9-Zone's

www.9-ZONE.com

Hand book on

Privacy Control and Cyber Security

Including WINDOWS 7 Security enhancements

By,

Payan Kumar Paruchuri

Disclaimer:-Whilst every effort has been made to ensure that the information contained herein is correct and up-to-date, Me or any related parties cannot accept any responsibility, legal or otherwise, for any errors or omissions. The materials contained herein are provided for general information purposes only and do not constitute any business advice. We accept no responsibility for loss which may arise from reliance on information contained herein, and we make no warranty, express or implied, regarding the information provided in this book.

Regards,
Pavan Kumar Paruchuri
MS-MVP
Consumer Security.

Our contact Options:-

- ✓ Visit the site www.9-zone.com and join Using google friend connect.
- ✓ Join our Orkut community :- http://www.orkut.co.in/Main#Community.aspx?cmm=37556764
- ✓ Join our Google Group:-
- ✓ http://groups.google.com/group/9-zone
- ✓ Add me on facebook:-
- ✓ http://facebook.com/9zone
- ✓ Follow me on twitter:-
- ✓ http://twitter.com/9zone
- ✓ e-mail me :- contactus@9-zone.com

About our site www.9-zone.com :-

Get tips and tricks on windows xp, vista, windows7, troubleshooting and virus issues, free downloads, software tutorials, administration and networking tutorials, articles on cyber security.

A)Various Tips/Tricks, tweaks and hacks for increasing performance, customization etc of :-
1)Windows Xp 2)Windows Vista 3)Internet
B)Troubleshooting section contains various tips and tricks to troubleshoot different administration and virus problems that is caused in the system due to various reasons .
C)Learn software contains learning bytes for using various software and understanding different computer and computing concepts
D)Careen'N'Fun contains stuff which is Just for entertainment and knowledge nothing else
E)Admin&Networking contains Learning bytes on Networking and administration,Currently updated with basic networking concepts, More like windows server administration, Unix,wireless networks are about to come soon.
F)Security section had A list of articles on few possible online and cyber frauds that are common in the modern cyber world.
G)Downloads section had Exclusive free and open source software hand picked by the team 9-zone.

About the book

- This Book contains the basics and some advanced topics related to cyber security.
- It is made to create some security awareness among the netigens and people using computer systems.
- As far as possible the articles covered and topics discussed here are kept as short as possible .
- This book is made using simple language so that a laymen can also understand it.

About the Author

- Pavan Kumar Paruchuri is the editor and designer of:- http://www.9-zone.com
- And Joint editor, designer of:-http://www.9-zone.org
- He is Recognized as Most valuable professional in consumer security by Microsoft for the year 2009-2010.
- He is a MCSE(Microsoft Certified Systems Engineer) on server 2003,
- A Qualified ICWA,
- A graduate in B.Com
- And presently doing CA(FINAL).

Visit

www.9-ZONE.com

Handbook on Privacy and Cyber Security

Pavan Kumar Paruchuri

Book dedicated to all my website readers and community (all that I own and moderate) members in orkut without whom I may not entered in the field of IT.

I am really thankful to my parents for their encouragement given in this regard.

And I thank all my friends for their support especially CA.Ranjit Jain and my community supporters Hemant, Karan and Bala Krishna.

Introduction

Imagine, you are sitting alone at McDonald's, eating your cheese burger slowly and just opened the laptop to pay mobile bill from the online banking account, by connecting through a public wi-fi hotspot, totally unaware of those malicious eyes watching your activity!!!

Ladies and Gentleman welcome to the world of cyberspace and technology, where privacy really matters.

Internet today has become a part and parcel of our life and we became very much attached to the internet facilities like chatting, e-mail, e-commerce, social networking etc, these indeed have really revolutionized and influenced our style of living.

> Tip: - Having a good internet security suite or else good security software like antivirus, anti-spyware, firewall etc. will protect your computer most of the time and will keep it almost trouble free.

The advent of social networking had created second home and life for most of us, in a virtual world called cyber space, and the penetration of e-commerce had saved a lot of time for us.

Everything looks good, but many people don't know about the dark side of the virtual world where they are leading their second life, the fact is that, it is exploited more than our real world by cyber criminals.

Spyware, Trojans, viruses, worms, phishing, key loggers, malware, spoofing, rootkits, spam, Oh my god what a huge list to mention, whether we are browsing from our home pc or from internet café or from a wi-fi hotspot it doesn't matter we are still watched by many eyes and there is no privacy for us.

- The system we are using might already be hijacked using a backdoor,
- Or it may contain a keylogger which is logging all our details,
- Or the bank website we have opened might be a fake one,
- If we are in a internet café then the system we are using might have a hardware keylogger,
- Or some one might be sniffing over our network,
- Or we may be reverse tracked from our gps device,
- Or even our keyboard strokes might be tapped by somebody
- Or there may be a hidden cam following us, or even our service provider himself got hijacked,
- Or the credit card swipe device in the shopping mall where we are going to pay the bill had a inbuilt card cloning device,
- Or the atm center we entered might be a fake and doesn't belong to any bank.

There is no end to these kinds of possibilities and there is countless number of possibilities, the only thing is the fact that Technology today is playing with our privacy.

At this point we need to think about three questions:-

1. How far **it is** secured?
2. How far **we are** secured?
3. How far **we can** secure?

Note:- An operating system is a large instruction set which make a computer to function, as the instruction list is very huge and many people will work on building it, it may have some errors.

Now let us discuss about these three things.

How far it is secured:-

While the internet and cyber world is not being controlled by a single authority and nor every country had strict privacy control measures and good cyber law framework we can't say that it is a secured place.

The only thing that is done: the organizations take steps and put in efforts to see that their

Note: - There are lakhs of computer viruses and other exploits over the computers and internet searching for victims and this number is increasing day by day.

servers are secure which in turns protect us to some extent. Like Microsoft will strictly protect their live.com servers which in turn protect our e-mail addresses and files hosted/stored in them, coming to their consumers they will just provide some educational tips and they cannot protect each and every computer of their users as it is practically impossible to do.
So we can say the cyber world is not fully secured.

How far we are secured:-

The only reason that most of we are playing safe in the cyber world is not that we are secured, but, we are just protected by our luck and it is true in most of the cases. There are thousands and lakhs of instances of identity theft, privacy violations, cyber attacks, and there are thousands of viruses/Trojans/spyware etc and hundreds are made daily, the mentioning of the figures would amount to a wasteful task as one can even bing/google it and check.

How far we can secure:-

Now this is the thing which is in our hands, starting from here we will be discussing about different online and offline privacy/security threats and measures that we should adopt to secure from them.

Tip: - Its always a best practice to update the operating system. As we saw previously that the operating system program is not necessarily error free the company which made it will release occasional patches to resolve those errors. So at least install the recommended updates and all security patches to keep your computer at its best performance and secured

Meet the Hackers

The term "hacker" is often used to refer to a computer pirate. Victims of hacking on computer networks like to think they have been attacked by experienced hackers who have carefully studied their system and developed specific tools to exploit its flaws.

The term hacker has had more than one meaning since it first appeared in the late 1950s. In the beginning, this word was favorably used to describe expert programmers. Then in the 1970s it was used to describe computer revolutionaries, who mostly went on to become the founders of major computer companies.

It was during the 1980s that this word was used to categorise people involved in video game piracy, by disabling the protections on these games and reselling copies of them.

Today, this word is often wrongly used to refer to people who break into computer systems.

Actually a Hacker is a person who had sound programming, networking and system administrative skills; He will not misuse his skills for malicious purposes. The person who uses these skills for malicious purposes is referred

as Cracker and not hacker but unfortunately people use the words hacker and cracker as synonyms

Types Of Hackers:-

Not all hackers are the same. There are different types of them, with their own technical name. Hackers are categorized by their 'hat':

White hats: hackers in the noble sense of the term, whose goal is to help improve computer systems and technologies, are generally responsible for the main computing protocols and tools we use today. E-mail is one of the best examples The good guys. They are harmless, and if they find some security flaw, then they tell the administrator, and help to fix it.

Black hat: Black hat hackers have no morals. They are the bad guys you hear about in the news, who sack websites and the like for profit or fun. These are also called as Crackers

Gray hat: Hackers with morals, that can be good or bad, but most likely both to most people. They may attack a site or network they do not agree with, but are generally harmless.

All the people who does attacks on cyber world need not be hackers or crackers, There are are many more types of them :-

"Script kiddies" (also sometimes called crashers, lamer and packet monkeys) are young network users who use programme/software and exploit tools they have found on the Internet, to attack other systems and users just for fun and with out having any actual target or aim. These people sometimes don't know what exactly they were doing.

"Phreakers" are hackers who use the switched telephone network (STN) to make free phone calls thanks to electronic circuits (called boxes, like the blue box, the violet box, etc.) connected to the telephone line in order to manipulate its functioning. The word "phreaking" therefore refers to telephone line hacking.

"Carders" mainly attack chip card systems (particularly bank cards) to understand how they work and to exploit their flaws. The term carding refers to chip card piracy.

"Software Crackers" are people aiming to create software tools that make it possible to attack computer systems or crack the copy protection of payware, Make a trail ware to a full version software A "crack" is therefore an executable program created to modify (patch) the original software so as to remove its protection.

The "1337" Language:-

This language, mainly used by script kiddies in the underground culture, is called "1337" language. It consists of replacing certain letters (vowels, most of the time) with numbers

l33t or Eleet (sometimes rendered Leet, 1337, or 31337), also known as Leetspeak, is an alphabet used primarily on the Internet, which uses various combinations of ASCII characters to replace Latinate letters. The term is derived from the word "elite", and the usage it describes is a specialized form of symbolic writing. Different "dialects" or varieties of leet are found on different online forums

Initially, the word l33t was used as an adjective, to primarily describe the behavior or accomplishments of others in the community, with “lame” being its antonym. In that usage Leet generally carries the same meaning when referring to either the game prowess, n00b ownage, or, in original usage, hacking expertise of another person. From adjective form its use then expanded to include use as an expletive or interjection in reaction to a demonstration of the former qualities. With the mass proliferation of Internet use in the 1990s into the 21st century, Leet has since become a part of Internet culture and slang. Leet may also be considered a substitution cipher, albeit with much variation from user to user.

Malicious programs -1

Virus

A virus is a program with the ability to reproduce and spread rapidly. It is often difficult to eliminate. A virus infiltrates a file and is spread as that file is copied and forwarded to other computers. At the very least a virus can cause problems by taking up storage capacity and memory and slowing general computer performance. However some viruses can destroy files, reformat hard drives or cause other damage. The term "virus" is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability. A true virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive.

> Tip:-Antivirus software which is not updated regularly is equal to a soldier in border who is living without food and without any communication with the officials. So it's a must practice to update the antivirus software regularly.

Computer worms

Worms differ from viruses in that they don't reproduce by infiltrating files it is a self-replicating computer program. For example, a network worm spreads by reproducing itself throughout a network system. An Internet worm sends copies of itself through the Internet system via poorly protected computers. An e-mail worm sends copies of itself via the e-mail system. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or devour files on a targeted computer.

> Note:- Virus is nothing but a small program containing a set of instructions which are usually destructive or offensive in nature and as the CPU had no commonsense or IQ it, when infected, It will blindly follow those instructions effecting the user.

Malware

Malware, malicious software, is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term "computer virus" is

> Tip:-Certain malicious programs name themselves as antivirus software or virus removal utilities but don't trust and install them only insist on good company antivirus software.

sometimes used as a catch-all phrase to include all types of malware, including true viruses.

Trojans

Trojans The name is derived from the Trojan Horse of Helen of Troy fame. It is a particular type of malware used to infiltrate a computer without the user's knowledge. Trojans may install a so-called "keystroke logger", which can record all the keystrokes entered on a computer keyboard or else install a back door or trap door (discussed in Other page) information is then passed on to fraudsters via the Internet Trojan Horses (not technically a virus) can be easily and unwittingly downloaded. For example, if a computer game is designed such that, when executed by the user, it opens a back door that allows a hacker to control the computer of the user, then the computer game is said to be a Trojan horse.

Another form of Trojan allows infected computers to be targeted for a "denial of service" attack. The aim is to deny the victim access to a particular service. Such an attack can effectively disable your computer or network - with possible disastrous consequences depending on the type of organization. Unlike viruses, Trojans cannot reproduce.

Trojan Horses (not technically a virus) can be easily and unwittingly downloaded. For example, if a computer game is designed such that, when executed by the user, it opens a back door that allows a hacker to control the computer of the user, then the computer game is said to be a Trojan horse.

They are classified based on how they breach and damage systems. The six main types of Trojan horse payloads are:

Remote Access (like backdoors)
Data Destruction
Downloader/dropper
Server Trojan(Proxy, FTP , IRC, Email, HTTP/HTTPS, etc.)
Disable security software
Denial-of-service attack (DoS)

Tip:-Keeping an antivirus is just like having a personal or family doctor; it may or may not cure your system, there are viruses and other malicious programs which can hide away from antivirus software. So prevention is always better than cure.

Logic bomb:-Also referred as a time bomb is a program that executes at a specific time or when certain instructions are executed, typically destroying or re-writing the data

Back Door:- A secret programming feature which allows unauthorized access to computer systems known as a method of intrusion

Trap door:- A hidden software or hardware mechanism that can be triggered to allow system protection mechanisms to be circumvented. It is activated in some innocent appearing manner. Software developers often

introduce trap doors to enable them to reenter the system and perform certain functions

Protection tips:-

Use a good Anti-virus Software like Microsoft Security essentials:-

Microsoft Security Essentials provides real-time protection for your home PC that guards against viruses, spyware, and other malicious software.

Microsoft Security Essentials is a free download from Microsoft that is simple to install, easy to use, and always kept up to date so you can be assured your PC is protected by the latest technology. It's easy to tell if your PC is secure — when you're green, you're good. It's that simple.

Microsoft Security Essentials runs quietly and efficiently in the background so that you are free to use your Windows-based PC the way you want—without interruptions or long computer wait times.

Get it from Here: - http://www.microsoft.com/security_essentials/

Malwarebytes is a site dedicated to fighting malware. Malwarebytes has developed a variety of tools that can identify and remove malicious software

from your computer. When your computer becomes infected, Malwarebytes can provide the needed assistance to remove the infection and restore the machine back to optimum performance.

Download link:-

http://www.malwarebytes.org/

click on the free version to get the download.

Malicious Software Removal Tool

The Microsoft Windows Malicious Software Removal Tool checks computers running Windows 7, Windows Vista, Windows XP, Windows 2000, and Windows Server 2003 for infections by specific, prevalent malicious software—including Blaster, Sasser, and Mydoom—and helps remove any infection found.

When the detection and removal process is complete, the tool displays a report describing the outcome, including which, if any, malicious software was detected and removed.

Download here:-

http://www.microsoft.com/security/malwareremove/default.aspx

Malicious Programs-2

Spyware, Ad-ware

These are also called privacy-invasive software

Spyware

While the term spyware suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habits, sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software, and redirecting Web browser activity.

> Tip:-Don't install or download any software or program from unverified or untrusted sources.

Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet or functionality of other programs. In an attempt to increase the understanding of spyware, a more formal classification of its included software types is captured under the term privacy-invasive software.

Adware

Adware or advertising-supported software adware is a software application in which advertising is displayed while the program is running. This may take the form of pop-ups or banners which appear on the computer monitor. Advertisers pay for the service and help to recover some of the costs of software development, thus keeping the price low or even free, whilst the programmer still makes a profit. Adware may run on a computer without the users knowledge, having been included in shareware or freeware downloaded from the Internet. Most adware affects the various Windows operating systems and may be noticeable by the presence of more pop-ups on the web browser and a possible reduction in computer performance. Some types of adware are also spyware.

> Tip:-Don't install any toolbars except they are made by reputed companies like Microsoft, yahoo, Google etc. My personal recommendation is don't use any toolbar they may cause performance and privacy related issues. And it's always better to have few selected addons for the browsers

Browser hijacking

Browser hijacking is a form of malware or spyware. Attacker use malicious software to take control of your computer's Internet browser and replaces the existing internet browser home page, error page, or search page with its own.

Suggested Software to protect your PC:-

Spybot - Search & Destroy detects and removes spyware, a relatively new kind of threat not yet covered by common anti-virus applications.

Spybot-S&D can also clean usage tracks, an interesting function if you share your computer with other users and don't want them to see what you have been working on. And for professional users, Spybot-S&D allows you to fix some registry inconsistencies and extended reports.

Download it from here:-

http://www.safer-networking.org/en/mirrors/index.html

Windows Defender detects and removes spyware

Windows Defender is software that helps protect your computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software by detecting and removing known spyware from your computer. Windows Defender features Real-Time Protection, a monitoring system that recommends

actions against spyware when it's detected, minimizes interruptions, and helps you stay productive.

Download link:-

http://www.microsoft.com/windows/products/winfamily/defender/default.mspx

key logger

There are hundreds of **key logger** programs available over the internet for download.

Tip:-While doing any e-commerce truncations like online purchases preferably use the service of virtual credit card instead of using internet banking or debit/credit card. Virtual credit card is a kind of prepaid credit card and banks like ICICI, HDFC are offering this service.

There are 2 types of software key loggers

* Normal key loggers which if installed in your system logs all the keystrokes and will save in a text file in your system itself.
* Remote key loggers which if installed in your system mail the logs of your keyboard to attacker using SMTP server or FTP server.

* Key loggers can be sent to your system through internet, Mail attachments, cd/dvd pen drives etc.

* The most interesting thing is a clever attacker can bind a key logger with other program like normal Winamp, Yahoo messenger and even Images/Photos.

There are hundreds of keylogging malware over the net just bing/google them or search in any virus encyclopedia to see for yourself.

> Note:-Alternate keyboard layout is nothing but changing your keys on the keyboard using software however users may feel difficult while typing because many of us got used to the qwerty keyboard and will be difficult for us to shift from it.

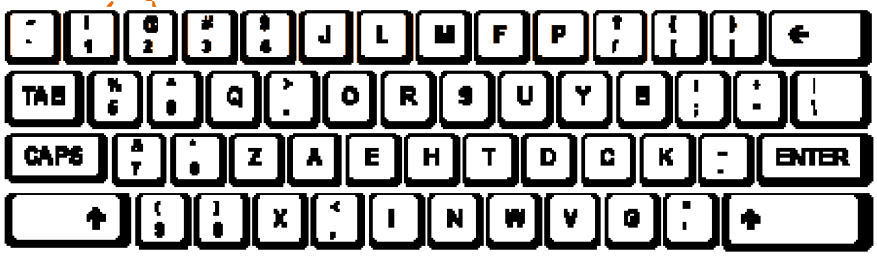
•Alternative keyboards make captured keystrokes look like nonsense

•You can customize your own board with Microsoft Keyboard Layout Creator

•Download link:- http://www.microsoft.com/globaldev/tools/msklc.mspx

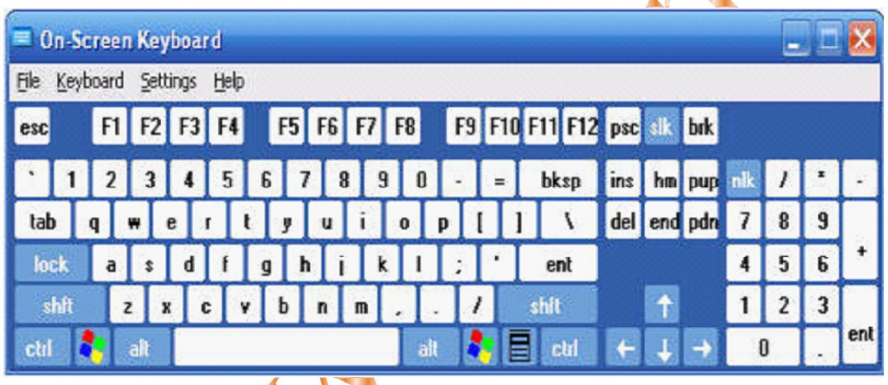
•This can also bypass / confuse Hardware key loggers

Because most key loggers expect you to be using the standard keyboard, using an alternative layout will make the data any keylogger intercepts as gibberish, unless they can convert it.



Software based keyboards are not very effective because Clicks are converted back to keystrokes. But they work in case of hardware key loggers (In xp go to start->all programs ->accessories ->accessibility->on screen keyboard)

Tip:-A good firewall can always alert the user about key logging, other malicious activities and will also protect from unauthorized intrusions into the system.



These are not 100% effective for software keyloggers because most of these programs convert the mouse click into a keyboard event message that must be sent to the external target program to type text, like the version that comes with Windows XP.

However Web-based Keyboards offer more protection

Tip:-Don't store your passwords in browsers even though you are the only person who uses it. At least do not store passwords or login information of your bank account.

Rootkits

- Root refers to top level user or super user or system administrator

- A rootkit is software which is typically a collection of tools that enable administrator-level access to a computer or computer network and to hide the attacker presence on a computer system.

- It allows the attacker to mask intrusion and gain root or privileged access to the computer and, manipulate the data set the operating system relies on, or alter the execution flow of the operating system, replace vital system executables

- A rootkit being a collection of several exploit tools may consist of Trojans, spyware used for the purpose of monitor network traffic and keystrokes, create a "backdoor" into the system for the hacker's use, alter log files, attack other machines on the network, and alter existing system tools to escape detection.

- Rootkits are designed to be difficult to detect by normal means of course it depends upon the programmer's skill.

- Rootkits make way for the attacker to execute further exploits at an ease. In short it is an attacker's spy-agent in the victim's computer.

- Rootkits misguide users as if they are safe and essential programs to run their systems by concealing running processes from monitoring programs, or hiding files or system data from the operating system. They may also prevent the antivirus scan to work.

- The presence of a rootkit on a network was first documented in the early 1990s. At that time, Sun and Linux operating systems were the primary targets for a hacker looking to install a rootkit. Today, rootkits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network.

Types of rootkits:-

Rootkits can be divided into

1) Firmware,
2) Virtualized,
3) Kernel,
4) Library and
5) Application level kits

And the sub types can be :-

- ✓ Memory-based and
- ✓ Persistent

Firmware:-

- John Heasman from Next Generation Security Software demonstrated a rootkit that hides itself in firmware.
- Completely erase the hard drive, reinstall the OS, and the rootkit is right back where it was before your exercise in futility.

- Firmware rootkits aren't an imminent threat, but Heasman's demonstration shows that we can't ignore the firmware in systems anymore.
- You probably don't even know the entire firmware device on your network, Many PCI cards, and even your system clock, have flashable memory.

Virtualized:-

- The lowest level of rootkits produced is virtualized rootkits.
- These rootkits function by the modification of the systems boot sequence, to be loaded instead of the original virtual machine monitor or operating system.
- A virtualized rootkit is able to intercept all hardware calls made by the guest operating system by loading the original operating system as Virtual Machine.

Kernel level:-

- These will cover backdoors on a computer system by writing additional code or by replacing portions of kernel code with modified code via device drivers.
- These are just used to protect backdoors from being detected or suspected.

Library level:-

- These usually patch, hook, or substitute standard application binaries with trojanized fakes, or the behavior of present applications can be modified by hooks, patches, injected code or some other manner.
- Many cracks and patches that are available over net for cracking software will mostly contain these kind of rootkits.

Rootkit Subtypes –

Memory-based –

- These types of attacks are usually used as information gathering missions by an attacker that has already discovered when a machine is normally turned on or running.

- These kinds of rootkits are extremely stealth and virtually impossible to detect due to the short life-span (removed upon reboot) nature of their existence.

Persistent Rootkits

- A persistent rootkit is one associated with malware that activates each time the system boots.
- Because such malware contain code that must be executed automatically each system start or when a user logs in, they must store code in a persistent store
- Generally these are stored in the Registry or file system or startup information.

Solution and detection :-

To get rid of rootkits you can use the following programs along with your regular antivirus software

F-Secure BlackLight

http://www.softpedia.com/progDownload/F-Secure-BlackLight-Rootkit-Detection-Download-32720.html

Rootkit reveler

http://technet.microsoft.com/hi-in/sysinternals/bb897445%28en-us%29.aspx

Tip:-Always use a good firewall in your system.

At least use the windows inbuilt firewall or prefer the following:-

ZoneAlarm Free Firewall blocks hackers from infiltrating your home PC by hiding your computer from unsolicited network traffic. By detecting and preventing intrusions, ZoneAlarm Free Firewall keeps your PC free from viruses that slow down performance, and spyware that steals your personal information, passwords, and financial data.

• Essential firewall protection

• Be invisible to others online

• New interface makes it even easier—smaller size keeps it light

Download from:-

http://www.zonealarm.com/security/en-us/zonealarm-pc-security-free-firewall.htm

Comodo Internet Security 4.0 includes a built-in sandbox which combines file system/registry virtualization and least-privileged user account principle in order to combat unknown malware.

During the setup process you will be given the choice to:

- Install the AntiVirus as a standalone
- Install the Firewall as a standalone
- Install both Firewall and AntiVirus

Download here:-

http://personalfirewall.comodo.com/free-download.html

Cookies

HTTP cookies, more commonly referred to as Web cookies, tracking cookies or just cookies, are parcels of text sent by a server to a Web client (usually a browser) and then sent back unchanged by the client each time it accesses that server. HTTP cookies are used for authenticating, session tracking (state maintenance), and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts

- ✓ Cookies store sensitive tracking and authenticating data of the user.
- ✓ These files are stored in the users PC in temporary internet files.
- ✓ The cookies can be opened by the notepad itself and there are many tools for decrypting them.
- ✓ By stealing cookies of a user the attacker can extract sensitive data from the code contained in those cookies
- ✓ The attacker can even directly login to the website by placing the user's cookie in his temporary internet files.

- ✓ The Attacker can steal the cookie in your system by using XSS attack or even by sniffing.

Also:-

- ✓ An attacker can easily steal passwords Stored in the web browsers browser.
- ✓ The attack in this case is almost similar to cookie staling method.

Prevention:- Always clear your browsing history cookies temporary internet files etc

Don't store you passwords inside the web browsers

Use cleaners like Ccleaner etc to clean the history and temporary files.

Tracking cookie

- ✓ A **tracking cookie** is a cookie that tracks or monitors your browsing behaviors like websites we are visiting, web browsing habits etc.

Tip:-Tracking cookies are generally removed many anti-spyware solutions like Zone alarm and even spybot search and destroy will also clear your browsing history and traces.. So if you have one then no need to bother.

- ✓ They will also collect information about pages and advertisements we have seen or any other activity during browsing.
- ✓ Marketers use this data to understand how users use their partner websites and optimize their networks for the average user that visits their networks.
- ✓ Tracking cookies even though not dangerous may however potentially affect your privacy.

Suggested tools:-

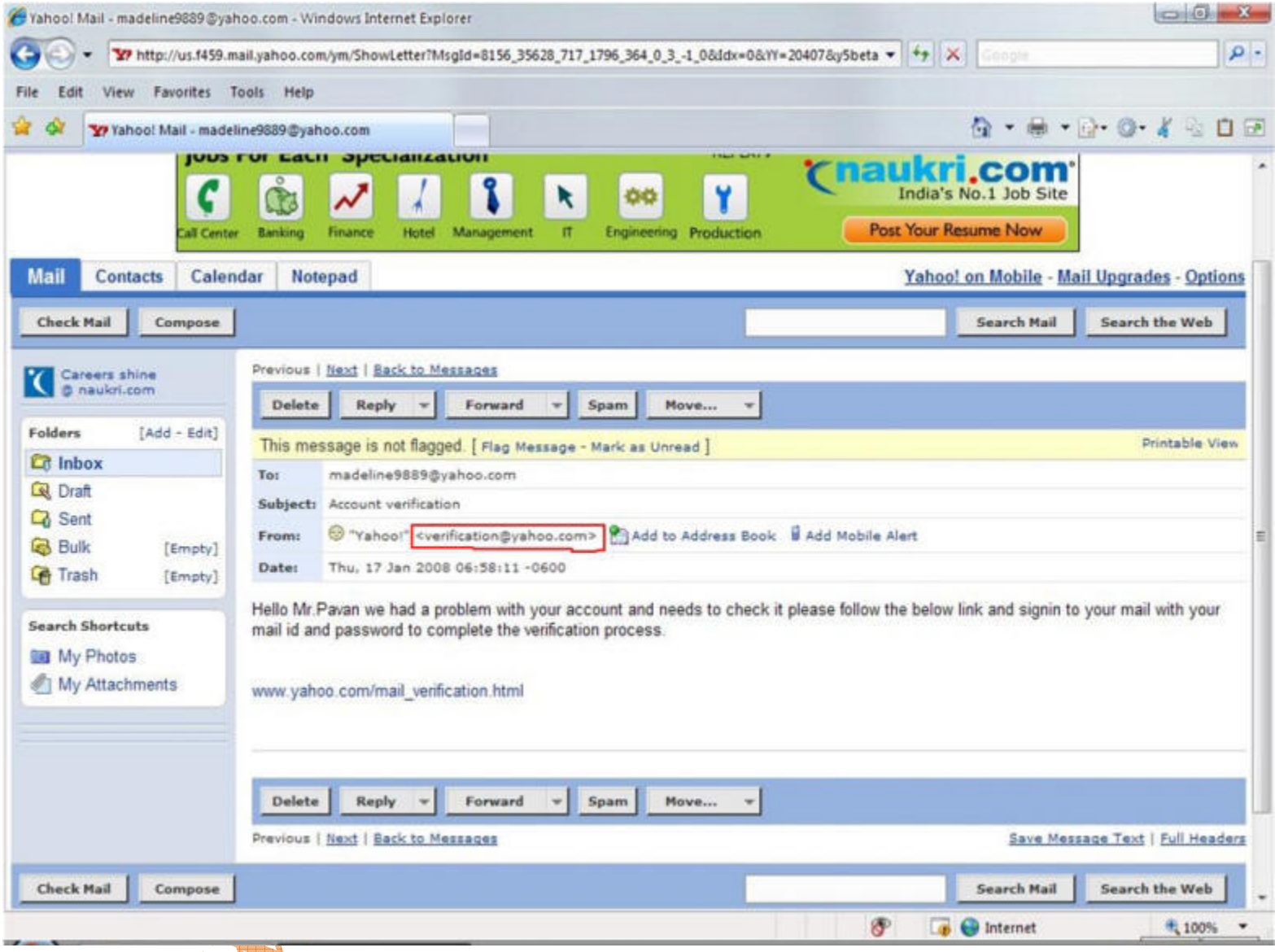
CCleaner is a freeware system optimization, privacy and cleaning tool. It removes unused files from your system - allowing Windows to run faster and freeing up valuable hard disk space. It also cleans traces of your online activities such as your Internet history. Additionally it contains a fully featured registry cleaner. But the best part is that it's fast (normally taking less than a second to run) and contains NO Spyware or Adware! :)

Download link:-

http://www.ccleaner.com/download

Phishing

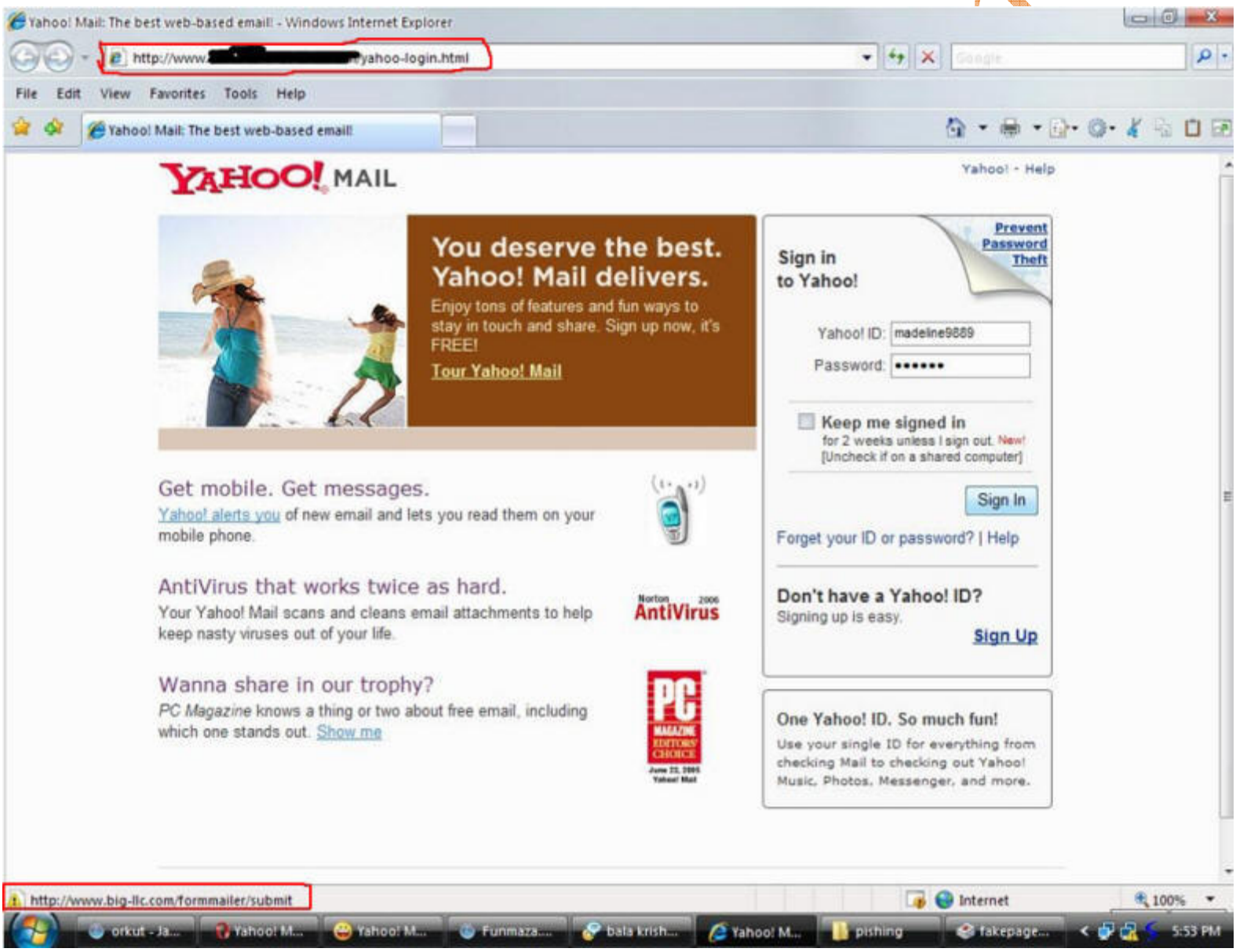
- First identified in 1996,
- Fraudsters acting as legitimate organizations such as banks send misleading e-mails requesting personal and financial details from unsuspecting recipients. OR
- A message requests the recipient to "update" or "validate" his account information by clicking on a link user's account, may get suspended. Or
- The message requests the recipient to send his personal details along with login information like id, password etc. as a reply to that mail or to any other mail id.
- To avoid having his account suspended, the user follows the e-mail instructions and the trap is sprung.
- The link directed opens a fake page of the official website.
- Thousands of such e-mails are sent out in the hope of catching out a few of the unwary.



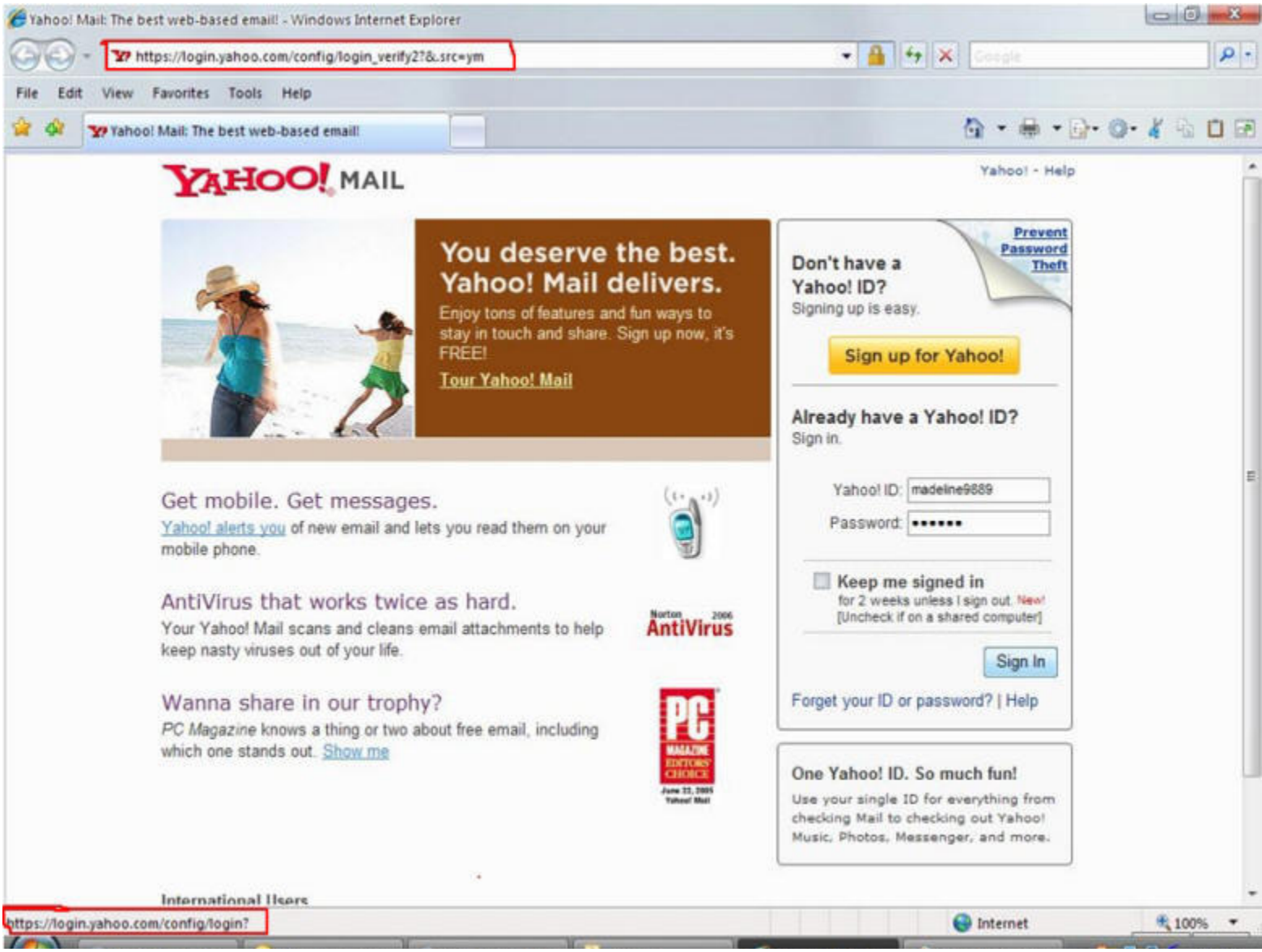
- **Example of phishing e-mail**

In the above image see the from email address it is from

verification@yahoo.com but it is a fake one and when the victim follows those instruction and open the html wrapped link he will get the following fake page:-



Let us compare this fake page with the original yahoo login page:-

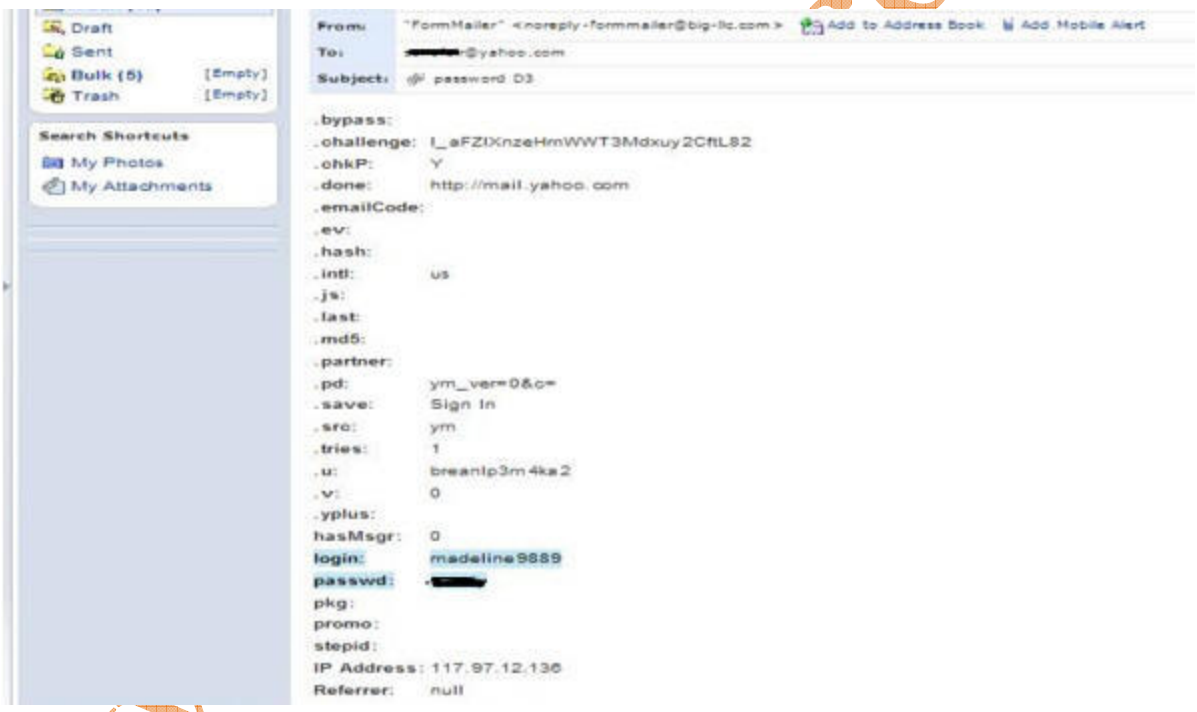


The only difference between these pages is in the red boxes and its the only way to detect a fake page

The original site had https (s referring to secured)

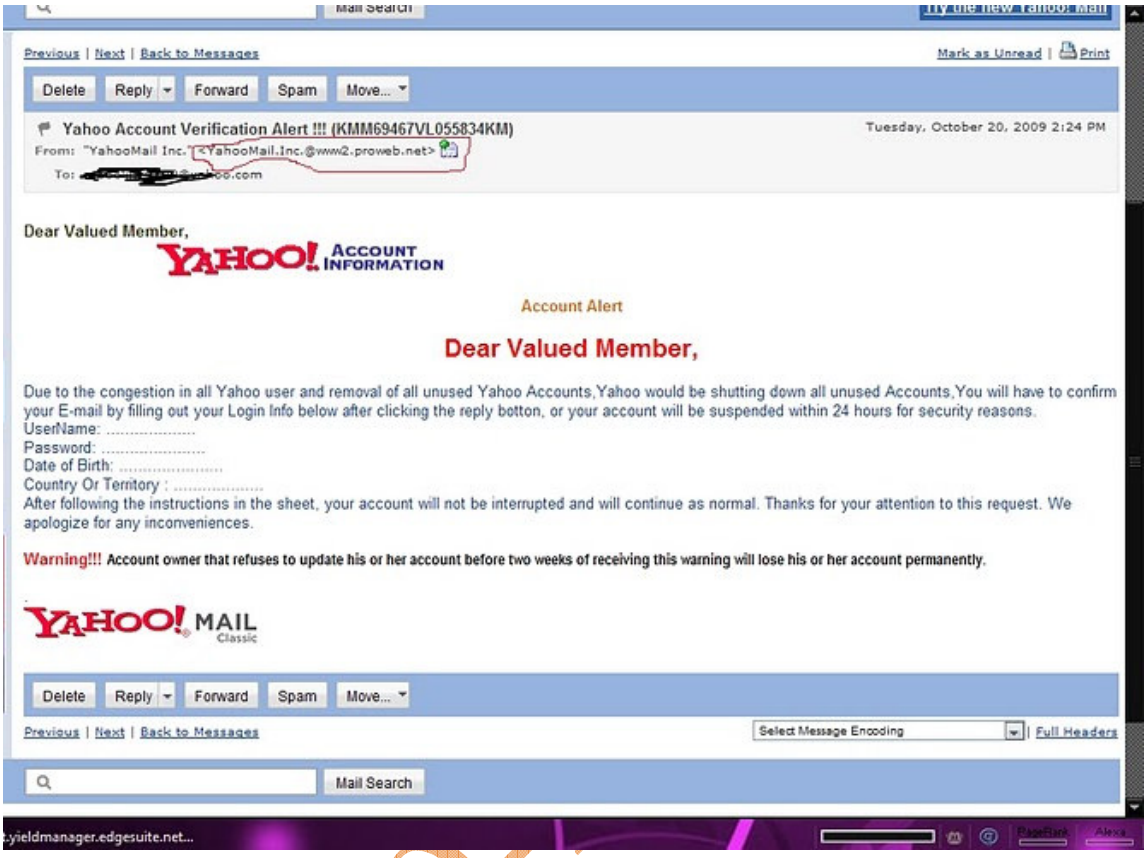
- You can clearly see the domain names in the red boxes are that of yahoo in original page where as its different in the fake page.
- Also we can check the site certificate to check whether its fake or original I will be dealing it in other chapter spoofing.

And finally the attacker gets the password of the victim directly in his inbox:-



There is another lame way of phishing; it was done on almost all famous e-mail service providers like yahoo, Hotmail, Google etc.

In this attack the spammer sends the following mail requesting the personal data of the users:-



I request u people not to fell for this lame trick and become victims. Remember Yahoo, Hotmail or even any other e-mail providers and even your banks will never ask for ur details in such a way.

Spamming and Fake E-Mail frauds

Spamming

In general spam can be defined as any unsolicited e-mail, usually in the form of advertising for a product or service. Spam wastes an enormous amount of people's time. Even though you may think an e-mail is spam, you often have to read the first sentence to be sure before deleting it. If you get dozens a day, the time wasted rapidly mounts up. Unfortunately there seem to enough people falling for the offers to make sending spam worthwhile.

> Tip: - Always delete the spam mails after marking them as spam in your e-mail account.
> Don't open any mail attachments sent from untrusted senders.
> Don't click on any links in those mails.

In addition to lost time, spam also uses up considerable bandwidth on the Internet. Despite bans, because the Internet is public it's almost impossible to prevent spam. There are organizations which try to fight spam using various techniques, and filters are available which recognize some spam

algorithmically, for example by the subject line or sender. But spammers know all the tricks and are often ahead of the game.

While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, Online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, and file sharing network spam.

Phishing e-mails, Virus hoaxes etc will also come under spam category.

Virus hoaxes

Virus hoaxes These are false alarm/warning messages normally spread through e-mails (chain messages) it's also a kind of spamming. At first a spammer send a mail containing fake information that a deadly virus is released and be careful of it .And now the unsuspecting recipients will in turn send the same to all of their contacts. However, some hoaxes go further, with a message giving directions to remove specific files from your system to get rid of the virus. This form is then no longer a hoax but is in itself a virus, because it leads

Tip: - Don't waste your time and time of your friends by forwarding the silly and stupid chain messages that contains something which never happens.

you to remove some vital file which may cause your computer to malfunction. Before reacting to any virus warning, even the one that appear genuine just google/bing it to check the genunity.

FAKE E-MAIL SCAMS

Ok i don't want to say much about this as many persons already know .

Don't ever believe the e-mail received by you saying that you have one some huge amount in a Internet lottery, or asking you about a business proposals etc.

> Tip: - Don't respond to these kinds of fake mails. By responding you are giving a hint to them that the e-mail of yours is active.
> And never fill out or give your personal information to them.

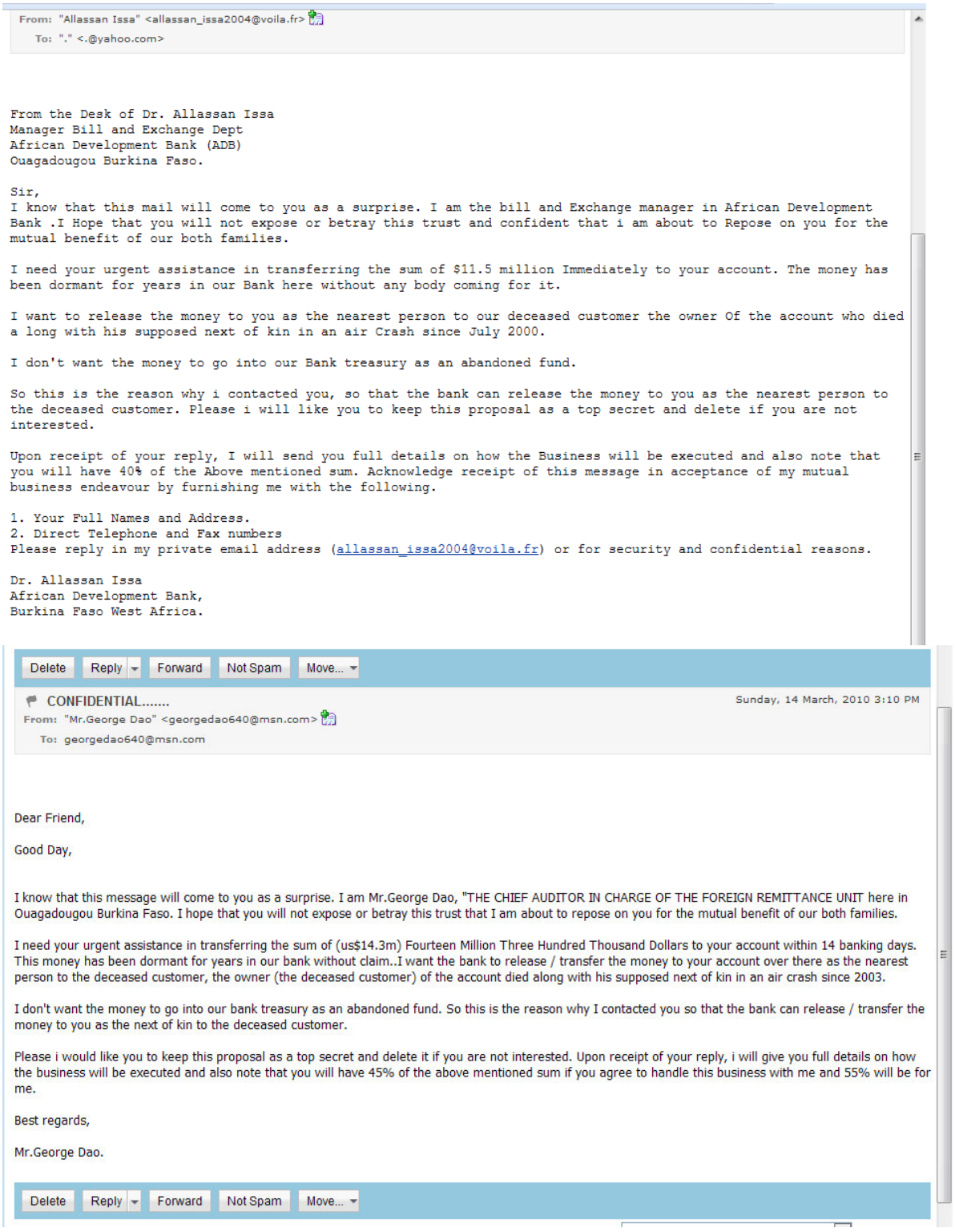
All of them are scams they will later request you money saying that they need it for paying taxes of for shipping bills etc and will fly away with those money.

Many people are already victims of these scams. Just see the following search results on these topics they are really thousands and lakhs in numbers

These e-mail will not contain your name and will have sentences like urgent, please respond, respond immediately, confidential etc.

These e-mail also request for our personal information like address, phone numbers etc.

I can give some example her in next page because I am getting at least 2 such mails daily :D



From: "Allassan Issa" <allassan_issa2004@voila.fr>
To: "." <.@yahoo.com>

From the Desk of Dr. Allassan Issa
Manager Bill and Exchange Dept
African Development Bank (ADB)
Ouagadougou Burkina Faso.

Sir,
I know that this mail will come to you as a surprise. I am the bill and Exchange manager in African Development Bank .I Hope that you will not expose or betray this trust and confident that i am about to Repose on you for the mutual benefit of our both families.

I need your urgent assistance in transferring the sum of $11.5 million Immediately to your account. The money has been dormant for years in our Bank here without any body coming for it.

I want to release the money to you as the nearest person to our deceased customer the owner Of the account who died a long with his supposed next of kin in an air Crash since July 2000.

I don't want the money to go into our Bank treasury as an abandoned fund.

So this is the reason why i contacted you, so that the bank can release the money to you as the nearest person to the deceased customer. Please i will like you to keep this proposal as a top secret and delete if you are not interested.

Upon receipt of your reply, I will send you full details on how the Business will be executed and also note that you will have 40% of the Above mentioned sum. Acknowledge receipt of this message in acceptance of my mutual business endeavour by furnishing me with the following.

1. Your Full Names and Address.
2. Direct Telephone and Fax numbers
Please reply in my private email address (allassan_issa2004@voila.fr) or for security and confidential reasons.

Dr. Allassan Issa
African Development Bank,
Burkina Faso West Africa.

Delete | Reply | Forward | Not Spam | Move...

CONFIDENTIAL.....
Sunday, 14 March, 2010 3:10 PM
From: "Mr.George Dao" <georgedao640@msn.com>
To: georgedao640@msn.com

Dear Friend,

Good Day,

I know that this message will come to you as a surprise. I am Mr.George Dao, "THE CHIEF AUDITOR IN CHARGE OF THE FOREIGN REMITTANCE UNIT here in Ouagadougou Burkina Faso. I hope that you will not expose or betray this trust that I am about to repose on you for the mutual benefit of our both families.

I need your urgent assistance in transferring the sum of (us$14.3m) Fourteen Million Three Hundred Thousand Dollars to your account within 14 banking days. This money has been dormant for years in our bank without claim..I want the bank to release / transfer the money to your account over there as the nearest person to the deceased customer, the owner (the deceased customer) of the account died along with his supposed next of kin in an air crash since 2003.

I don't want the money to go into our bank treasury as an abandoned fund. So this is the reason why I contacted you so that the bank can release / transfer the money to you as the next of kin to the deceased customer.

Please i would like you to keep this proposal as a top secret and delete it if you are not interested. Upon receipt of your reply, i will give you full details on how the business will be executed and also note that you will have 45% of the above mentioned sum if you agree to handle this business with me and 55% will be for me.

Best regards,

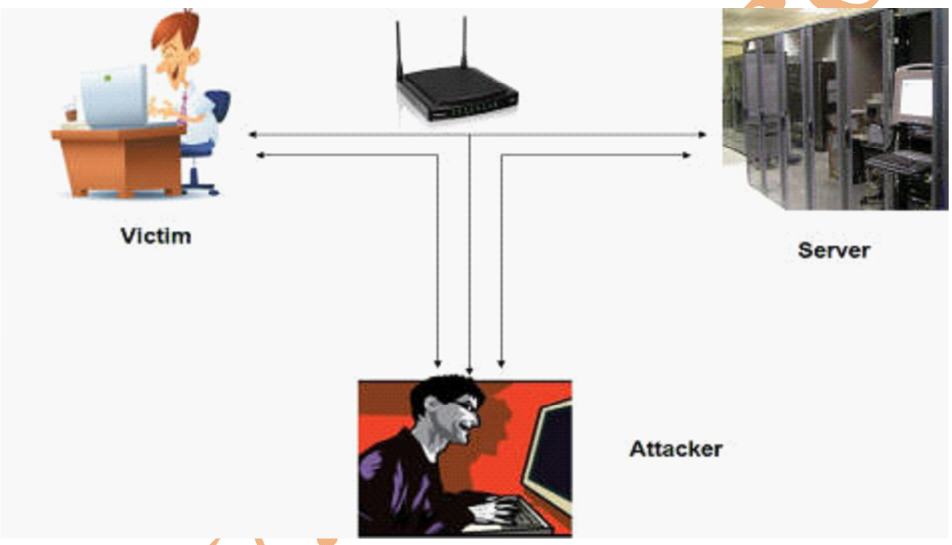
Mr.George Dao.

Delete | Reply | Forward | Not Spam | Move...

Sniffing and Spoofing

Spoofing attack is a situation in which one person or program successfully disguises as another by falsifying data/identity and thereby gaining an illegitimate advantage.

Man-in-the-middle attack and internet protocol spoofing :-



Just see the above image for better understanding. Here in this case the attacker spoofs the victim that he is the server and also spoofs the server that he the victim Thus gaining access to all information which is flowing in both the directions. The attacker may use sniffer to do this.

IP spoofing:-A technique to access a computer by using a false identity. This makes the host computer assume the hacker's computer has a trusted address.

ARP spoofing:- A procedure through which the hacker modifies the address resolution protocol (ARP) table for hacking purpose. An ARP table stores IP address and the corresponding MAC address of the computer that would be contacted to transfer data when a packet arrives on the network, the destination computer MAC address is searched. This ARP spoofing can be prevented by either using methods to deny changes in MAC address without proper authorization.

Tip: - Don't click on any links in e-mail; instead type them in the browser.
Some fake URL's will be misleading in nature like If orkut.com is correct url some attackers may set Orkult.com or orkat.com or even fatsorkut.com etc. to mislead users.

DNS spoofing:- *DNS spoofing is an attack in which the hacker modifies the IP address assigned to a web site to the IP address of the hacker's computer.*

E-mail address spoofing:- This technique is commonly used by Spammers to hide the origin of their e-mails and leads to problems such as misdirected bounces (i.e. e-mail spam backscatter). The sender information shown in e-mails (the "From" field) can be spoofed easily. E-mail address spoofing is done in quite the same way as a writing a forged return address using snail mail. As long as the letter fits the protocol, (ie. stamp, postal code) the SMTP protocol will send the message. It can be done

using to a mail server with telnet. (Refer to our phishing page section where we have spoofed the e-mail of yahoo*)*.

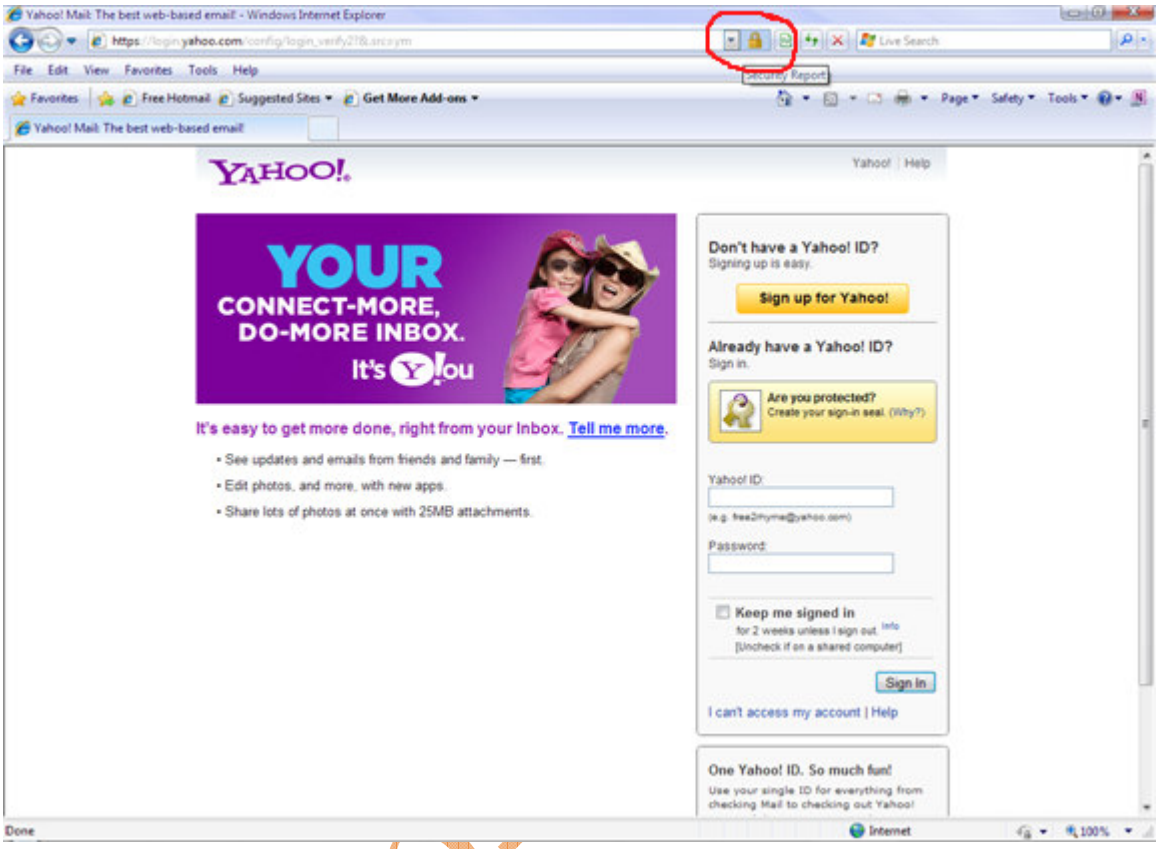
Tip: - Upgrade your internet explorer to version 8 and always keeps its phishing filter on.

A sniffer or packet analyzer or a network analyzer is a software program or hardware which can log/analyze/Captures the information over a network traffic.

Sniffers are originally made to maintain and monitor information on a network. Some companies write sniffer programs to detect network problem. But there are malicious programs used by hackers to capture information over a network these are also called underground sniffers. When installed in a router the sniffer can capture almost any data passing through the network like passwords, credit card numbers etc..

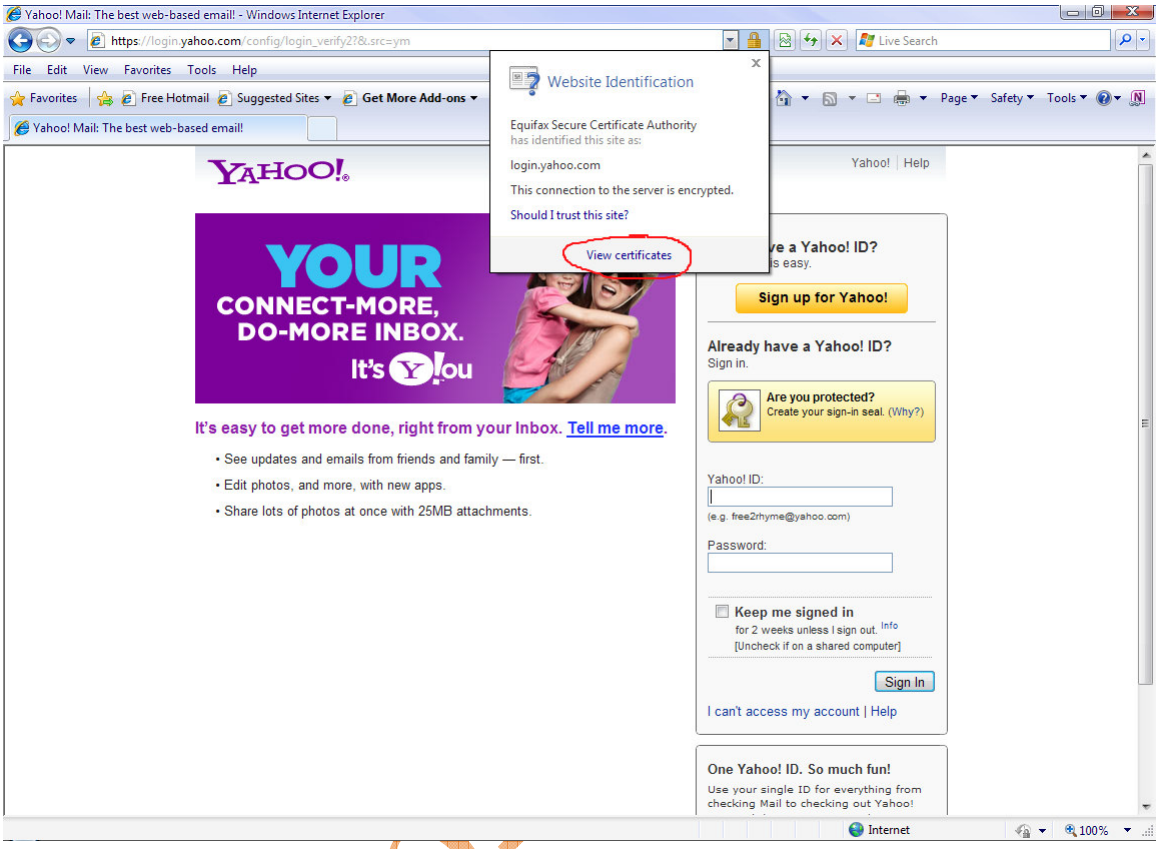
Procedure for determining a spoofed website using the site verification certificate:-

Tip: - While you are at the login screen of e-mail or bank account check whether the url in the address bar is converted to https instead of http.



Identify the lock icon in this page (rounded in red)

It contains the security report of the Https site. Just press on it.

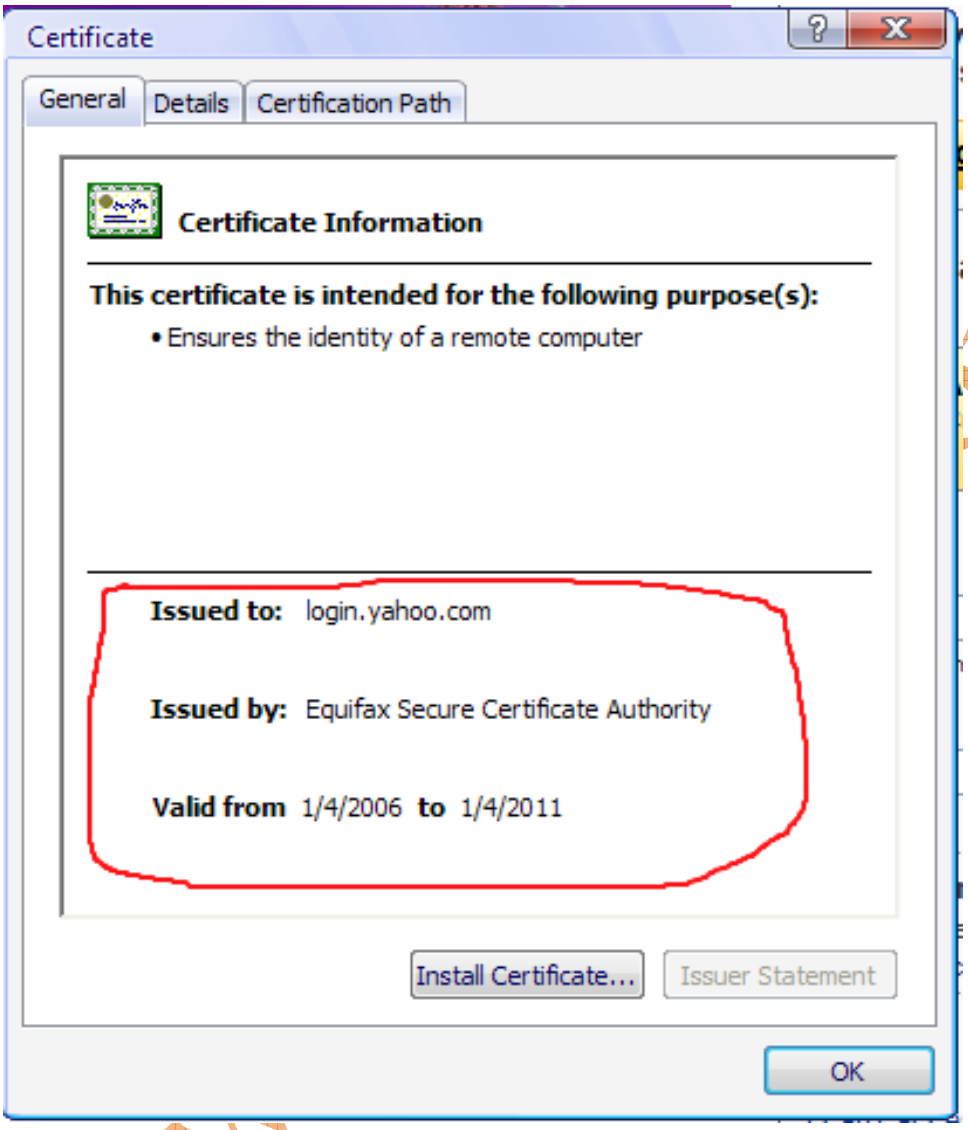


Now you will see a small pop up containing certain site information.

Now just click on view certificate (rounded in red)

We will get the following window containing certificate details like the issuer and to whom it was issued and for what purpose and when will it get expired.

We can see very clearly that the certificate was issued to Yahoo.com so this certificate is trusted and the site we have opened is original. Otherwise the situation would have been different.


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
Issued to: login.yahoo.com
Issued by: Equifax Secure Certificate Authority
Valid from 1/4/2006 to 1/4/2011
Install Certificate...
Issuer Statement
OK

XSS-Cross Site scripting attacks

These exist due to poor programming and coding and due to lack of input output validation of HTML code. These attacks are aimed at the client s or end users who use the webpage/application.

In these attacks, the attacker inserts/injects a malicious html code or any other script like java, asp etc into the existing html code of the webpage effecting all the victims who opens the webpage.

Tip: - Never run any java script codes in the browser when you are logged into certain site (like e-mail, social networking or banking etc.)

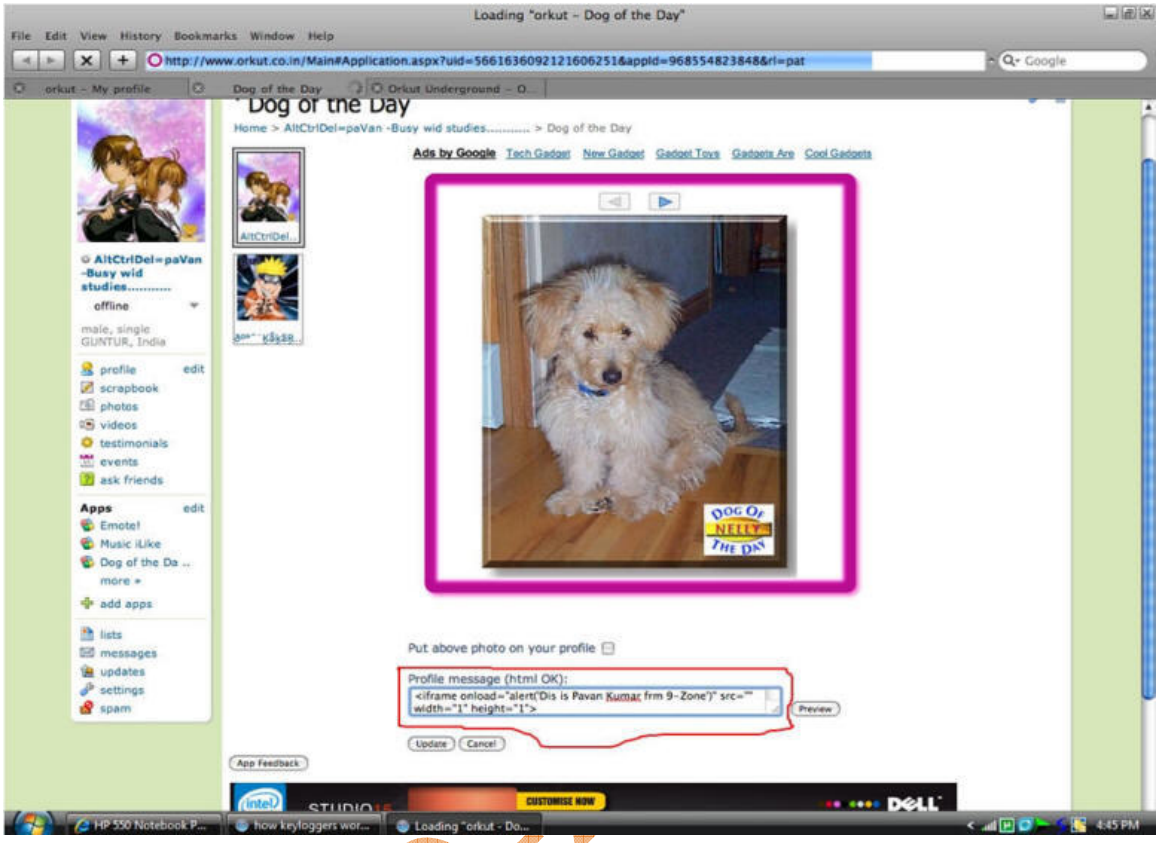
People who are the advanced users in Orkut a famous social networking site are much aware of these kinds of attacks

Tip: - When suddenly redirected from a page do not login immediately, close your bowser, delete browsing history and cookies, then type the website again for logging in.

The attacker may also inject a code which may redirect the user to an identical fake page and may steal his/her login information.

See the java script made by us using an xss exploit alert box

> Tip: - Some XSS attacks are used to steal cookies so if you are suspecting any xss attack then do clear your history and cookies in your browser and quickly change your password.



The exploit weakness was found in the dog of the day app available in orkut

See the red box, this is where the place where I injected the xss script.

Of course it was detected by orkut and patched later

Note:- I was not the person who dis covered this flaw ..I found it some where and used it for demo.

Social Engineering:-

Well there is lot to explain about this but I am just providing a brief info. A person may be your co-worker or neighbor who is an attacker wants to extract information from you. Some how he will get your bank account details gathers your personal information like date of birth, address, job title etc etc .He can now use these details for retrieving your password through phone banking or some thing else right ??

> Tip:-Always select a good and strong password that is almost difficult to guess even by your friends and family.

Even If one knows about all your personal information then he can simply click on forgot password tab in the e-mail website like yahoo gmail etc and can reset your password.

Or the attacker may call you pretending that he is your banker or your office systems

> Tip:-Dispose of your bills, bank statements, credit/debit card transaction slips, or any document containing your personal data properly if possible tear them into pieces and dispose.

administrator or something else to extract information from you

So what i want to say is keep the security questions (the option given in any password protected websites like banks e-mails etc) a logic less answer so that at least it cannot be guessed by any one. And where ever possible give some fake details.

Dumpster diving:-

This is one of the cheap stupid but very dangerous activity, In the above example we said that the attacker had some how collected your personal information right?

Do you think how??

You have just thrown your atm transaction slip in dustbin with out destroying it and now the attacker come to your hose at night time and search the dustbin to get the slip .Now he is well informed with your account number your balance etc . Hey don't laugh coz this is a common hacking technique, your telephone bills, photo copies of certificates, hall tickets, electricity bills all shall reveal at least some information to the attacker.

Let us consider the following examples for better understanding:-

- An attacker will initially collect all your information.
- Like will get your telephone bills, atm transaction slip, electricity bills, and also enquire about your business and profession.
- One fine day he uses a fancy mobile number to call upon your mobile.
- He simply says that he is your banker and tell all the details about you and your bank account since he had already collected them.
- Now he will say that they are having some problem with your bank account or credit card and will request for your password or pin number to solve the problem immediately.
- He will also add that the process requires high priority and is very urgent failing to attend it will result in closer or suspension your bank account.
- Then not all but most of us become panic and will give all most all the details asked by him and that's all we are doomed :D .

Example 2:-

- Many people have the habit of keeping their parents or children's name as e-mail or bank account password.
- And some people will have a habit of placing their last digits of mobile number or else vehicle registration number as credit card pin number.

- And do you know any attacker will first collect and try these details for breaking your password.
- So always select a difficult password having a combination of special characters, caps keys, numbers etc.
- Even while creating e-mail or other accounts where ever you need to give a security question select the answer in such a way that only you can answer it that is the answer for security question should be like your second password.
- Otherwise the attacker will simply click on forget password option and will give all your personal details to get your password reset.

Tip:-Especially for women please stop writing your pin numbers and password in small paper slips that are kept in your hand bags. Some crooks will be there who will stare at your slips and card for extracting numbers or stealing them.

Security in Internet centers

Until now we have discussed about many exploits and frauds that can be present in the today's cyber world. So by this time many of you got a question how much extent you can rely on the net centers.

Let me suggest you the following tips for your safety:-

If you are planning to plug in your pen drive at a public place or a different system then first read our article on protecting the pen drive from viruses (right click and open in new window/tab)

Before you start surfing in the public system go to internet options and delete cookies, history and temporary internet files (found in internet explorer tools menu)

Now if you are planning to do sensitive transactions then first go to the any of the following links and do a online anti-virus scan

http://quickscan.bitdefender.com/

http://www.eset.com/onlinescan/

Dont neglect this step thinking that its a time waste coz security is more important

These online scanners will search for viruses and even key loggers but you have to make sure that there is no hardware key logger in that system by looking at the cpu back panel

There is a chance of spoofing in a net center, by changing some simple system settings in the computer one can easily redirect you to a fake page so beware of phishing

If you are planning to use credit card never hand it over to any person in the net center, just enter the information all by yourself and do not allow any body to see it.

Dont allow anybody to watch your activity over your shoulder, if some one is doing so then simply ask him not to stare at your system.

Turn off remote desktop in the system which you are using (right click on my computer-properties-remote-remove tick marks on both items and click ok)

If you are an advanced user then use process explorer to check for suspicious programs running in the system.

While logging into any site check whether remember me or remember password option is turned on or not, if turned on then just simply deselect it Finally i suggest, if you want to go to net centers then give preference to the branded one.

Now the last step go to internet options and delete cookies, history and temporary internet files (found in internet explorer tools menu) this will delete you activity on the system.

Security in social networking site and instant messengers

Many of got used to IM like yahoo/live messenger, and social networking sites like orkut, facebook etc.

But do your ever wonder how much secured you are at those places ??
Many of you are almost insecure and can be attacked easily in those places, so let me suggest you few tips and trick for safety.

First and foremost is donot click on any suspicious link even if it sent by your friends, if it is sent by your friend then first get a confirmation from him and then open.

Secondly dont login from unofficial and third party sites, use only the official websites.

Instant messengers:-
http://www.9-zone.com/
http://www.9-zone.org/
http://twitter.com/9zone

Its easy for any one to trace your Ip and location while chatting you through messengers like yahoo, skype etc.

So preferably login from web based messengers like http://webmessenger.yahoo.com/ or you can chat right from your mail box (in yahoo and gmail u can directly chat from the inbox of your e-mail)

If you use normal messenger then stay in invisible mode

Dont add unknown people in your messenger list

Dont accept any files from strangers, they may contain viruses

Avoid giving personal information to strangers (u can give fake details or modified details)

Dont respond to spam/advertisements messages, if you get one then simply pres report spam option.

keep your firewall always on when chatting from normal software based messengers

Social networking sites:-

Avoid posting your personal and sensitive data in your profile

Especially for girls:-Never upload any photo of your or your friends to any of the online album also dont keep your photo as display picture.
Even boys also dont upload any of your relative/girlfriends pics into the online albums and never think that they cannot be copied, no online album is secured

Dont run any java scripts and most importantly those grease monkey scripts unless u are a advanced user and well known abt them

Beware of phishing and xss and cookie stealing in social networking sites
Dont add unknown people to your account
If you want to interact with strangers then you also create a fake account.

Dont try to install skins/themes which you got from unofficial sources.

Wi-Fi And Lan security

An eavesdropper:- is a technique in which web traffic is captured on other sites that use the unsecured HTTP address. This will not amount to be a problem when viewing normal websites like news/blogs/cricket scores etc. But when coming to sites where you need to submit logon information then comes the problem if that site doesn't use encryption.

In addition to Web browsing, other services including POP3 or IMAP e-mail and FTP file transfers are vulnerable to Wi-Fi eavesdroppers. Services like these transfer their data in clear-text, including the login credentials. Most of these services can be secured with SSL encryption, which would mean they were protected from Wi-Fi snooping; however, most users do not secure their data, which leaves the login credentials and messages vulnerable to eavesdroppers when accessed via a POP3/IMAP e-mail client, such as Microsoft Outlook, over an unsecured network.

Piggybacking:- refers to access of a wireless Internet connection by bringing one's own laptop computer within the range of another's wireless

connection, and using that service without the subscriber's explicit permission or knowledge. It is a legally and ethically controversial practice, with laws that vary by jurisdiction around the world. While completely outlawed or regulated in some places, it is permitted in others.

So to avoid this always password protect your network.

Evil Twin Or Wiphishing Or rogue access point:- These may identify themselves as "Free WiFi", An "evil twin" can be a laptop or any other machine set-up to trick users into logging onto the Internet via their "rogue" connection by mimicking the legitimate hotspot's network name and login page (where applicable). Once logged on, the hacker can create fake login prompts for popular email and banking applications thereby stealing the user's most valued login credentials.

What can be done to guard against such attacks? Look for connections that offer an SSL-encrypted login page (evidenced by https versus http in the address bar and a lock in the lower right hand corner of your web browser) that has been verified as authentic by public authorities.

Also remember the same kind of attack can be done in Lan i.e in Internet center and even for cable net users.

Some tips:-

- ✓ Its always a best practice to protect your system and internet connection with a strong password.
- ✓ Set password for each and every user in your system.
- ✓ Use proxies and virtual private networks
- ✓ Update your operating system regularly
- ✓ Use a good firewall and antivirus system and do update them regularly.
- ✓ Turn off file sharing.
- ✓ Use web based e-mail and don't use software based like thunderbird, outlook etc.
- ✓ Encrypt your files (in vista and windows 7 you can do it with bitlocker)

- ✓ A wired Ethernet connection is not a safe alternative to a WiFi hotspot. A hacker in another room can intercept all the traffic on a hotel's network, and can also easily attack any vulnerable computers.

- ✓ Programs that update themselves automatically can be easily hijacked at Hotspots (or any WiFi network) to download malware so disable autoupdate of your software.

- ✓ Turn off your internet connection and wi-fi when not in use.

- ✓ Use public dns like open dns or else Google dns for configuring your dns server .

- ✓ Don't auto connect to open connections unless you trust them.

Some Windows 7 Security Enhancements

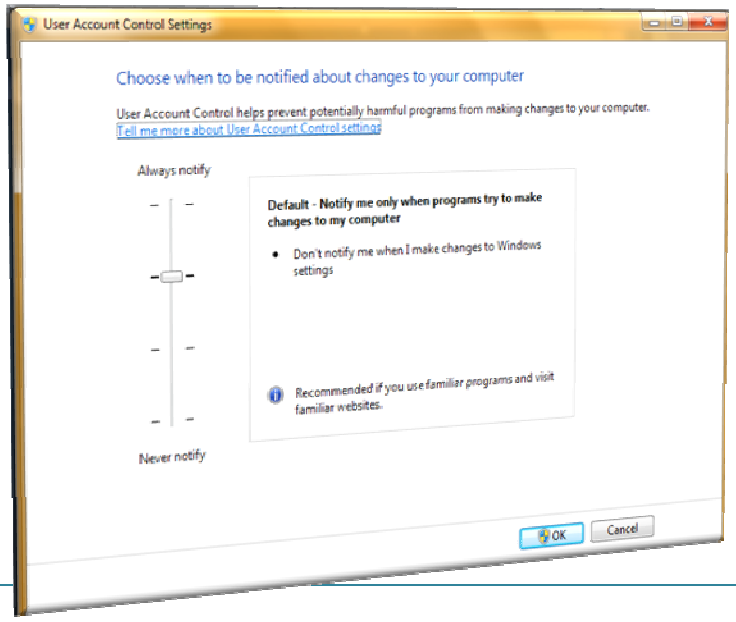
- ✓ BitLocker To Go
- ✓ AppLocker
- ✓ Security tools
- ✓ Parental Control
- ✓ Roll back system changes
- ✓ Data backup
- ✓ Internet explorer 8
- ✓ More control on UAC

More Control On UAC

User account control Has been made more flexible

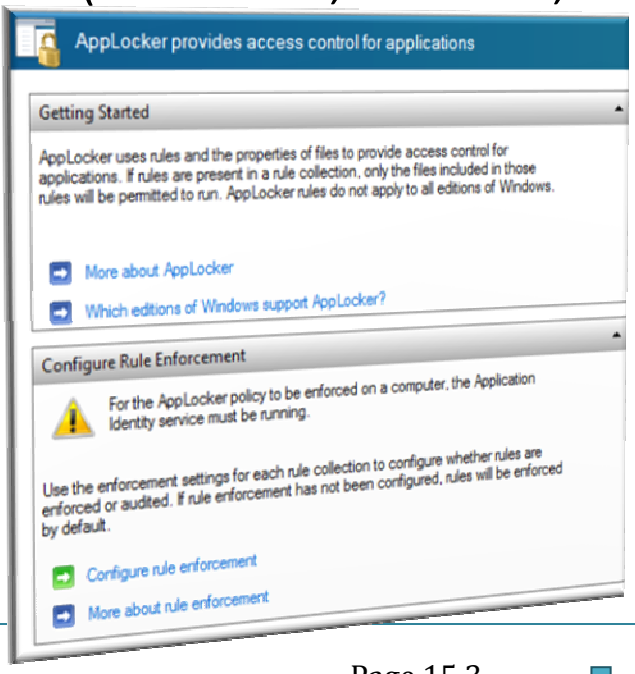
You are free to adjust UAC levels using a slider with four settings:

- Never notify,
- Only notify me when programs try to make changes to my computer,
- Always notify me,
- Always notify me and wait for my response.

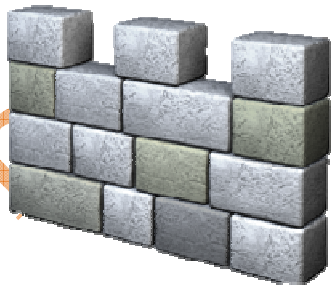


Lock Your applications Using AppLocker

- ✓ Using this you can block other users to access Executable, Windows Installers, Scripts, a specific publisher or path.
- ✓ For accessing it fire up group policy editor (start->type gpedit.msc and press enter)
- ✓ Now go to Computer configuration -> Windows Settings -> Security Settings -> Application Control Policies -> AppLocker.
- ✓ Right click on one of the options (Executable, Installers, or Script) and create a new rule.



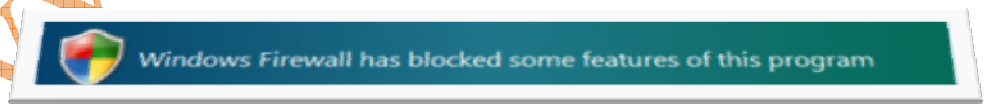
Tools Provided to Protect Your security



Windows Defender helps protect your computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software by detecting and removing known spyware from your computer.

Microsoft Security Essentials provides real-time protection for your home PC that guards against viruses, spyware, and other malicious software. And is Free……

Windows Firewall can help protect your PC from hackers and malicious software. In Windows 7, it's still powerful—but more flexible and easier to use.



The Microsoft Windows Malicious Software Removal Tool checks computers for infections by specific, prevalent malicious software—including Blaster, Sasser, and Mydoom—and helps remove any infection found.

Parental Control

- ✓ Set limits on the hours that your children can use the computer,
- ✓ The types of games they can play,
- ✓ And the programs they can run

Access it from :-

Control Panel

User Accounts and Family Safety

Parental Controls

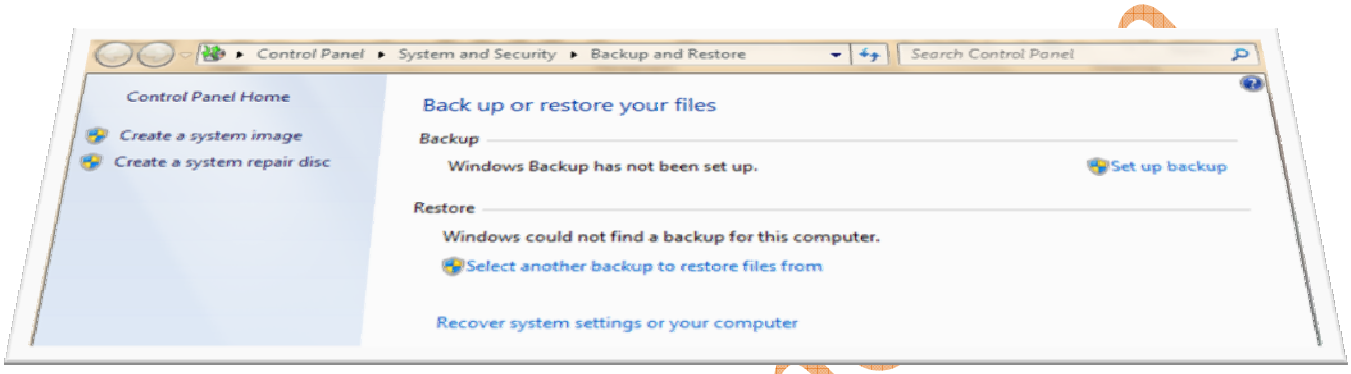
Roll Back system changes after restart

This Feature is primarily aimed at shared consumer PCs

After the user logs off, the configurations are reset back to normal

- For enabling :-
- Open Control Panel from Start Menu.
- Go to User Accounts
- Click on Manage another Accounts.
- Now select the user for which you want to set up PC Safeguard
- Click on Setup PC Safeguard
- Now click on advanced options to lock the drives u want.

Data Backup



- ✓ Once you set up a backup, Windows 7 keeps track of the files and folders that are new or modified and adds them to your backup.
- ✓ You can back up files to an external hard drive, your network, or a DVD.

Internet Explorer 8

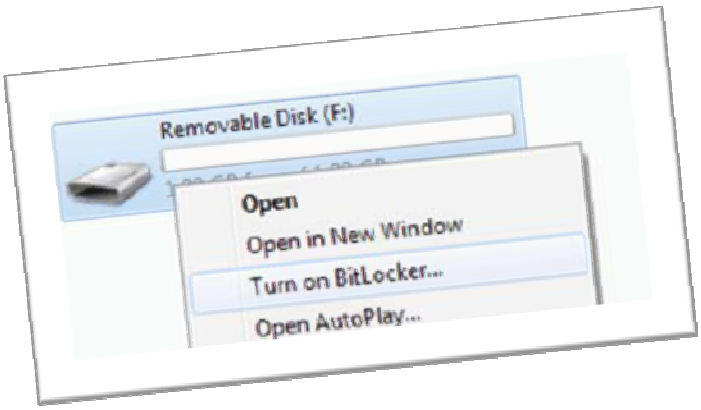
The Default browser of windows 7

- ✓ InPrivate Browsing, where data about your browsing session is not stored and temporary Internet files, web address history, cookies and passwords are all disabled.
- ✓ Protected Mode, which protects you from drive-by downloads that can happen just from visiting a website.

- ✓ SmartScreen Filter, which uses a red warning screen to prevent you from visiting unsafe sites.
- ✓ ClickJack Prevention, which allows IT pros to insert a tag that blocks clickjacking, a type of cross-site scripting.

BitLocker To Go

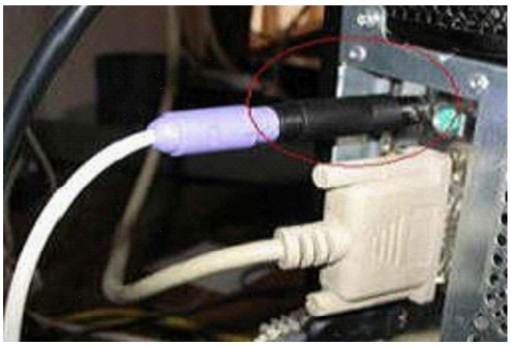
- Now encrypt your data on usb drives and removable storage devices using BitLocker to go.
- Just right click on the drive and select turn on BitLocker.



Hardware Based Attacks

Key loggers are the things which will steal the key strokes made by the user on the keyboard and stores them for retrieval. These are usually meant for monitoring the user activity on the system

Well if you think that key loggers are just Trojan programs or little software (software based Key-loggers will be discussed later in this book) then you are wrong because there are actually two types of key loggers The Is software and the other is hardware



Attackers and cyber criminals have learnt to use these key-loggers to steal private information, ids, passwords, credit card numbers etc.

Now let us first check out the hardware key-loggers: These small devices connect directly on the end of a keyboard to the port on the computer and look rather unassuming. The image here will give you and idea about how they look and work.

After installing this in the above shown manner it starts recording the keystrokes given on key board. At a later time the person who installed the key-logger can come back to retrieve it. They are easily removed.

So when ever you are browsing in a public internet café don't forget to check the back side of the CPU.

Credit/Debit Cards: you know the small innocent looking device in the right side is capable of reading and copying your entire credit card information and can create a duplicate one?

These are called credit/Magnetic card cloners or skimming machines these devices copies information from a credit card by reading the magnetic strip and can create a clone.

They fit into your palm and can be unnoticed many times; these also have a nice PC interface.

Credit card skimming can be done in restaurants, shopping malls etc. when we hand over our card to others for swiping.

As this device is very much portable and can fit in the palm, the fraudster can easily swipe the card in this small device to record the data and will later connect it to his pc to make a duplicate one.

So it is always advisable for every one in taking time to swipe their card themselves instead of handing it to others and enter the pin while no one is noticing.

And most importantly never ever use your card for swiping at un-trusted shops or restaurants the reason is very simple the card swiping machine itself may be a fake one or it may have a inbuilt card reader.

ATM Scam ever wondered that the swiping device of the atm center is actually a skimming machine which we discussed above and the pamphlet holder in the atm center or the atm machine itself had a hidden camera watching at the keyboard to track our pin number?

Yes its possible.

The fraudster will install a skimming device in place of the card swiping area and will put a security cam somewhere to take a not of our pin number. Later he will get back those devices to extract our data. He will immediately

clone our card and since he is also having our pin which was captured by his security cam h can easily withdraw the money from our account.

Check out the image in the right side we can see that a card skimmer is being attached in the area of swiping.

Now check here even after installing the skimmer the ATM machine looks good and innocent and many of us will not get any suspicions

Now notice this image we can find the hidden wireless security cam in the pamphlet holder and there are few cases where the security cam is affixed in the atm machine itself.

So be careful about any unusual items or equipment or wires in an atm center.

You know there are many instances of fraudsters placing fake ATM centers in busy areas, people how think it as a genuine atm will go in swipe their card and enter the pin.

The swiping area is actually a skimmer and the keyboard on the fake machine can log the data entered, later after some time the attacker will remove the atm machine from that spot and will recover all the card details given to them by innocent people.

So when ever you are entering into and atm center or about use and atm machine do take time to confirm whether its real one or not at least ask some one in that area whether the machine existed from long back or not.

If you are suspicious about anything then do report the same in the authorized branch.

If the atm machine performs very slow and is rejecting card or behaving in some unusual way then quickly change your pin in another atm center and do contact your bank.

Always protect your pin number, change it frequently, remember it and don't writ it anywhere and don't share it with any one.

Conclusion

- First thing I want to thank you people for reading this whole book ☺
- As this is my first book there may be some mistakes rolled in it (like grammatical or spelling etc) I hope you people will understand those things ☺
- Finally what I want to say is, we are operating in a much unsecured environment.
- What I have covered in this book is a drop in an ocean and there are many possibilities and many new are being discovered.
- However I hope that the things mentioned here will help you people to some extent in defending against cyber-attacks.
- Depending upon the success of this book I will come out with the part-2 of this edition, by end of June, which will be covering more items that will surely help you ☺
- You can find the latest updates regarding this book and content at www.9-zone.com
- Also you can find some information regarding protecting you pendrives, Virus removal instructions etc. in our site
- Click on http://www.youtube.com/watch?v=Pe0ZASy9Isw to watch a video presentation on windows 7 security enhancements.

Thank you

About the book

- This Book contains the basics and some advanced topics related to cyber security.
- It is made to create some security awareness among the netigens and people using computer systems.
- As far as possible the articles covered and topics discussed here are kept as short as possible .
- This book is made using simple language so that a laymen can also understand it.

About the Author

- Pavan Kumar Paruchuri is the editor and designer of:-http://www.9-zone.com
- And Joint editor, designer of:-http://www.9-zone.org
- He is Recognized as Most valuable professional in consumer security by Microsoft for the year 2009-2010.
- He is a MCSE(Microsoft Certified Systems Engineer) on server 2003,
- A Qualified ICWA,
- A graduate in B.Com
- And presently doing CA(FINAL).

Visit

www.9-ZONE.com