



Internet Security

tutorialspoint

SIMPLY EASY LEARNING

www.tutorialspoint.com



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



<https://twitter.com/tutorialspoint>

About the Tutorial

With the ever-increasing usage of Internet, numerous activities take place in your computer and it can be for either good or bad. These activities vary from identity theft to people who hack into computers and steal private passwords, documents and files. The fact is that everything is online and opens us to these frauds and makes us victims, unless you have taken the necessary steps to protect your computer.

In this tutorial, we will discuss how to use Internet in a safe and secure way, and the precautions that we need to take in order to protect ourselves from the open environment of Internet.

Audience

This tutorial has been prepared mainly for those professionals that are within the IT industry and who are IT specialists, System administrators, Security administrators and in the other applicable departments.

This tutorial is intended to make the reader comfortable in getting started with Internet Security and its various other functions.

Prerequisites

It is a basic tutorial where the reader can easily understand the concepts explained with a simple knowledge of how a company or an organization deals with its Internet Security. However, it will help if you have some prior exposure of cookies, phishing attacks, spamming, 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

Table of Contents

About the Tutorial.....	i
Audience	i
Prerequisites	i
Copyright and Disclaimer	i
Table of Contents	ii
 1. INTERNET SECURITY – OVERVIEW	 1
Impact from an Internet Breach	2
 2. INTERNET SECURITY – COOKIES.....	 3
Types of Cookies	3
How to Block Cookies and Delete Them?	4
 3. INTERNET SECURITY – PHISHING	 10
How to Detect a Phishing Email?	11
 4. INTERNET SECURITY – SOCIAL NETWORK.....	 14
 5. INTERNET SECURITY – CHROME	 16
 6. INTERNET SECURITY – MOZILLA	 20
 7. INTERNET SECURITY - INTERNET EXPLORER.....	 23
 8. INTERNET SECURITY – SAFARI.....	 26
 9. INTERNET SECURITY – GAMING.....	 29
 10. INTERNET SECURITY – CHILD SAFETY.....	 31
Why is it so Important?	31
Social Rules Regarding Child Internet Safety	31
Use Software to Keep Track	32

11. INTERNET SECURITY – SPAMMING	35
Techniques Used by Spammers	35
Anti-Spam Techniques	35
Anti-Spamming Tools	36
12. INTERNET SECURITY – CHATTING	38
Risks from Chatting	38
13. INTERNET SECURITY – FILE DOWNLOAD.....	39
What can be Potentially Harmful?.....	39
How to Minimize the Risks to be Infected from File Download	39
14. INTERNET SECURITY – TRANSACTIONS	42
Check if You are Doing a Secure Transaction?	42
What Should You do as a System Administrator?.....	43
15. INTERNET SECURITY – BANKING	44
How to do an e-Banking Transaction Safely?.....	44
Credit Cards.....	45
Credit Card Generator	46
Credit Card Fraud Detection Techniques	46
Best Practices to Protect your Bank Transactions.....	48
16. INTERNET SECURITY – E-COMMERCE	49
Top e-Commerce Platforms.....	49
How to Buy in a Secure Way?	52
Setup a Secure Online Shop	52
17. INTERNET SECURITY – CERTIFICATES.....	53
Components of a Digital Certificate	53
Levels of Validations	55

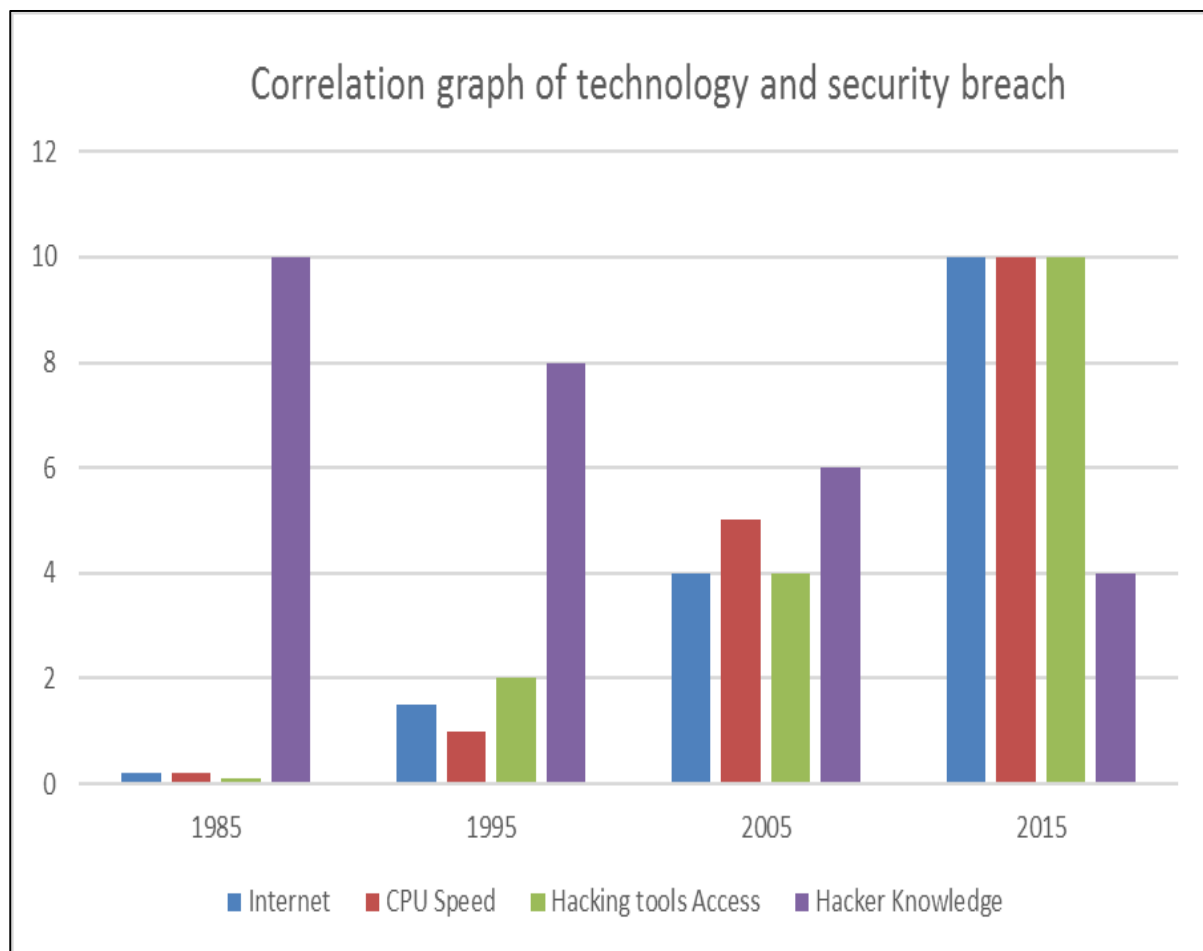
18. INTERNET SECURITY – EMAIL SECURITY.....	56
Hardening a Mail Server	56
Securing Email Accounts.....	58
19. INTERNET SECURITY – IDENTITY THEFT	60
What is Identity Theft?.....	60
How Does ID Thefts Take Place?.....	61
20. INTERNET SECURITY – CYBERCRIME	63
Types of Cybercrime.....	63
21. INTERNET SECURITY – LAWS.....	64
United States Cyber Crime Law	64
Mexico Cyber Crime Law	64
22. INTERNET SECURITY – CHECKLIST	66
Basic Checklist	66

1. Internet Security – Overview

With the usage of Internet, a number of activities take place in your computer which can be for good or bad and varies from identity thefts to people who hack into computers and steal private passwords, documents and files. The fact is that everything is online and opens us to these frauds and makes us victims, unless you have taken the necessary steps to protect your computer.

It is quite strange that till date, a lot of people don't give much importance to Internet Security. They think that their computers are invisible, but as soon as they start using their computers for anything that involves logging onto the Internet, they are an easy prey, even for a teenaged hacker.

The following image gives you an idea of how things have changed over the years.



Impact from an Internet Breach

The potential losses in this “cloud” are discussed as follows.

Here is a list of some losses that can have a direct impact on you and others:

- **Losing Your Data** – An Internet breach can swipe away all the data that you have gathered over the years.
- **Reputation Loss** – Just think your Facebook account or business email have been hacked by a social engineering attack and it sends fake information to your friends, business partners. You will need time to gain back your reputation after such an attack. Or your webpage has been hacked and the hacker puts up an ugly picture on it, so a new customer that is visiting your webpage to get some information will see this picture named “HACKED” and the chances that he will go away without contacting you will be too high.
- **Identity Theft** – This is a case where your identity is stolen (photo, name surname, address, and credit card details) and can be used for a crime like making false identity documents or anything else.

2. Internet Security – Cookies

Cookies are files, generally from the visited webpages, which are stored on a user's computer. They hold a small amount of data, specific to a particular client and website, and can be accessed either by the web server or the client computer which can be usernames, password, session token, etc.

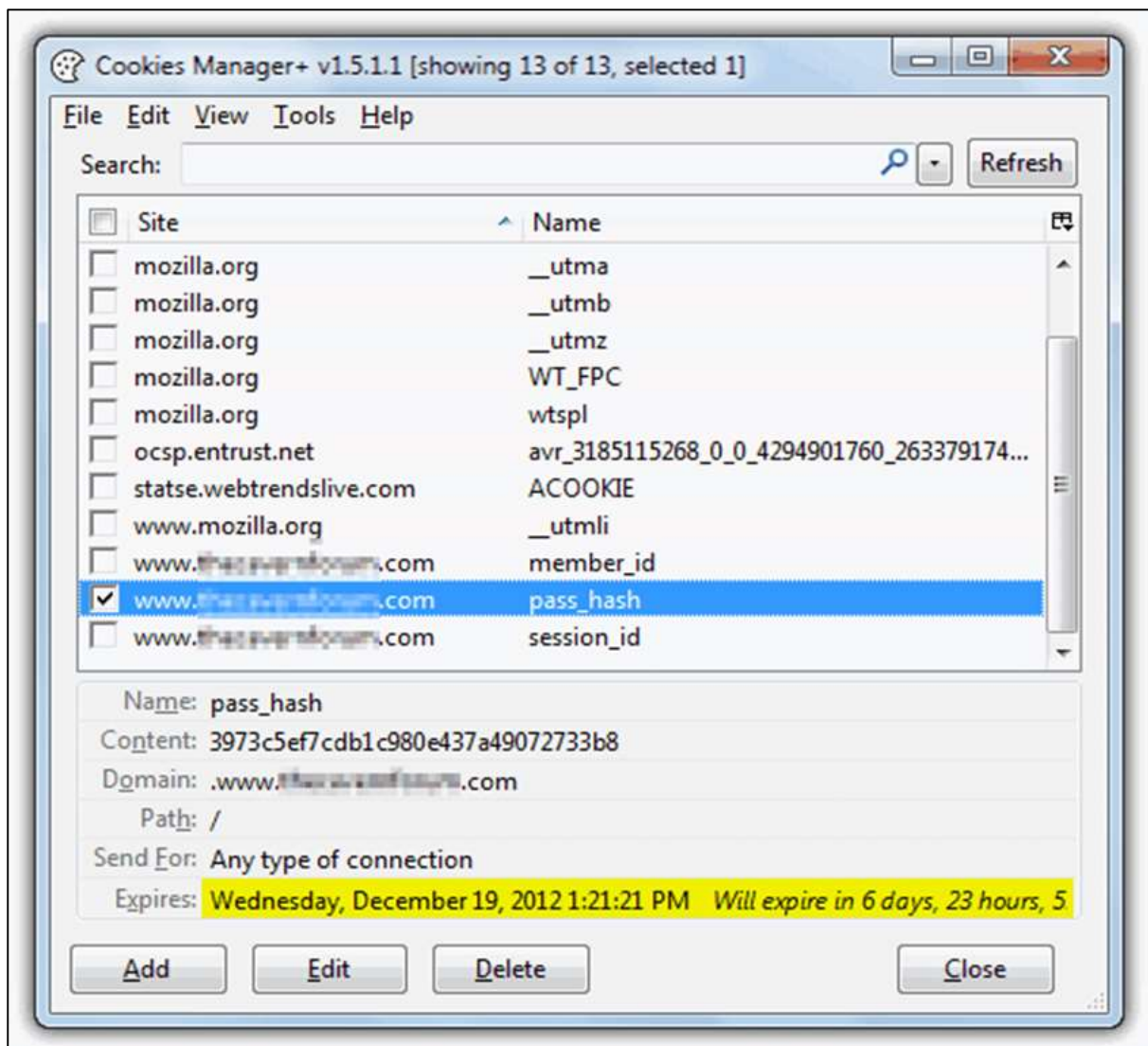
This allows the server to deliver a page personalized to a particular user, or the page itself can contain some script which is aware of the data in the cookie and so is able to carry information from one visit to that website.

Types of Cookies

There are three different types of cookies:

- **Session Cookies:** These are mainly used by online shops and allows you to keep items in your basket when shopping online. These cookies expire after a specific time or when the browser is closed.
- **Permanent Cookies:** These remain in operation, even when you have closed the browser. They remember your login details and password so you don't have to type them in every time you use the site. It is recommended that you delete these type of cookies after a specific time.
- **Third-Party Cookies:** These are installed by third parties for collecting certain information. For example: Google Maps.

The following screenshot shows where the data of a cookie is stored and to do this, I have used a plugin of Firefox which is called Cookies Manager+. It shows the date when a cookie will expire.



How to Block Cookies and Delete Them?

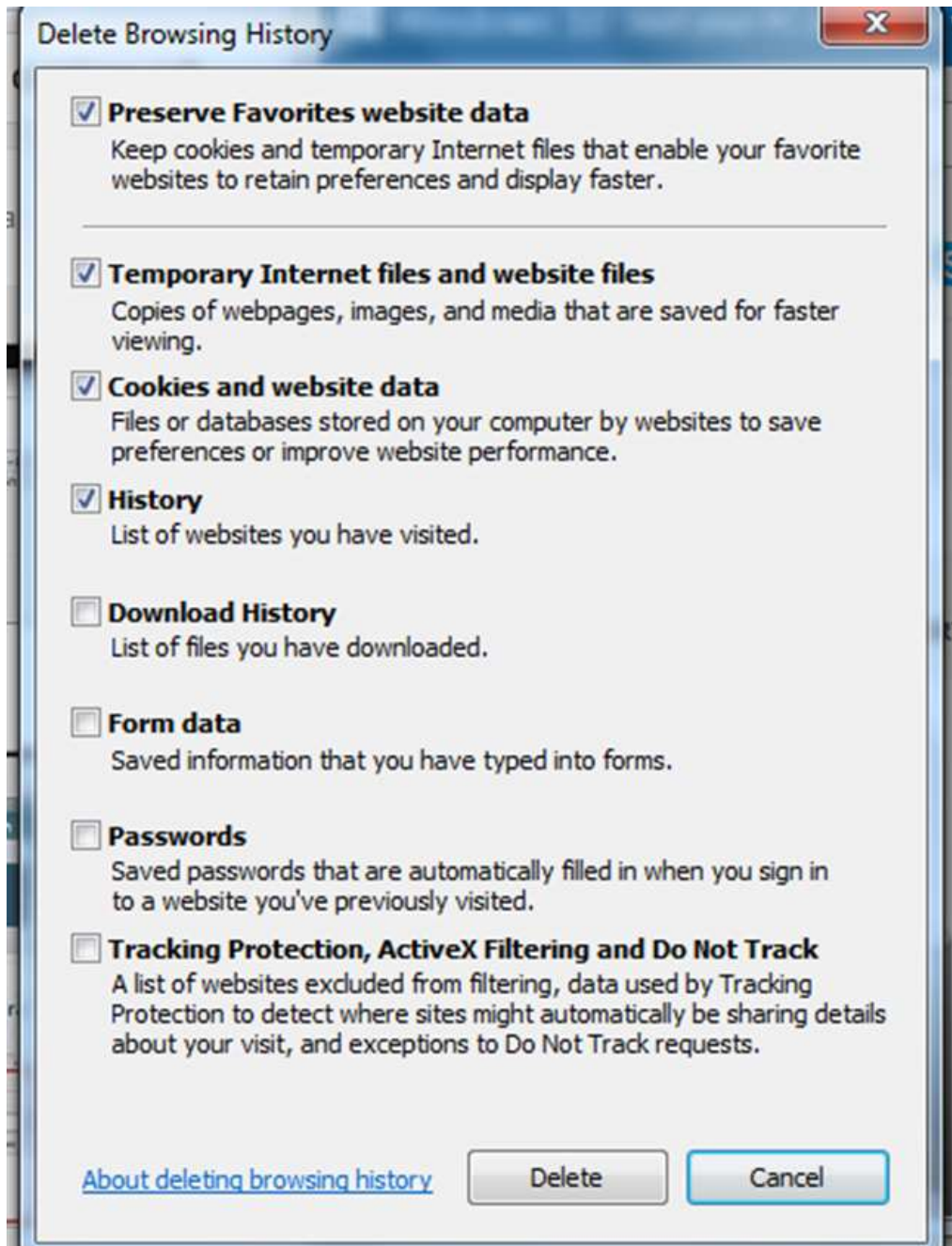
For security reasons that you think are right, the cookies can be disabled or deleted and it varies according to the Internet browsers.

Internet Explorer

You can use the following steps to clear cookies in the Internet Explorer.

- **Step 1:** Press Start.
- **Step 2:** Click Control Panel.
- **Step 3:** Double click Internet options.
- **Step 4:** Under the General Tab, you will see 'Delete temporary files, history, cookies, saved passwords...' Click Delete.

- **Step 5:** The Delete Browsing History dialog box will appear, click the 'cookies' checkbox
- **Step 6:** Click delete button at the bottom of the dialog box
- **Step 7:** You will be taken back to the Internet properties dialog box. Click 'ok'.

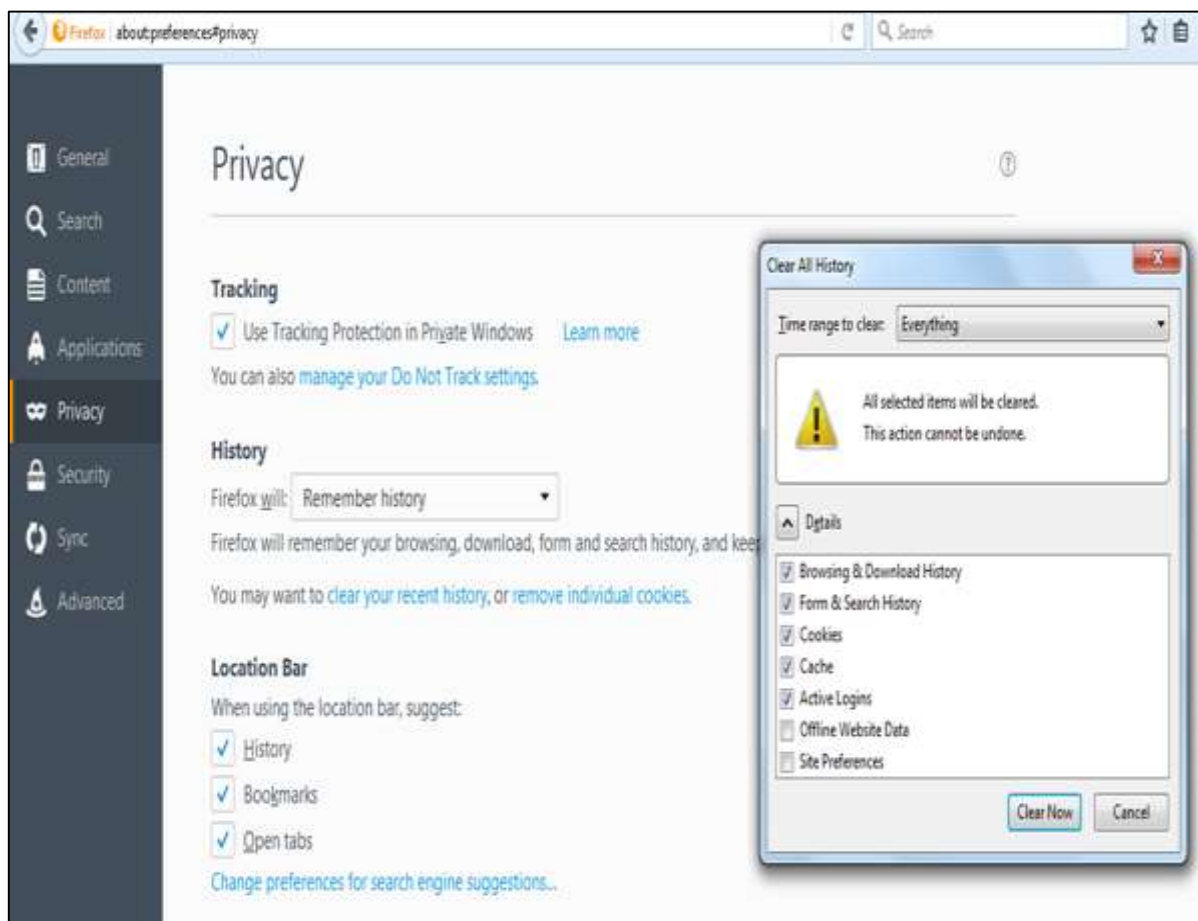


Firefox

Keep in mind that the more popular a browser is, the higher the chance that it is being targeted for spyware or malware infection.

- **Step 1:** Look at the top end of your Firefox window and you will see a 'Firefox' button. Click on it and click 'Options'.

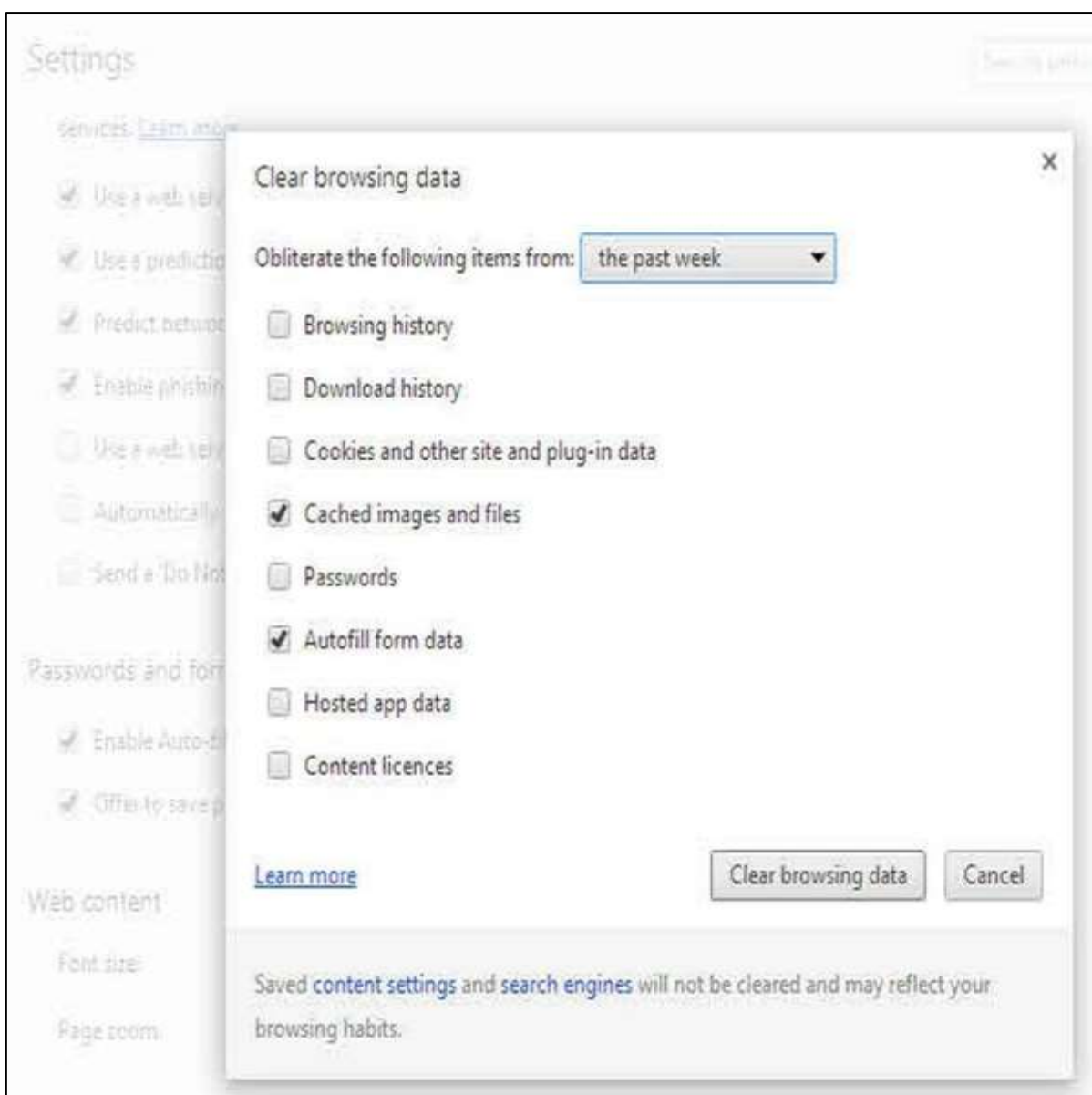
- **Step 2:** Click on 'Privacy'.
- **Step 3:** You will see 'Firefox will:' Set it to 'Use custom settings for history'.
- **Step 4:** Click on the 'Show Cookies' button on the right side.
- **Step 5:** If you want to delete cookies set by individual sites, enter the complete domain or partial domain name of the site you want to manage in the search field. Your search will retrieve the list of cookies set for that site. Click 'Remove Cookie'.
- **Step 6:** If you want to delete all cookies, click the top of the Firefox window and click on the Firefox button. Click on the History menu and pick out 'Clear Recent History...' Select 'Everything' for the 'Time Range to Clear' option. Then click on the downward arrow located next to 'Details'. This will open up the list of items. Click 'Cookies' and make sure all the other items are unselected. Click on the 'Clear Now' button at the bottom. Close your 'Clear Recent History' window.



Chrome

- **Step 1:** At the top right hand side of your browser toolbar, click on the Chrome icon.
- **Step 2:** Click on Settings.

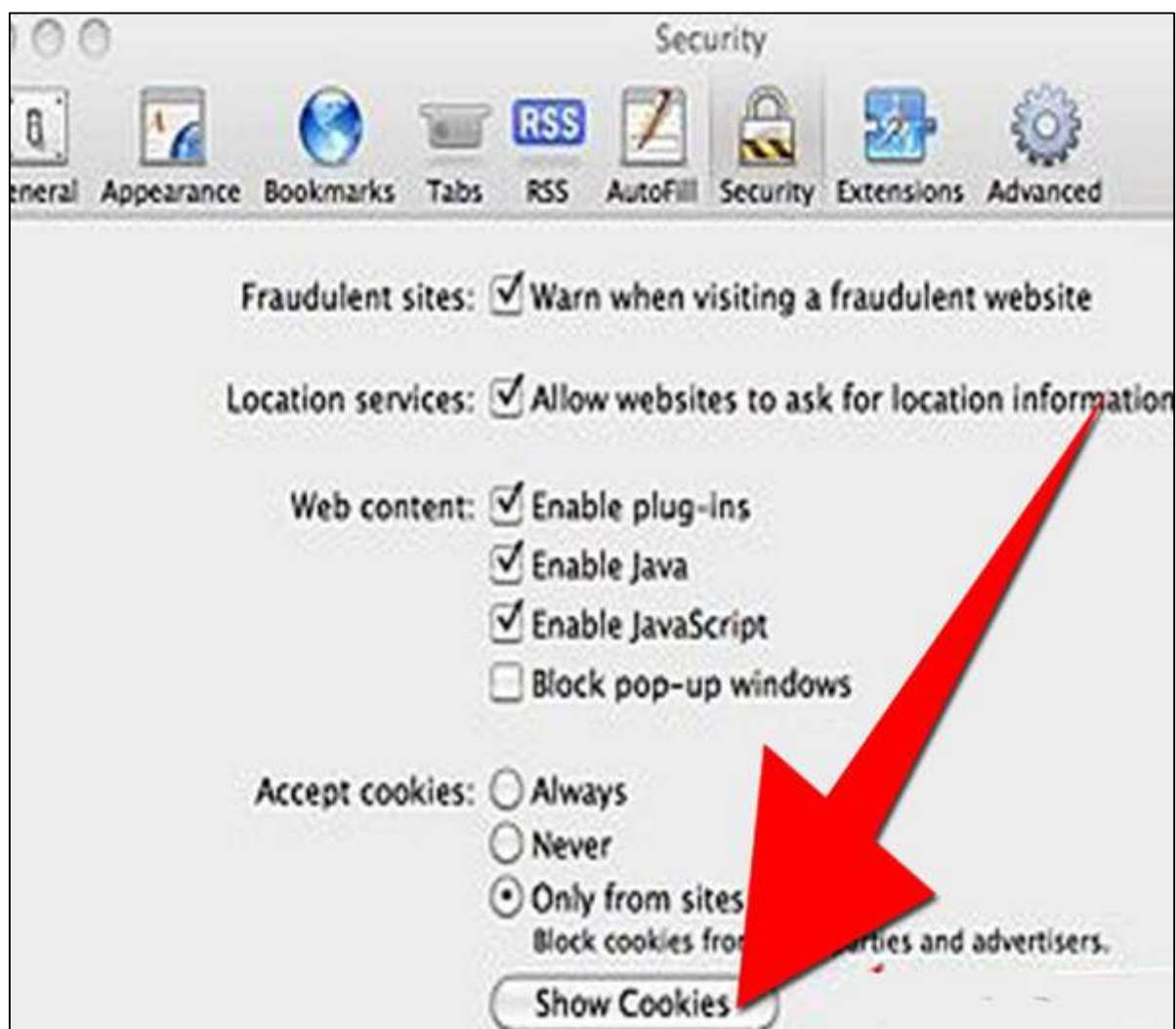
- **Step 3:** Scroll to the bottom and click 'Show advanced settings'.
- **Step 4:** Under 'Privacy', you will see 'Content Settings', click on it.
- **Step 5:** Under 'Cookies', you will see 'All cookies and site data', click on this. Please note that you can block cookies altogether from being set on your browser by clicking 'Block sites from setting any data.' Unfortunately, many websites you browse will stop working if you do this. It is better if you just periodically clear your cookies manually instead of preventing them from being set by your browser.
- **Step 6:** You will see a full listing of all your cookies. You can click REMOVE ALL to clear all your cookies or you can pick a particular website and clear your cookies from that site.



Safari

This guide is for OSX Lion:

- **Step 1:** Open Safari.
- **Step 2:** Click Safari and then on Preferences. Click on 'Privacy'.
- **Step 3:** Click on 'Details'.
- **Step 4:** You will see a list of websites that store cookies. You can remove single sites by clicking the 'Remove' button and selecting a site. If you want clear all cookies, click 'Remove All'.
- **Step 5:** When you have finished removing sites, click 'Done'.



Opera

Step 1: Click 'Settings' at the top of the Opera browser.

Step 2: Click 'Preferences' and select 'Advanced'.

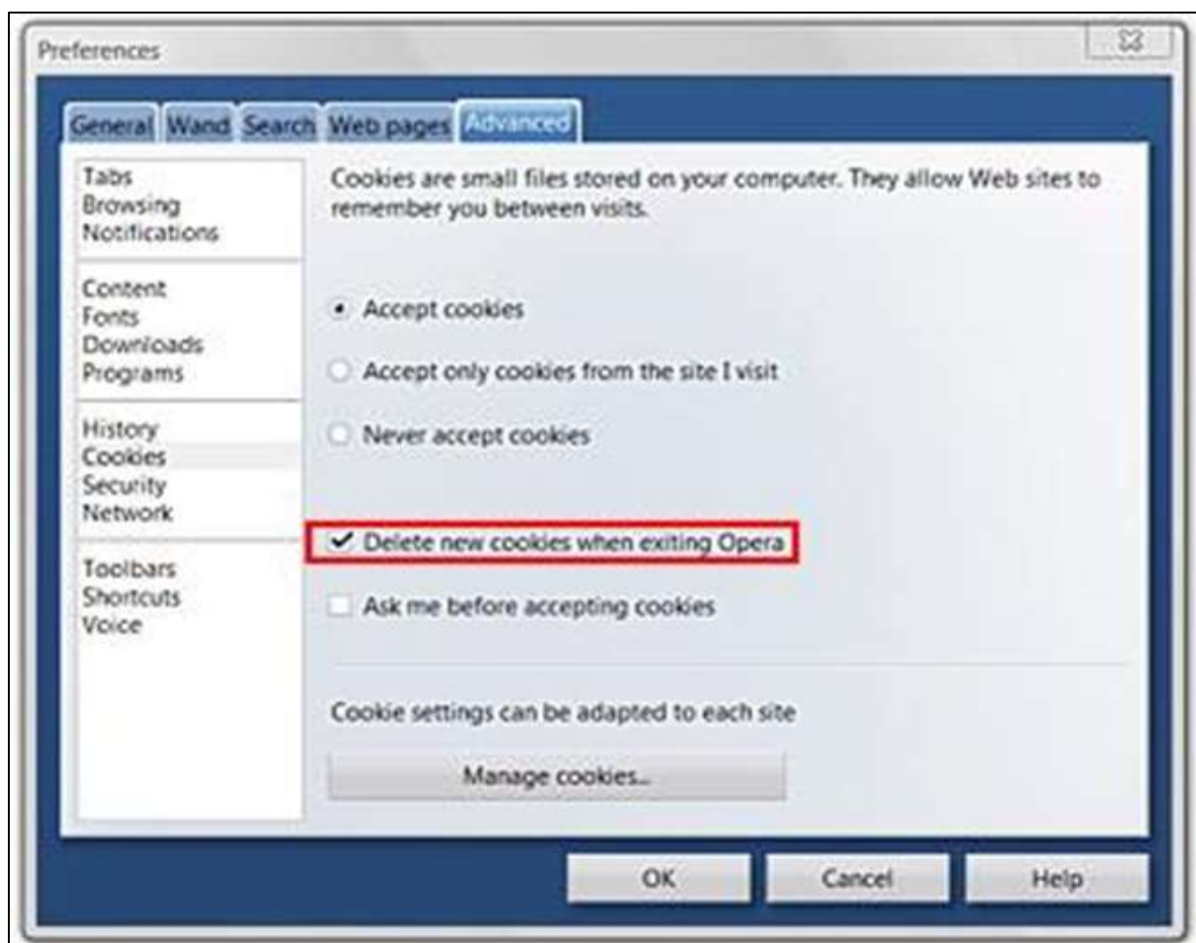
Step 3: In the 'Advanced' screen, select 'Cookies'.

Step 4: At this point, you can select one of three options:

- Accept all cookies (this is the default setting)
- Accept cookies only from sites you visit and
- Never accept cookies.

If you block cookies, most of the sites you visit will stop working. This is usually not a good choice. Your best default choice is to accept cookies only from sites you visit. This blocks cookies set by advertising networks and other third party sites. These third party sites set cookies to track your movements across sites to enhance their ad targeting capabilities.

Step 5: Select 'Delete new cookies when exiting Opera'. If you want to use a specific website but don't want to keep any cookies for that site between your visits, select this option. It is not a good idea to use this option for sites you visit frequently.



3. Internet Security – Phishing

Many of us have received similar emails as shown in the following screenshot. They appear as if coming from a genuine source, but in fact if we analyze them a little carefully, they are not. Such emails are called “phishing” because it depends on the users whether they will follow the procedure that the scammer is requesting or if they (user) will delete that email and be safe.



The links in the email may install malware on the user's device or direct them to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details. These techniques are too much in use with cybercriminals, as it is far easier to trick someone into clicking a malicious link in the email than trying to break through a computer's defenses. Although some phishing emails are poorly written and clearly fake.

How to Detect a Phishing Email?

There are several ways to detect a Phishing Email, some of these methods are discussed here for better understanding.

Spelling and Bad Grammar

Cyber criminals generally make grammar and spelling mistakes because they use dictionary too often to translate in a specific language. If you notice mistakes in an email, it might be a scam.

Links in Email

Links in the email are always with hidden URLs, you don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the following example the link reveals the real web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's web address.



Links also may redirect you to .exe, or zipped files. These are known to spread malicious software.

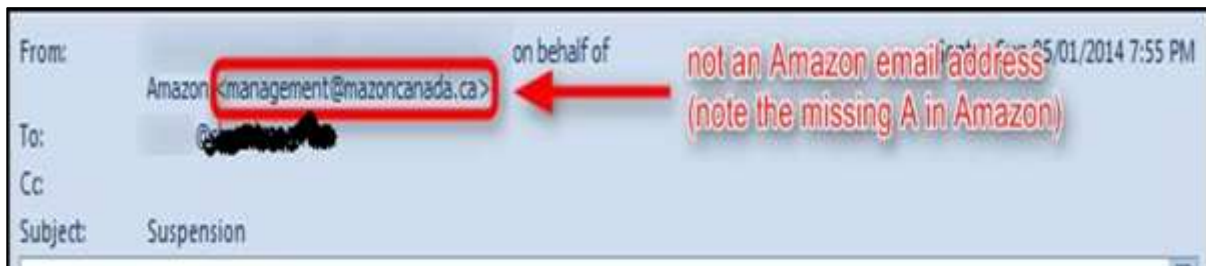
Threats or They are too Good to be True

Cybercriminals often use threats that your security has been compromised. The above screenshot shows it very well. In our case the subject talking about Suspension.



Spoofting Popular Websites or Companies

Scam artists use graphics in email that appear to be connected to legitimate websites, but actually they take you to phony scam sites or legitimate-looking pop-up windows. In our case, there is this email of Amazon which is not a genuine one.



Salutation

Generally, if it is genuine you will have a personalized email like Dear Mr. John, but the cybercriminals, they don't know your name except the email address, so they will use just a part of your email in the salutation or a general salutation.



Got Phished by Mistake?

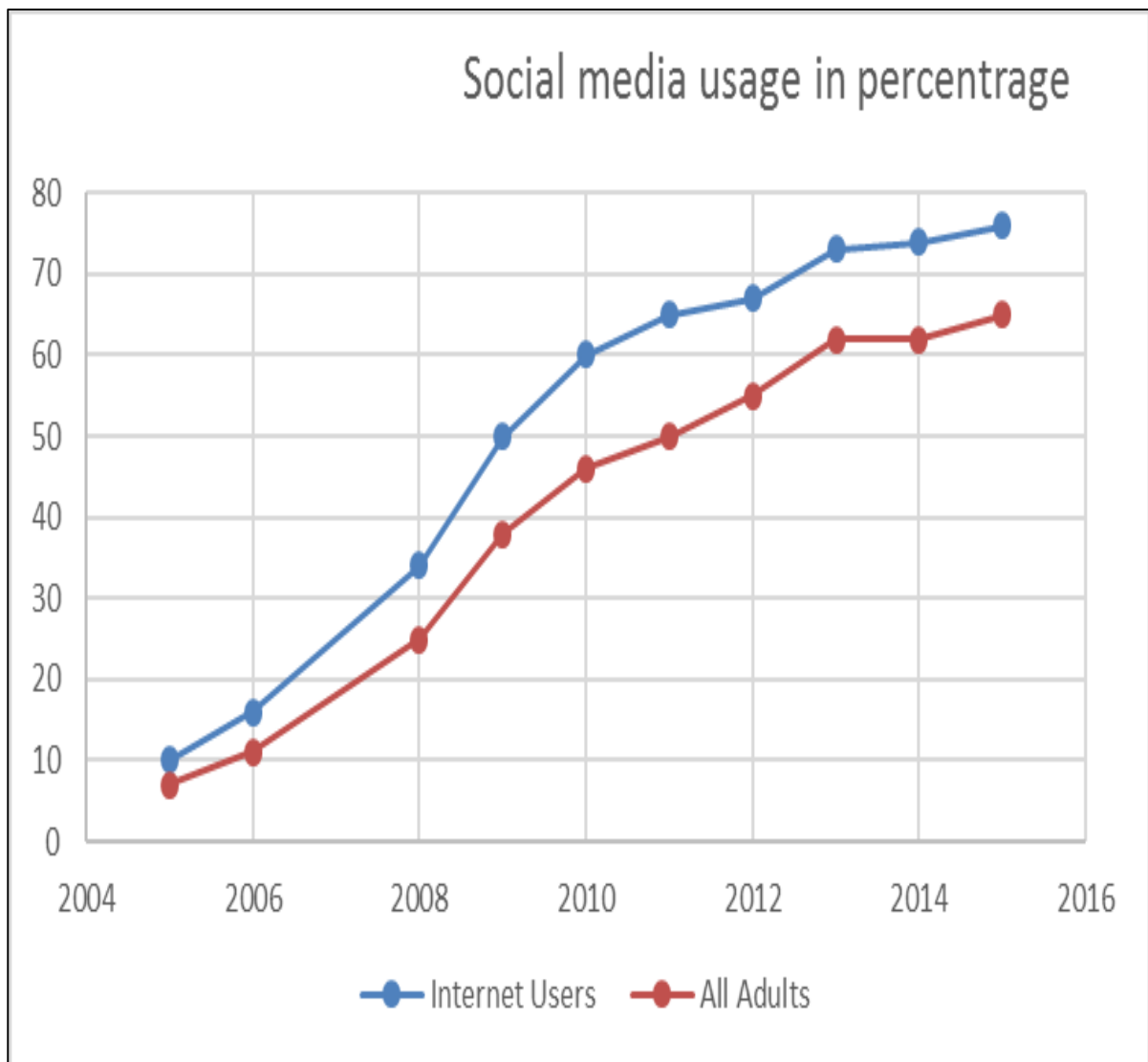
What to do in case you think that by mistake, you got phished? In such a case, you can take the following measures:

- Change the passwords immediately of the account that you think has been hacked.
- Check if any money has been withdrawn or any payment done through your account. You can contact your financial institution directly for this.
- Contact the authority on whose behalf you got that email. You should also report to your account administrator.

4. Internet Security – Social Network

Social Networking is the use of Internet based on social media systems to get in touch with family, friends, customers, classmates, etc. Social Networking can be done for social purposes, business purposes or both. The programs show the associations between individuals and facilitate the acquisition of new contacts.

Social Networking is becoming more and more popular nowadays. For better understanding of its popularity, see the following graph.



As you can see two thirds of the population are using social media which makes it very attractive for cybercriminals. They can hack an account of others and make profiles for different purposes which can be used as a bridge to attack their social network, or to get their data.

Profile Impersonation

The top threat for year 2015 in social media was **Profile Impersonation**. Many of us have seen in Facebook the fake profiles of someone that we know. This generally is made into a phishing link to your known social network. One precaution to avoid such phishing is to report the fake account immediately and let the concerned authorities take action. If you accept the friend request sent by such a fake profile, all your personal photos and other data can be stolen from your account and the hacker can use it in different ways.

5. Internet Security – Chrome

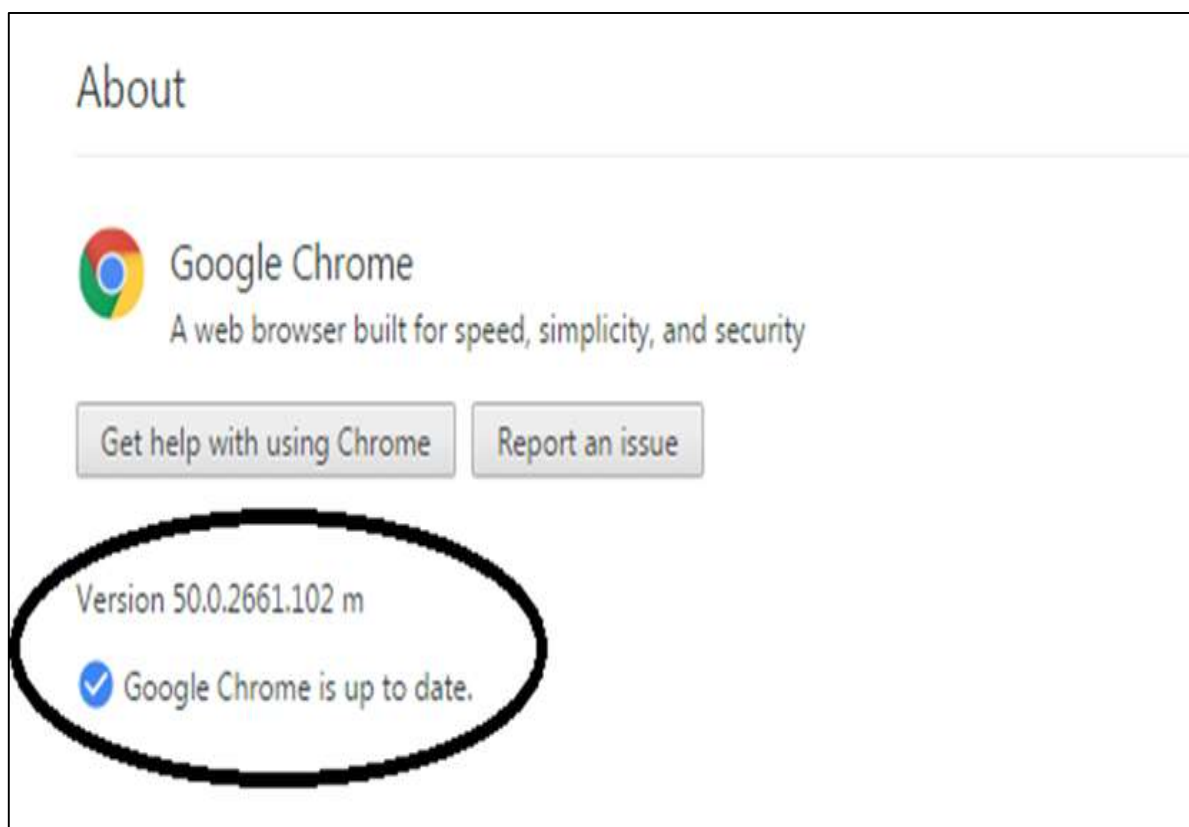
In this section, we will see the most used explorer from the security viewpoint. What settings should it have in order to minimize the attack surface that can come from visiting different webpages which might be infected.

To download the latest Chrome version, go to the following link and download it – <https://www.google.com/chrome/browser/desktop/index.html>

After installing, we need to secure the Chrome browser by following these steps:

Enable Automatic Update Downloads

Google Chrome automatically updates every time it detects that a new version of the browser is available. The update process happens in the background and doesn't require any action on your part. To check whether there is an update, go to **Menu – Help – About Google Chrome**.



Block Pop-Ups

To block pop-ups, go to Menu -> Preferences -> Show advanced settings... -> click the Privacy/Content Settings button. Scroll down to Pop-ups, chose "Do not allow..."

This setting will block any webpage that wants to show a pop-up without your permission.



Block Plug-In

To block plug-ins, go to Menu -> Preferences -> Show Advanced Settings... -> click the Privacy/Content Settings button. Scroll down to Plug-ins, chose "Detect and run important..."

This setting sometimes can put the chrome browser at risk.



Set your browser to not set passwords

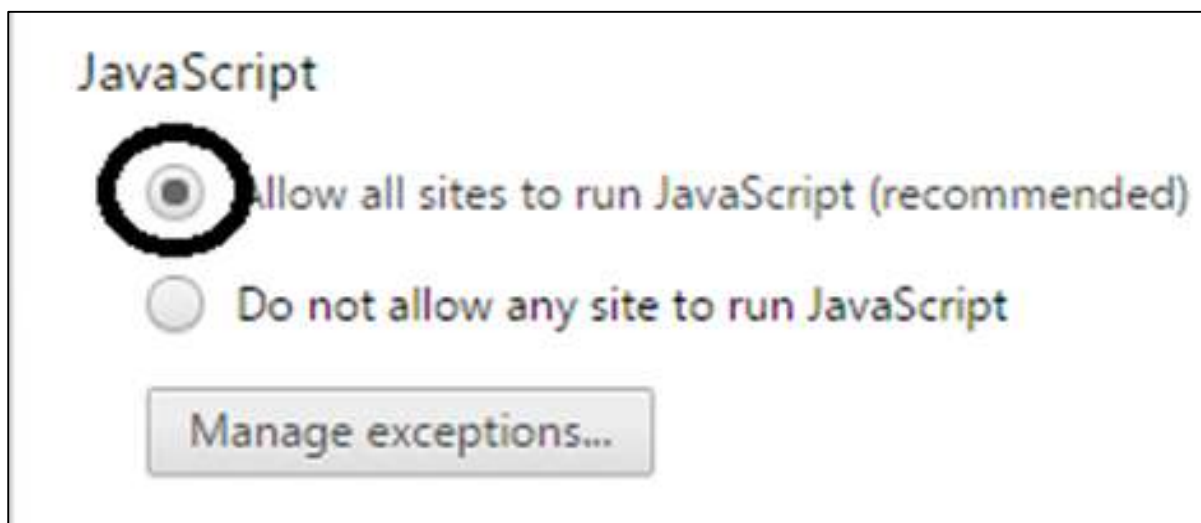
Go to Menu -> Preferences -> Show advanced settings... -> under Passwords and forms, uncheck the "Enable Autofill..."

This will help you in a way that if any unauthorized user gains access into your computer, they will not have the chance to auto log in webpages that request your username and password.



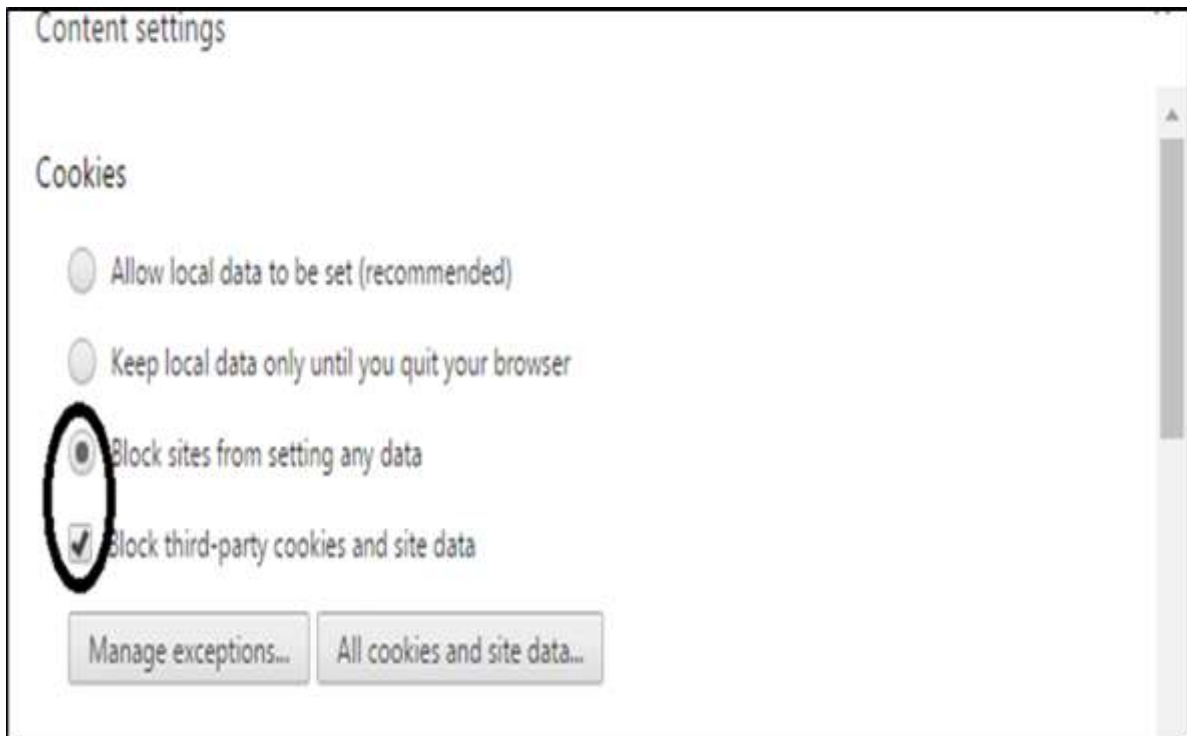
Java/JavaScript

Go to Menu -> Preferences -> Show advanced settings... -> click the Privacy/Content Settings button. Under JavaScript, chose "Allow all sites..."



Block Cookies

Go to Menu -> Preferences -> Show advanced settings... -> click the Privacy/Content Settings button. Under Cookies, choose "Block sites..." and "Block third-party...". This will block the cookies to send information to the servers that you don't trust.



Install Adblock plug-in

To do this, go to menu -> Settings -> Extensions -> Scroll to the bottom -> Click "Get more extensions" -> search for Adblock -> Install AdBlock by getadblock.com which is very good and very effective.



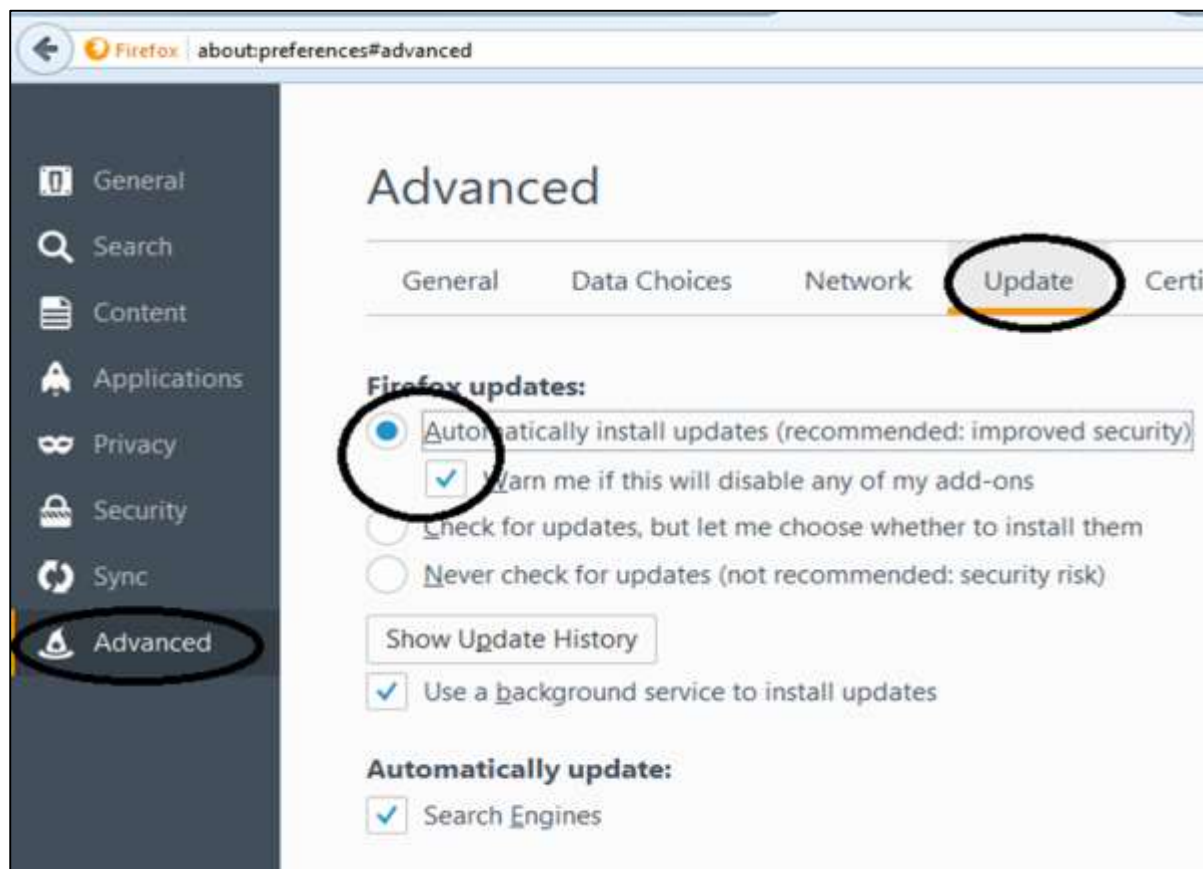
6. Internet Security – Mozilla

To download the latest Mozilla Firefox browser version, you can click on the following link – <https://www.mozilla.org/en-US/firefox/new/?scene=2&f=79>

Then after installing it, we need to secure the Mozilla browser by following these steps:

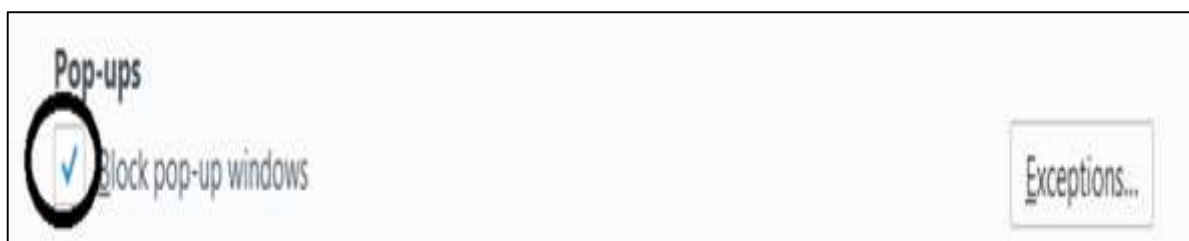
Auto-install the updates

You can auto-install the updates by going to Menu -> Options -> Advanced -> Update Tab. Check all the checkboxes and select "Automatically install..." & "Warn me...".



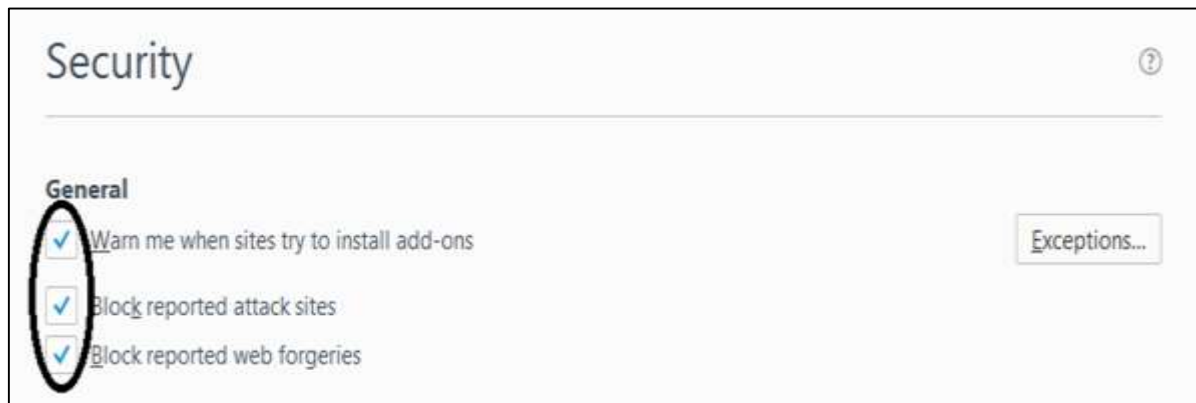
Block Pop-ups

To block pop-ups, follow the path Menu -> Options -> Content. Make sure the first two boxes are checked (Block pop-ups & Load images).



Block add-ons/phishing

Go to Menu -> Options -> Security. Check the top three boxes that start with "Warn me..." and "Block..."



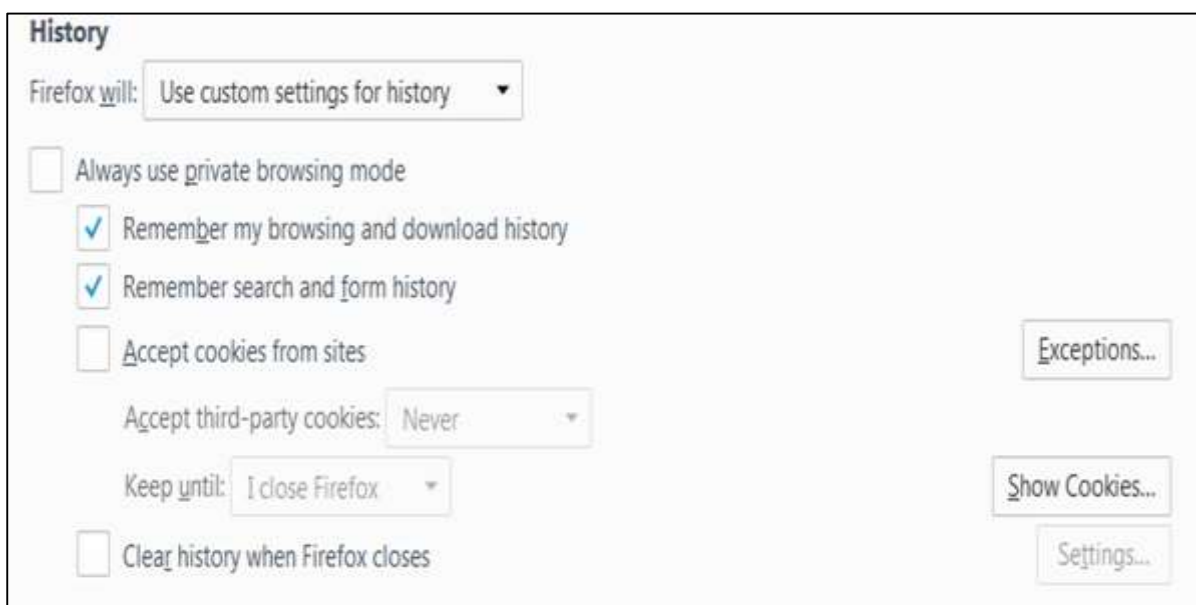
Set to forget passwords

Go to Menu -> Options -> Security. Uncheck the "Remember logins..." box.



Blocking Cookies

To block cookies, go to Tools Menu -> Options -> Privacy -> History -> Check the "Remember..." box under and uncheck "Accept Cookies from sites".



Install Adblock Plus

Get Add-ons – type Adblock plus created by Wladimir Palant.



Adblock Plus 2.7.3
By Wladimir Palant

Blocks annoying video ads on YouTube, Facebook ads, banners and much more.

Adblock Plus blocks all annoying ads, and supports websites by not blocking unobtrusive ads by default (configurable).

Adblock Plus allows you to regain control of the internet and view the web the way you want to. The add-on is supported by over forty filter subscriptions in dozens of languages which automatically configure it for purposes ranging from removing online advertising to blocking all known malware domains. Adblock Plus also allows you to customize your filters with the assistance of a variety of useful features, including a context option for images, a block tab for Flash and Java objects, and a list of blockable items to remove scripts and stylesheets.

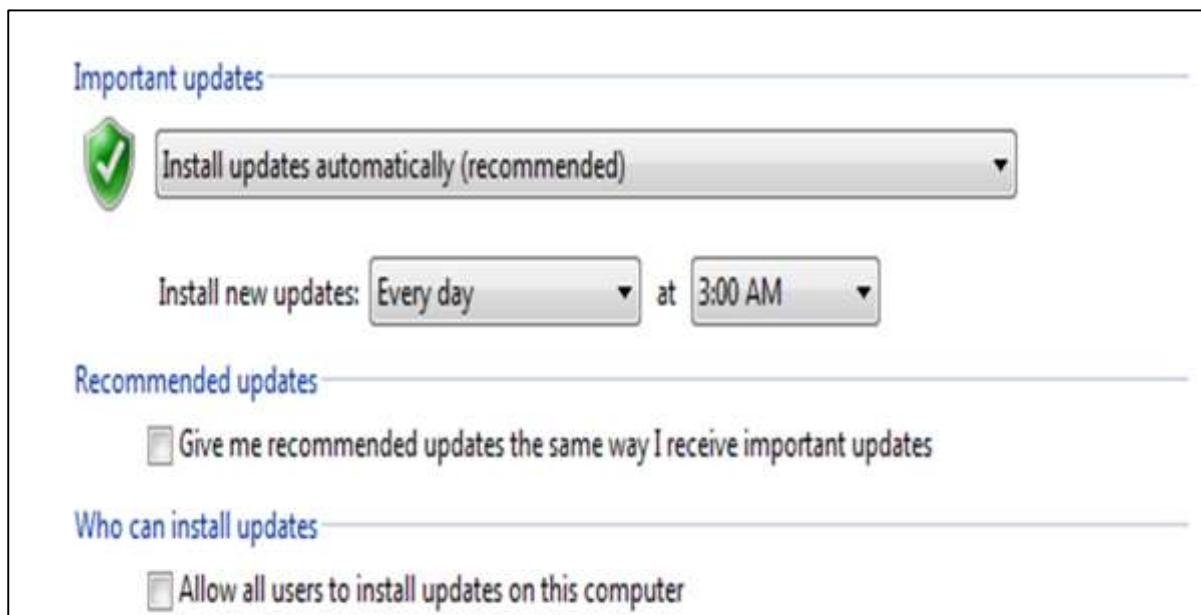
Starting with Adblock Plus 2.0 there is an option in Filter Preferences to allow some non-intrusive advertising. The goal is to support websites using non-intrusive ways to advertise and to encourage more websites to do the same. Read more

7. Internet Security - Internet Explorer

Internet explorer is the browser of Microsoft and by default is incorporated with Windows OS and doesn't work on other Operating Systems.

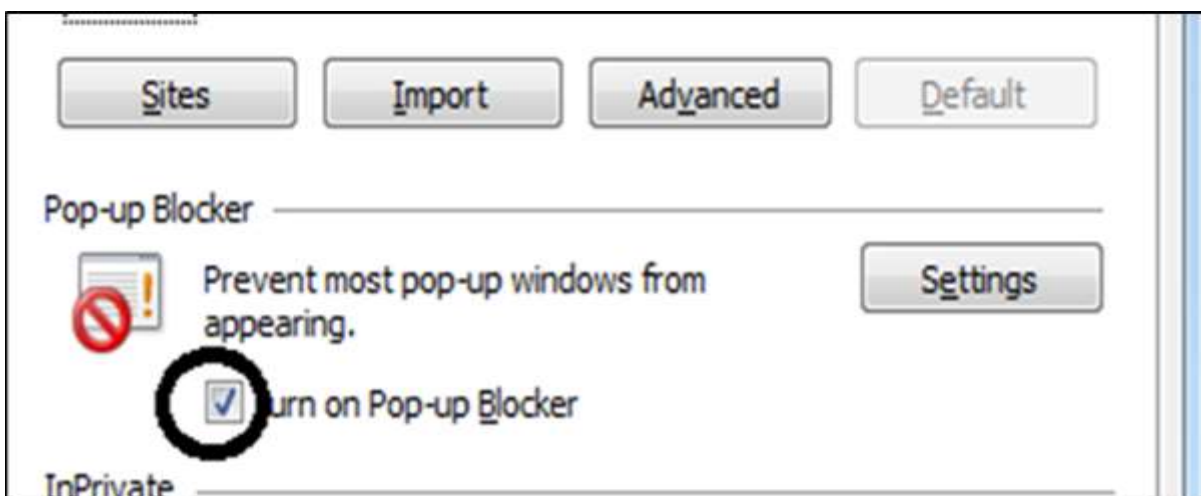
Auto-download Updates

Updates for Internet Explorer are handled by Windows Update located in Control Panels. Set it to Daily updates as shown in the following screenshot.



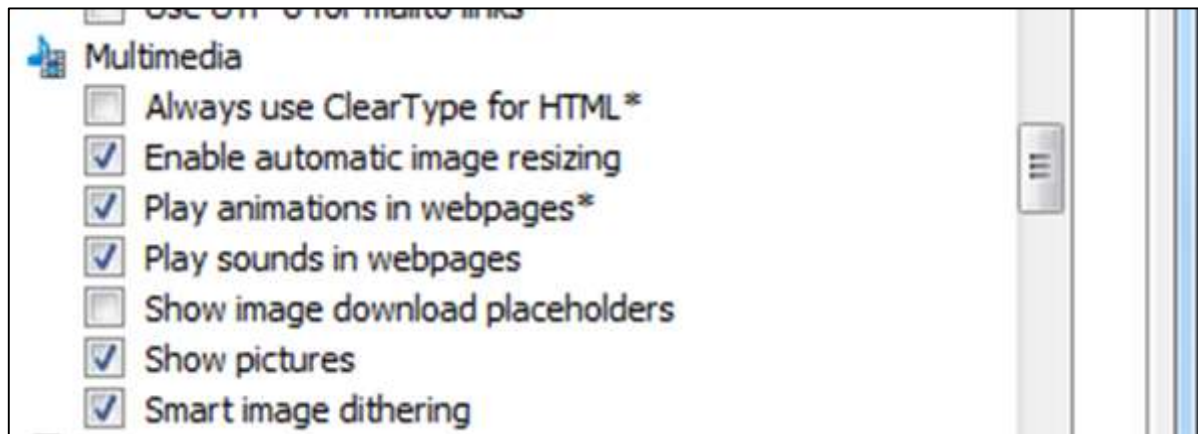
Block Pop-ups

To block pop-ups, go to Tools Menu -> Internet Options -> Privacy tab and set the slider to MEDIUM. Check the "turn on pop-up blocker" box.



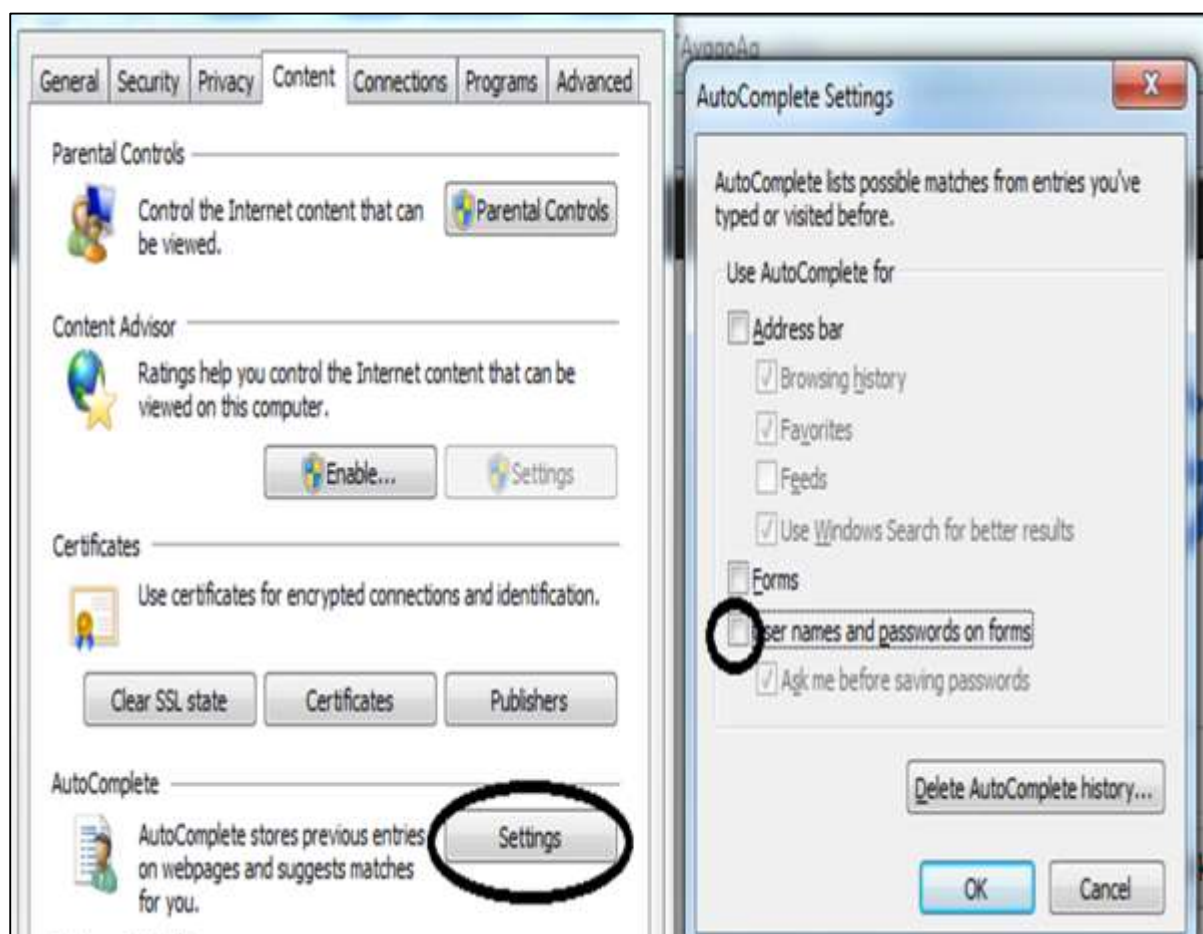
Block Plugins

To block plugins, go to Tools menu -> Internet Options -> Advanced tab and scroll down to Multimedia. Uncheck "Play animations" and "Play sounds" in webpages if they are checked.



Delete Passwords

Go to Tools menu -> Internet Options -> Content tab and click the AutoComplete Settings button and uncheck the "user names and passwords..." box.

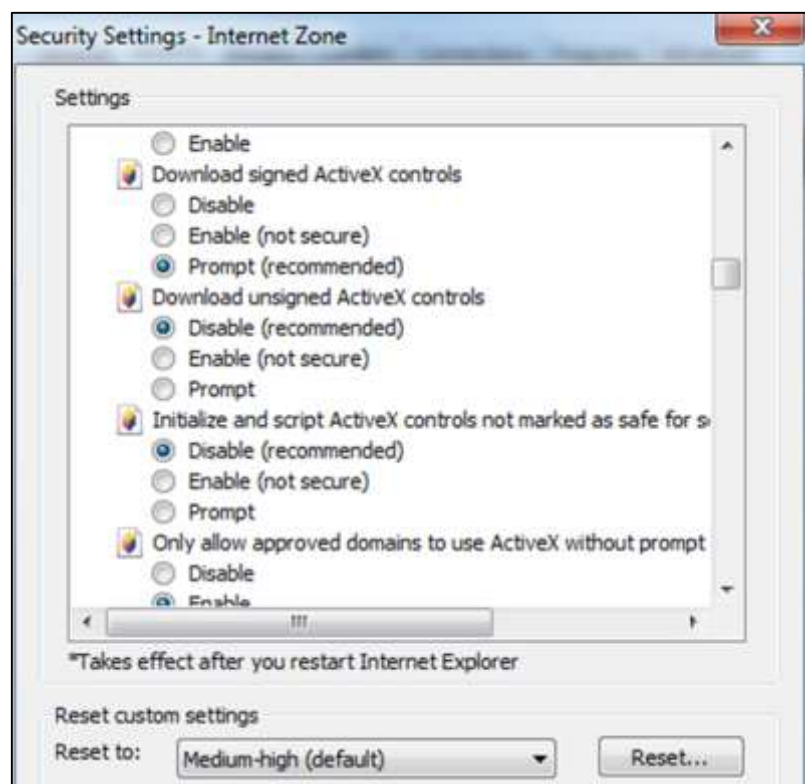


Block Cookies

To block cookies, go to Tools menu -> Internet Options -> Privacy tab and click the "Advanced" button. Check the "Override" box and the "Accept" button for First-party cookies and "Prompt" button for Third-party cookies. The "Always allow..." button should not be checked. Click OK. When done, click on Apply button.



The next step is to go to Tools Menu -> Internet Options -> Security -> Custom level -> Download unsigned ActiveX controls -> Disable (Recommended).

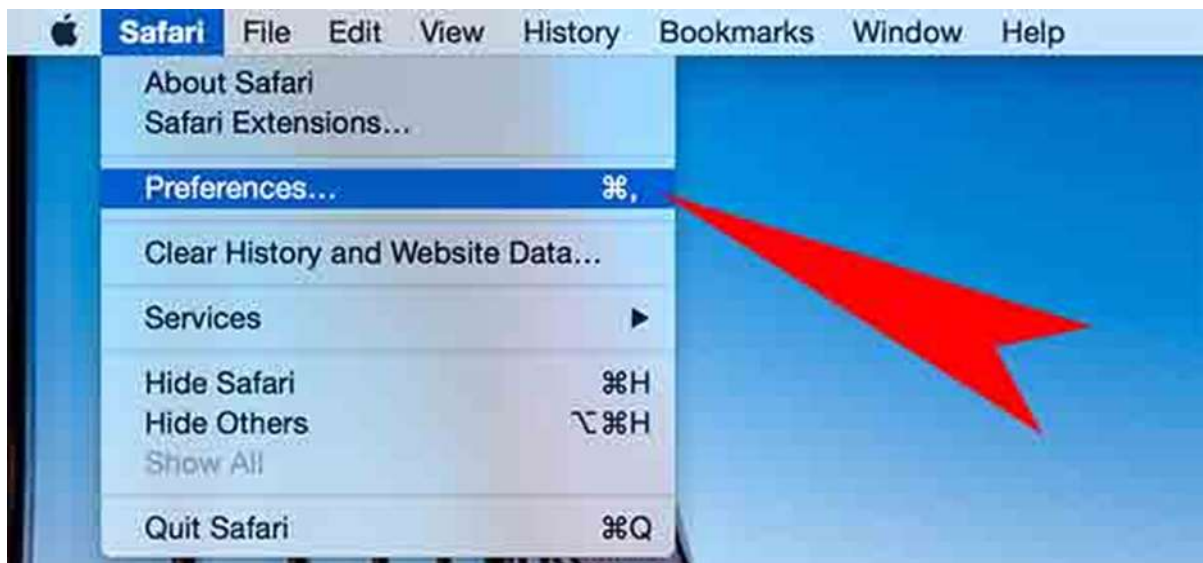


8. Internet Security – Safari

Safari is a web browser developed by Apple based on the WebKit engine. It comes included in the iOS and is said to be slightly different from other browsers.

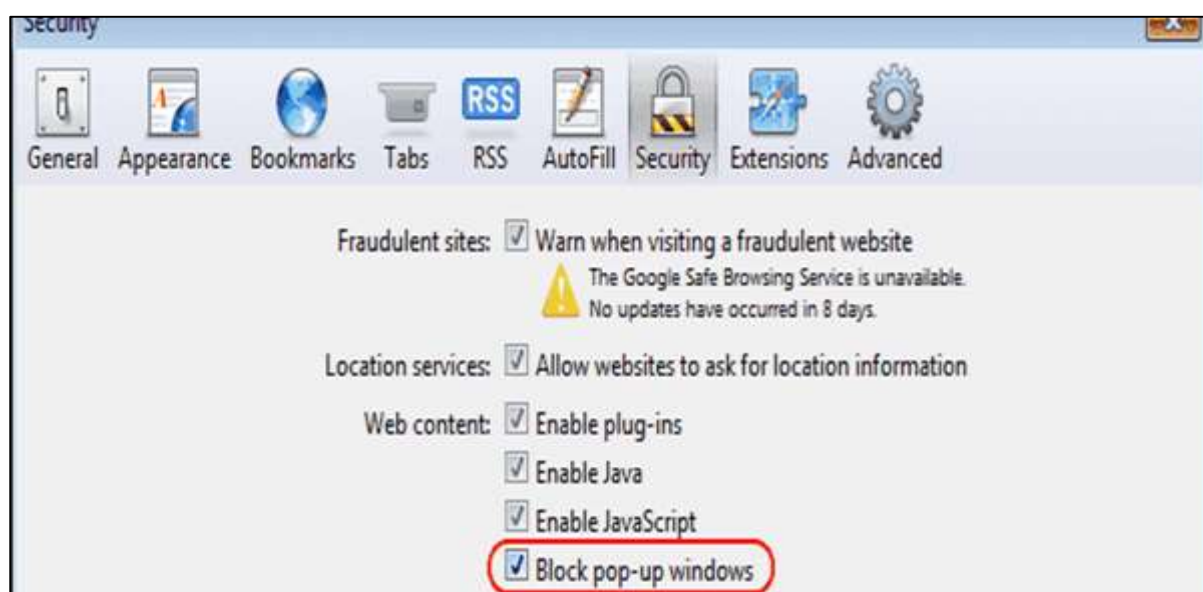
Auto-download Updates

Updates for Safari are handled by **System Preferences -> Software Update** located under the Apple menu. Set to Daily updates.



Block Pop-ups

Go to Safari Menu – Preferences – Security tab and make sure the “Block pop-up windows” box is checked.



Block Plugins/Phishing

Go to Safari menu -> Preferences -> Security tab and uncheck the "Enable plug-ins" box.

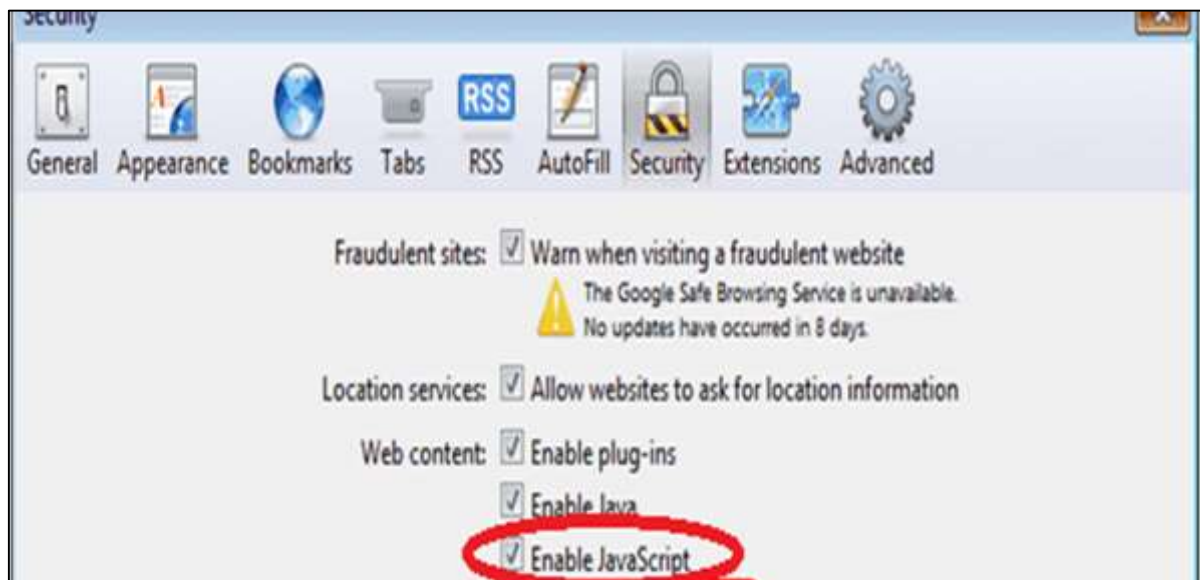
Delete Passwords

Go to Safari menu -> Preferences -> AutoFill tab and uncheck the "user names and passwords" box.



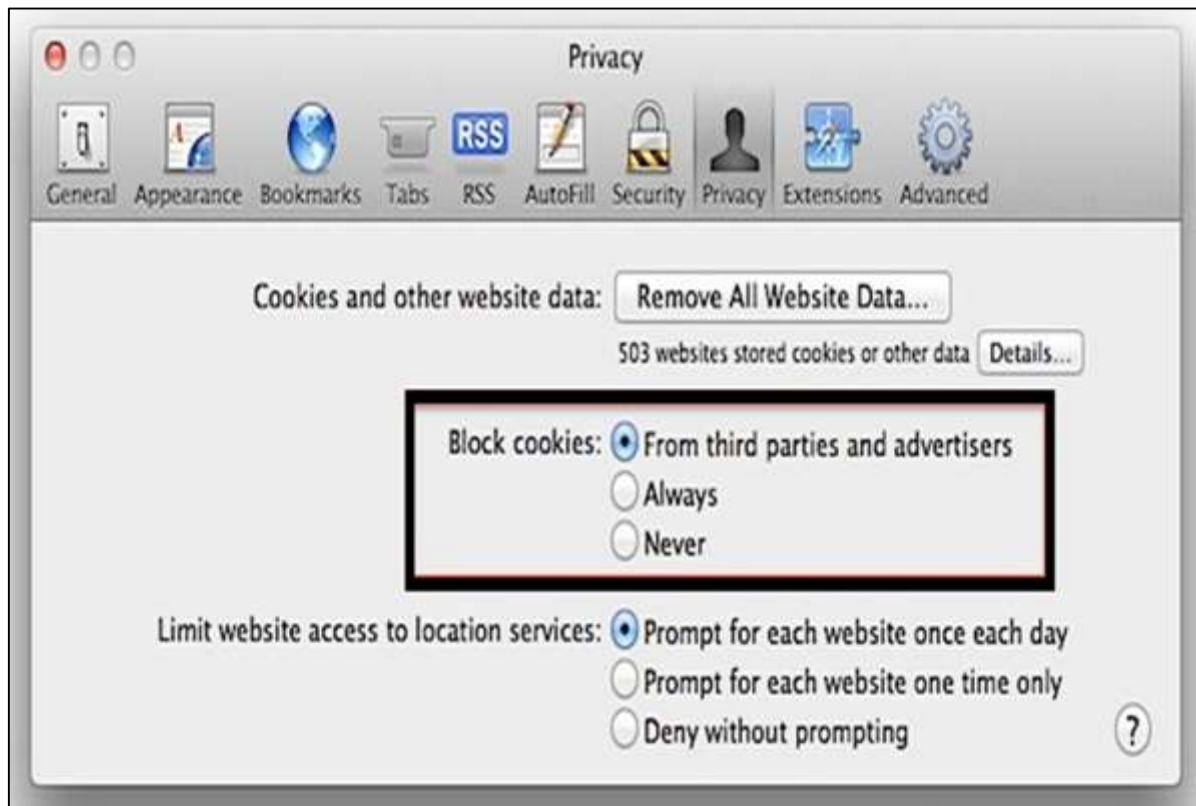
Java/JavaScript

Go to Safari menu -> Preferences -> "Enable JavaScript" checked.



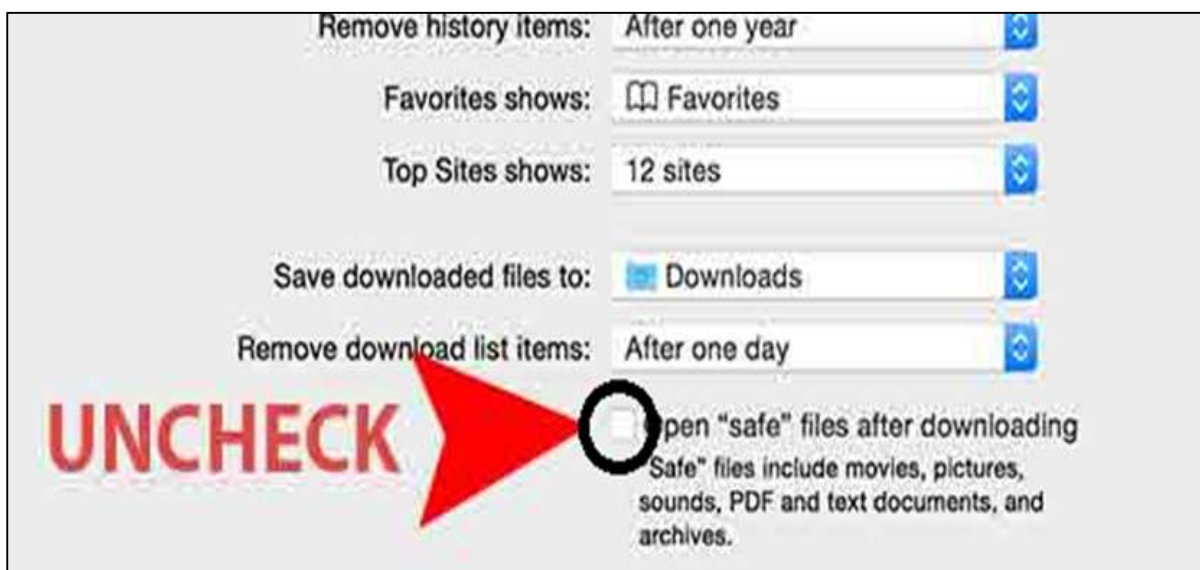
Block Cookies

Go to Safari menu -> Preferences -> Privacy tab and select "Block cookies: From third parties...".



Disable Auto-Open of Open Files

In Safari, you can choose not to open them after downloading, go to the Safari Menu - Preferences - General tab. Uncheck the box that says Open "safe" files...



9. Internet Security – Gaming

Online games are played over the Internet which can vary from complex graphics to multiple users. They involve many technologies most often use Java, Flash, etc. which is made possible using media streaming for user interaction. In general, online gaming utilizes various forms of socializing like forums, chat rooms, so this interaction with other users that some of them can be malicious may be hackers.

There are different types of online games:

- Single user playing game like Miniclip
- Multiple player games
- Cross-platform online game
- Real-time strategy game like Imperia
- Browser games which utilizes directly the Internet explorers

Risks from Online Games

Nowadays most of the online games are multiple user games and the risk that comes from other users are very high and are as shown below:

- **Viruses** – The player can be attacked from email attachments, phishing or instant messaging. This can result to the hacking of the user computer or the network.
- **Malicious Software** – Attackers can use online games to redirect the genuine users to a fake webpage to steal their credentials.
- **Hacking that comes from Hacked Gaming Servers** – This hacking can come when the server of the game has been compromised because of its vulnerability as a result this can put all the users in danger who are connected to this gaming server.
- **Insecure Game Coding** – This is another type of known vulnerability where all the data of users like name, surname, credit card information can be stolen because of an insufficient security on the programming code.

Social Risks

This risk comes from social interaction with other malicious users who want to steal your data which can be:

- Your personal Information
- Credit card details
- They can pretend to be a child and contact other children asking them to reveal other information.

Threats in Online Gaming

Threats at games are of different types and for different purposes which can be to gain unauthorized access to play the game generally. This technique is done by stealing others' password.

A few other very often used techniques are:

- Dictionary attack
- Social engineering
- Malware infection
- Corruption the genuine authentication software
- Phishing user ID and password by sending emails.

Hackers can cheat at the game for the purpose of:

- Stealing virtual property
- To obtain higher levels of plays
- Corrupting the gaming software which controls the levels of play
- Skipping the policies
- For making DoS to the gaming provider.
- Paying for the game by using Trojans to hack and steal the Card ID and other details

What to do for secure online game playing?

- Encrypt critical game data
- Minimize client's data
- Create a security tutorial for the players
- Complex password policy
- Audit trails and logs
- Patching bugs
- Always use an antivirus software on your computer.
- Be prudent when opening files and links sent by other users over instant messaging of game.
- Validate authenticity of the new release of software's.
- Create complex passwords.
- Update your computer. Connect securely with your browser.

10. Internet Security – Child Safety

In this section we will focus on Children's safety as the Internet is a fact for all of us and it interferes in our daily lives. We will discuss the practical steps that we need to take without bothering them (children) and some programs used for this purpose.

Why is it so Important?

Generally, children or teenagers like to participate in chat rooms or social media which offer chats too, for many reasons to express themselves, curiosity, talk to other children around the world and to share their experiences. But on the other side, the kids need to know that in this environment there are people with bad intentions too. So the kids can be potential victims to bullies, harassments, etc. Also they can reveal information regarding the family members to other unknown persons with bad intentions.

As Internet is a place where anonymity can remain for the moment, it is a dangerous asset for unsupervised children. A kid or a teenager can be seduced by a stranger, who is polite at first contact and is willing to listen to them but on the other side he can be a pedophile luring who's only aim is to have a meeting which can lead to a sexual assault.

Even a small information that can be given by the child can be very dangerous because the attacker can trace down the information given by the kid.

As mentioned in the games section, many of them allow for voice as well text chatting between sessions. Kids should be prudent while using gaming chats in the same way as they do for chat rooms and social media, and should be cautious of overly eager new friends who ask them insisting for their mobile phone number, their address, or a face-to-face meeting.

Social Rules Regarding Child Internet Safety

Here are a few simple pointers regarding child Internet safety.

The computer should be placed in the living room with the monitor facing towards the room so there nothing to hide. Always check if your child quickly changes the screen when you pass by, or is hiding files or disks — someone may have sent them inappropriate content like pornography.

Discuss with your child exactly what is OK and what is not OK regarding what kind of websites are appropriate for them, which chat rooms to visit, and what kinds of things they can talk about there. Only let your kids use monitored chat rooms. Avoid ".alt" chat rooms — they focus on alternative topics that may be inappropriate for kids. Get to know your child's online friends as you do with their school and neighborhood friends. Surf the web and chat online yourself so you understand what it is that your child is doing.

Make clear to your child that they need to **tell you if they receive any upsetting messages** while chatting, and that you will not be angry with them and ban the Internet as a result. Make it clear to the child that you understand that they cannot control what other people say to them and that they are not to blame if this happens.

Set time limits for Internet usage – Software is available that enforces these limits which we will see in another section. Usage time should not be at late night. Do not permit your child to be left alone in cyberspace for long periods of time — this is when they are most vulnerable.

Tell your child that **people in chat rooms are always strangers** who can potentially harm – No matter how often they chat with them, and no matter how well they think they know them. Tell them that people can lie about who they are, and their new friend can be a grown up instead of a 12-year-old child.

Never reveal personally identifiable information – This can be their real name, gender, age, school, phone number, or where they live. Have them use a chat pseudonym that is non-provocative and does not hint at who they really are in reality. They must also watch other people's personal information, such as friends' names and phone numbers.

Don't let your kids open attachments to email messages from friends or file-sharing services without you being there to approve and scan the content for viruses.

Tell the kids that it is important **not to meet online friends face to face without your knowledge**. Determine the person's true identity before permitting any meeting and if they are not sure they should ask you. Make sure such meeting happens in a public place, and accompany them.

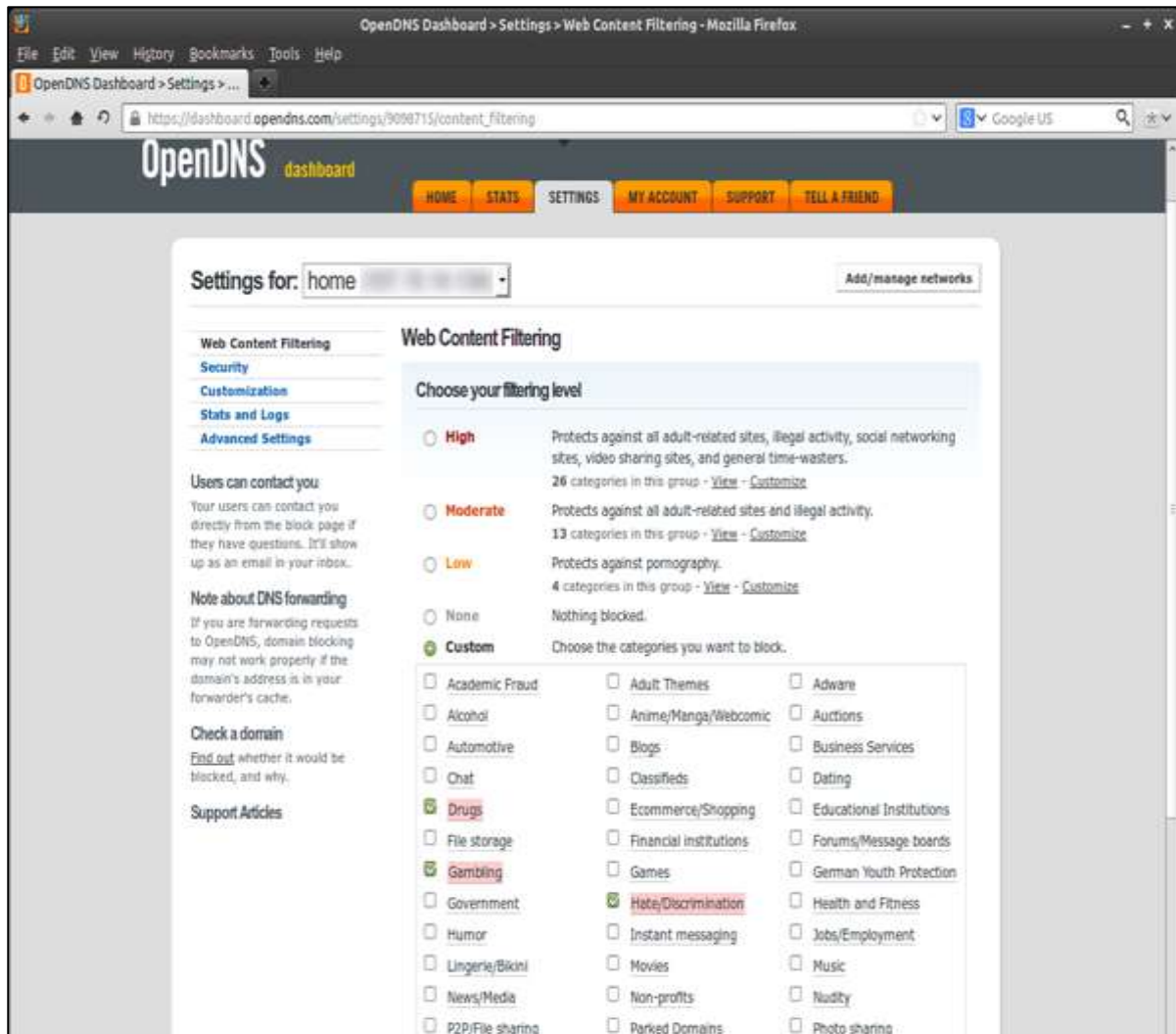
Use programs to save writing logs – Most chat programs allow you to block a user by right-clicking on their name in your contact list and choosing the "Block" or "Ignore" feature. In the next section we will see what software's we should use.

Use Software to Keep Track

Here is a list of software that are helpful in keeping a track of what is being viewed on your computer.

OpenDNS

The first one in the list is OpenDNS, which can be easily downloaded from the following link – <https://www.opendns.com/home-internet-security/>. It has a free version and it allows the parents to filter all web content of all the devices that are connected to the network, this filters allow parents to select categories and add new webpages to be blocked as it can be entered in the monitoring mode, so you allow the child to navigate for the first hour and then you block all the webpages that you think are not good.



ContentWatch Net Nanny 7

This product can be bought through – <https://www.netnanny.com/products/netnanny/>. As per the PCMagazine, it is a very good product and it offers all the features that a parental control software needs like Internet filter based on categories and time management. The Internet navigation can be set to a specific limit for all the day.

Another option it has is to mask profanity; it hides all the vulgar language in the webpages. Then it has social media monitoring as it alerts you for all the new friends of your child along with the chats, messages and user profiles. It also creates a limited profile for your child and as a remote administrator you can check remotely the reports of navigation. But the computer will be the base installation.

Net Nanny Users Family Reports Requests Devices Help Logout

Reports View reports on your account to better inform your decisions.

Everett family

Summary - Pornography - www.gigantits.com

Today Last 7 Days Last 30 Days

Page Title / URL	Actions	Users	Date	Devices
GIGANTITS! Movies of Women with BIG ... http://www.gigantits.com/	Blocked	Clementine	Sep 4, 2014 8:44:32 AM PDT	asus Nexus 7
GIGANTITS! Movies of Women with BIG ... http://www.gigantits.com/	Blocked	Clementine	Sep 4, 2014 9:19:17 AM PDT	WIN-ER797ADCS70

Qustodio Parental Control 2015

It can be downloaded from <https://www.qustodio.com/en/>. This parental control software gives options like Internet filter based on categories and time management. The Internet navigation can be set to a limit for all the day, while application control and social media monitoring alerts you for all the new friends of your child and the chats and messages along with any new user profiles. It also creates a limited profile for your child along with a safe search technology.

QUSTODIO INTERFACE SUPERVISION FEATURES PROTECTION SETTINGS

Individual activity by user

ALEXANDER MONICA JOSEPH

Last 30 days
Alexander's Activity Summary
Last seen: June 27, 2012 - 7:49 AM

Activity Summary Activity timeline Web activity Social activity Rules

Time spent behind computer

Activity summary by day, week or month

Different activity views and rules

Since your last visit
Today
Last 7 days
Last 15 days
Last 30 days

11. Internet Security – Spamming

Spam is a form of email which is used to send to different email accounts and in general contains advertising about any product or services. But the real problem is when they contain malwares that can damage the user's data.

Generally, they are sent to a massive list of emails for the mail purpose that a small percentage of users might open them and respond. They are used to such treatment because they are cheap in infrastructure investment, not too much time consuming and simple.

Techniques Used by Spammers

In this section, we will discuss the different techniques used by the spammers.

- **Domain Spoofing** – The spammer sends an email on behalf of a known domain so the receivers think that they know this person and open it.
- **Poisoning Filters** – A filter can be poisoned by adding text with the same color of the background to reduce the scoring of the filters.
- **Directory Harvesting** – In directory harvesting, spammers generate email addresses by using known email addresses from corporates or ISP (Internet Service Provider).
- **Social Engineering** – Spammers send promotional emails to different users such as offering huge discounts and tricking them to fill their personal data.
- **Junk Tags** – Spam Words can be hidden by including invalid HTML tags within the words.
- **Invalid words** – Special characters are inserted in the spam words. For example: V!AGRA.

Anti-Spam Techniques

In this section, we will discuss various anti-spam techniques and their advantages.

- **Signature Based Content Filtering:** Most anti-spam email companies use this type of filtering because it checks the received email with certain patterns after saving the message to the disk.
- **Naive Bayes Spam Filtering:** Bayesian filter scans the context of the e-mail when it looks for words or character strings that will identify the e-mail as spam.

- **Black Listing RBL:** This is a type of database that updates the IP address and domains based on a reputation and the system administrators who use these RBL don't receive email from domains that are blacklisted from this RBL.
- **Sender Policy Framework:** The IP address of the domain of the sender is compared with the genuine list of the IP addresses that the domain should have and if it is not same, then that email is dropped.

Anti-Spamming Tools

In this section, we will discuss different anti-spamming tools and their benefits.

Aevita

AEVITA Stop Spam Email – <http://www.aevita.de/web/stopspam/>

How it works: This tool will replace all your e-mail addresses on your page with specially encoded email addresses. The AEVITA Stop SPAM Email introduces codes that Spambots will "choke" on, but which a normal mailing program ignores. Therefore, people can still send you an email but spammers can't get your address!

Spam Experts

Spam Experts Desktops – <https://www.spamexperts.com/solutions/smes-private-users/desktop.html>

How It Works: It works as a spam filter with any email program and automatically intercepts spam. It does depend on specific keywords to detect spam, but checks the content of a message whether to accept or reject it. It also checks for filtering spam in the background and also it maintains a list of blocked senders.

Spameater

Spam Eater Pro – <http://www.hms.com/spameater.asp>

How It Works: It is also a spam email notification system, it reduces spam by 95%, it offers you a set of complex rules.

SpamWeasel

SpamWeasel – <http://www.mailgate.com/>

How It Works: It removes spam before it gets into the inbox. If it is suspected for spam but not sure, then it is stamped but not deleted. It supports POP accounts.

AntispamSniper

Antispam Sniper – <http://antispamsniper.com/outlook-plugin.html>

How It Works: AntispamSniper for Outlook provides professional antispam and anti-phishing protection for your mailbox. A combination of several methods for automatic email classification results in an excellent filtering quality with the minimum error rate. The plug-in has a built-in option allowing deleting spam from the server by headers. The good messages deleted by mistake from server by header can be restored within a certain period of time after deletion. The plug-in filters POP3, IMAP and Exchange accounts.

Spam Reader

Spam Reader – <http://www.spam-reader.com/index.shtml>

How It Works: Spam Reader is a free anti-spam add-on for Microsoft Outlook. The software uses the most reliable approach to block junk emails. The Bayesian Algorithm is based on statistical analysis, capable to be adjusted to user's needs and detect up to 98% of spam messages. The Spam Reader automatically scans all incoming mails and sends detected spam messages to the special folder for further review.

MailWasher

Mail Washer free – <http://mailwasher.net/>

How It Works: MailWasher is free to use and won't ever expire. It works with Outlook, Outlook Express, Incredimail, Thunderbird, Windows Mail, GMail, Hotmail and every other email program.

12. Internet Security – Chatting

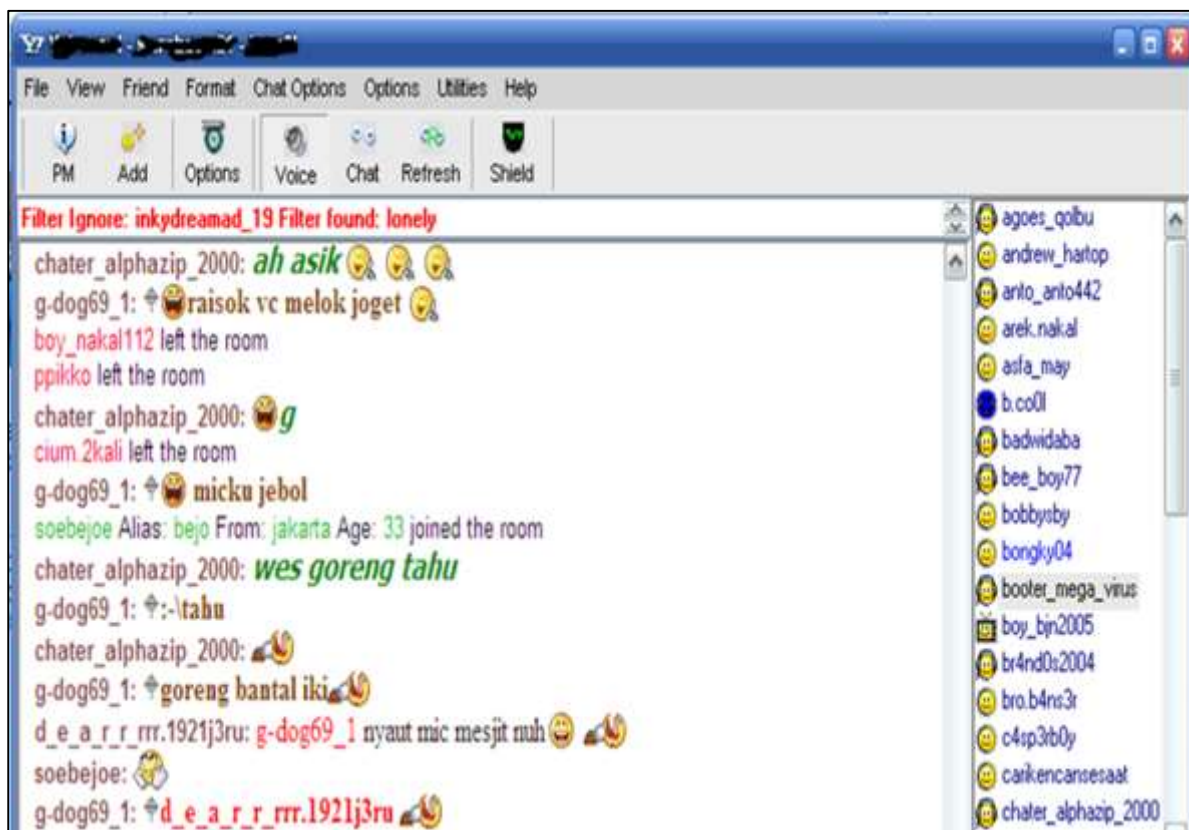
Chatting is a communication over the Internet that offers a real-time transmission of text messages from the sender to a receiver. Chat messages are generally short in order to enable other participants to respond quickly. Thereby, feeling similar to a spoken conversation, this tool is an attractive place for cyberattacks to hack account and get data.

Risks from Chatting

Nowadays most of the chatting platforms and instant messaging websites are a big place of frauds and the risk that come from the other users are very high and are as follows:

- **Viruses** – Chatting can be attacked from emails attachments, phishing or instant messaging. This can result to the hacking of a user computer or a network.
- **Malicious software** – Attackers can use the chat rooms to redirect the genuine user to a fake webpage to steal their credentials.
- **Hacking that comes from Hacked Chat Servers** – This hacking can come when the server of the game has been compromised because of its vulnerability as a result this can put in danger all the users that are connected to this chatting server.

Regarding the security of your computer, it is the same as the gaming section.



13. Internet Security – File Download

In this chapter, we will deal with file downloading which is one of the main reasons why computer and networks gets infected. Downloading can be for many reasons from entertaining like downloading songs, movies, clips also for information gaining like documents PDF, WORD, photos, etc. or for software updates.

What can be Potentially Harmful?

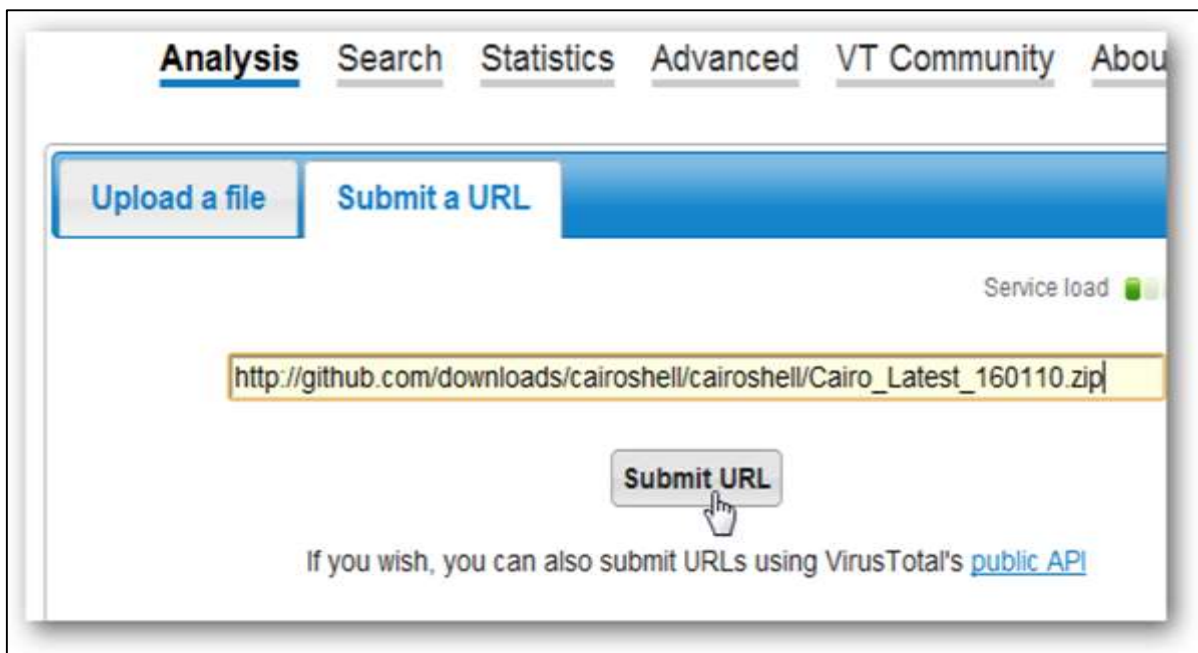
With the file downloaded, if you don't see the extensions and if they are the bad ones, then while installing your computer can get infected.

In-adversely installing adware's where the pop ups can come time after time. Spywares can be installed that enables hackers to get financial information.

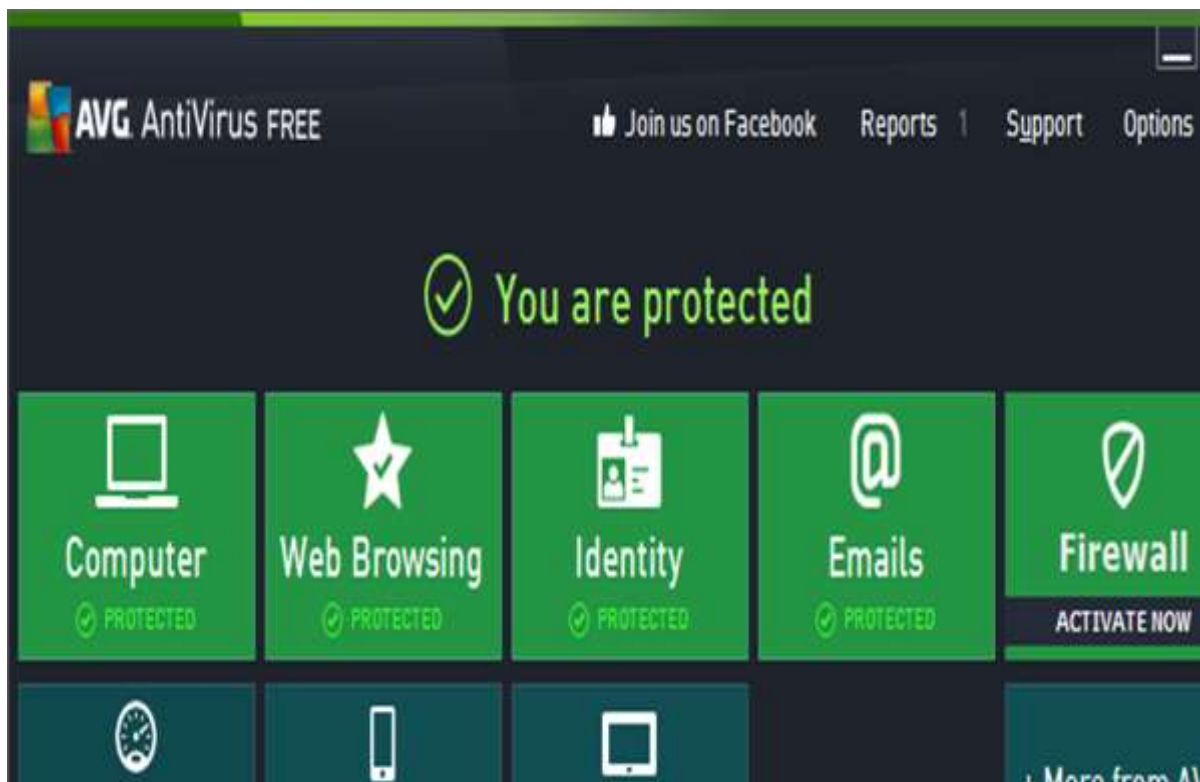
How to Minimize the Risks to be Infected from File Download

While visiting webpages that you think are safe, you can download the files that you need, but it is better to use <https://virustotal.com/>. You can go to this website and check the URL of the website which you are planning to enter. You can enter the URL and it checks for you, if the site has is infected by any virus or malware and can harm you. Or before downloading the document you copy the URL and paste it in virustotal to scan it.





Make sure that you have an antivirus installed and it is updated. Always scan the downloaded file for a possible virus.

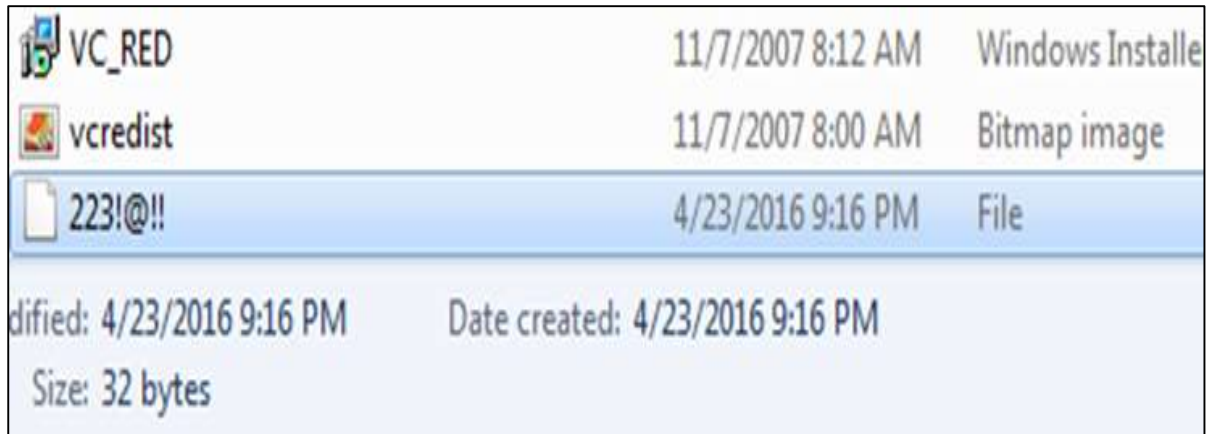


Double-check the .exe files with extreme caution because 90% of the viruses use such extensions to attach themselves. These are files used by programs to run on your computer.

Always use trusted webpages to download your files. For example, for Microsoft products always get them from Microsoft.com. For hardware drivers, download them from their official webpages.

Always avoid the peer-to-peer websites like uTorrent downloads as they are from unauthenticated resources.

Skip downloading the files that people call them as they like. For example, you can see the following image for better understanding:



VC_RED	11/7/2007 8:12 AM	Windows Installer Package
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

Check the files that you download with a MD5 Hash Value Checker. It is also commonly used to check the integrity of a file, and verify the downloaded files. One of them can be downloaded from – <http://www.winmd5.com/>

14. Internet Security – Transactions

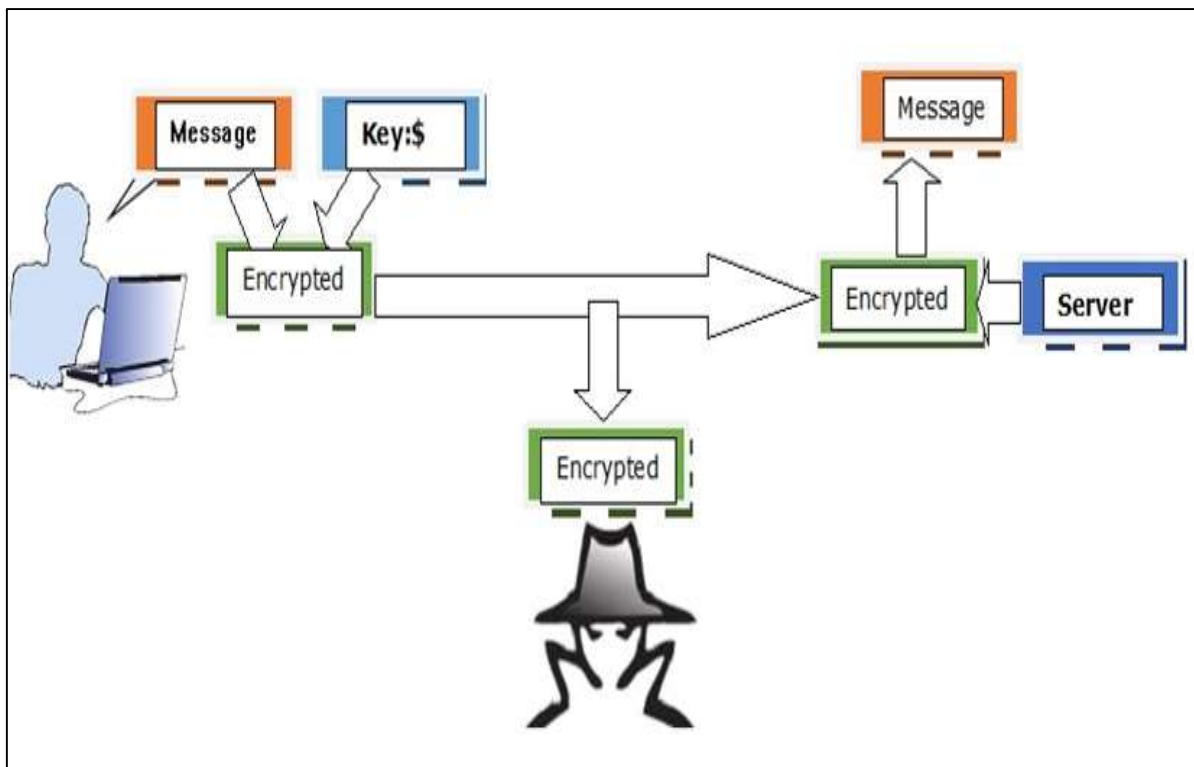
Nowadays the security of the transactions are very important because these days most of the things are happening online.

The transactions happen in the following forms:

- When you go in a market and you use a POS for payment, then a transaction occurs.
- In your mobile phone when you download an android app to order something like the eBay app.
- When you pay something through an online payment service like paypal.com.

Check if You are Doing a Secure Transaction?

Generally a secure transaction happens in an encrypted form which happens between the site that we are connected to and the browser that we are using. It happens through a file in which the website provides its details, which we will deal further in the following sections. A simpler indication is recognizing the difference between a secure and insecure connection of which **Https://** is a secured site, while **Http://** is not secured.



If you or your users are using Google Chrome, you can push them to always connect securely, if the webpage supports it. Always prefer the HTTPS extension, if you are using a Mozilla Firefox there is an add-on called **HTTPS Everywhere**.

We should do a transaction only through webpages that we know or when they have a good reputation. So, in simple words you should visit those webpages that you trust and even though you trust, it is recommended to do the transactions through payment gateways like PayPal, so you don't transmit bank account details to third parties.

A good resource is www.mywot.com that gives you the rates of the websites and their reputation based on millions of users, who trust their transaction to these websites.

At the end of the month always make a physical check of your transactions if they are matching to your expenditure or not. If it is not, then it is recommended to block your payment cards or accounts immediately.

After finishing the transactions, it is recommended that you always clear history, caches and cookies. Especially if you are using another computer that is not yours.

What Should You do as a System Administrator?

As a system administrator, you should have in mind some rules that will help our customers to make a secure transaction.

- In the first place, you should check if there is any **policy compliance** for the system that we are offering, like PCI, or HIPAA. Generally, these policies have security guidelines too, like hardware or software that provides access controls, integrity controls, auditing and transmission security.
- Another thing is that a **session should be limited** based on time and IP. So when your user signup form is getting the account open, the system will lock out after sometime and find out if there is a possibility of any man-in-the-middle attack. The IP restriction should not allow it.
- Make a **Usage Policy** for your system, so the user knows their limit and gains knowledge regarding the security.
- Check if your system has the proper configuration for making a financial transaction. The system should have a **2-factor authentication**, where a passcode or a pin number is sent to your client's mobile phone every time an online transaction takes place and will only be approved once you confirm the purchase by entering the code. This ensures that the client is who he says he is by asking for something he knows, and something he has, like a phone.



15. Internet Security – Banking

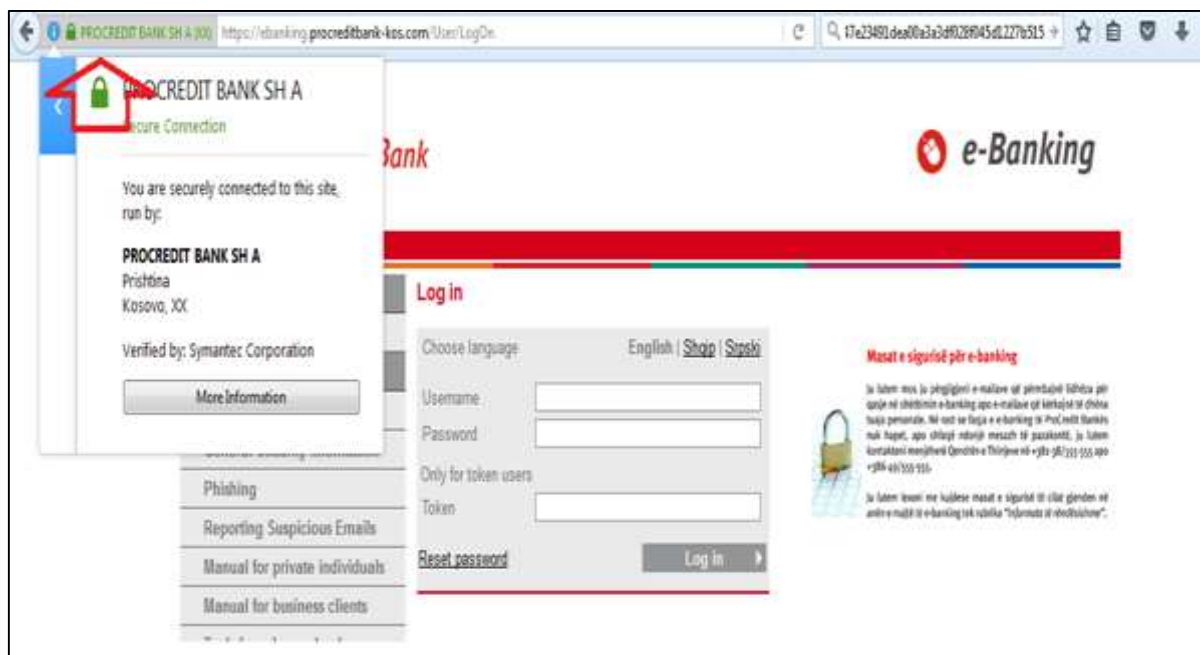
In this chapter, we will deal with banking security issues related to e-banking or the so called Internet banking, and credit or debit cards based security issues.

E-banking is an electronic payment gateway which enables all the customers of a bank to do banking transactions through their computers without the need to go physically to the bank.

Normally to create an e-banking account the client has to go physically to the bank to be able to open it and authenticate it when it opens. A customer can link this account with their loans, current account and many other bank products.

How to do an e-Banking Transaction Safely?

Always enter the e-banking link by typing it yourself and not through an arriving email it can be a phishing mail. Always connect through a secure connection to the website and check if the webpage is authenticated like in the following image, where the connection is a secure **Https**: and the authenticity of web I have checked it through the green bar which is a certificate which means that this web is pre-authenticated.



Be cautious of any unexpected or suspicious looking pop-ups that appear during your online banking session. Think about the process you normally go through to make a payment to someone – be suspicious if it differs from the last time you used it.

Never give anyone your login details in full either by email or over the phone – your bank will never request these in this way. Check your bank statements regularly and contact your bank immediately if you find any transactions that you did not authorize.

When you send money via your online bank account, always double check the amount you are sending as well as the account number and sort code you are sending it to.

Credit Cards

Generally, these cards are issued by card providers like banks and they are connected with the client's bank accounts and help to make payments and as this too is being used more often increasing the possibilities of frauds.



Credit card fraud is a theft carried out by using a credit card or any alike payment mechanism as a fake source for fraud transaction. A common type of fraud happens when an offender purchases an item online, by utilizing a credit card number that they have obtained in unethical ways.

Credit card transactions are obtained by:

- Credit card generator site on the Internet.
- Unethical merchant spreading credit card data of their clients.
- Hackers can get the data from a skimmer, which is a hardware that the hackers put in the ATMs or a POS.
- By finding discarded copies of vouchers.
- By hacking computers where the credit card details are stored in a cache.



Credit Card Generator

The most commonly used tool for cracking credit cards is **Credit Card Generator** (www.darkcodign.net). This Credit card generator is a command-line Python program which uses a .php script. It generates the credit card numbers that are used in the test e-commerce websites. It generates 13 and 16-digit VISA, MasterCard and Amex numbers. If installed, it can steal passwords and credit card numbers along with bank details.

Another one is called as the **RockLegend's Cool Card Generator**, but there are not many details given about it.

Credit Card Fraud Detection Techniques

In this section we will discuss the various Credit Card Fraud Detection Techniques.

Pattern Detection

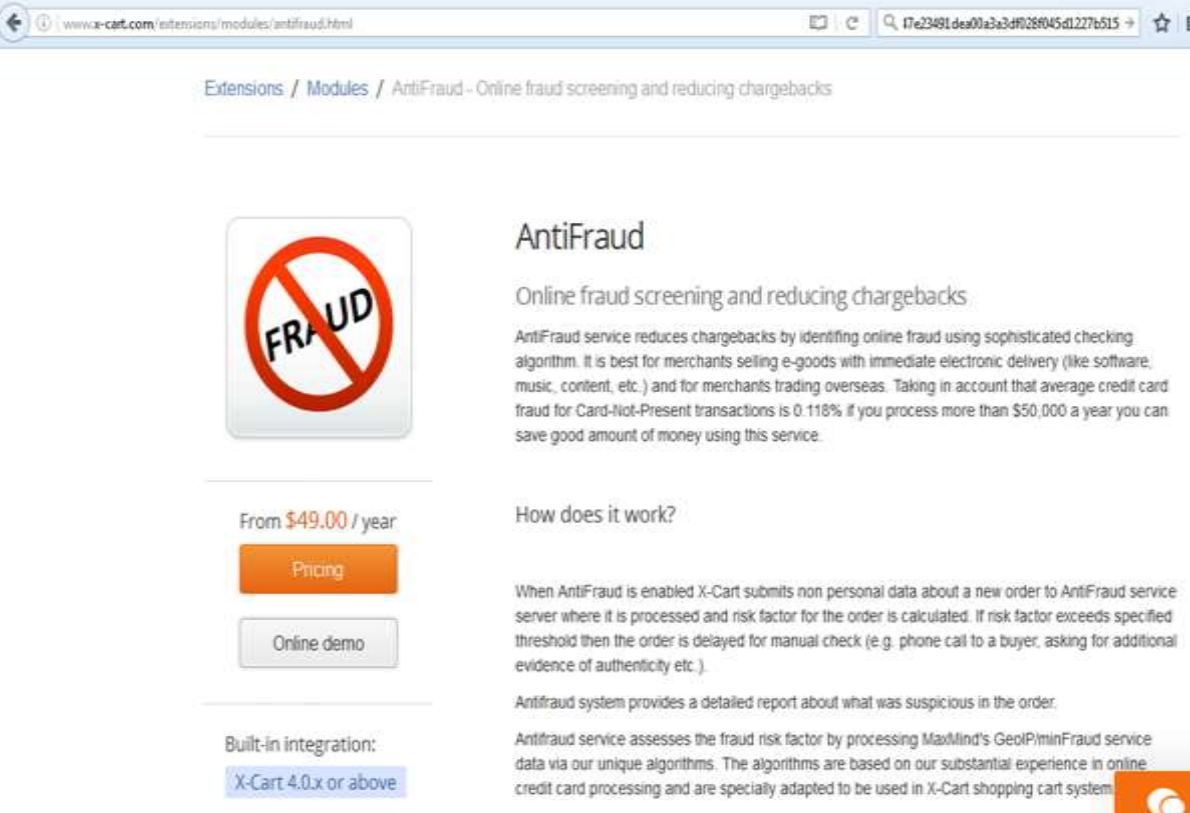
- This technique marks a person as a fraudster if many orders are placed to be delivered at the same address by different credit cards.
- If multiple orders are being sent from the same IP address.
- If the credit card changes by a few digits.
- If the person submits the same credit card with different expiry dates.

Fraud Screening Detection

This technique is developed by Visa and it detects fraud possibilities based on a score where 150 order variables are taken into consideration.

Xcart: Online Fraud Screening Service

For more details on this online fraud screening service, you can logon to – <http://www.x-cart.com/extensions/modules/antifraud.html>



Extensions / Modules / AntiFraud - Online fraud screening and reducing chargebacks

AntiFraud

Online fraud screening and reducing chargebacks

AntiFraud service reduces chargebacks by identifying online fraud using sophisticated checking algorithm. It is best for merchants selling e-goods with immediate electronic delivery (like software, music, content, etc.) and for merchants trading overseas. Taking in account that average credit card fraud for Card-Not-Present transactions is 0.118% if you process more than \$50,000 a year you can save good amount of money using this service.

From \$49.00 / year

Pricing

Online demo

Built-in integration:
X-Cart 4.0.x or above

How does it work?

When AntiFraud is enabled X-Cart submits non personal data about a new order to AntiFraud service server where it is processed and risk factor for the order is calculated. If risk factor exceeds specified threshold then the order is delayed for manual check (e.g. phone call to a buyer, asking for additional evidence of authenticity etc.).

Antifraud system provides a detailed report about what was suspicious in the order.

Antifraud service assesses the fraud risk factor by processing MaxMind's GeoIPminFraud service data via our unique algorithms. The algorithms are based on our substantial experience in online credit card processing and are specially adapted to be used in X-Cart shopping cart system.

Card Watch

This is an incentive for UK Banks to raise the awareness of Card Fraud Prevention. You can get more information about this from the following link – <http://www.cardwatch.org.uk>

MaxMind Credit Card Fraud detection

You can get more information about this from the following link – <https://www.maxmind.com/en/home>

This is also a leading platform that leads in detecting potential card frauds and it was developed by proprietary technologies. It analyses the scores' risk factor or each online transaction in real time, so for the merchant they need less time to analyze the transactions.

Best Practices to Protect your Bank Transactions

Following are a few pointers, which are necessary to be remembered while making any transactions.

- Protect your security code always by a hand while entering it in an ATM or POS.
- Never leave unattended credit cards.
- Check your credit card transactions after any purchase.
- Keep separate credit cards in the wallet if possible.
- Keep a record of account number and expiry dates in a safe place.
- Never sign a blank bank receipt.
- Destroy your unused cards or bank statements by burning or destroying them properly.
- Report stolen cards or documents immediately.
- Never give your bank details by phone or email.
- Report any susceptible charge in your card.

16. Internet Security – e-Commerce

In this chapter, we will deal with e-Commerce. What are the most used and secure platforms? What it is needed to secure them?

E-commerce is all about selling or buying goods and services from Internet and paying through this medium. This transaction happens between clients to business, B2B, client to client and as in between there is money transaction we should be cautious when using and also while setting up e-commerce sites.

Top e-Commerce Platforms

Here is a list of some well-known e-Commerce platforms and how their security configuration works.

Magento

You can get further details of this platform on the following link – <https://magento.com>

This platform is one of the best as it is developed by eBay and it can be easily get integrated with a PayPal gateway. It has both free and paid versions to choose from. The vulnerabilities are patched too fast.

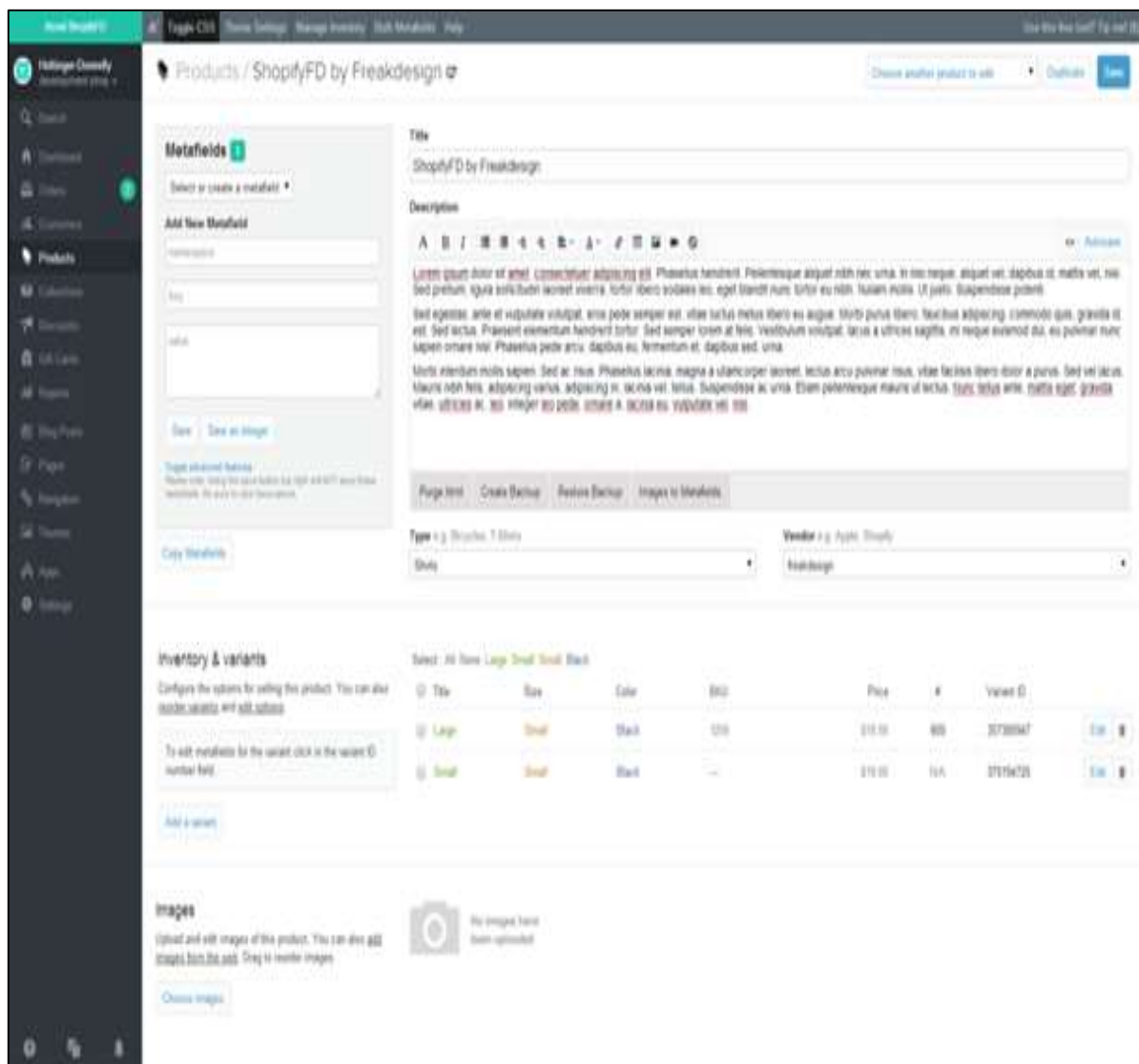


It also has a vast variety of plugins and customization options. It has SaaS solutions: Elastic scalability, high resilience and availability, PCI compliance, global availability and automated patching, while still maintaining flexibility in software customization that our merchants require.

Shopify

You can get further details of this platform on the following link – <https://www.shopify.com>

So if you're trying to design the checkout page to be exactly how you want, Shopify is probably not for you. In fact, none of the hosted solutions will offer customizable checkout process, so you can jump the Self-Hosted section right away. Shopify has many apps that you can download and install on your store, which further extend the default or introduce new functionalities.

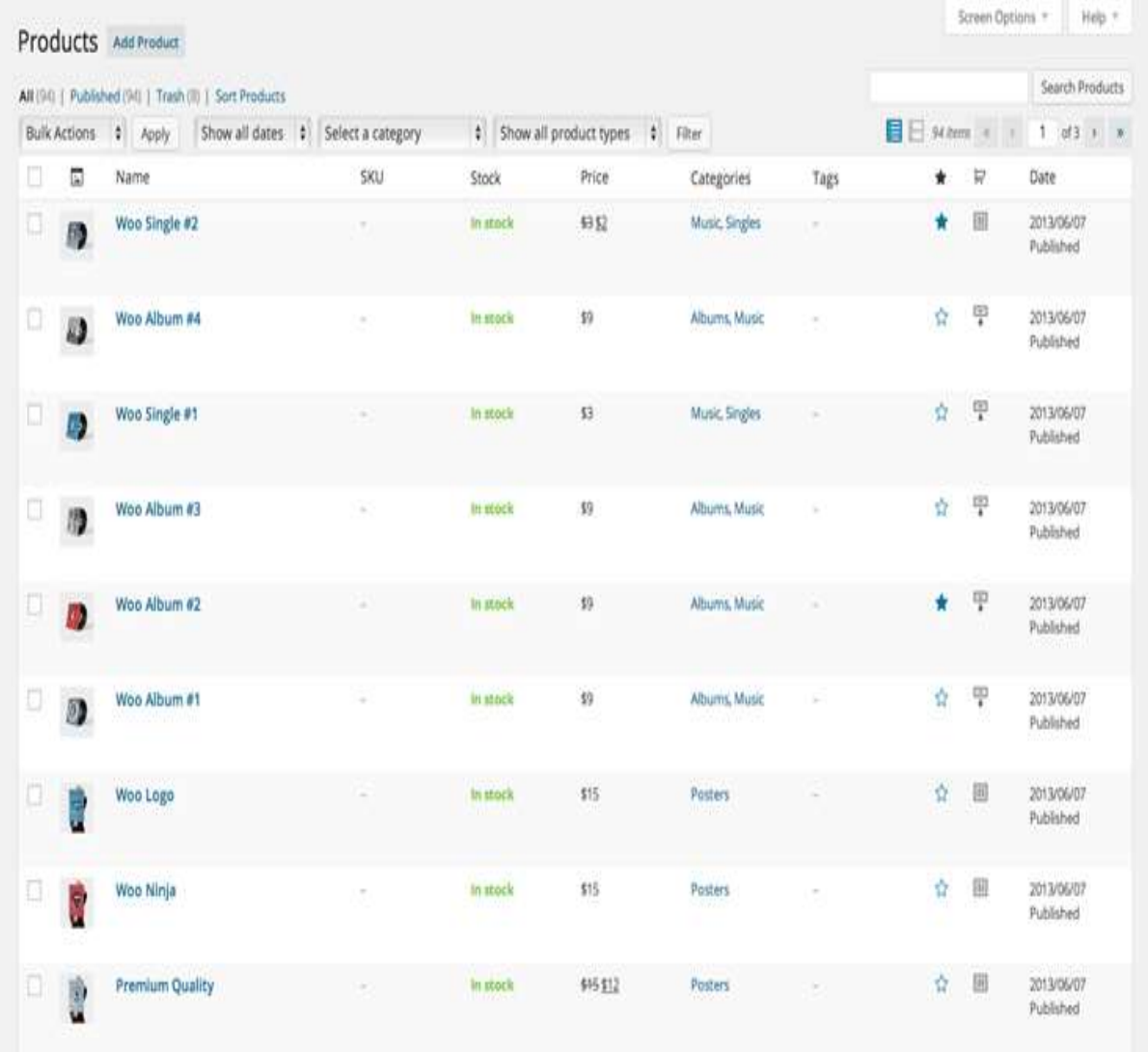


WooCommerce

You can get further details of this platform on the following link – <https://wordpress.org/plugins/woocommerce/>

WooCommerce is a free e-commerce plugin that allows you to sell anything and very practically. Built to integrate seamlessly with WordPress, WooCommerce is the world's favorite e-commerce solution that gives both store owners and developers complete control owing to the use of WordPress templates.

With endless flexibility and access to hundreds of free and premium WordPress extensions, WooCommerce now powers 30% of all online stores – more than any other platform.



Name	SKU	Stock	Price	Categories	Tags	Date
Woo Single #2	-	In stock	\$3.52	Music, Singles	-	2013/06/07 Published
Woo Album #4	-	In stock	\$9	Albums, Music	-	2013/06/07 Published
Woo Single #1	-	In stock	\$3	Music, Singles	-	2013/06/07 Published
Woo Album #3	-	In stock	\$9	Albums, Music	-	2013/06/07 Published
Woo Album #2	-	In stock	\$9	Albums, Music	-	2013/06/07 Published
Woo Album #1	-	In stock	\$9	Albums, Music	-	2013/06/07 Published
Woo Logo	-	In stock	\$15	Posters	-	2013/06/07 Published
Woo Ninja	-	In stock	\$15	Posters	-	2013/06/07 Published
Premium Quality	-	In stock	\$45.12	Posters	-	2013/06/07 Published

Bigcommerce

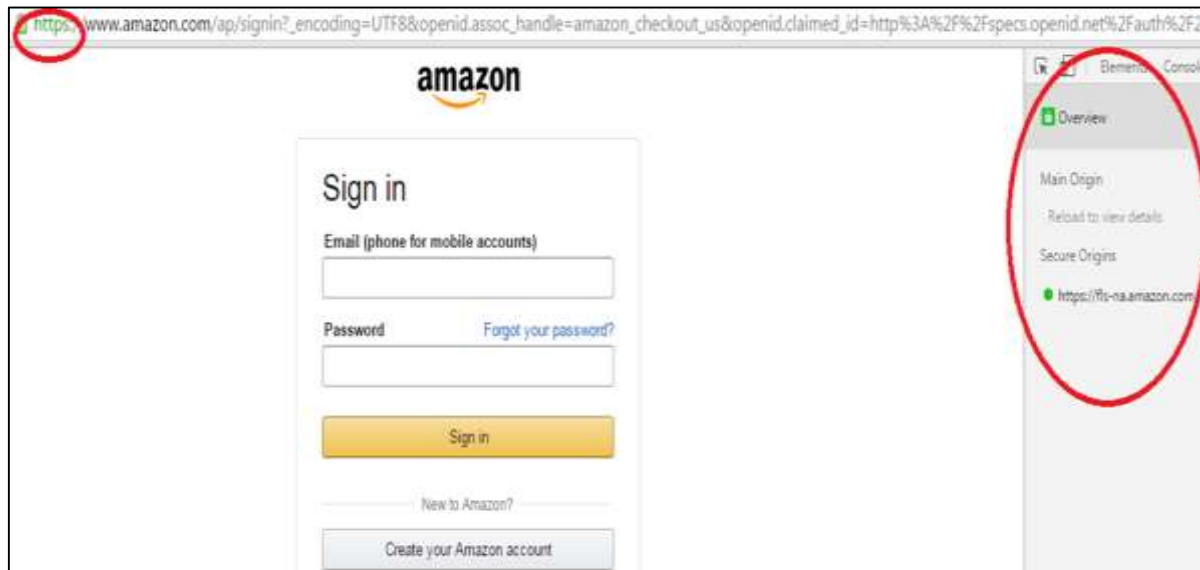
You can get further details of this platform on the following link – <https://www.bigcommerce.com>

It has over 115 e-commerce templates, unlimited product uploads and a mobile view as well. It effects integration with Amazon and eBay, and it also can be integrated with most

of the payment gateways. From the security point of view, it is very secure because it is PCI compliant.

How to Buy in a Secure Way?

As you know, in order to navigate and purchase goods, services online the retailers should always be authenticated through Digital certificates, from the security point of view this parameter is not negotiable.



Some of the secure online stores which have multi-seller platforms are –

- Amazon.com
- Ebay.com
- Aliexpress.com

It is important to mention that in these platforms there are scammers too. So in this case before buying from any seller you should see the reviews from the other buyers and what is their reputation, which are generally marked by stars.

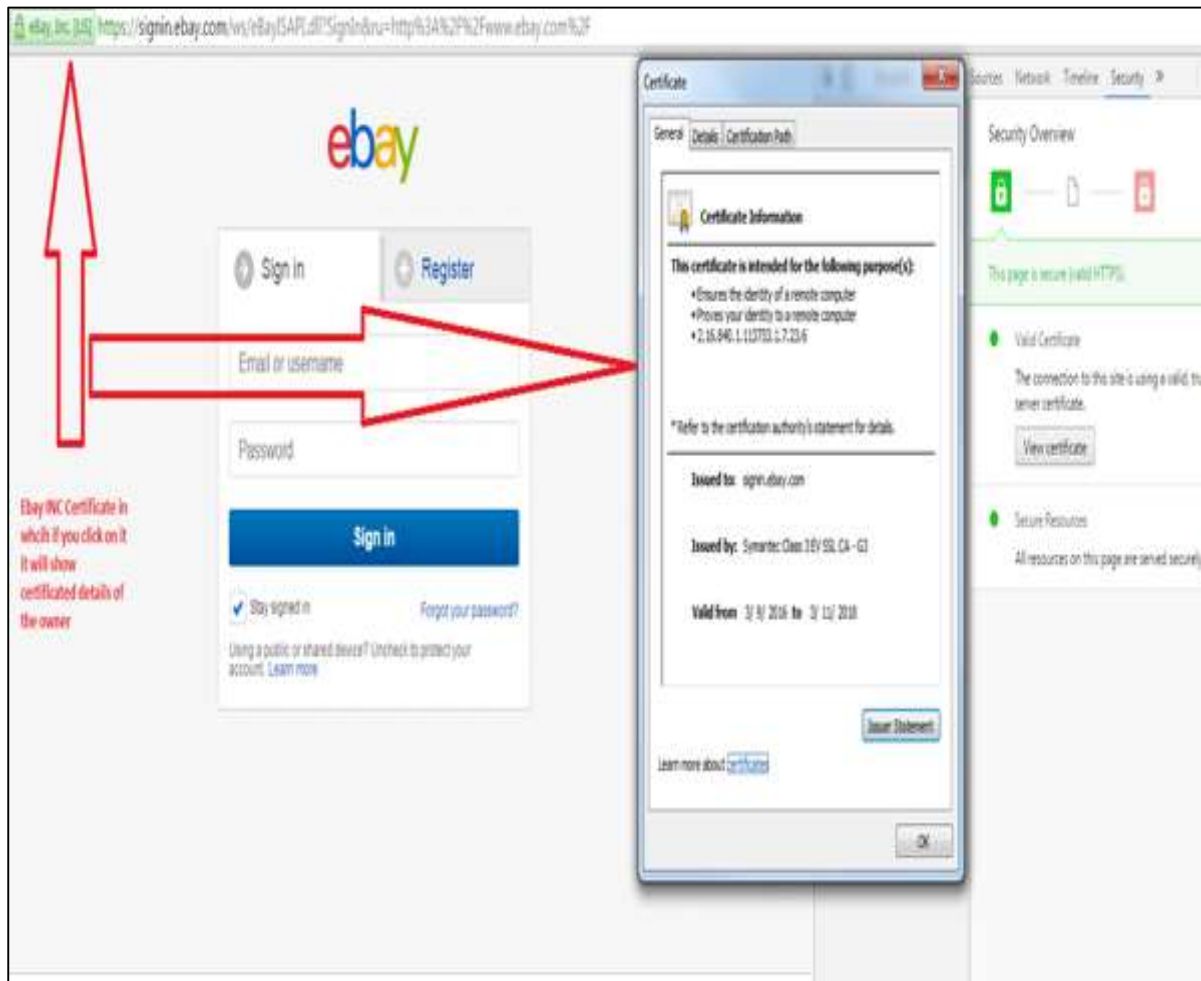
Setup a Secure Online Shop

In order to be reliable from the customer's point of view, it is mandatory that your e-commerce site has to be compliant with the PCI standards. These standards are proprietary information standard for sites that handles payment online and uses credit cards like Visa, MasterCard, American Express, Discover, JCB and others. They would need full documentation and information to set up this Compliance. All the details can be found on their official site:

https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

17. Internet Security – Certificates

Digital Certificates are a standard of security for establishing an encrypted link between a server and a client. Generally, between a mail server or a webserver, which protects data in transitions by encrypting them. A Digital Certificate is also a Digital ID or a passport which is issued by a Third Party Authority which verifies the identity of the server's owner and not claiming a false identity.

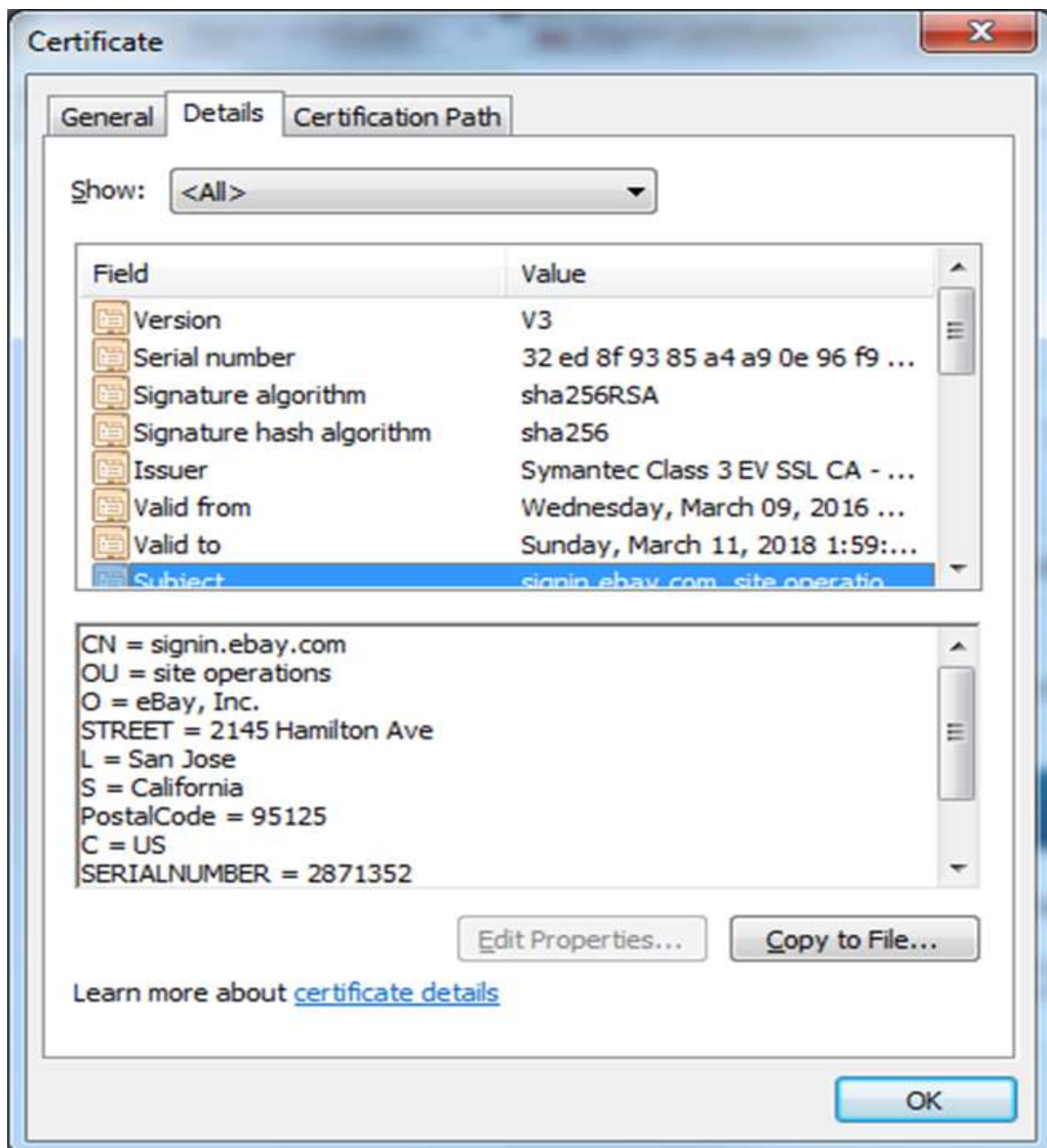


Components of a Digital Certificate

All these following components can be found in the certificate details:

- **Serial Number:** Used to uniquely identify the certificate.
- **Subject:** The person, or entity identified.
- **Signature Algorithm:** The algorithm used to create the signature.
- **Signature:** The actual signature to verify that it came from the issuer.

- **Issuer:** The entity that verified the information and issued the certificate.
- **Valid-From:** The date the certificate is first valid from.
- **Valid-To:** The expiration date.
- **Key-Usage:** Purpose of the public key (For example: encipherment, signature, certificate signing...).
- **Public Key:** The public key.
- **Thumbprint Algorithm:** The algorithm used to hash the public key certificate.
- **Thumbprint:** The hash itself, used as an abbreviated form of the public key certificate.



Levels of Validations

In this section we will discuss the various levels of validations of an SSL (Secure Sockets Layer) Certificate. Some of the most important ones are as follows:

- **Domain Validation SSL Certificate:** It validates the domain that is registered by a system administrators and they have administrator rights to approve the certificate request, this validation generally is done by email request or by a DNS record.
- **Organization Validated SSL Certificates:** It validates the domain ownership and also the business information like the Official Name, City, Country, etc. This validation is done by email or DNS record entering and the certificate authority would also need some genuine documents to verify the Identity.
- **Extended Validation SSL Certificates:** It validates domain ownership and organization information, plus the legal existence of the organization. It also validates that the organization is aware of the SSL certificate request and approves it. The validation requires documentation to certify the company identity plus a set of additional steps and checks. The Extended Validation SSL Certificates are generally identified with a green address bar in the browser containing the company name.

The reviews and some of the biggest digital certificate providers' details can be found in the following link – <https://www.sslshopper.com/certificate-authority-reviews.html>

18. Internet Security – Email Security

In this chapter, we will explain the security measures that have to be taken in a mail server and on a client site.

Hardening a Mail Server

For hardening a mail server, you will need to adhere to the following steps:

Step 1. Configure mail server not to have Open Relay

It's very important to configure your mail relay parameters to be very restrictive. All mail servers have this option, where you can specify which domains or IP addresses your mail server will relay the mails to. This parameter specifies for whom your SMTP protocol should forward the mails to. An open relay can harm you because spammers can use your mail server for spamming others, resulting in your server getting blacklisted.

Step 2. Set up SMTP authentication to control user access

SMTP Authentication forces the people who use your server to obtain permission to send mail by first supplying a username and password. This helps to prevent any open relay and abuse of your server. If configured the right way, only known accounts can use your server's SMTP to send an email. This configuration is highly recommended when your mail server has a routed IP address.

Step 3. Limit connections to protect your server against DoS attacks

The number of connections to your SMTP server should be limited. These parameters depend on the specifications of the server hardware and it's a nominal load per day. The main parameters used to handle connection limits include: Total number of connections, total number of simultaneous connections, and maximum connection rate. To maintain optimal values for these parameters may require refinement over time. It **prevents Spam Floods and DoS Attacks** that target your network infrastructure.

Step 4. Activate Reverse DNS to block bogus senders

Most of the messaging systems use DNS lookups to verify the existence of the sender's email domain before accepting a message. A reverse lookup is also an interesting option for fighting off bogus mail senders. Once Reverse DNS Lookup is activated, your SMTP verifies that the senders IP address matches both the host and domain names that were submitted by the SMTP client in the **EHLO/HELO Command**. This is very valuable for blocking messages that fail the address matching test.

Step 5. Use DNSBL servers to fight incoming email abuse

One of the most important configurations for protecting your email server is to use **DNS – based blacklists**. Checking if the sender domain or IP is known by DNSBL servers world-wide could cut down the amount of spam received substantially. Activating this option and using a maximum number of DNSBL servers will greatly reduce the impact of

unsolicited incoming email. The DNSBL servers list along with all known spammers IPs and domains for this purpose are all stored in a website, the link for this website is – <https://www.spamhaus.org/organization/dnsblusage/>

Step 6. Activate SPF to prevent spoofed sources

The Sender Policy Framework (SPF) is a method used to prevent spoofed sender addresses. Nowadays, nearly all abusive email messages carry fake sender addresses. The SPF check ensures that the sending MTA is allowed to send mail on behalf of the sender's domain name. When SPF is activated on your server, the sending server's MX record (the DNS Mail Exchange record) is validated before any message transmission takes place.

Step 7. Enable SURBL to verify message content

The SURBL (Spam URI Real-time Block Lists) detects unwanted email based on invalid or malicious links within a message. Having a SURBL filter helps to protect users from malware and phishing attacks. At present, not all mail servers support SURBL. But if your messaging server does support it, activating it will increase your server security, as well as the security of your entire network since more than 50% of Internet Security threats come from email content.

Step 8. Maintain local IP blacklists to block Spammers

Having a local IP blacklist on your email server is very important for countering specific spammers who only target you. Maintenance of the list can take resources and time, but it brings real added-value. The result is a speedy and reliable way to stop unwanted Internet connections from bothering your messaging system.

Step 9. Encrypt POP3 and IMAP authentication for privacy concerns

The POP3 and IMAP connections were not originally built with safety in mind. As a result, they are often used without strong authentication. This is a big weakness since users' passwords are transmitted in clear text through your mail server, thus making them easily accessible to hackers and people with malicious intent. The SSLTLS is the best known and the easiest way to implement strong authentication; it is widely used and considered reliable enough.

Step 10. Have at least two MX records for any failover

Having a failover configuration is very important for availability. Having one MX record is never adequate for ensuring a continuous flow of mail to a given domain, which is why it's strongly recommended to set up at least two MXs for each domain. The first one is set as the primary, and the secondary is used if the primary goes down for any reason. This configuration is done on the **DNS Zone level**.

Securing Email Accounts

In this section, we will discuss how to secure the email accounts and avoid them from getting hacked.

Securing on the Client Site

The most important thing is to **Create complex passwords**. As there are many techniques available to crack the passwords like brute-force, dictionary attacks and password guessing.

A strong password contains:

- 7 to 16 characters.
- Uppercase and lowercase letters
- Numbers
- Special characters

Change password

To reset your password, provide your current password OR the answer to your security question.

☒ Current password:

OR

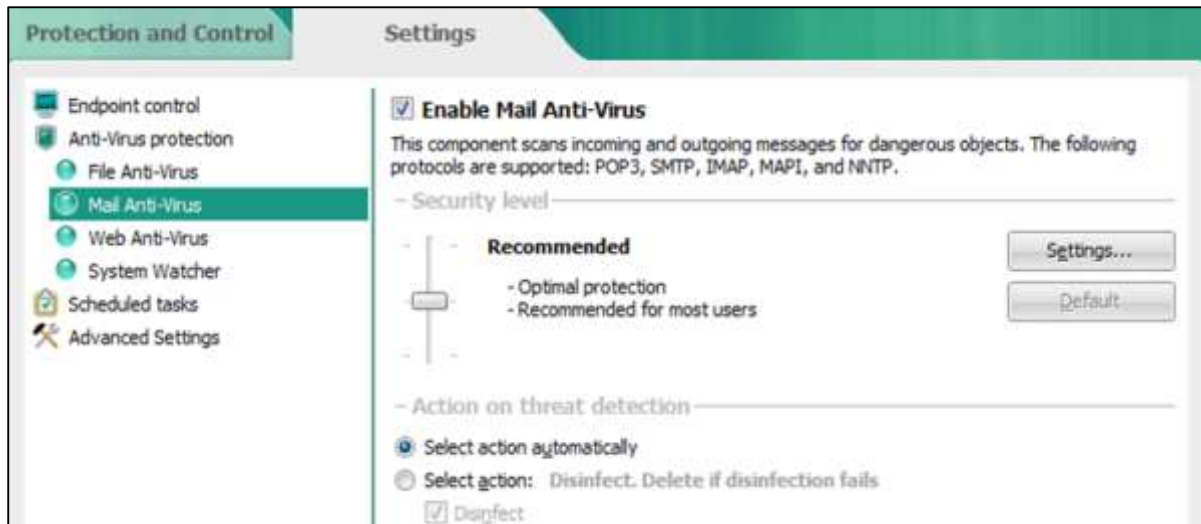
☐ What was your first phone number?

New password: Password strength: **Strong**

Confirm new password:

Always connect the email password with another genuine email that you have access to. So in case this email is hacked, you have the possibility to gain access again.

Install in your computer a mail antivirus, so that every email that is coming in your email client is scanned like attachments and phishing links.



If you are in the habit of using web access, then never open attachments with the **.exe** extensions.

It is recommended to use an encrypted email when communicating officially with important data. So it is better that the communication to be encrypted between the end users, a good tool for this is **PGP Encryption Tool**.

19. Internet Security – Identity Theft

In this chapter, we will discuss regarding the identity theft. What is it? How to prevent it and what measures do we need to take to prevent them?

What is Identity Theft?

Identity theft is an action when someone steals your name, surname and other personal data and uses them to do something unlawful. Nowadays, this is a very sensitive issue because many people transmit their sensitive data over Internet and the big as well as small companies have to take their incentives for anti-fraud policies in the work place.

In home too, we should be prudent to minimize this risk. It is worth a mention that more than 50% of identity theft is done by people whom the victim knows. Mainly this identity theft is done for financial profit.



A good website that will help you with ID theft is – <https://www.consumer.ftc.gov>, which has detailed steps about what to do, how to report, etc. in such cases.



How Does ID Thefts Take Place?

There are quite a few ways in which people or hackers can steal your ID. Some of the most commonly used ways are as follows:

- Most of the skilled people in such activities rummage through trash looking for invoices, bills and other papers with your personal information.
- By stealing wallets which can contain your ID card, credit card, and other personal identification details, etc.
- Stealing expired applications for preapproved credit cards and fill them out with a different address.
- Take important documents such as birth certificates, passports, copies of tax returns and the likes during a burglary of your house.
- Steal the Social numbers and identities of children who are especially vulnerable because they don't have credit histories and it may be many years before the theft is discovered.
- Steal personal information from a book or a newspaper article.
- Steal personal information of a relative or someone that he or she knows well, perhaps by being a frequent visitor to their home.

- Hack into a computer that contains your personal records and steal the data.
- “Shoulder surf” by watching from a nearby location as he or she punches in a mobile phone.
- By phishing methods mentioned in the upper section by requesting you in general to fill a form with your data.

Consequences of not Reporting an ID fraud?

Following are a few consequences which might happen if you don't report an ID fraud to the concerned authorities.

- The criminals can take mortgages, buy expensive stuff, etc.
- The criminals may run up huge amounts of debt, then file for bankruptcy in the victim's name, ruining their victim's credit history and reputation.
- Make a terrorist attack.
- Using these ID's, they can also indulge in human trafficking.

How to prevent ID theft?

To prevent any ID theft, you can take care of the following important pointers:

- Shred all the unused documents before throwing.
- Don't give any personal and sensitive information over the phone.
- Don't make your passwords like your birthday, your name, etc. which will be easier for people to guess and understand.
- Keep your document in a secure place at house away from your roommate or cleaning lady, etc.
- Check to make sure you are aware of all accounts listed on your name, and balances of these accounts are up-to-date.

What to do if you are a victim of ID theft?

You can do the following things as soon as u get to know that you have been a victim of ID Theft.

- Immediately call the police to file a report with your local law enforcement agency.
- Document all your steps like keep all the correspondence and copies of the documents.
- Call your bank to cancel all your ATM and POS transactions.

20. Internet Security – Cybercrime

As in all the previous chapters, we have dealt with different ways to protect ourselves as to how we should not get into any scenario of a potential fraud. Now let us see what is our outer limit of what all we can do without making a computer crime or as it is called a cybercrime.

Types of Cybercrime

Following are some of the most prominent cybercrimes happening around the world.

Financial Cybercrime

This crime is when you utilize your skills or third party access for the main purpose to get financial profit. Like accessing an e-bank portal in an unauthorized way and make transactions, make e-commerce payments and take goods without permission.

Another widespread financial cybercrime is Credit card cloning all this has been mentioned in the previous chapters.

DoS Attack or Cyber Extortion

This type of a crime is when you threaten a company or a person that you will stop their services in case you are not “rewarded” with money to let the services run, which generally are Webserver, mail servers or other computer networks. We hear a lot of such cases on a daily basis across the world.

Cyberterrorism

This is an act of terrorism committed through the use of computers. It can be a propaganda on the Internet, that there will be bomb attacks during the holidays, which can be considered as cyberterrorism.

Here are some other pointers that will make u a Cybercriminal:

- If you **produce a virus** or any other type of malware that damages computers and networks around the world, for financial or non-financial profit.
- If you make **unsolicited bulk mails** like spam to spread something.
- If you make a **phishing or social engineering attack** you can be jailed depending on the country, you are living in.
- If you own or create a black market for drug, weapon selling, child pornography selling.
- If you crack or pirate a software, music or videos over the Internet you can be jailed for author copyrights.

21. Internet Security – Laws

As mentioned in the previous chapter, Cybercrime is a crime like all the other crimes and as such it has a law implication in most of the countries in this section we will see there to find the laws regarding the cybercrime in mainly in sXxxxthe biggest countries.

United States Cyber Crime Law

To logon to the webpage of United States Department of Justice you can click on the following link – <https://www.justice.gov> and the section that have implications on cyber space is:

SECTION 2: Prohibition of Unfair or deceptive acts or practices relating to spyware.

(<https://www.govtrack.us/congress/bills/110/hr964/text>)

The main statutes that are related to cybercrimes are found in the following link which has a manual prosecution of the US –

<https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>

The other sections which tells you how you can have indirect implications are:

- 18 U.S.C §2320 Trafficking in counterfeit goods or services – <https://www.law.cornell.edu/uscode/text/18/2320>
- 18 U.S.C §1831 Trade of secret offenses – <https://www.justice.gov/usam/usam-9-59000-economic-espionage#9-59.100>
- 47 U.S.C §605 Unauthorized publication or use of communications – <https://www.justice.gov/usam/criminal-resource-manual-1066-interception-radio-communications-47-usc-605>

The penalties vary from a fine \$50000 or twice the value of the crime up to 20 years in prison, if it is a repeated crime.

Mexico Cyber Crime Law

The portal of the Government of Mexico a dedicated webpage which has all the information, you can read all of it by clicking on the following link – <http://www.gob.mx/en/index>, it has detailed material about all its agencies.

The law having implications in cyberspace is as follows:

Section 30-45-5: Unauthorized computer use. Full law information is found on the following link –

<http://law.justia.com/codes/new-mexico/2011/chapter30/article45/section30-45-5>

Brazil Cyber Crime Law

The portal of the Department of Justice in Brazil is – www.jf.gov.br, which has all the information about its laws.

The law having implications in cyberspace is as follows:

Art.313 –A. Entry of false data into the information system.

Art.313 –B. Unauthorized Modification or alteration of the information system.

Canada Cyber Crime Law

The portal of Department of Justice in Canada is – <http://laws-lois.justice.gc.ca/eng/>, which has all the information about its laws.

The law having implications in cyberspace is as follows:

- Canadian Criminal Code Section 342.1

United Kingdom Cyber Crime Law

The portal of Department of Justice in UK is – <http://www.legislation.gov.uk/>, which has all the information about its laws.

The law having implications in cyberspace is as follows:

Computer Misuse act of 1990 Chapter 18 –

<http://www.legislation.gov.uk/ukpga/1990/18/contents>

European Cyber Crime Law

The portal of European Union Legislation webpage is – http://europa.eu/index_en.htm, which has all the information about its legislations and regulations.

The law having implications in cyberspace is as follows, they are found in –

- **Section 1** – Substantive Criminal Law
- **Title 1** – Offences against the confidentiality, integrity and availability of computer data and systems.

India Cyber Crime Law

The portal of Department of Justice in India is – <http://lawmin.nic.in/>, which has all the information about its laws.

The law having implications in cyberspace is as follows:

- The information Technology ACT.2000 (No.21 of 2000)
- Chapter XI Offences –
http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf

22. Internet Security – Checklist

In this chapter, we will discuss the creation of a basic checklist which will keep us safe and protected from hackers and other malware at the workplace and in the home environment as well.

Basic Checklist

Here is a basic checklist of things that you should do to ensure Internet Security:

- **Account setup** – There should be an appropriate policy that when an employee comes to the organization, who opens the account and what rights or privileges does the employee has, etc. What are the limits of the usage of computer resources?
- **Password Change Policy** – There should be a policy where the frequency of the password change should be mentioned and the complexity of passwords that need to be used.
- **Helpdesk Procedure** – There should be a proper procedure as to when someone calls the helpdesk user. They should first identify themselves based on something like a user ID or any other unique identification.
- **Access Privileges** – This procedure should state how the access is granted to different parts of the network and there it should be mentioned who has authorized this access and whether they can authorize any extra access if needed.
- **Violation** – There should be a policy for reporting any violations to any policy.
- **Employee Identification** – They should be forced to wear an ID badge and any guest coming in should be registered if possible with a temporary or a visitor badge.
- **Privacy Policy** – There should be a policy where the employees should check up to what level are they authorized to give information and when this level is passed to whom they should speak to.
- **Document Destruction** – It should be checked if all the documents which are of no use any further are shred or burned.
- **Physical Restriction Access** – Physical access should be protected with limited access and they should be allowed only for the employees.
- **Antivirus in Place** – It is mandatory in such cases to check if the antivirus is functioning with all it functions like mail antivirus, file scanning, web scanning, etc.
- **Network Filtering** – It is highly recommended to check if your network is filtered with all the accounts to the level of access of different employees. In the home environment you need to check for your parental control software, if it is in place or not.