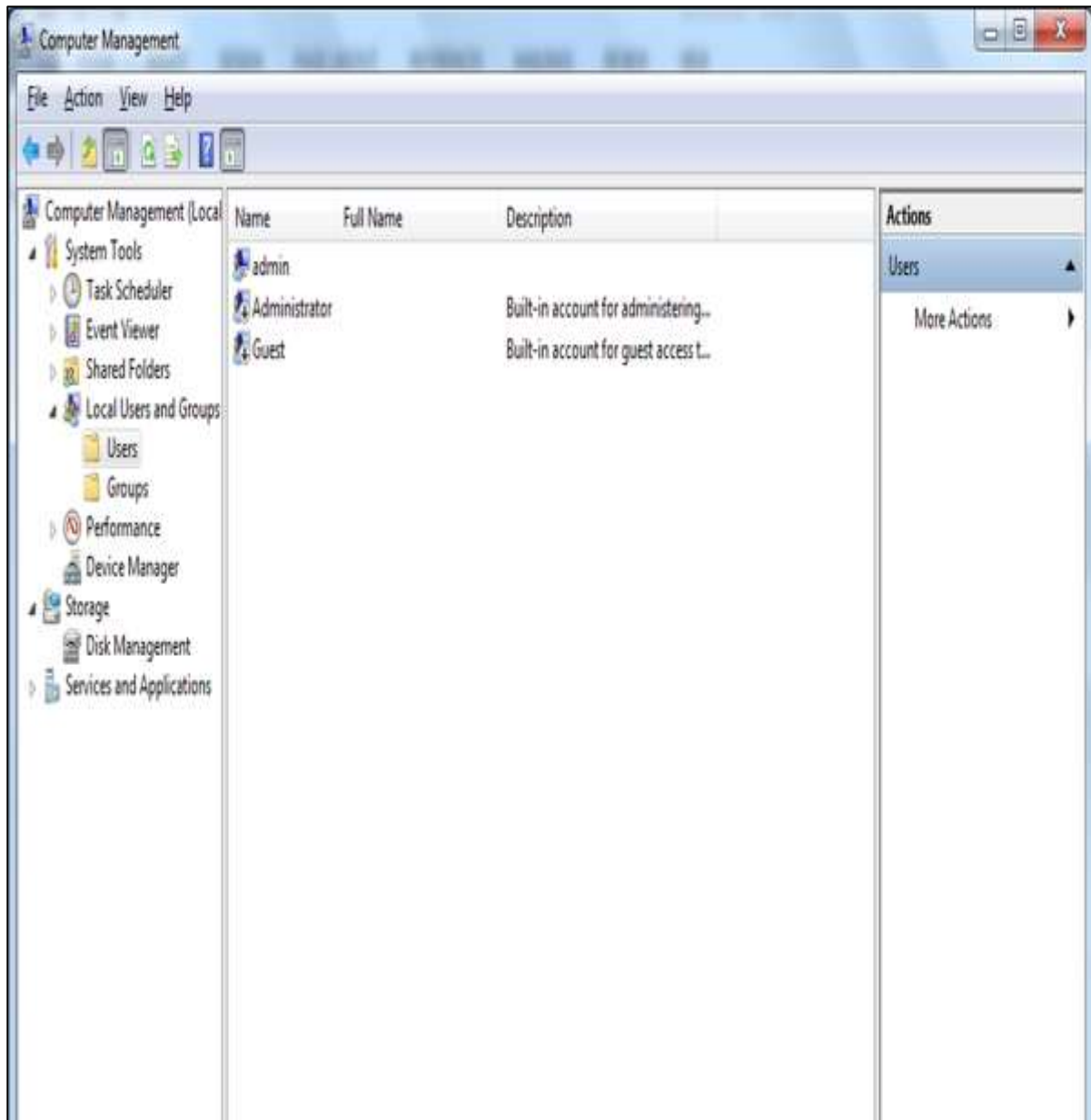
---

Following are the list of guidelines for Windows Operating System Security.

Use the licensed versions of Windows OS, not the cracked or pirated ones and activate them in order to take genuine updates.

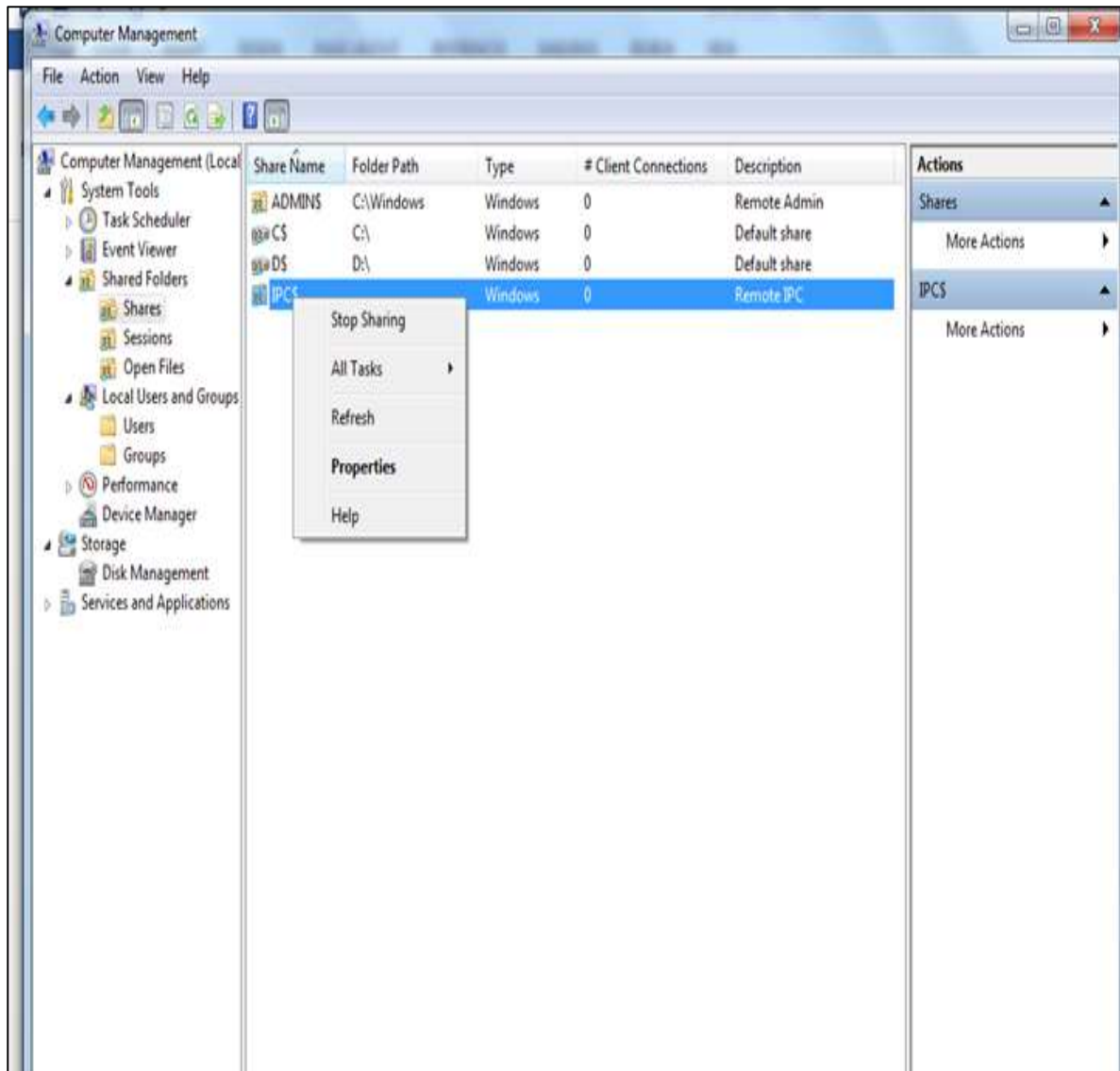


**Disable Unused Users:** To do this, Right Click on Computer – Manage – Local Users and Groups – Users, then disable those users that are not required. In my case, I disabled the Guest and Administrator users and I created a new non-default like Admin.

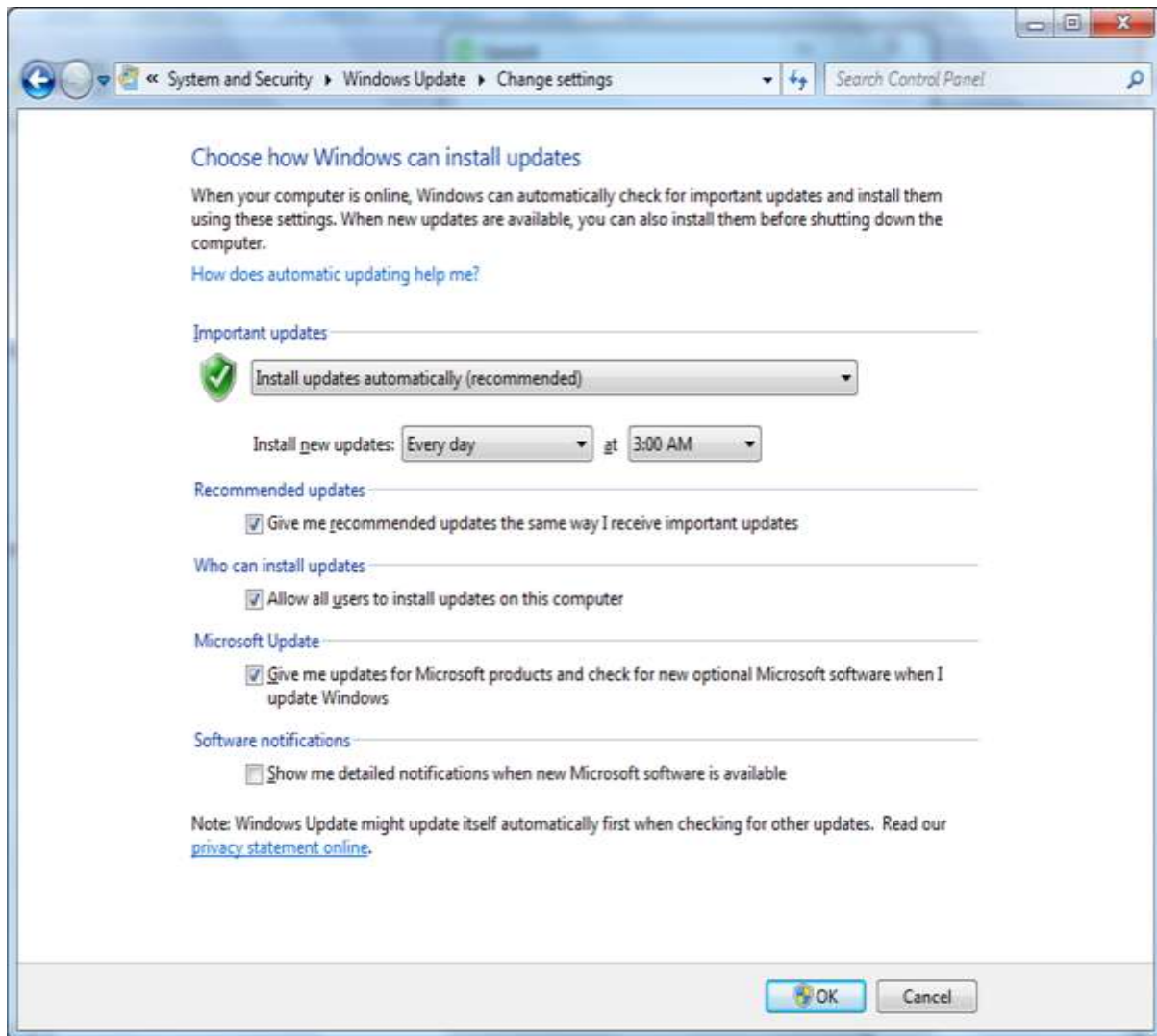


**Disable unused shares:** By default, Windows OS creates shares, please see the following screenshot. You have to disable them and to do this, you follow:

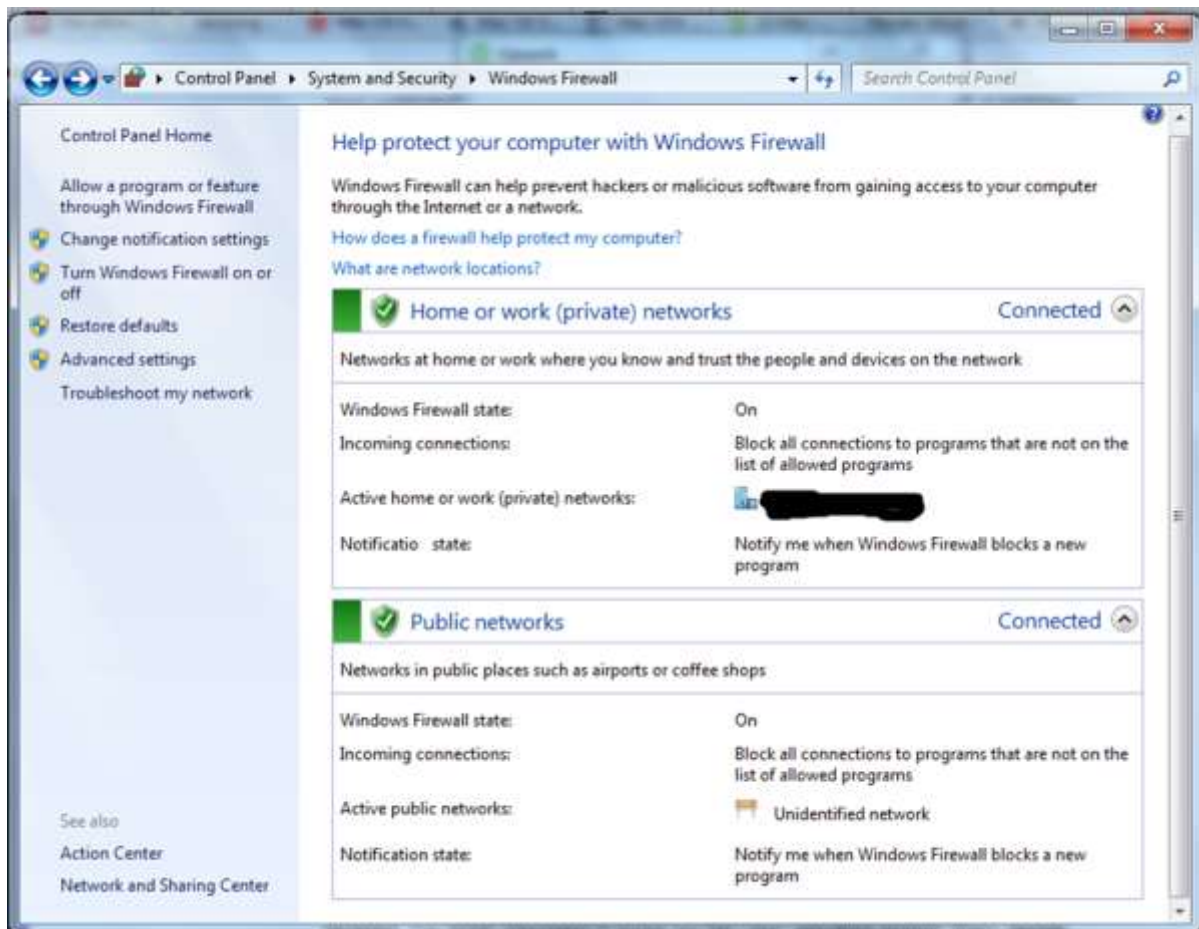
**Right Click on My Computer – Manage – Shared Folders – Right Click Stop Sharing.**



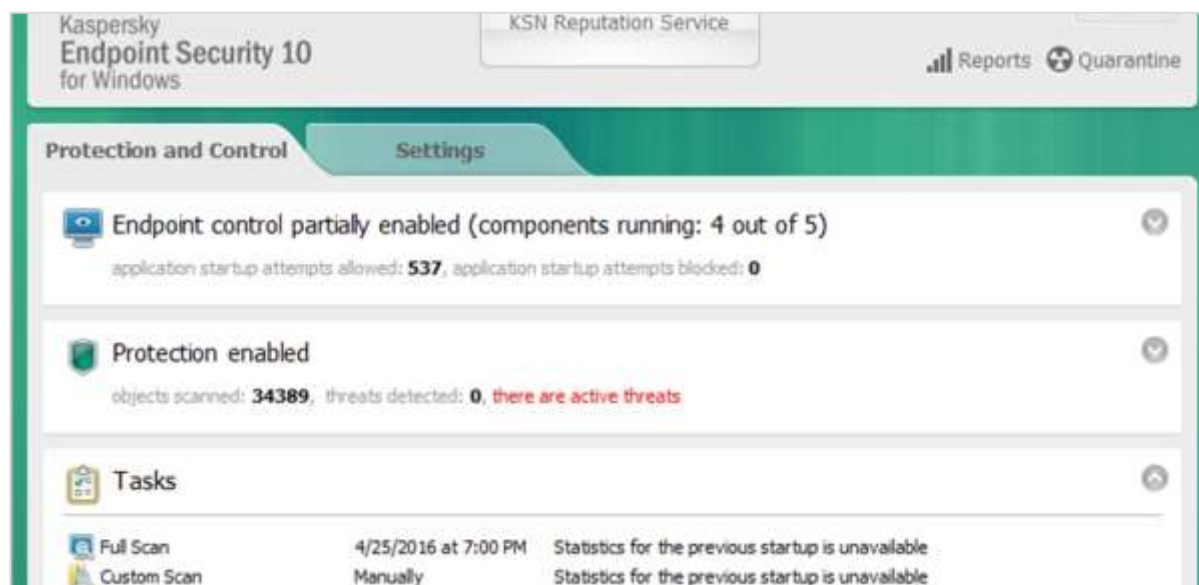
The next step is to take updates regularly for Windows OS. It is recommended to do them automatically and periodically. To set this up, go to **Control Panel – System and Security – Windows Updates –OK.**



Put your Windows System Firewall up, this will block all the unauthorized services that make traffic. To set this up, go to **Control Panel – System and Security –Windows Firewall**.



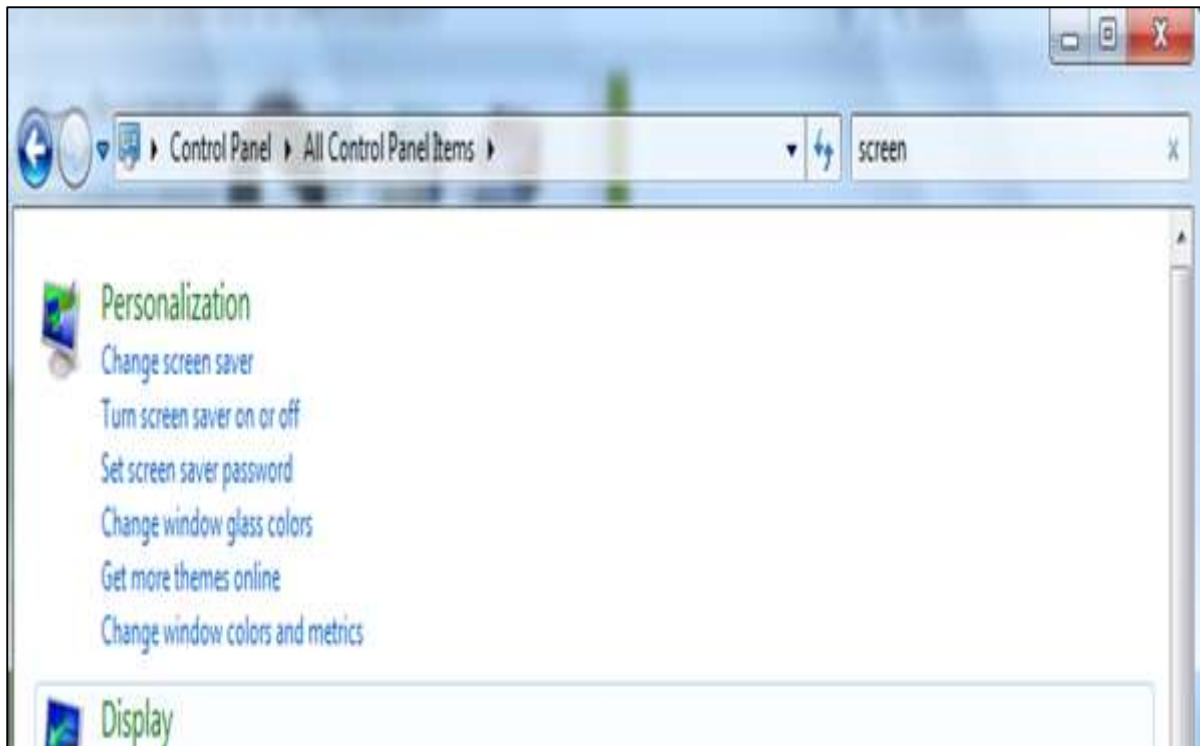
Install a licensed antivirus and take updates, in the coming sections we will cover in detail about antiviruses. It is **strongly recommended** not to download from torrents and install cracked versions.



You should always Configure a password protected Screen Saver. To set this up, please follow this path:

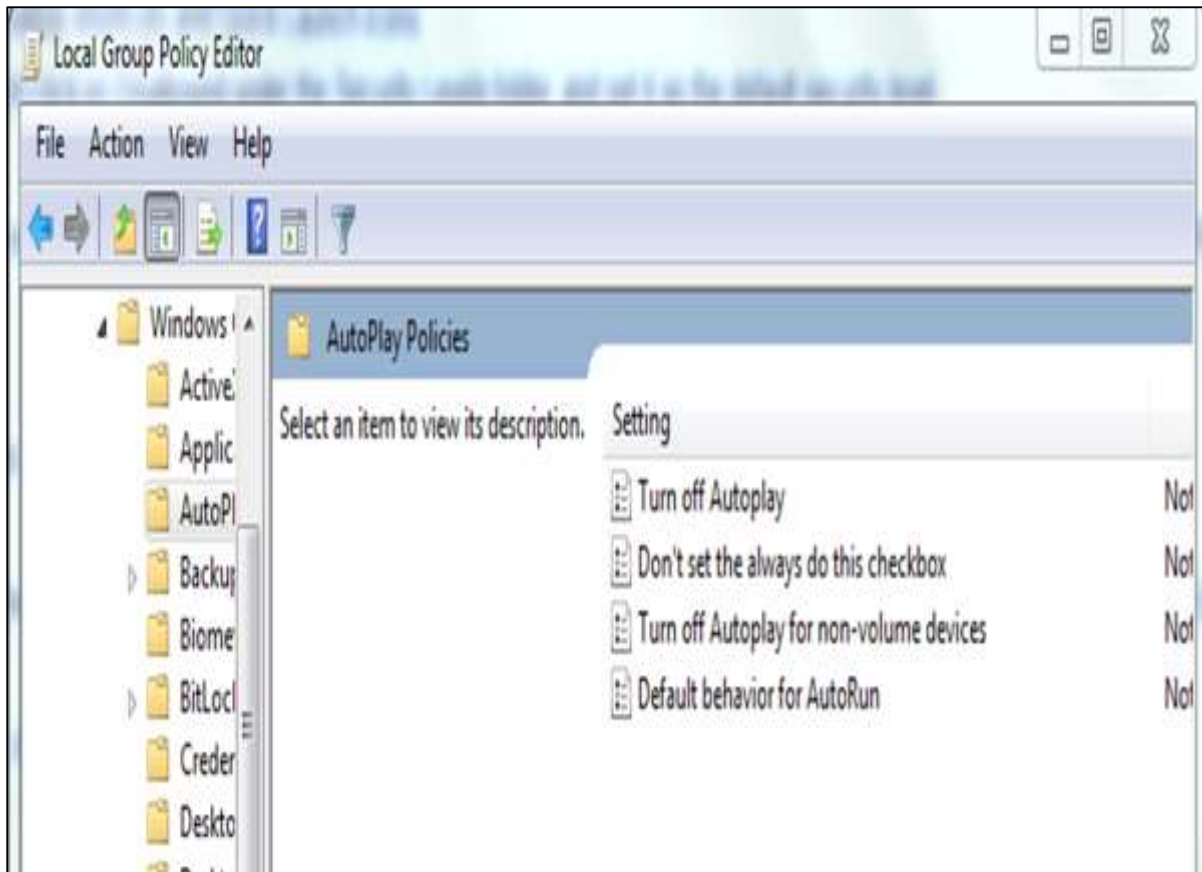
**Control Panel – All Control Panel Items – Personalize – Turn Screen Saver on or off – Check “On resume, display logon Screen”.**



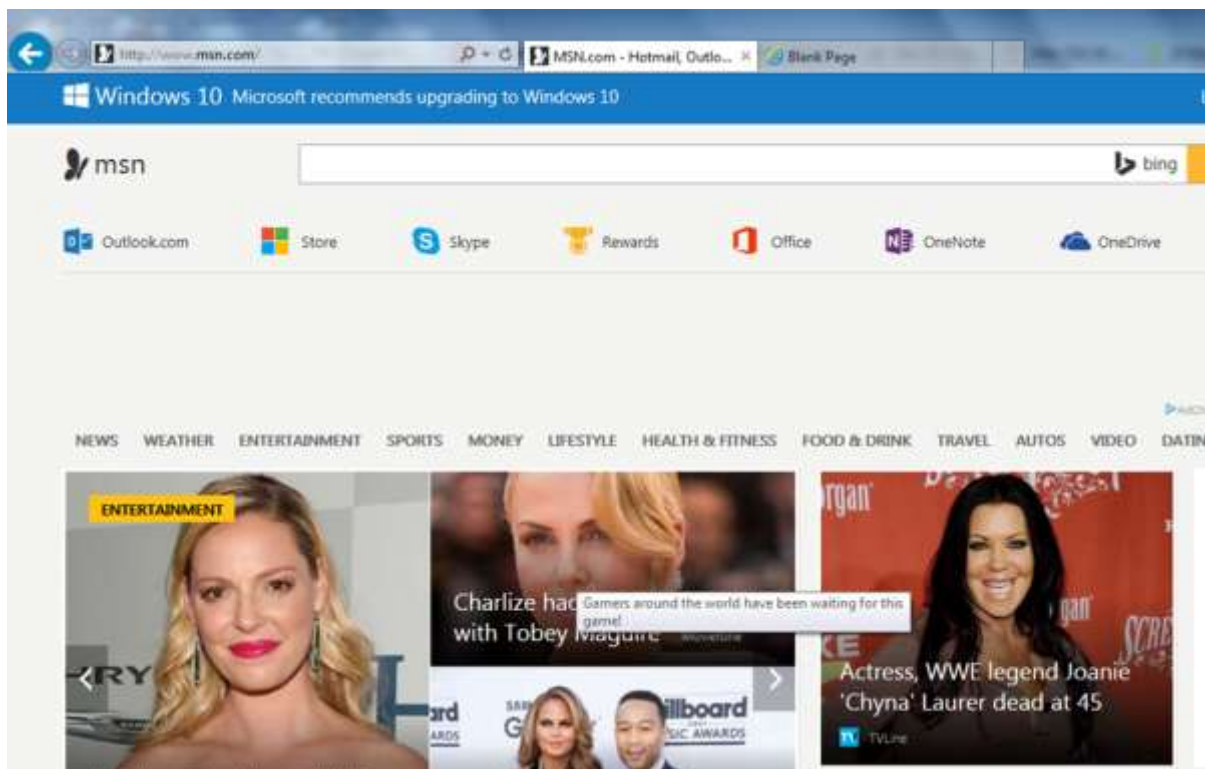


Disable Autoplay for Removable Media. This blocks the viruses to run automatically from removable devices.

To disable it go to – **Start – on Search box type Edit Group Policy –Administrative Templates – Windows Components – Autoplay Policy – Turn off Autoplay – Enable – Ok.**

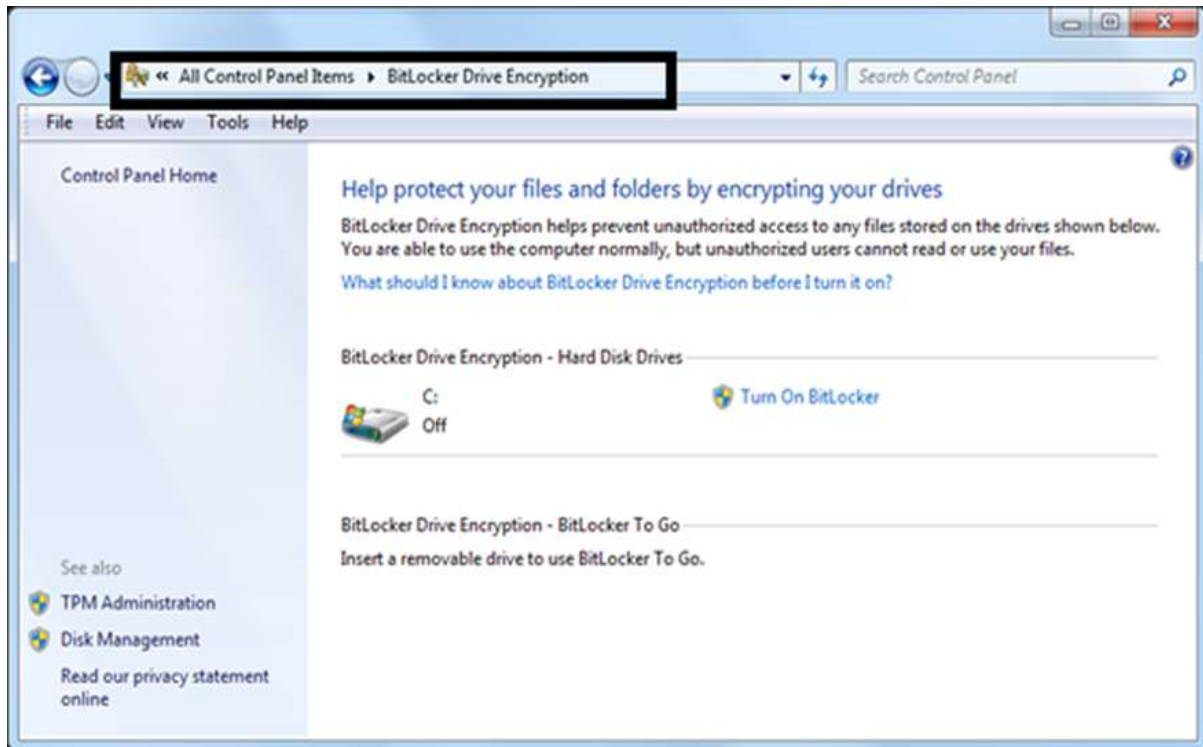


Install only trusted internet explorer browsers like Internet explorer, Chrome or Mozilla Firefox and then update them regularly. Missing the updates can lead to possible hacking.



Enable the BitLocker Drive Encryption to encrypt hard drives, but it is only available in Windows & Ultimate and Upper Versions.

To enable it follow the path: **Start – Control Panel – System and Security – BitLocker Drive Encryption.**



**Set Bios Password:** This option differs based on different computer producers and we need to read manufacturer guidelines, this option secures your computer one layer upper in the OS.

## Guidelines for Mac OS X Security

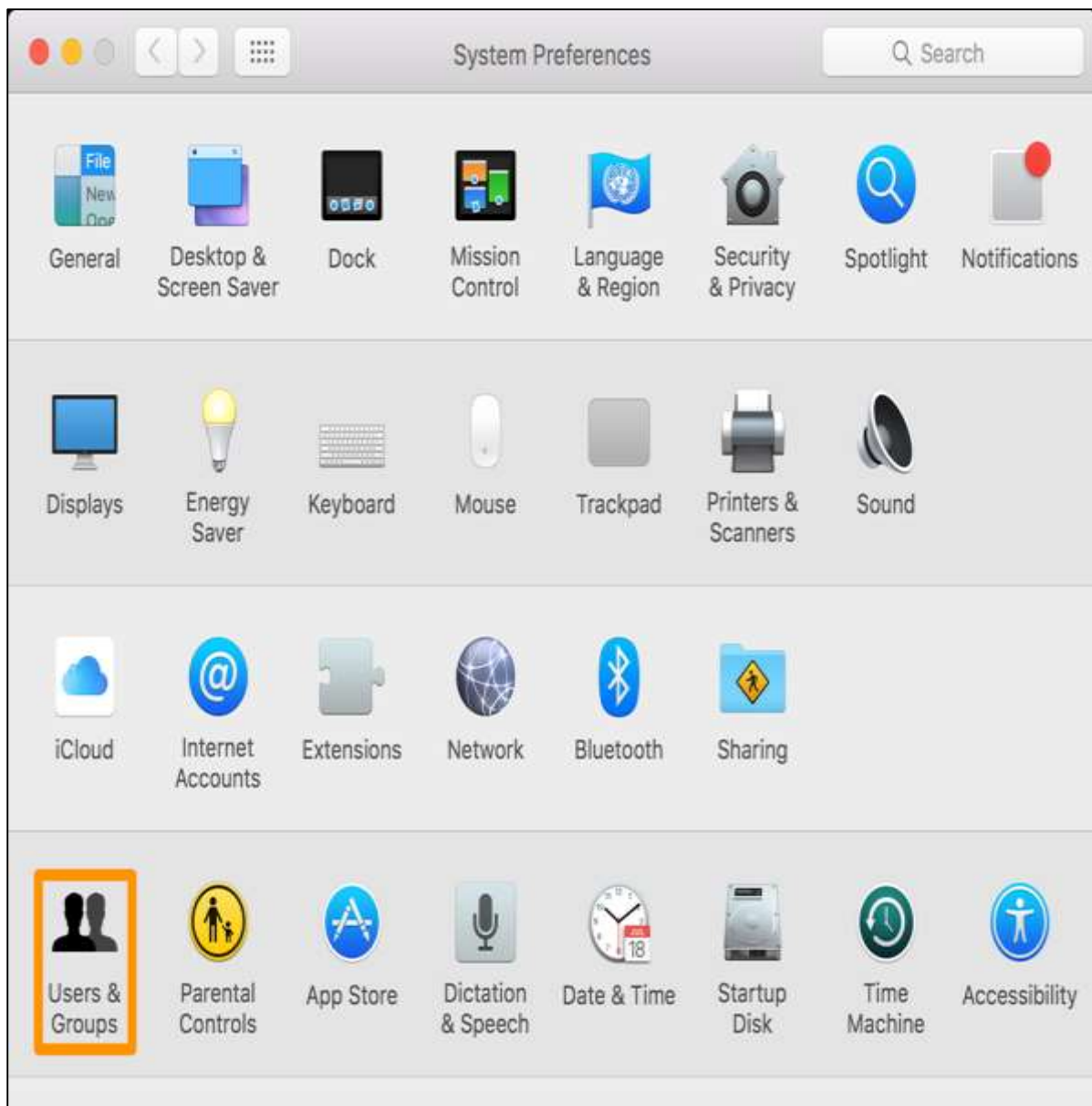
Following are the list of guidelines for Mac OS X Security.

Use licensed versions of Mac OS X and never use the cracked or pirated ones. Once installed, activate them in order to take up the genuine updates.



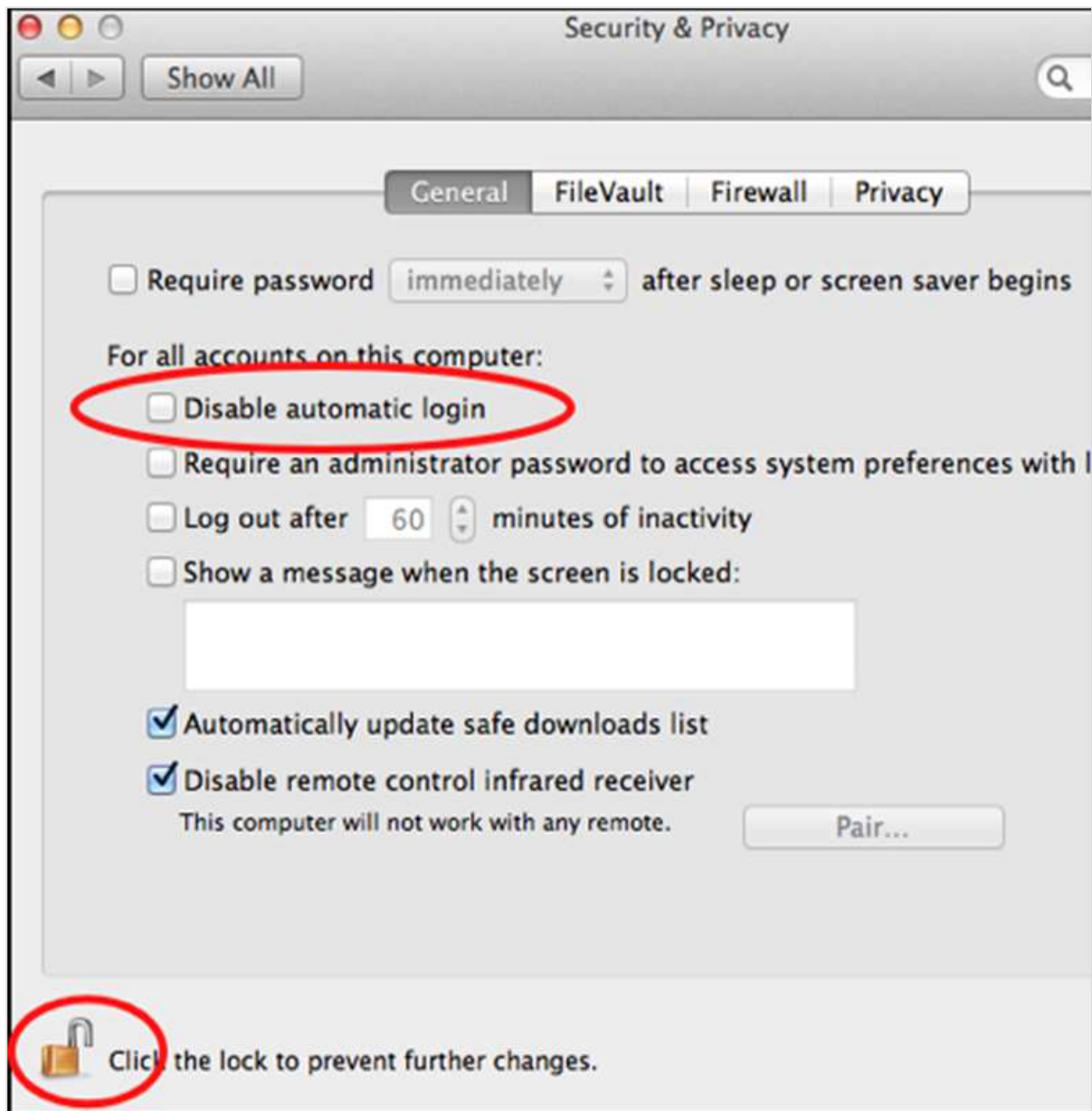
Set password for the root user and create a less privileged user. By default, the root user of the Mac OS X doesn't have a password, so you have to put one and then create a user with less privilege for daily usage.

To set it up follow: **Apple menu – System Preferences – Click Users & Groups**



**Disable Auto Logon:** By default, the Mac OS X is configured to automatically logon the first administrative user that is created. Also it displays all valid usernames in the login windows.

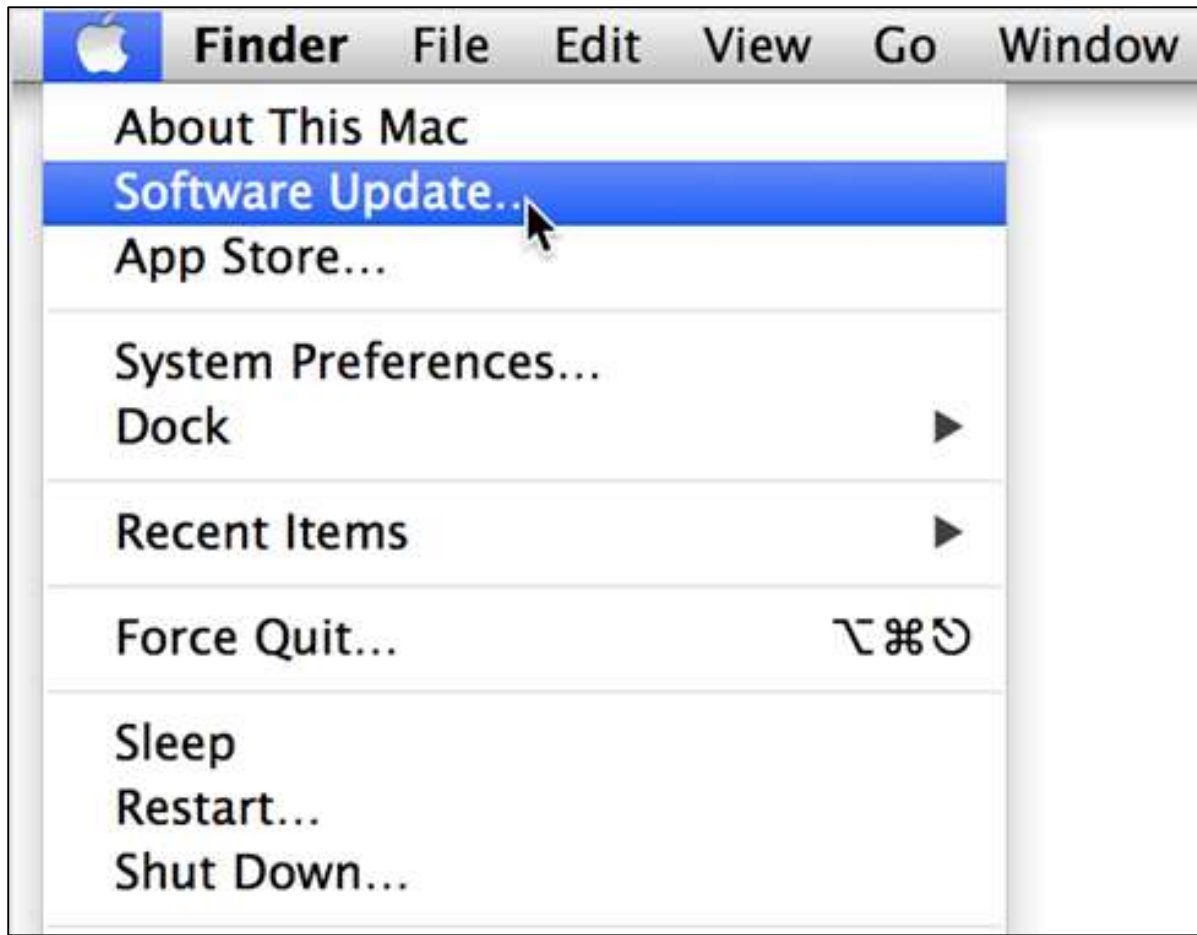
To disable this, you have to: **Open System Preferences – Accounts – User – Uncheck the Log in automatically – Click on Login Options (tab) – Set “Display Login Windows as” = Name and Password.**



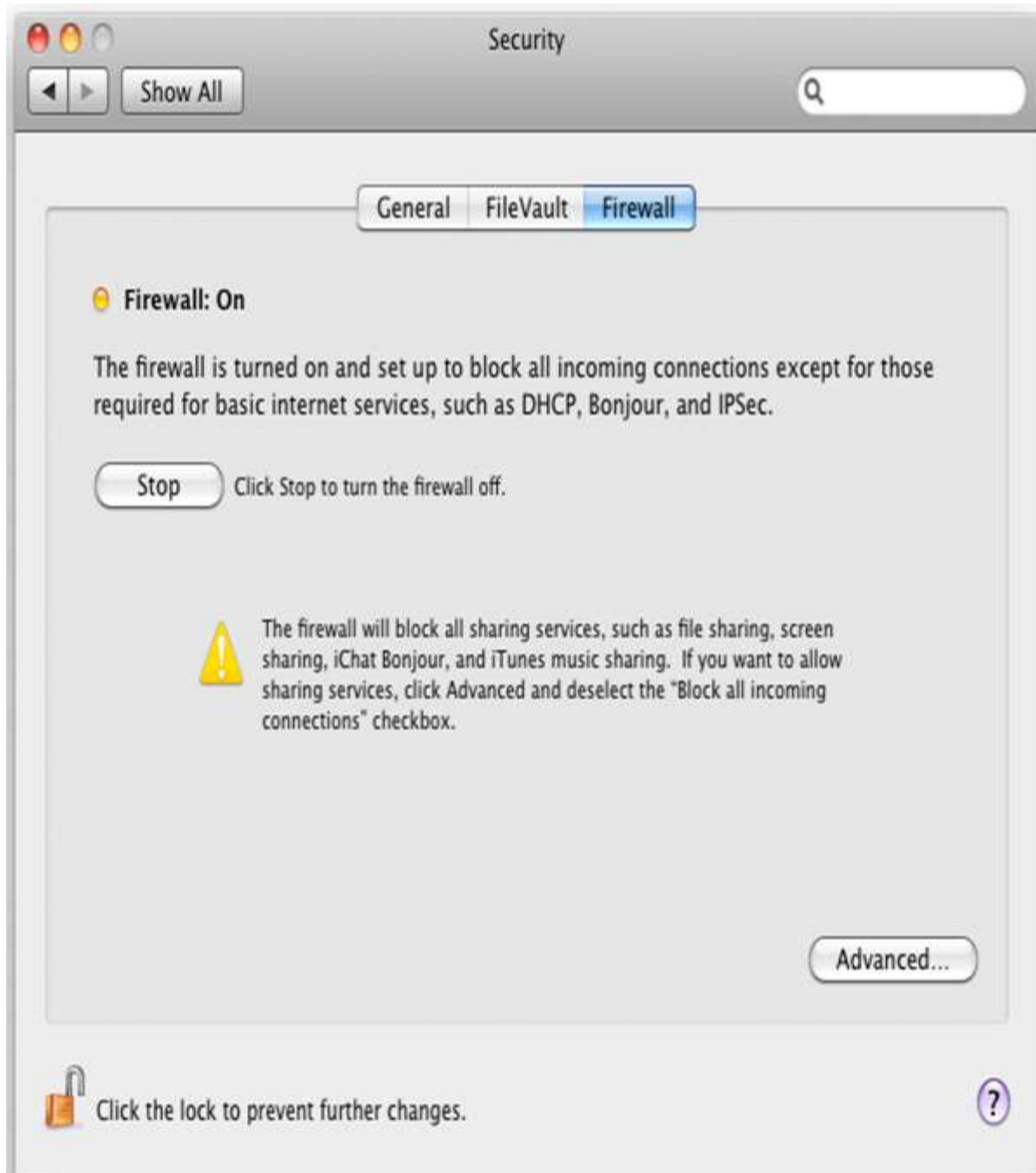
**Update Mac OS X:** In order to secure our systems, we need to take our updates and patches of Mac OS X.

To do so we follow this path: **Click on System Preferences –Software Update – Change the default “weekly” to “daily” – Quit System Preferences.**

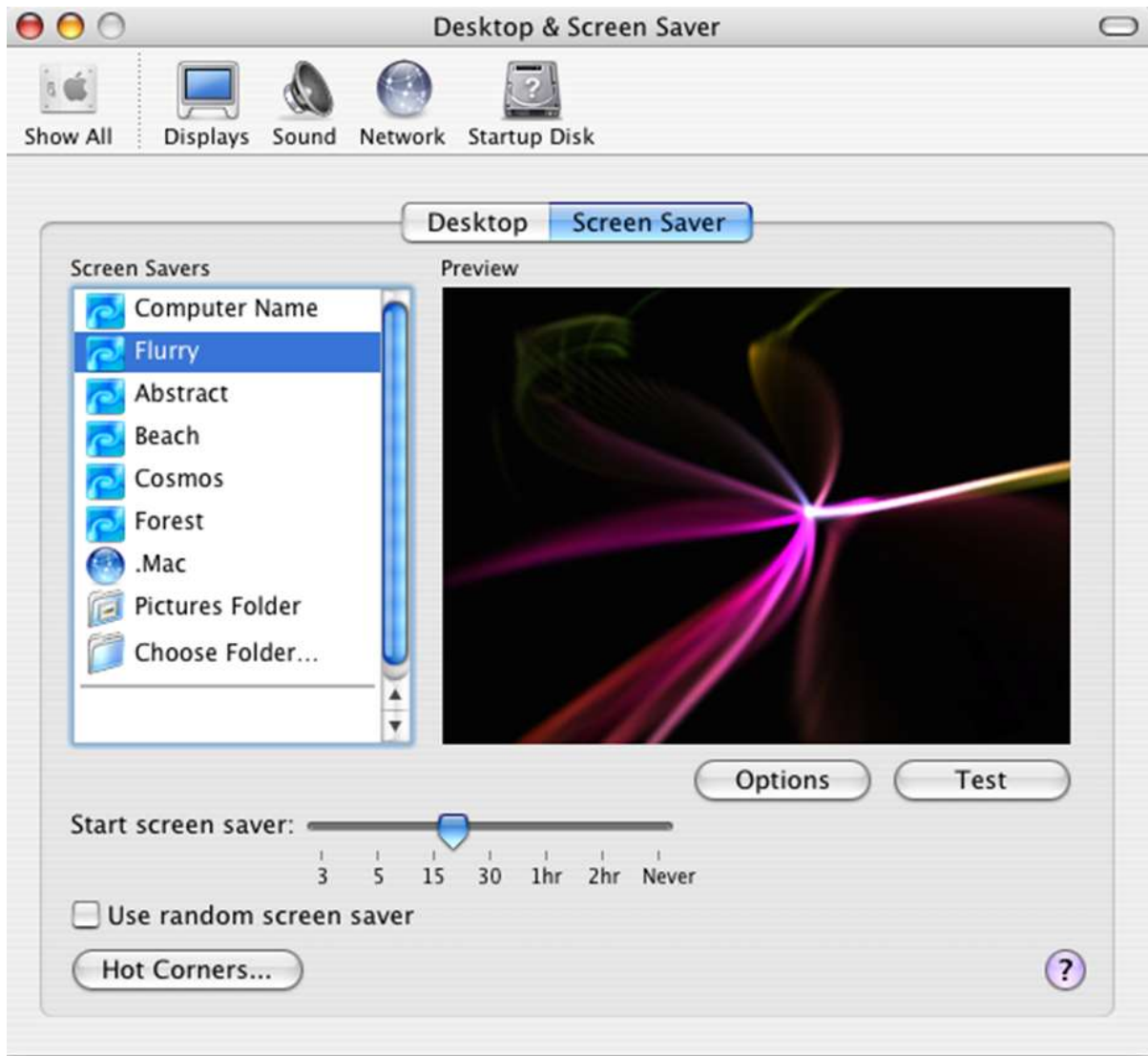
You better do it weekly because it will not overload your networks, in case you have a large network.



Put your Mac OS X system firewall up. The go to **System Preferences – Sharing – Firewall – Click on Start.**



**Configure Screen saver password protected:** To set this up, follow this path – **System Preferences – Screen Effect – Activation – Set "Time until screen effect starts" = 5 Minutes – Set "Password to use when waking the screen effect" = use my user-account password.** It is recommended to be less than 5 minutes.



**Put Open Firmware password:** Double click the application icon to open it. Click on the "Change" button to modify the security settings. If you are enabling the security features, enter a password into the – **Password and Verify boxes**. Click OK. Enter your System Administrator Account.



**Encrypt folders:** Mac OS X has FileVault, which encrypts information in your home folder. You can see the FileVault in the following screenshot.

Click **Apple Menu – System Preferences – Security & Privacy – FileVault – Click the lock Icon to unlock it, then enter an administrator name and password.**

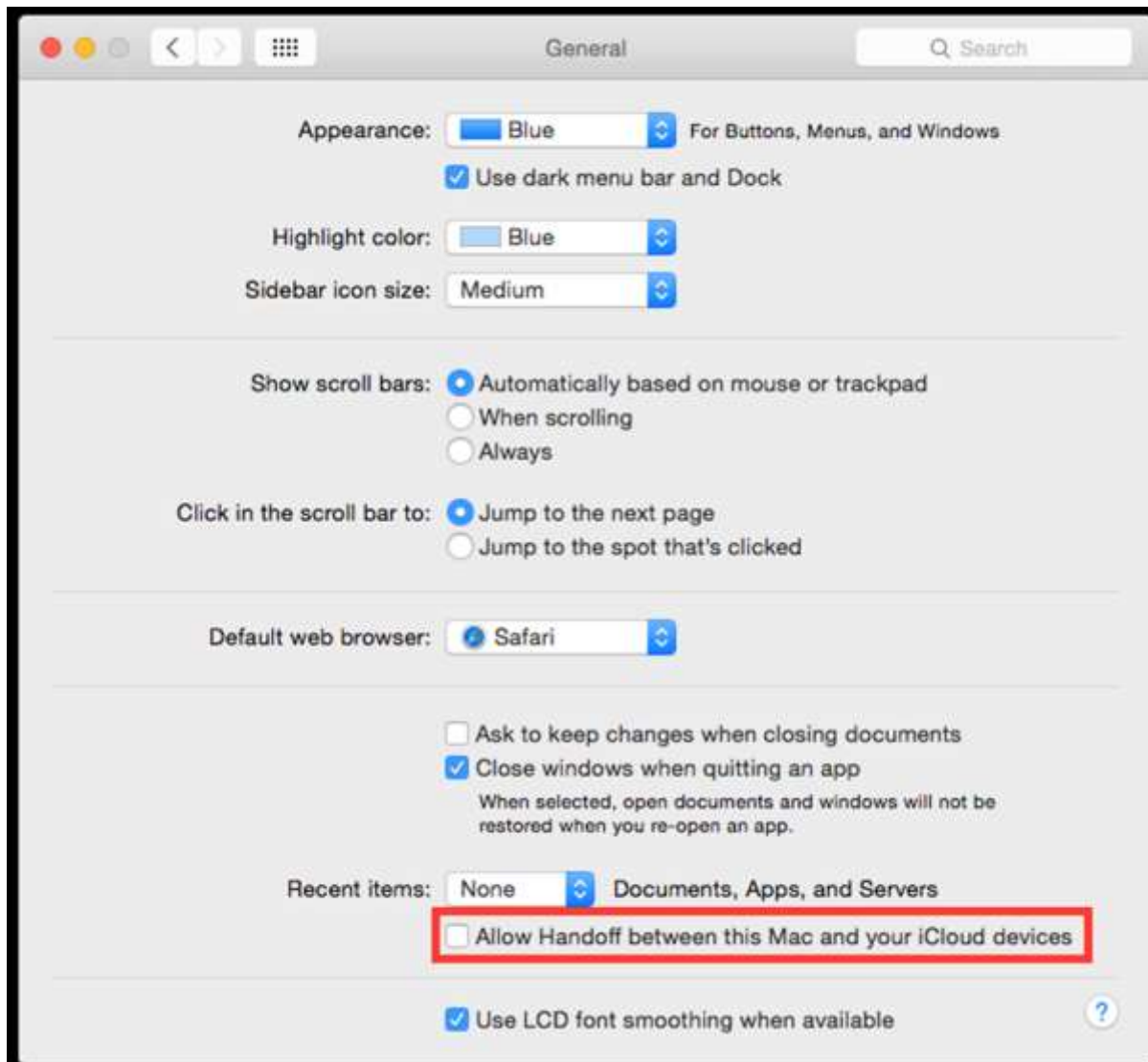


Then you will have to **Turn On FileVault**.



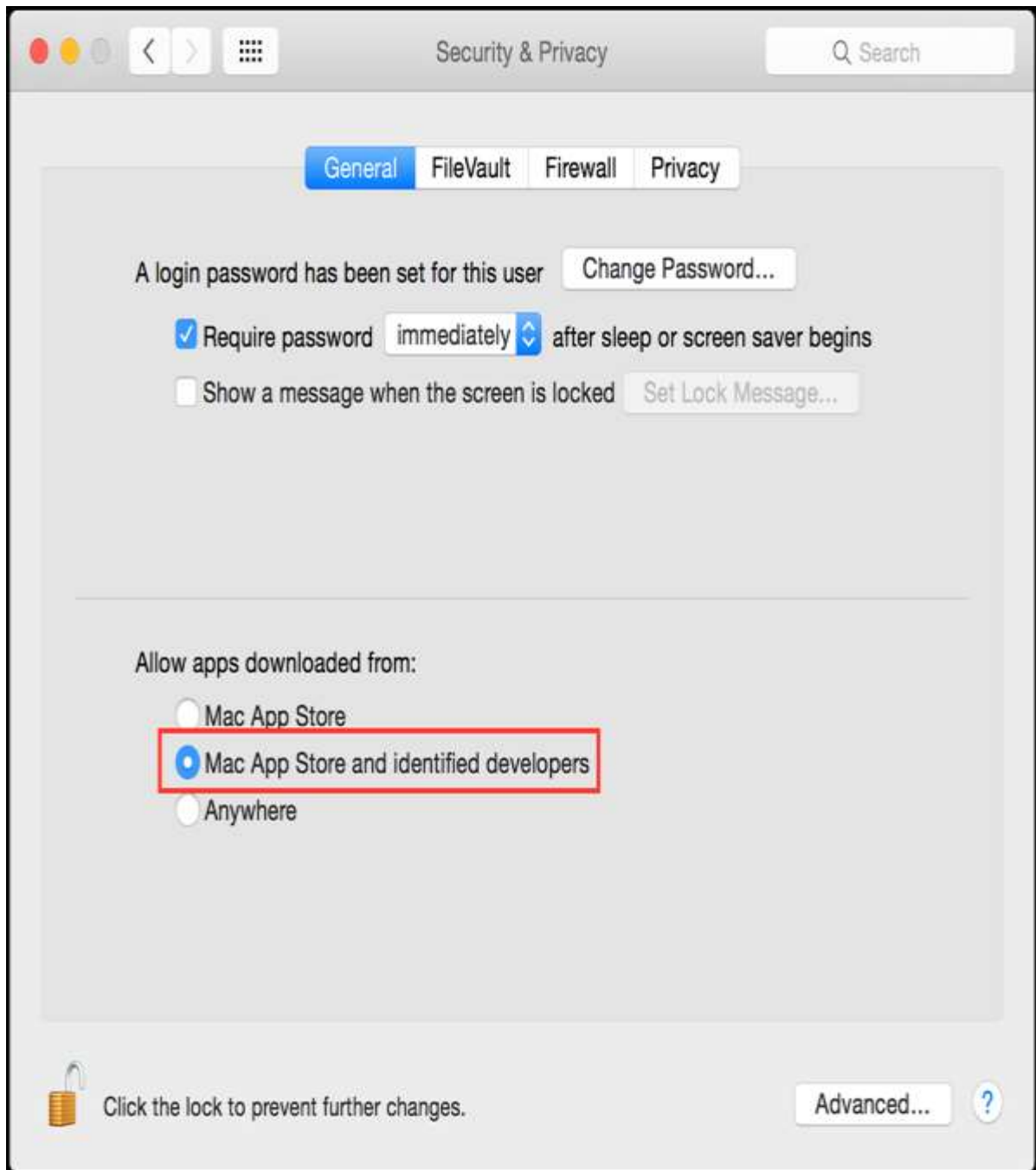
**Disable Handoff:** Handoff is a feature to keep your work in sync, but it needs to send some data to Apple to work. It is suggested to disable it.

To do so: **Click System Preferences – General – Uncheck "Allow Handoff between this Mac and your iCloud devices"**.



**Allow only signed Apps:** To reduce the surface of attack, it is suggested not to run untrusted code not signed with a proper key.

To allow only apps signed by an authorized developer, you should follow the path – **System Preferences – Security & Privacy – General – Set “Allow apps download from” to “Mac App Store and identified developers”**.



## 6. Computer Security – Antiviruses

In the previous chapter, we saw how to secure our computers and one of the points was installing and updating antivirus software. Without this software there is a high chance that your systems and networks will be hit and will suffer hacking attacks and also can be affected by the various viruses.

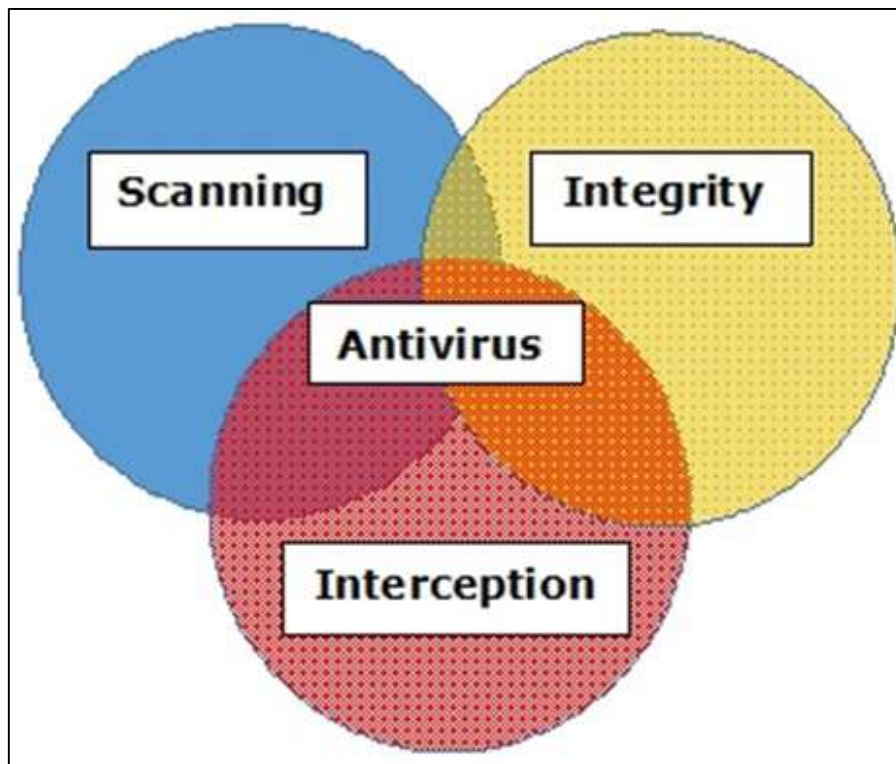
It is important that the antivirus scan engine and virus signatures to be updated regularly, we do this because if your system is hit by the latest malware it will be detected.

### Basic Functions of Antivirus Engines

All antivirus engines have three components to function accordingly. It is important to have a look at these functions because it will help us for better manual cleaning of viruses in case we need.

- **Scanning:** When a new virus is detected in the cyberspace, antivirus producers start writing programs (updates) that scans for similar signature strings.
- **Integrity Checking:** This method generally checks for manipulated files in OS from the viruses.
- **Interception:** This method is used basically to detect Trojans and it checks the request made by the operating system for network access.

The following image shows the schema for an antivirus engines functionality.




## Online Virus Testing

If the system administrator does not have an antivirus installed or suspects a file that is infected. They would recommend to use the online testing antivirus engine which (according to me) is one of the best – <https://virustotal.com/>.

Q. Why this option?

Ans. It is a free and independent service. It uses multiple antivirus engines (41 anti-virus engines), so its result will be showing for all the 41 engines. It updates the engines in real-time.

For further clarity, please see the following screenshot, wherein I uploaded a file with virus and the result is **33/41 (Detection Ratio)**, which means that it has virus and did not pass the class, so it should not be opened.



SHA256: cf0b683e4df6425cc7c66cd03148590a84b4088082b93ed89306e9f844dfa6c9

Detection ratio: **33 / 41**

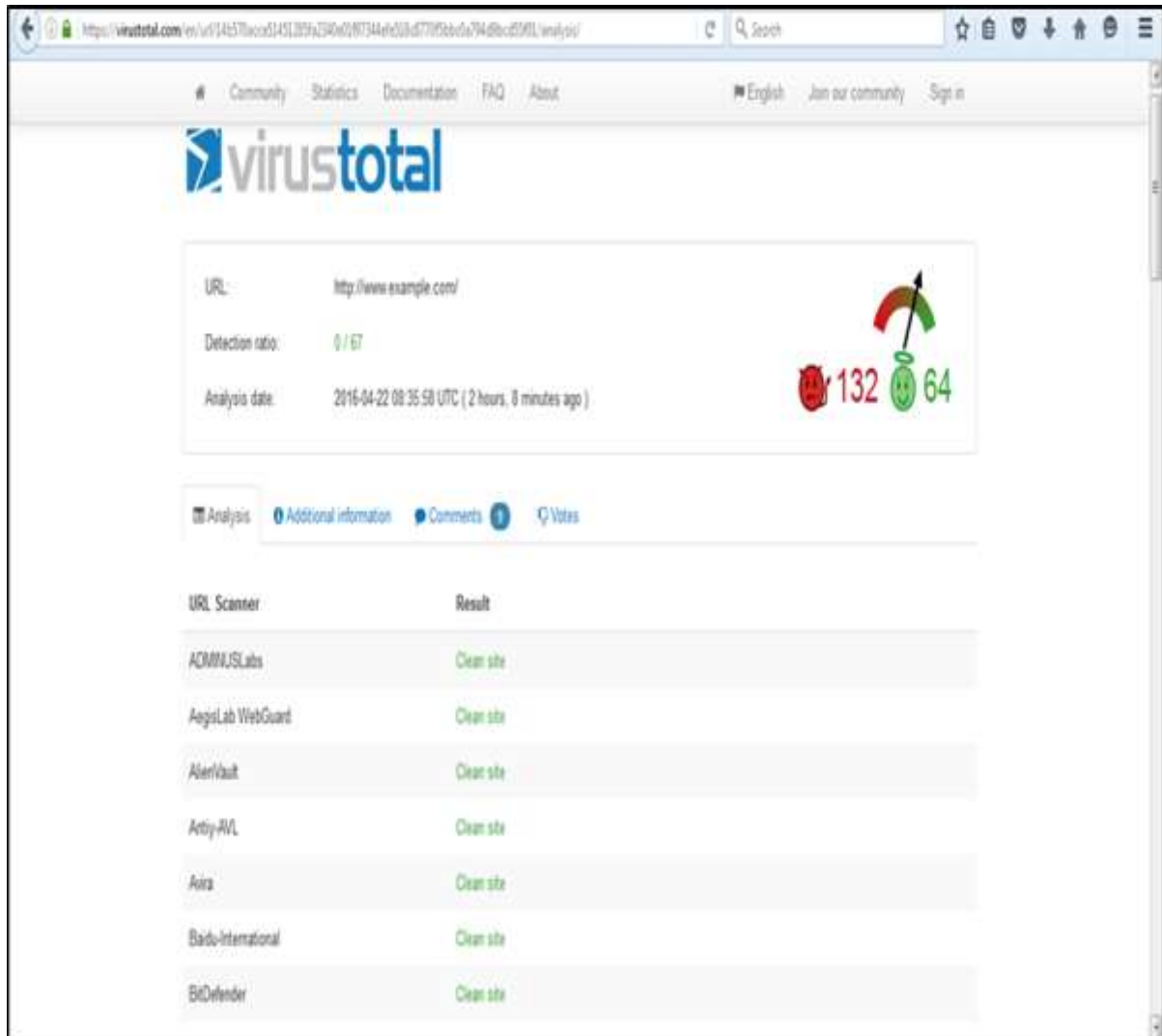
Analysis date: 2009-10-01 18:37:05 UTC ( 6 years, 6 months ago )

Analysis Relationships Additional information Comments Votes

Antivirus	Result	Update
AVG	CodeRed	20091001
AhnLab-V3	BinImage/Code_Red	20091001
AntiVir	Worm/CodeRed	20091001
Antiy-AVL	Worm/Win32.CodeRed	20091001
Authentium	Malware!2469	20091001
Avast	Win32.CodeRed	20090930
BitDefender	Win32.IISVorm.CodeRed.A	20091001

A good feature of this site is URL checking, before entering to a website you can enter the URL and it checks for you if the site has infection and can harm you.

I did a test with a URL and it came out to be clean and that too 100%, so I can visit it without my computer being infected.



## Free Antivirus Software

As this tutorial is hands-on practice, I will show you where to get free antiviruses and where to download Web in case you don't have enough budget.

The free versions of anti-viruses have nearly identical malware detection scores to the paid versions produced by the same company, but the commercial antivirus makes a small difference in the performance of security and in our case we are system administrators and we want maximum protection in the work environment.

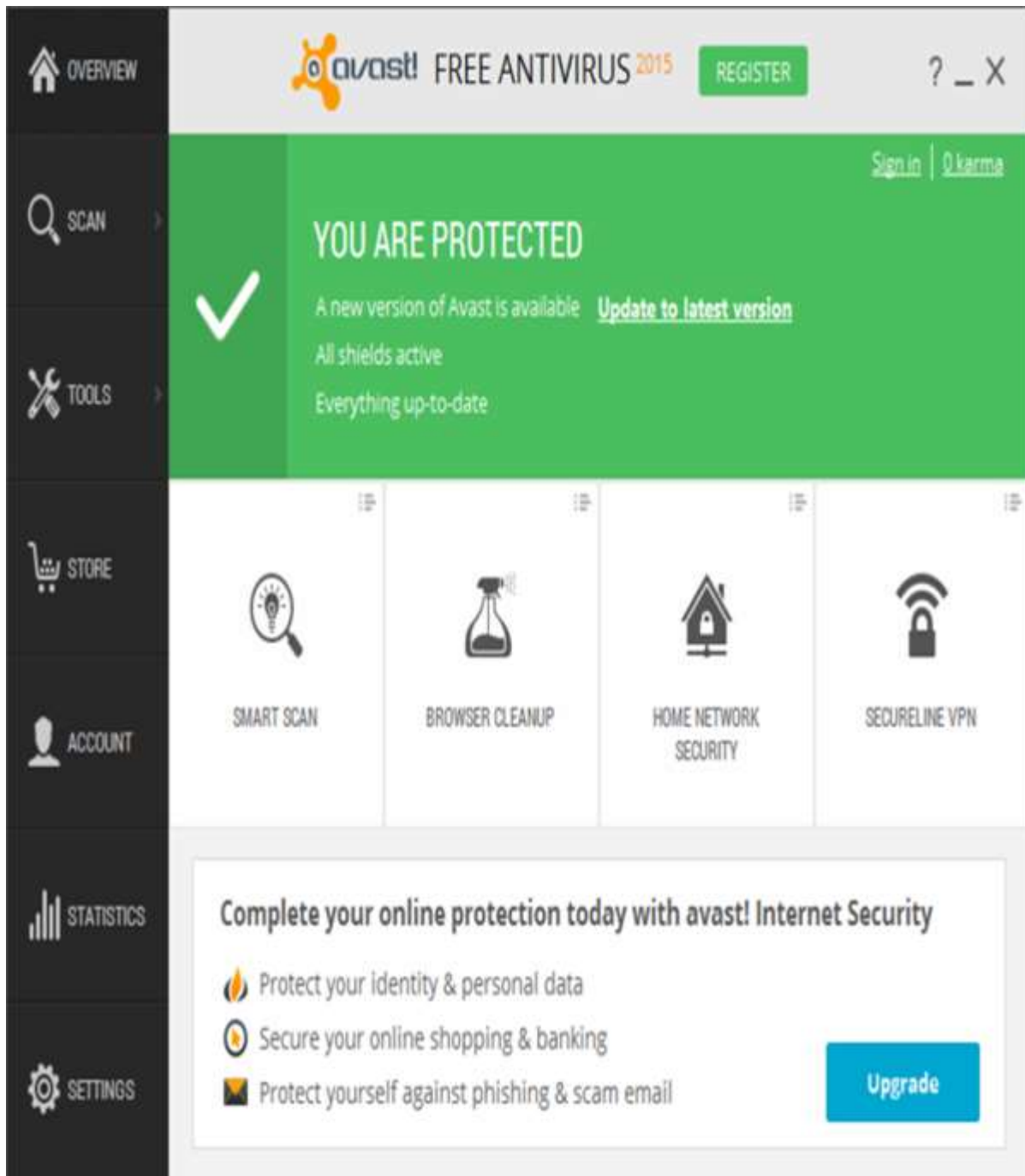
From the PCMagazine (<http://www.pcmag.com>) you can get a review which are the best top rated free antiviruses at the moment. In the following URL you can check by yourself <http://www.pcmag.com/article2/0,2817,2388652,00.asp>

Let us understand in detail about some of these antivirus software:

## Avast Antivirus

This antivirus has good scores in malware blocking and anti-phishing test scans, it can be downloaded from <https://www.avast.com/en-eu/index>

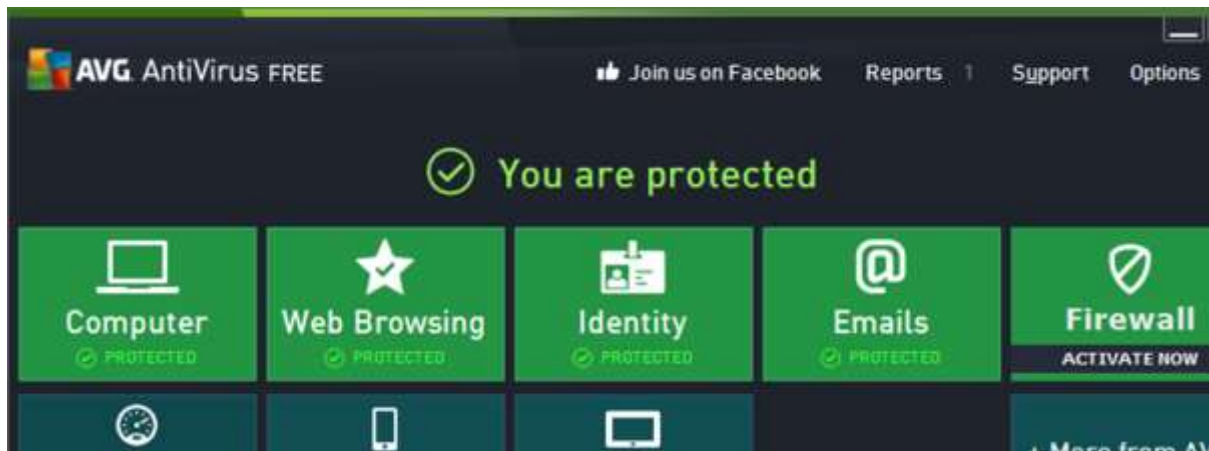
For server installation you need a commercial version.



## AVG Antivirus

---

It can be downloaded from <http://www.avg.com/us-en/free-antivirus-download>. For server installation you need to purchase the commercial version.



## Panda Antivirus 2016

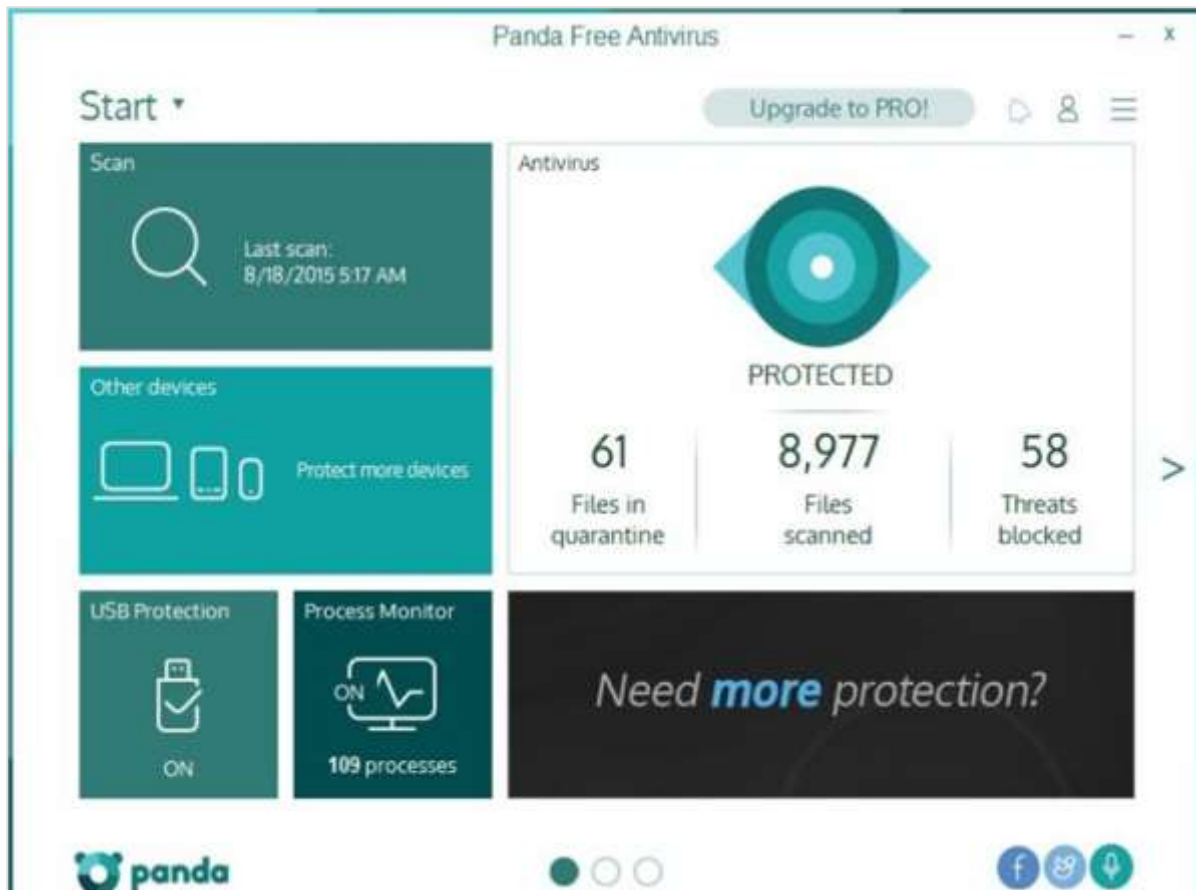
---

It can be downloaded from <http://www.pandasecurity.com/usa/homeusers/downloads/>  
It has the following good features:

- Rescue Disk
- USB protection
- Process Monitor

For server installation you will need to purchase the commercial version.





## Bitdefender Antivirus

It can be downloaded from <http://www.bitdefender.com/solutions/free.html>. A good feature in this antivirus is that it can work entirely in the background. No configuration setting. For server installation you need to buy the commercial version.

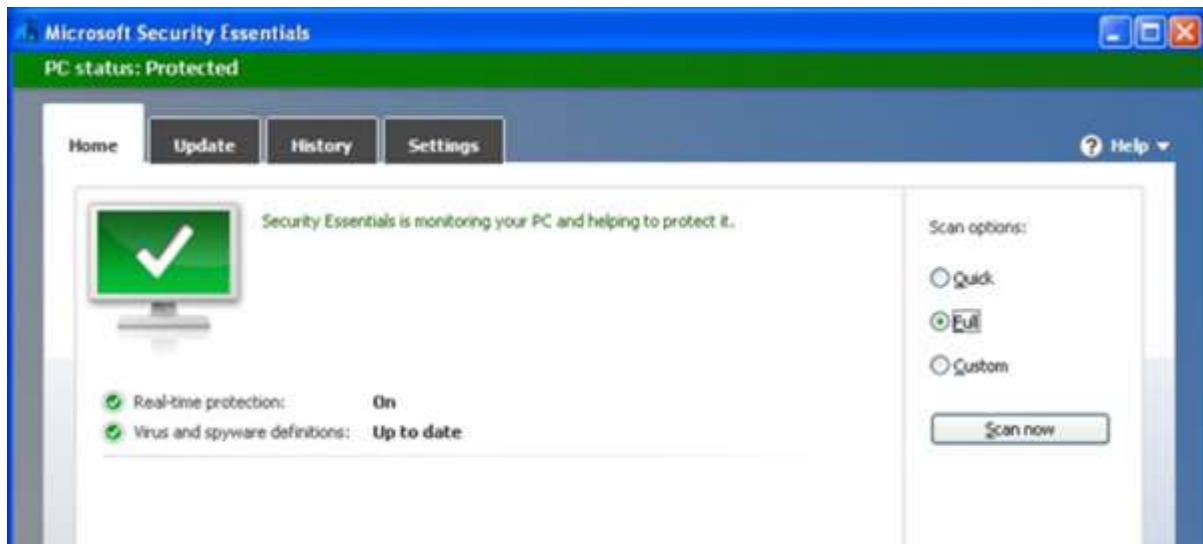


## Microsoft Security Essentials

---

Even though it is not among the top-most free antiviruses owing to the Microsoft brand, it is worth a mention that Microsoft itself offers you a free antivirus which is called as Microsoft Security Essentials.

It can be downloaded from <http://windows.microsoft.com/en-us/windows/security-essentials-download>



## Commercial Antivirus

---

I should mention that all the producers of free antiviruses offers their commercial versions too. Based on PC magazine, the best commercial antiviruses are:

- Kaspersky Anti-Virus
- Bitdefender Antivirus Plus 2016
- McAfee AntiVirus Plus (2016)
- Webroot SecureAnywhere Antivirus (2015)

Please see the following link to check by yourself:

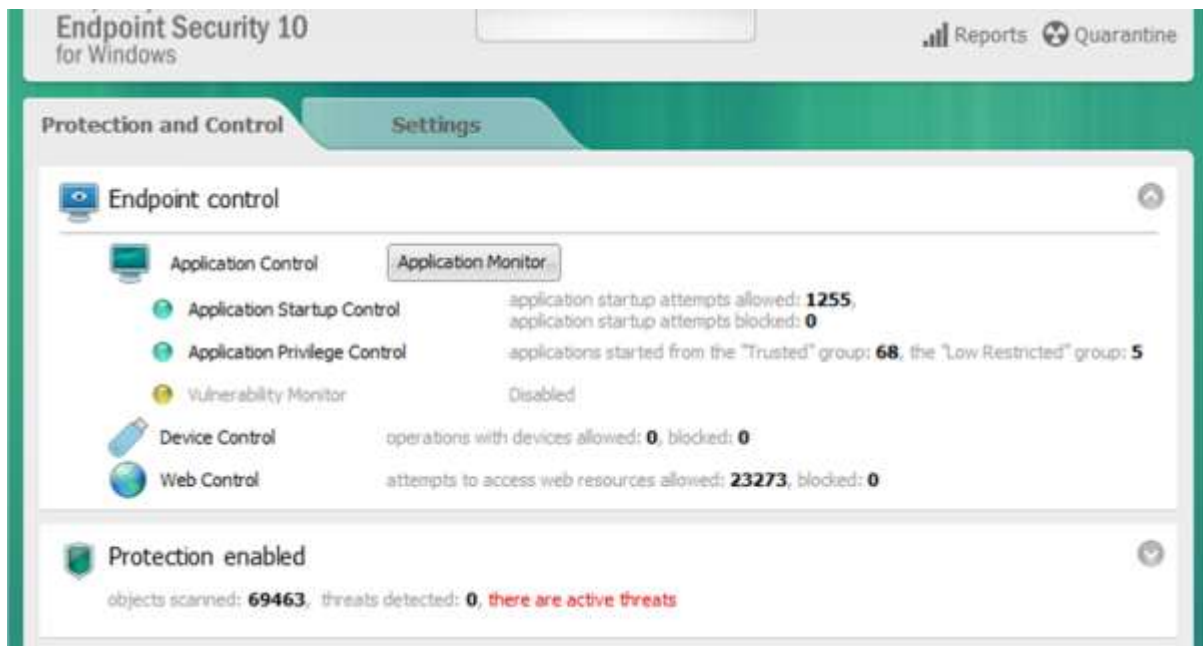
<http://www.pcmag.com/article2/0,2817,2372364,00.asp>

## Kaspersky Antivirus

---

It can be downloaded as a free trial from <http://www.kaspersky.com/free-trials/anti-virus>

It has an excellent score in anti-phishing. It also gives a useful bonus in security tools like credit card protection in your computers.

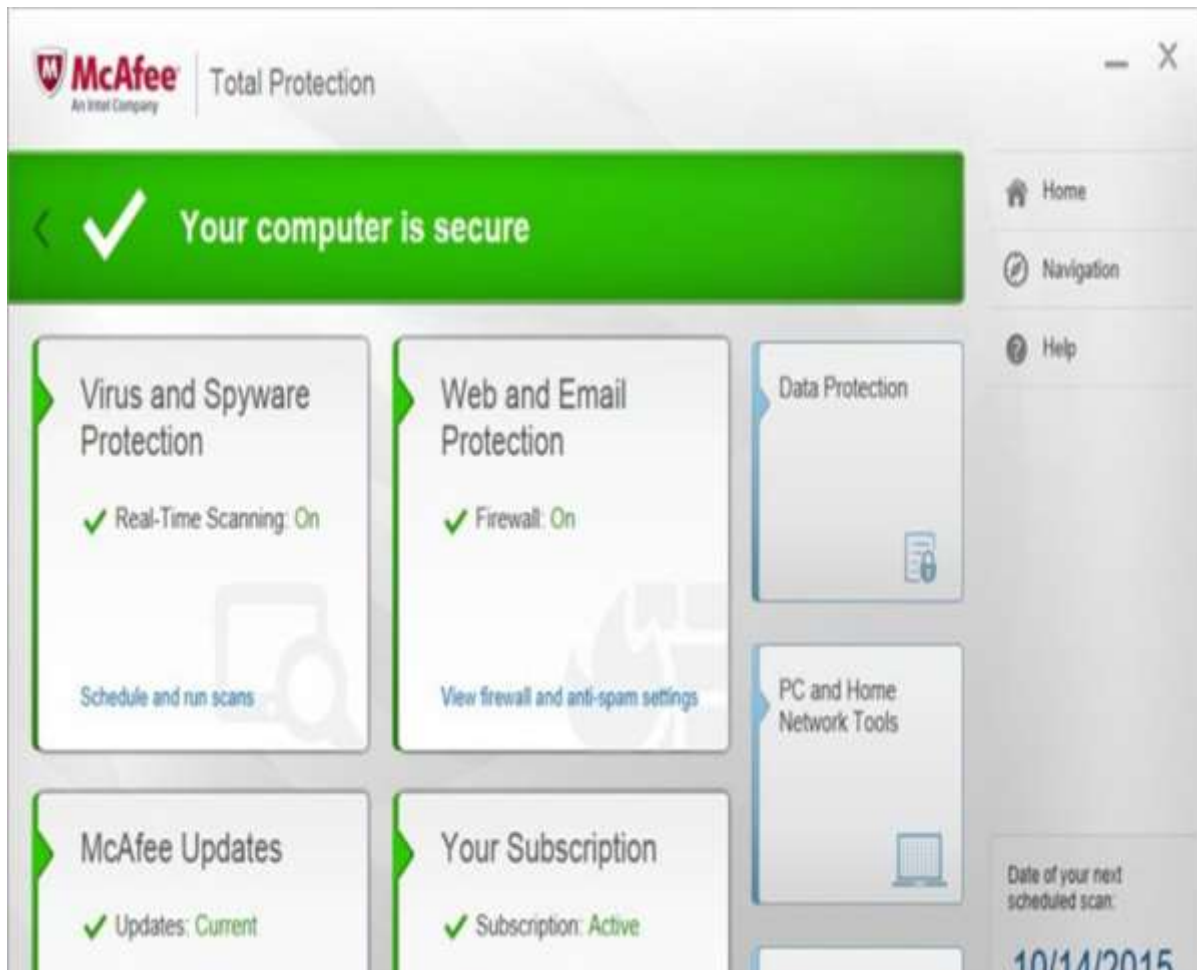


## McAfee AntiVirus Plus

It can be downloaded as a free trial from –

<http://home.mcafee.com/downloads/OneClickTrial.aspx?culture=en-us>

It protects all the operating systems like Windows, Mac OS, Android, and iOS devices. very good malicious URL blocking and anti-phishing.



## Webroot SecureAnywhere Antivirus

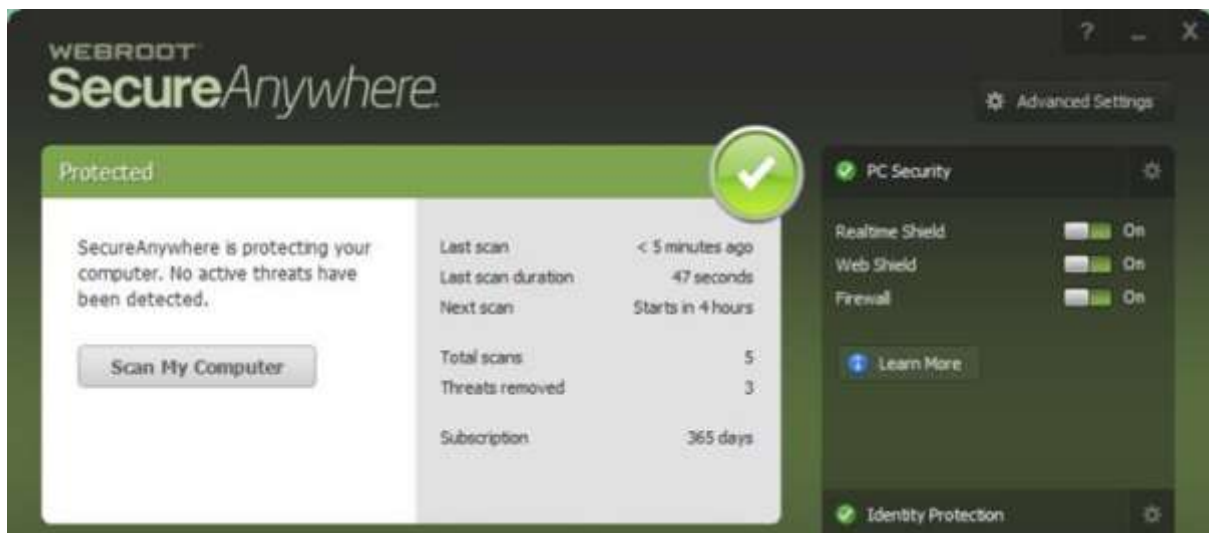
---

It can be downloaded as a free trial from –

<http://www.webroot.com/us/en/home/products/av>

Some of its prominent features are:

- Recover files encrypted by ransomware
- Uses tiny amount of disk space
- Very fast scan
- Handles unknown malware
- Includes firewall



# 7. Computer Security – Malwares

In the previous chapter we treated antiviruses which helped us to protect our systems but in this chapter we will treat malwares, how to detect them manually, what are their forms, what are their file extensions, signs of an infected computer, etc. They are important to be treated because the infection rates of businesses and personal computers are too high in nowadays.

They are self-replication programs that reproduce their own codes by attaching themselves to other executable codes. They operate without the permissions or knowledge of the computer users. Viruses or malwares like in real-life, in computers they contaminate other healthy files.

However, we should remember that viruses infect outside machines only with the assistance of a computer user only. These can happen by clicking a file that comes attached with email from an unknown person, plugging a USB without scanning, opening unsafe URLs for that reason. We as system administrators have to remove the administrator permissions of users in these computers. We categorize malwares in three types:

- Trojans and Rootkits
- Viruses
- Worms

## Characteristics of a Virus

---

Following are a couple of characteristics of any virus that infects our computers.

- They reside in a computer's memory and activates themselves while the program that is attached starts running.

**For example:** They attach themselves in general to the **explorer.exe** in windows OS because it is the process that is running all the time, so you should be cautious when this process starts to consume too much of your computer capacities.

- They modify themselves after the infection phase like they source codes, extensions, new files, etc. so it is harder for an antivirus to detect them.
- They always try to hide themselves in the operating systems in the following ways:
  - Encrypts itself into cryptic symbols, and they decrypt themselves when they replicate or execute.

**For example:** You can see this in the following image for better understanding as in my computer I found this file.

VC_RED	11/7/2007 8:12 AM	Windows Install
vcredist	11/7/2007 8:00 AM	Bitmap image
223!@!!	4/23/2016 9:16 PM	File
Modified: 4/23/2016 9:16 PM		Date created: 4/23/2016 9:16 PM
Size: 32 bytes		

After finding this file, I opened it with a text editor and as thought the text was not understandable as shown in the following screenshot.

```

223!@!! - EditPlus
File Edit Document Project Tools Browser ZC Window Help
aGVsbG8gdGhpcyBpcyBhIHZpcnVzISE=

```

After finding this, I tried it on a base64 decoder and I found that it was a Virus file.

## Encode to Base64 format

Simply use the form below

hello this is a virus!!

> ENCODE <

ASCII

aGVsbG8gdGhpcyBpcyBhIHZpcnVzISE=

This virus can cause the following to your computer:

- It may delete important data from your computer to gain space for their processes.
- It may avoid detection by redirection of disk data.
- It may perform tasks by triggering an event with itself. For example, this happens when in an infected computer pop-up tables etc., show up automatically on the screen.
- They are common in Windows and Mac OS because these operation systems do not have multiple file permissions and are more spread out.

## **Working Process of Malwares and how to Clean it**

---

Malwares attach themselves to programs and transmit to other programs by making use of some events, they need these events to happen because they cannot –

- Start by themselves
- Transmit themselves by using non-executable files
- Infect other networks or computer

From the above conclusions, we should know that when some unusual processes or services are run by themselves we should further investigate their relations with a possible virus. The investigation process is as follows:

To investigate these processes, start with the use of the following tools:

- fport.exe
- pslist.exe
- handle.exe
- netstat.exe

The **Listdll.exe** shows all the **dll files** being used, while the **netstat.exe** with its variables shows all the processes that are being run with their respective ports.

You can see the following example on how I mapped the process of Kaspersky antivirus which I used along with the command **netstat-ano** to see the process numbers and task manager to see to which process belongs to this number.



The image shows a Windows Task Manager window and a Command Prompt window. The Command Prompt displays the output of the command `netstat -ano`, showing active connections. A red box highlights a list of established connections from 127.0.0.1:1113 to 127.0.0.1:1576, all with PID 2396. A red arrow points from the 'osppsvc' service in the Task Manager Services tab to the corresponding PID 2396 in the netstat output.

**Active Connections (from netstat -ano):**

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	2324
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	824
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	2324
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:902	0.0.0.0:0	LISTENING	2700
TCP	0.0.0.0:912	0.0.0.0:0	LISTENING	2700
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	528
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING	912
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING	640
TCP	0.0.0.0:1028	0.0.0.0:0	LISTENING	360
TCP	0.0.0.0:1029	0.0.0.0:0	LISTENING	632
TCP	0.0.0.0:1113	0.0.0.0:0	LISTENING	2396
TCP	0.0.0.0:2869	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:34017	0.0.0.0:0	LISTENING	2388
TCP	0.0.0.0:40201	0.0.0.0:0	LISTENING	2324
TCP	127.0.0.1:1113	127.0.0.1:1263	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1276	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1286	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1344	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1439	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1510	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1519	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1522	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1527	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1529	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1533	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1535	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1536	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1541	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1544	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1547	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1550	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1553	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1556	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1558	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1559	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1563	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1566	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1568	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1576	ESTABLISHED	2396
TCP	127.0.0.1:1113	127.0.0.1:1580	TIME_WAIT	0
TCP	127.0.0.1:1113	127.0.0.1:1582	TIME_WAIT	0
TCP	127.0.0.1:1113	127.0.0.1:1583	TIME_WAIT	0
TCP	127.0.0.1:1113	127.0.0.1:1586	TIME_WAIT	0

**Windows Task Manager Services List:**

Name	PID	Description	Status	Group
WSearch	3740	Windows S...	Runn...	N/A
osppsvc	3136	Office Soft...	Runn...	N/A
Vmacthlp	3068	VMware D...	Runn...	N/A
AuthdSe...	2700	VMware Au...	Runn...	N/A
WMPNetwo...	2572	Windows M...	Runn...	N/A
AVP	2396	Kaspersky ...	Runn...	N/A
VMware NA...	2344	VMware N...	Runn...	N/A
stsvcs	2000	Windows I...	Runn...	N/A
SSDPDRV	1888	SSDP Disco...	Runn...	LocalServic...
FDResPub	1888	Function Di...	Runn...	LocalServic...
DiagTrack	1852	Diagnostics...	Runn...	N/A
AdobeARM...	1824	Adobe Acr...	Runn...	N/A
AcuWSSch...	1632	Acunetix ...	Runn...	N/A
AcuWSSch...	1548	Acunetix ...	Runn...	N/A
WinDefend	1528	Windows D...	Runn...	secsvcs
MpsSvc	1448	Windows Fi...	Runn...	LocalServic...
DPS	1448	Diagnostc ...	Runn...	LocalServic...
BFE	1448	Base Filter...	Runn...	LocalServic...
Spooler	1404	Print Spooler	Runn...	N/A
VMUSArbS...	1220	VMware US...	Runn...	N/A
TeamViewer	1216	TeamViewe...	Runn...	N/A
NlaSvc	1124	Network Lo...	Runn...	NetworkSe...
LanmanWor...	1124	Workstatio...	Runn...	NetworkSe...
Dnscache	1124	DNS Client	Runn...	NetworkSe...
CryptSvc	1124	Cryptogra...	Runn...	NetworkSe...
WinHttpAut...	996	WinHTTP ...	Runn...	LocalService
WdService...	996	Diagnostic ...	Runn...	LocalService
nsi	996	Network St...	Runn...	LocalService
netprofm	996	Network Li...	Runn...	LocalService
FontCache	996	Windows F...	Runn...	LocalService

Then we should look for any **modified, replaced or deleted files** and the **shared libraries** should also be checked. They generally infect executable program files with extension like **.EXE, .DRV, .SYS, .COM, .BIN**. Malwares changes extension of genuine files, for example: File.TXT to File.TXT.VBS.

If you are a system administrator of a webserver, then you should be aware of another form of malware which is called as **webshell**. It generally is in a .php extension but with strange file names and in an encrypted form. You should delete them in case you detect them.

After that is done, we should update the antivirus program and rescan the computer again.

## Detecting a Computer Error from a Virus Infection

---

In this section we will treat how to detect a computer or OS fault from a virus because sometimes people and system administrators mix the symptoms.

The following events are most likely not caused by a malware:

- Error while the system is booting in bios stage, like Bios's battery cell display, timer error display.
- Hardware errors, like beeps RAM burn, HDD, etc.
- If a document fails to start normally like a corrupted file, but the other files can be opened accordingly.
- Keyboard or mouse doesn't answer to your commands, you have to check the plug-ins.
- Monitor switching on and off too often, like blinking or vibrating, this is a hardware fault.

On the other hand, if you have the following signs in your system, you should check for malware.

- Your computer shows a pop-up or error tables.
- Freezes frequently.
- It slows down when a program or process starts.
- Third parties complain that they are receiving invitation in social media or via email by you.
- Files extensions changes appear or files are added to your system without your consent.
- Internet Explorer freezes too often even though your internet speed is very good.
- Your hard disk is accessed most of the time as you can see from the LED light on your computer case.
- OS files are either corrupted or missing.
- If your computer is consuming too much bandwidth or network resources this is the case of a computer worm.
- Hard disk space is occupied all the time, even when you are not taking any action, for example installing a new program.
- Files and program sizes changes comparing to its original version.

### Some Practical Recommendations to Avoid Viruses:

- Don't open any email attachment coming from unknown people or from known people that contain suspicious text.
- Don't accept invitation from unknown people on social media.
- Don't open URL sent by unknown people or known people that are in any weird form.

### Virus Information

---

If you have found a virus but you want to investigate further regarding its function. I would recommend you to have a look at these virus databases, which are offered generally by antivirus vendors.

- **Kaspersky Virus Database** – ([http://www.kaspersky.com/viruswatchlite?hour\\_offset=-1](http://www.kaspersky.com/viruswatchlite?hour_offset=-1))
- **F-Secure** – ([https://www.f-secure.com/en/web/labs\\_global/threat-descriptions](https://www.f-secure.com/en/web/labs_global/threat-descriptions))
- **Symantec – Virus Encyclopedia** – ([https://www.symantec.com/security\\_response/landing/azlisting.jsp](https://www.symantec.com/security_response/landing/azlisting.jsp) )

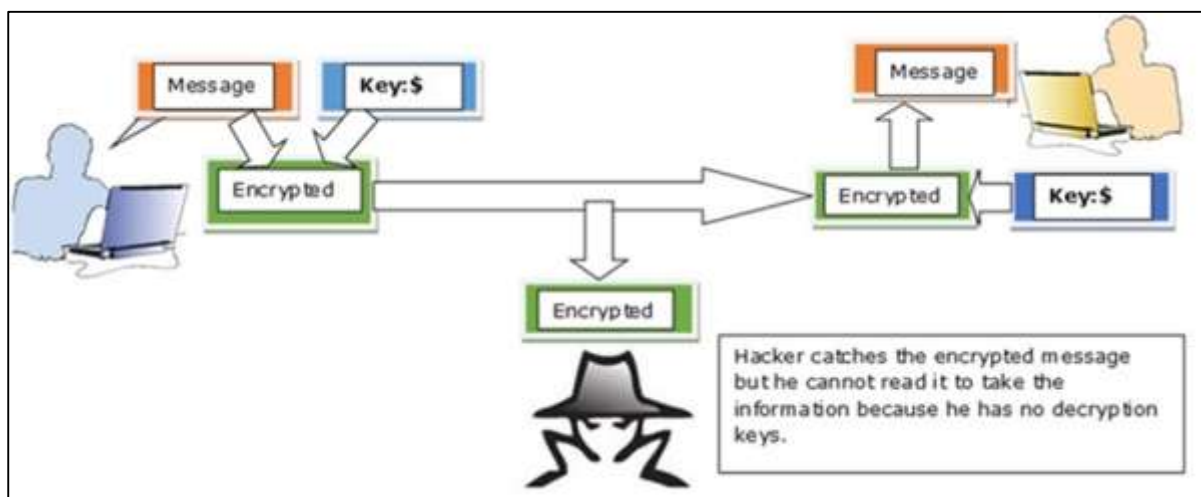
# 8. Computer Security – Encryption

In this chapter, we will discuss about the how important Encryption is for Computer Security.

## What is Encryption?

Encryption is a transformed type of genuine information where only the authorized parties know how to read it, so in the worst case scenario if somebody has access to these files they would still not be able to understand the message in it.

The bases of encryption are since the ancient times. A good example is the pigeon couriers, where the kings used to send messages to their commandants in the battle field in a specific code, when the enemies caught them, they could not read them, just that the message was lost, but if arrived at the destination commandant had the decryption vocabulary so they could decrypt it.



We should mention that encryption is for good or bad purpose. The bad case is the scenario in which most of the malware files are in an encrypted form, so it cannot be read by everyone except the hacker.

## Tools Used to Encrypt Documents

In this tutorial we will focus more on the practices than on the theoretical aspects for better understanding. Let us discuss about some tools that we use to encrypt documents:

- **Axcrypt:** it is one of the best opensource encryption file softwares. It can be used in Windows OS, Mac OS and Linux as well. This software can be downloaded from – <http://www.axantum.com/AxCrypt/Downloads.aspx>
- **GnuPG:** This is an opensource software again and it can be integrated with other softwares too (like email). It can be downloaded from – <https://www.gnupg.org/download/index.html>

- **Windows BitLocker** – It is a Windows integrated tool and its main functions is to secure and encrypt all the hard disk volumes.
- **FileVault** – It is a Mac OS integrated tool and it secures as well as encrypts all the hard disk volume.

## Encryption Ways of Communication

---

System Administrators should use and offer to their staff a secure and encrypted channels of communication and one of them is **SSL (Secure Sockets Layer)**. This protocol helps to establish a secure and encrypted connection between the clients and the servers. Generally, it is used for **Web Servers, Mail Servers, FTP servers**.

### Why do you need this?

If you have an online shop and your clients are using their credit card and their personal data to purchase products from it. But they (Data) are at the risk to be stolen by a simple wiretapping as the communication is in clear text, to prevent this, SSL Protocol will help to encrypt this communication.

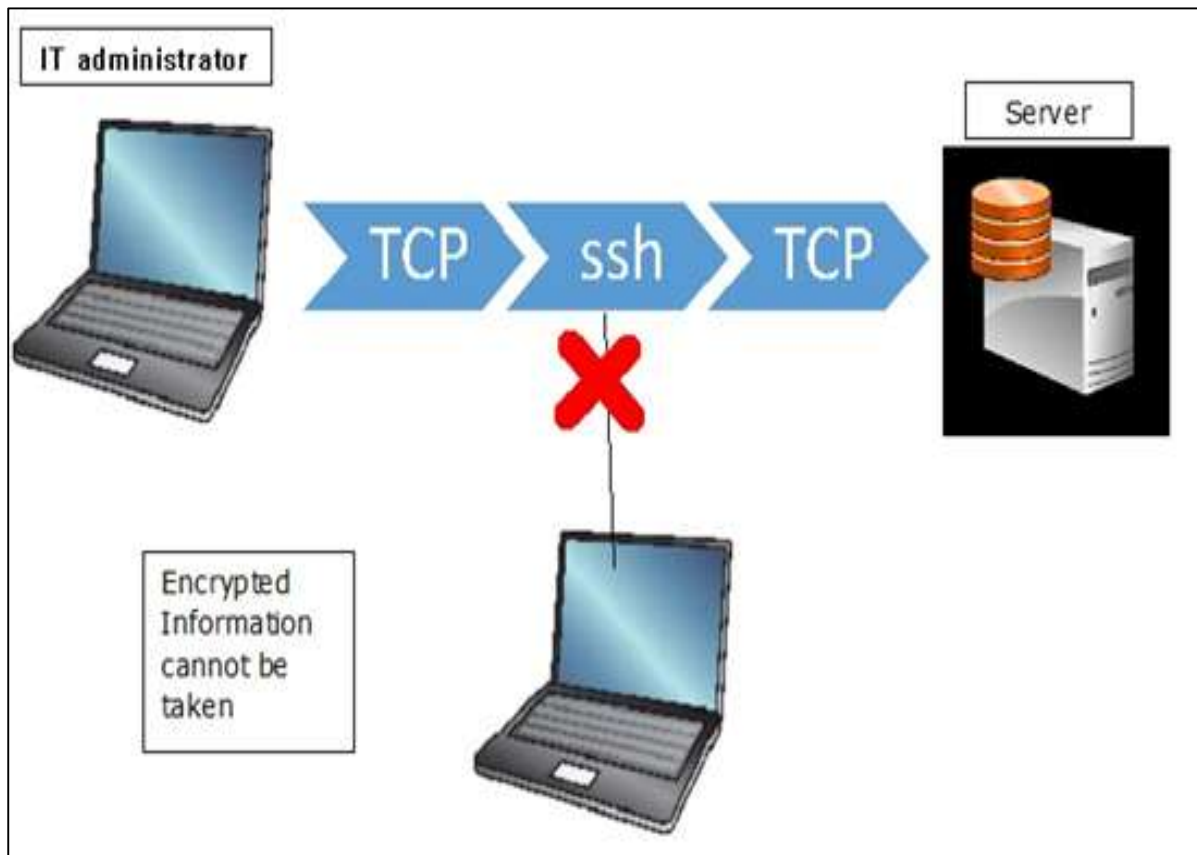
### How to see if the communication is secure?

Browsers give visual cues, such as a lock icon or a green bar, to help visitors know when their connection is secured. An example is shown in the following screenshot.



Another tool used by the system administrator is the **SSH (Secure Shell)**. This is a secure replacement for the telnet and other unencrypted utilities like **rlogin, rcp, rsh**.

It provides a secure channel encrypted in the communication host to host over internet. It reduces the man-in-the-middle attacks. It can be downloaded from – <http://www.putty.org/>.



# 9. Computer Security – Data Backup

In this Chapter, we will discuss backups which is a process of saving data that can be over a network or a computer.

## Why is Backup Needed?

---

The main purpose is to recover the lost data from an unpredictable event like deletion by mistake or file corruption which in many cases is caused by a virus. An example is **Ransomware**, which encrypts all your data when your computer gets infected and the second is to roll back the data at a specific time you want. This is a scenario that happens often in companies which have applications and databases and they want to test their applications with a specific version of data.

## How is this Process Managed at Big Companies?

It is suggested that in bigger companies which have a large volume of data, it is necessary to have a backup administrator, which is one of the most trusted persons in the company because he has access to all the data of that organization and generally deals with the backup routine check and the health of the backup.

## Backup Devices

---

In this section we will see the backup devices from smaller to enterprise solutions. For a personal computer, they are:

**CD and DVD, Blue-Rays** – They are used for home/personal usage where people can store their documents, mainly personal or office related documents because they have small capacities varying from 750MB to 50GB.



**Removable Devices** – They are again for home usage (data, documents, music, photos, movies) which can be a Removable USB or external hard disks. Their capacities lately have increased a lot, they vary from 2 GB to 2 TB.



**Network attached storage (NAS)** – They are generally devices that are used in small businesses for backup purposes because they offer a centralized manner of backup. All the users can connect through the network to access this device and save data.

They are lesser in cost when compared to other solutions and they also offer a good fault tolerance as they are configured in RAID (redundant array of independent disks). They can be rack or non-rack mounted. They offer a good level of authentication of users and web console managing.





**Storage Area Network (SAN)** – These are generally devices that are used for big businesses for backup purposes. They offer a high speed of network for storage the biggest producers are **EMC Corporation, DELL.**



## Types of Backups Based on Location

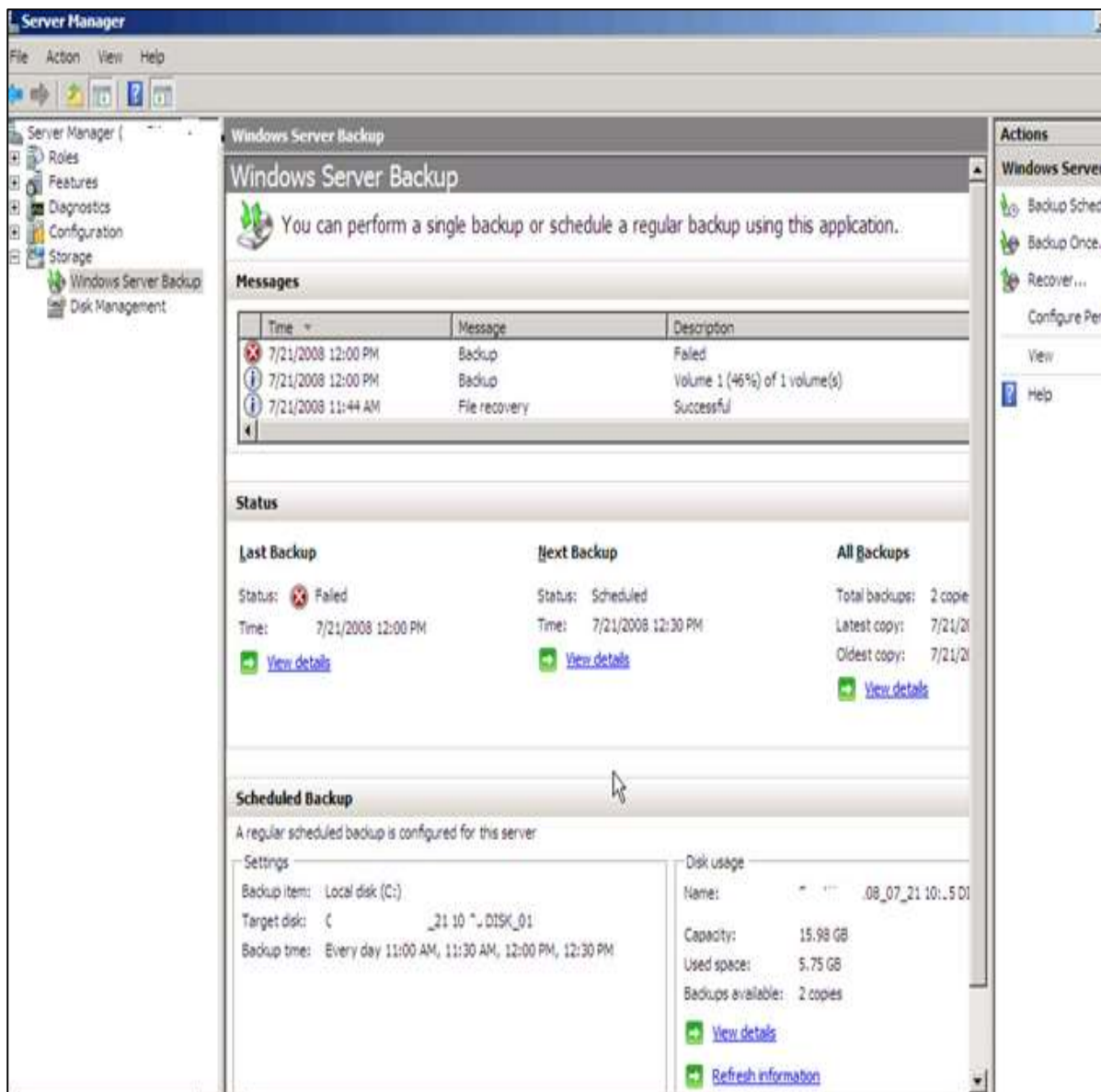
---

The types of backup can vary on the size of the business, budget and the data importance.

They are divided in two types:

- Local Backups
- Online Backups

Generally local backups store the data in a CD, NA Storages, etc. as there can be a simple copying of files or by using any third party software. One of them in the server is the Windows backup which is included in the Windows Server Edition License.



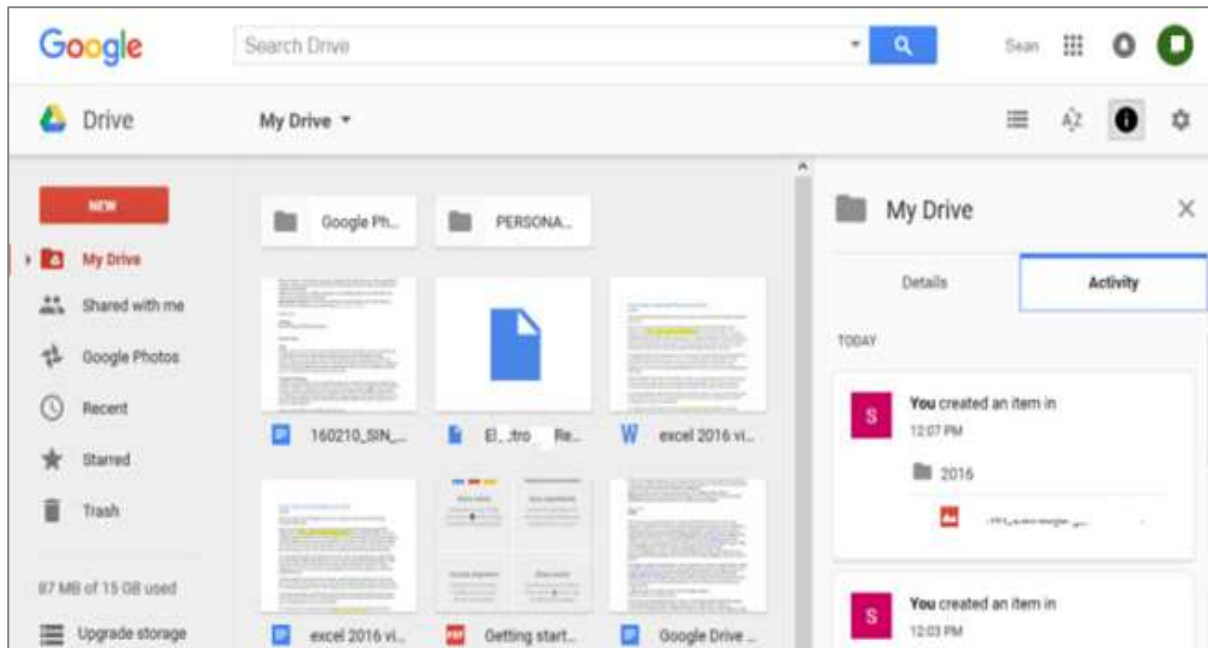
Another one is Acronis which is one of the best in the market – <http://www.acronis.com/en-eu/>

## Online Backup or Cloud Storage

One of the biggest trend is online storage where the companies and users can store their data somewhere in the cloud, and it is cheaper as well rather than doing it all by yourself. There is also no need for any backup infrastructure and maintenance.

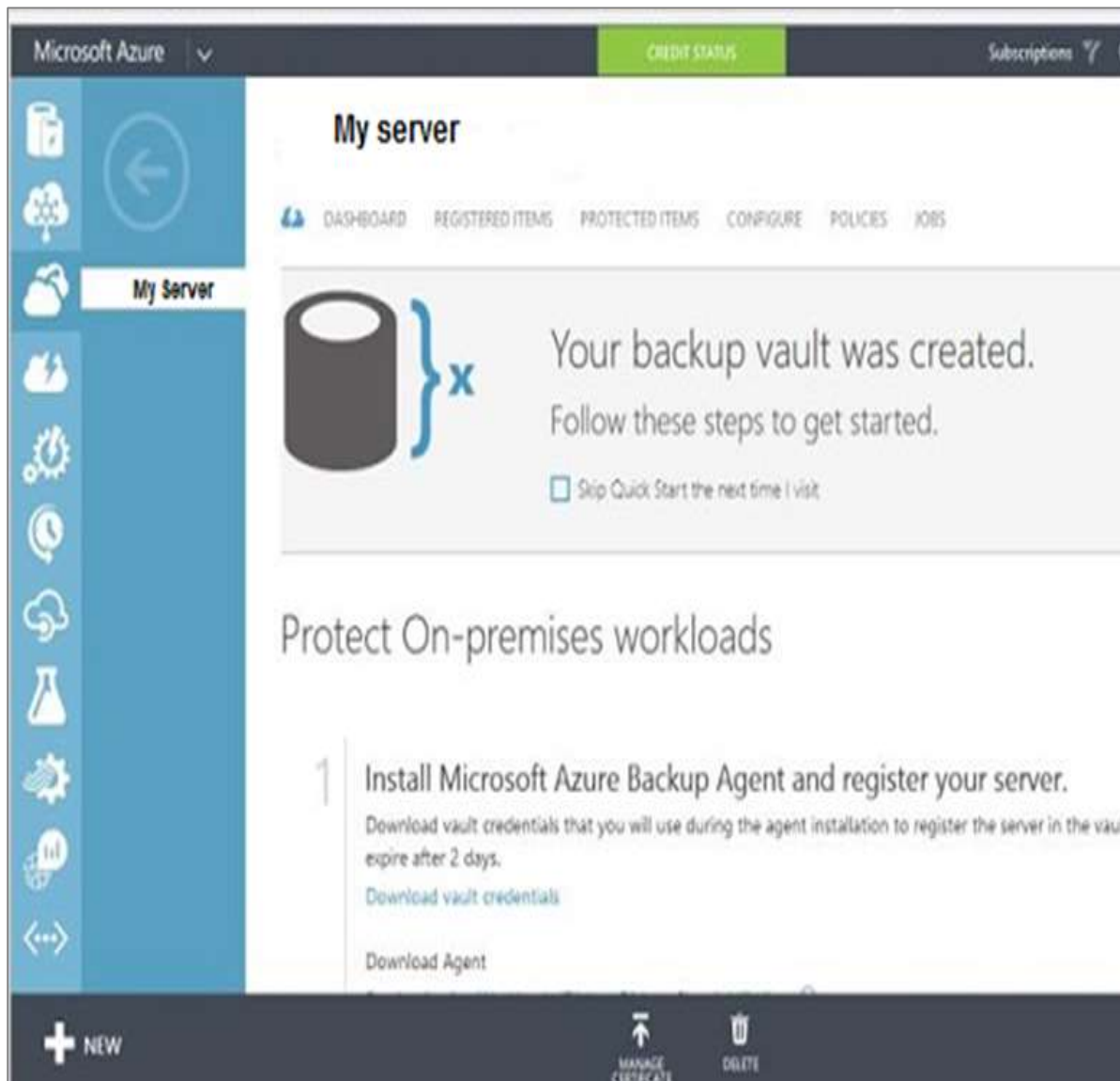
For a personal user it is offered for free by the biggest vendors like Microsoft. It offers OneDrive and you can store up to 5GB in their cloud and it has an interface for different Operating Systems.

The second is the Google Drive, which is a product by google, wherein the files synchronizes automatically.

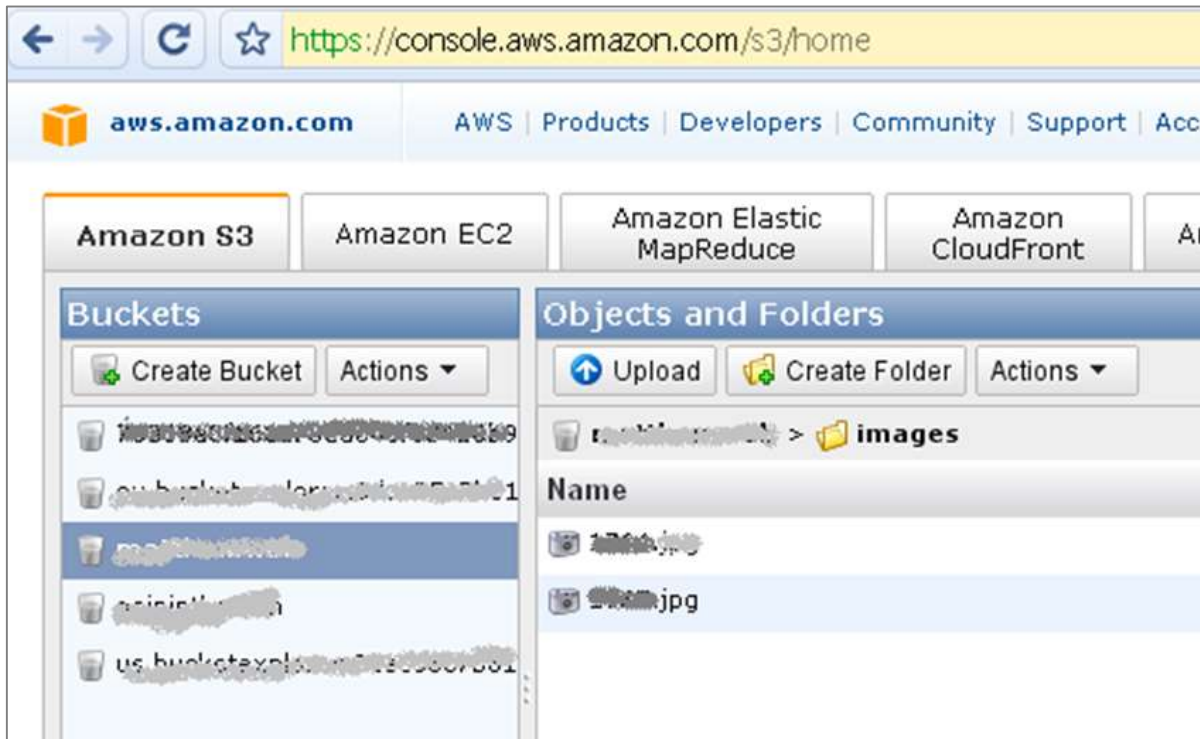


The full list can be seen in PCMagazine – <http://www.pcmag.com/article2/0,2817,2413556,00.asp#>. For small or big companies, mentioned before, online or cloud backup solution are a good solution for them because of the cost and the liability.

The biggest vendors offering such service are Microsoft with AZURE solution – <https://azure.microsoft.com/en-us/documentation/scenarios/storage-backup-recovery/> which is offering a very high performance and scalability for this solution.



The other is Amazon with its product S3 details about this product can be found on – <http://aws.amazon.com/s3/>



# 10. Computer Security – Disaster Recovery

Disaster recovery is generally a planning process and it produces a document which ensures businesses to solve critical events that affect their activities. Such events can be a natural disaster (earthquakes, flood, etc.), cyber-attack or hardware failure like servers or routers.

As such having a document in place it will reduce the down time of business process from the technology and infrastructure side. This document is generally combined with Business Continuity Plan which makes the analyses of all the processes and prioritizes them according to the importance of the businesses. In case of a massive disruption it shows which process should be recovered firstly and what should be the downtime. It also minimizes the application service interruption. It helps us to recover data in the organized process and help the staff to have a clear view about what should be done in case of a disaster.

## Requirements to Have a Disaster Recovery Plan

Disaster recovery starts with an inventory of all assets like computers, network equipment, server, etc. and it is recommended to register by serial numbers too. We should make an inventory of all the software and prioritize them according to business importance.

An example is shown in the following table:

Systems	Down Time	Disaster type	Preventions	Solution strategy	Recover fully
Payroll system	8 hours	Server damaged	We take backup daily	Restore the backups in the Backup Server	Fix the primary server and restore up to date data

You should prepare a list of all contacts of your partners and service providers, like ISP contact and data, license that you have purchased and where they are purchased. Documenting all your Network which should include IP schemas, usernames and password of servers.

### Preventive steps to be taken for Disaster Recovery:

- The server room should have an authorized level. For example: only IT personnel should enter at any given point of time.
- In the server room there should be a fire alarm, humidity sensor, flood sensor and a temperature sensor.

These are more for prevention. You can refer the following image.



- At the server level, RAID systems should always be used and there should always be a spare Hard Disk in the server room.
- You should have backups in place, this is generally recommended for local and off-site backup, so a NAS should be in your server room.
- Backup should be done periodically.
- The connectivity to internet is another issue and it is recommended that the headquarters should have one or more internet lines. One primary and one secondary with a device that offers redundancy.
- If you are an enterprise, you should have a disaster recovery site which generally is located out of the city of the main site. The main purpose is to be as a stand-by as in any case of a disaster, it replicates and backs up the data.

# 11. Computer Security – Network

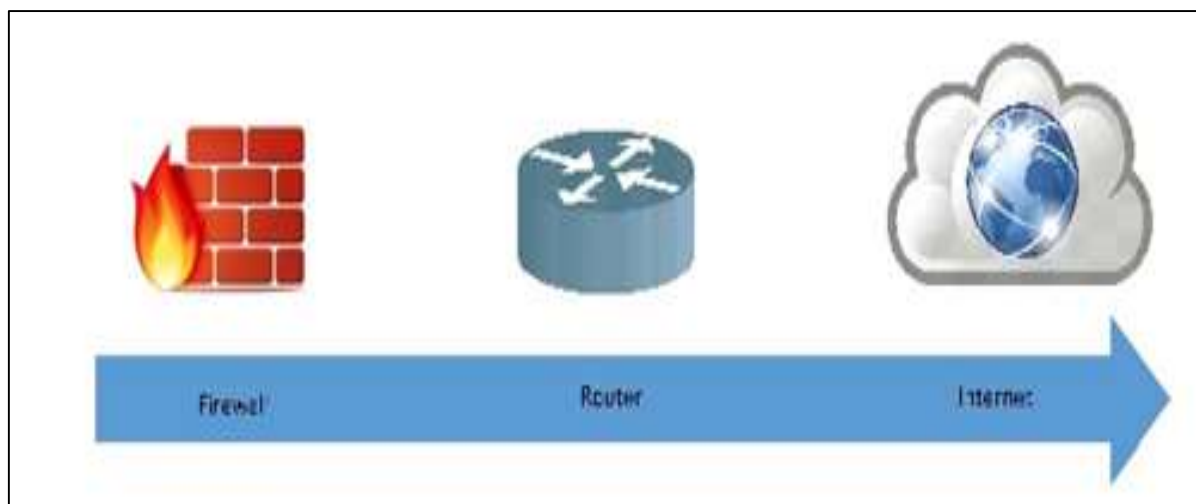
In this chapter we will discuss regarding the network from the view of security. We will also look into which are the systems that help us as system administrators to increase the security.

**For example:** We are system administrators of a large chain of super markets, but our company wants to go online by launching an online selling platform. We have done the configuration and the system is up and working, but after a week we hear that the platform was hacked.

We ask a question to ourselves – What did we do wrong? We skipped the security of the network which is as important as the set up because this hacking can directly influence the company's reputation resulting in decrease of sales and market value.

## Devices that Help us with Network Security

**Firewalls:** They can be software or applications which operate at the network level. They protect Private networks from external users and other networks. Generally, they are a compound of programs and their main function is to monitor the traffic flow from outside to inside and vice versa. Their position is generally behind a router or in front of the router depending on the network topologies.



They are also called Intrusion detection devices; their traffic rules are configured according to the company policy rules. For example, you block all incoming traffic to port POP because you don't want to receive a mail so as to be secured from all possible mail attacks. They log all the network attempts for a latter audit for you.

They also can work as packet filters this means that the firewall takes the decisions to forward or not the packet based on source and destination addresses and ports.



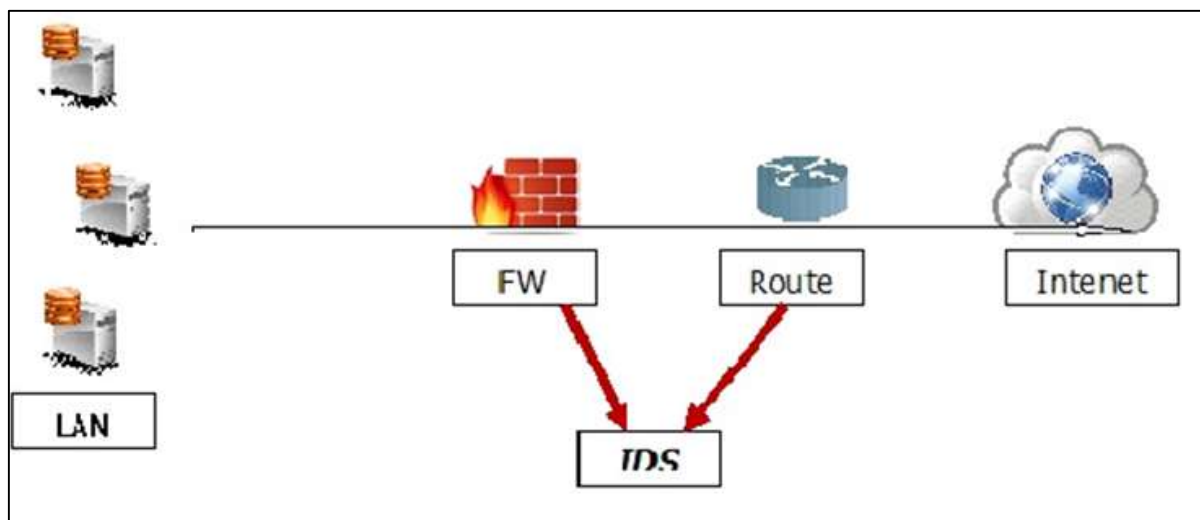
Some of the recommended brands are –

- Cisco ASA Series
- Checkpoint
- Fortinet
- Juniper
- SonicWALL
- pfSense

## Intrusion Detection Systems

Intrusion Detection Systems are also as important as the firewall because they help us to detect the type of attack that is being done to our system and then to make a solution to block them. The monitoring part like tracing logs, looking for doubtful signatures and keeping history of the events triggered. They help also the network administrators to check the connection integrity and authenticity that occur.

Let us see the schema of their positions:



## Intrusion Detection Tools

One of the best intrusion detection tool is **Snort**, you can take information and download the same from – [www.snort.org](http://www.snort.org)

It is software based, but is an opensource so it is free and easy to configure. It has a real time signature based network – IDS, which notifies the system administrators or attacks like port scanners, DDOS attacks, CGI attacks, backdoors, OS finger printing.



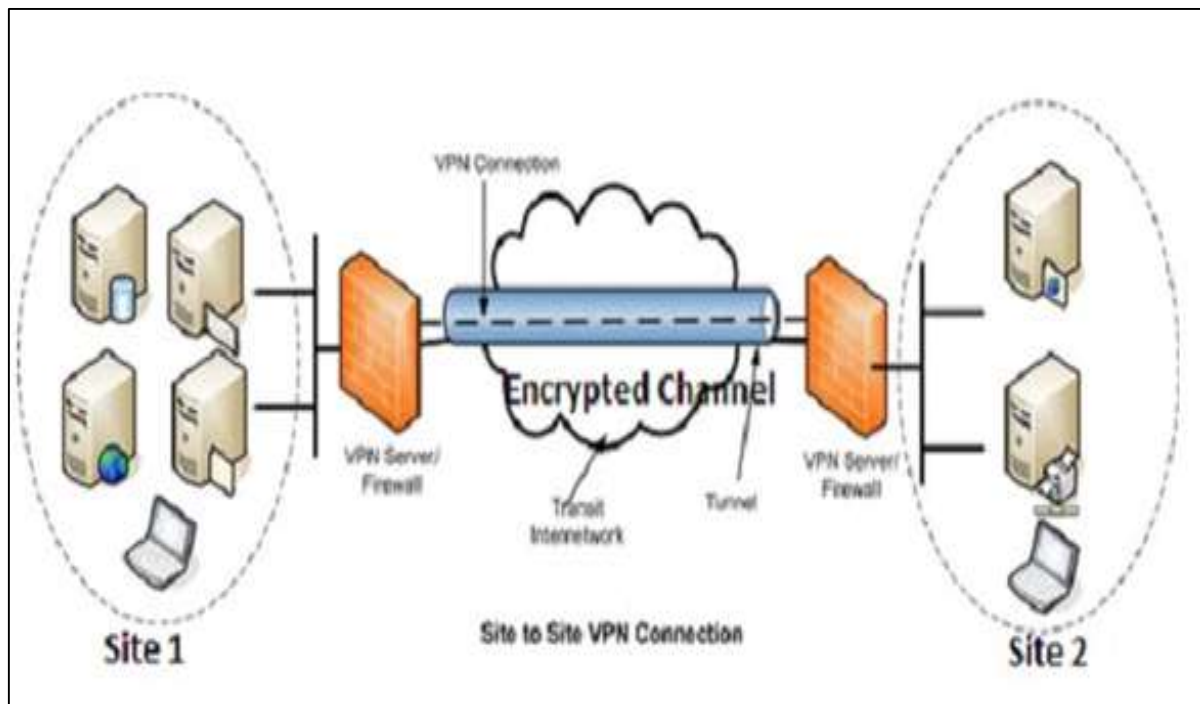
The other IDS are:

- BlackICE Defender
- CyberCop Monitor
- Check point RealSecure
- Cisco Secure IDS
- Vanguard Enforcer
- Lucent RealSecure.

## Virtual Private Network

This type of a network is widely used in a small business or enterprise networks. It helps to send and receive data across the internet, but in a secure and encrypted way. Generally, this network is created between two secure network devices like two firewalls.

An example is a connection between two ASA 5505 firewalls as shown in the following image.



# 12. Computer Security – Policies

In this chapter we will explain security policies which are the basis of security for the technology infrastructure of your company.

In a way they are the regulatory of the behaviors of your employees towards the use of technology in the workplace, that can minimize the risk of being hacked, information leak, internet bad usage and it also ensures safeguarding of company resources.

In real life you will notice the employees of your organization will always tend to click on bad or virus infected URL's or email attachments with viruses.

## Role of the Security Policy in Setting up Protocols

---

Following are some pointers which help in setting up protocols for the security policy of an organization.

- Who should have access to the system?
- How it should be configured?
- How to communicate with third parties or systems?

Policies are divided in two categories:

- User policies
- IT policies.

User policies generally define the limit of the users towards the computer resources in a workplace. For example, what are they allowed to install in their computer, if they can use removable storages.

Whereas, IT policies are designed for IT department, to secure the procedures and functions of IT fields.

- **General Policies:** This is the policy which defines the rights of the staff and access level to the systems. Generally, it is included even in the communication protocol as a preventive measure in case there are any disasters.
- **Server Policies:** This defines who should have access to the specific server and with what rights. Which software's should be installed, level of access to internet, how they should be updated.
- **Firewall Access and Configuration Policies:** It defines who should have access to the firewall and what type of access, like monitoring, rules change. Which ports and services should be allowed and if it should be inbound or outbound.
- **Backup Policies:** It defines who is the responsible person for backup, what should be the backup, where it should be backed up, how long it should be kept and the frequency of the backup.

- **VPN Policies:** These policies generally go with the firewall policy, it defines those users who should have a VPN access and with what rights. For site-to-site connections with partners, it defines the access level of the partner to your network, type of encryption to be set.

## Structure of a Security Policy

---

When you compile a security policy you should have in mind a basic structure in order to make something practical. Some of the main points which have to be taken into consideration are:

- Description of the Policy and what is the usage for?
- Where this policy should be applied?
- Functions and responsibilities of the employees that are affected by this policy.
- Procedures that are involved in this policy.
- Consequences if the policy is not compatible with company standards.

## Types of Policies

---

In this section we will see the most important types of policies.

- **Permissive Policy:** It is a medium restriction policy where we as an administrator block just some well-known ports of malware regarding internet access and just some exploits are taken in consideration.
- **Prudent Policy:** This is a high restriction policy where everything is blocked regarding the internet access, just a small list of websites are allowed, and now extra services are allowed in computers to be installed and logs are maintained for every user.
- **Acceptance User Policy:** This policy regulates the behavior of the users towards a system or network or even a webpage, so it is explicitly said what a user can do and cannot in a system. Like are they allowed to share access codes, can they share resources, etc.
- **User Account Policy:** This policy defines what a user should do in order to have or maintain another user in a specific system. For example, accessing an e-commerce webpage. To create this policy, you should answer some questions such as –
  - Should the password be complex or not?
  - What age should the users have?
  - Maximum allowed tries or fails to log in?
  - When the user should be deleted, activated, blocked?
- **Information Protection Policy:** This policy is to regulate access to information, how to process information, how to store and how it should be transferred.

- **Remote Access Policy:** This policy is mainly for big companies where the user and their branches are outside their headquarters. It tells what should the users access, when they can work and on which software like SSH, VPN, RDP.
- **Firewall Management Policy:** This policy has explicitly to do with its management, which ports should be blocked, what updates should be taken, how to make changes in the firewall, how long should be the logs be kept.
- **Special Access Policy:** This policy is intended to keep people under control and monitor the special privileges in their systems and the purpose as to why they have it. These employees can be team leaders, managers, senior managers, system administrators, and such high designation based people.
- **Network Policy:** This policy is to restrict the access of anyone towards the network resource and make clear who all will access the network. It will also ensure whether that person should be authenticated or not. This policy also includes other aspects like, who will authorize the new devices that will be connected with network? The documentation of network changes. Web filters and the levels of access. Who should have wireless connection and the type of authentication, validity of connection session?
- **Email Usage Policy:** This is one of the most important policies that should be done because many users use the work email for personal purposes as well. As a result information can leak outside. Some of the key points of this policy are the employees should know the importance of this system that they have the privilege to use. They should not open any attachments that look suspicious. Private and confidential data should not be sent via any encrypted email.
- **Software Security Policy:** This policy has to do with the software's installed in the user computer and what they should have. Some of the key points of this policy are Software of the company should not be given to third parties. Only the white list of software's should be allowed, no other software's should be installed in the computer. Warez and pirated software's should not be allowed.

# 13. Computer Security – Checklist

In this chapter, we will discuss on an advanced checklist that we will use in order to educate users and IT staff too, when it comes to any security issues, they should come as natural expressions.

Based on all the chapters and especially on the security policies, the following table has a list of checklist that touches most of the components that have been discussed in this tutorial.

Checklist	Status of task
<b><u>Server Room</u></b>	
Server rack installed properly	
Air conditioning present	
Temperature monitoring and alarm system is in place	
Automatic smoke/fire detection is available	
Water entry prevention detector is available	
Fire extinguisher is in place	
Local LAN wiring is done properly	
<b><u>Business Critical Services</u></b>	
Redundant power supplies are available	
RAID systems are available	
UPS systems are in place	
Emergency systems are in place	

Documentation is up to date	
Professional support is provided	
SLAs are signed	
Emergency plan is prepared	
<b><u>Business Internet Account</u></b>	
Redundant lines	
Insurance for ICT equipment is available	
<b><u>Information Systems</u></b>	
Server is installed according to the Setup Policies Manuals	
Standard GPOs are configured on the Server	
System security is done	
System documentation is up-to-date	
Data backup is configured properly and done regularly according to backup policies	
To check proper naming of all computers, network devices to be in line with IT Policy	
Standard Whitelist Software to be aligned on all PCs	
All PCs in domain system	
Administrator privileges are taken from computer users	
Program privileges are on minimum needed level	



<b><u>Information Security</u></b>	
Identity and access management is configured	
Data access possibilities are minimized to needed level	
Virus protection software is installed on each PC	
<b><u>Human Factor</u></b>	
ICT System and email Usage Policy is rolled-out (should be checked as per the disciplinary safeguards)	
Staff awareness training is provided regularly	
Responsibilities are documented	
<b><u>Maintenance of Information Systems</u></b>	
Security updates are installed on all PC's	
ICT internal alert and notification system is configured	
Security update action plan is done	
Security update roll out plan is in place	
<b><u>General</u></b>	
Network IP address schema are in line	
<b><u>Network Security</u></b>	
Firewall access rules and open ports are compliant with the firewall policy	
Protection of sensitive information is in place	

Restriction of communication services is enabled	
VPN is configured properly with the partners	
WLAN security is enabled on all WIFI devices	
Limited internet access is configured	
BYOD regulations are implemented	
<b><u>Network Management</u></b>	
Bandwidth Management System is configured	
Network Monitoring System is available	
DRP files are up to date	

Please keep in mind that this list can be modified according to your company needs and staff too.

# 14. Computer Security - Legal Compliance

In this section we will explain some important compliances that are around the technology industry. Nowadays technology compliance is becoming more important because it is developing too fast and legal issues are raising more often than ever. What is compliance, let's say for example we want to develop a health managing software, it has to be developed in accordance with the standards of the Health Organization in that Country and if it will be international it has to be in accordance with the country where it will be marketed, which in this case is Health Information Portability and Accountability Act.

## What are the Main Compliances?

---

Some regulations, standards and legislations which companies may need to be in compliance are as follows:

### **Sarbanes Oxley Act (SOX) of 2002:**

The Sarbanes Oxley Act was created for the high-profile financial scandals to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. Among other provisions, the law sets rules on storing and retaining business records in IT systems. It is important because most of the biggest banks in the recent years have suffered from data breach. If you are in the financial industry you should check this act and its details can be found online. You can click on the following link for more information – [https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley\\_Act](https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act)

### **Health Insurance Portability and Accountability Act of 1996 (HIPAA):**

In this act, the Title II includes an administrative section that mandates standardization of electronic health records systems and includes security mechanisms designed to protect data privacy and patient confidentiality. It should have hardware or software that provides access controls, integrity controls, auditing and transmission security. So if you are a system administrator in the health system you should read and check your systems if they are in compliance with this act. For further information, you can click on the following link – [https://en.wikipedia.org/wiki/Health\\_Insurance\\_Portability\\_and\\_Accountability\\_Act](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act)

### **FERC Compliance**

This compliance is important because it deals with energy industry. Businesses should implement policies and procedures to not only protect key electronic assets, but also to report and recover when a cyber-attack occurs. Further information on this can be found on the following link – <http://www.ferc.gov/enforcement/compliance.asp>

### **Payment Card Industry Data Security Standard (PCI DSS)**

This has to do with the retail online stores industry mostly. This as a compliance doesn't have a direct law impact, but if it is neglected, you can be charged for other law infringements. It was developed jointly by American Express, Visa, MasterCard, Discover and JCB. It requires the use of firewalls, data encryption, monitoring and other controls to ensure confidential information. More information can be found on Wikipedia – [https://en.wikipedia.org/wiki/Payment\\_Card\\_Industry\\_Data\\_Security\\_Standard](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard)

We have discussed most of the important compliances that have a bigger impact, also it is worth to mention that Legal compliances can change according to countries but these major ones which we mentioned are almost similar in every country.