

# INTRODUCTION TO CYBER SECURITY

Jeetendra Pande

# Index

<b>1.1 INTRODUCTION .....</b>	<b>8</b>
1.1.1 HISTORY OF INTERNET .....	8
1.1.1.1 <i>Internet Addresses</i> .....	10
1.1.1.2 <i>DNS</i> .....	12
1.1.1.3 <i>Internet Infrastructure</i> .....	13
1.1.1.4 <i>World Wide Web</i> .....	14
<b>1.2 INTRODUCTION TO CYBER CRIME.....</b>	<b>15</b>
1.2.1 CLASSIFICATION OF CYBER CRIMES.....	16
1.2.2 REASONS FOR COMMISSION OF CYBER CRIMES .....	18
<b>1.3 MALWARE AND ITS TYPE.....</b>	<b>19</b>
1.3.1 ADWARE.....	19
1.3.2 SPYWARE.....	19
1.3.3 BROWSER HIJACKING SOFTWARE.....	19
1.3.4 VIRUS.....	19
1.3.5 WORMS .....	20
1.3.6 TROJAN HORSE .....	20
1.3.7 SCAREWARE .....	21
<b>1.4 KINDS OF CYBER CRIME .....</b>	<b>21</b>
1.4.1 CYBER STALKING .....	21
1.4.2 CHILD PORNOGRAPHY .....	22
1.4.3 FORGERY AND COUNTERFEITING.....	22
1.4.4 SOFTWARE PIRACY AND CRIME RELATED TO IPRs .....	22
1.4.5 CYBER TERRORISM.....	22
1.4.6 PHISHING.....	22
1.4.7 COMPUTER VANDALISM .....	22
1.4.8 COMPUTER HACKING .....	22
1.4.9 CREATING AND DISTRIBUTING VIRUSES OVER INTERNET.....	23
1.4.10 SPAMMING .....	23
1.4.11 CROSS SITE SCRIPTING.....	23
1.4.12 ONLINE AUCTION FRAUD .....	24
1.4.13 CYBER SQUATTING.....	24
1.4.14 LOGIC BOMBS.....	24
1.4.15 WEB JACKING .....	24
1.4.16 INTERNET TIME THEFTS .....	24

1.4.17 DENIAL OF SERVICE ATTACK.....	24
1.4.18 SALAMI ATTACK.....	24
1.4.19 DATA DIDDING.....	25
1.4.20 EMAIL SPOOFING.....	25
<b>2.1 AUTHENTICATION .....</b>	<b>26</b>
<b>2.2 ENCRYPTION.....</b>	<b>27</b>
<b>2.3 DIGITAL SIGNATURES .....</b>	<b>28</b>
<b>2.4 ANTIVIRUS.....</b>	<b>29</b>
<b>2.5 FIREWALL .....</b>	<b>30</b>
<b>2.6 STEGANOGRAPHY .....</b>	<b>31</b>
<b>3.1 COMPUTER FORENSICS .....</b>	<b>33</b>
<b>3.2 WHY SHOULD WE REPORT CYBER CRIME?.....</b>	<b>36</b>
<b>4.1 INTRODUCTION .....</b>	<b>40</b>
<b>4.2 SOME RECENT CYBER CRIME INCIDENTS .....</b>	<b>40</b>
<b>5.1 INTRODUCTION .....</b>	<b>47</b>
<b>5.2 COUNTER CYBER SECURITY INTIATIVES IN INDIA.....</b>	<b>47</b>
<b>6.1 GENERATING SECURE PASSWORD .....</b>	<b>52</b>
6.1.1 GUIDELINE FOR SETTING SECURE PASSWORD.....	52
<b>6.2 USING PASSWORD MANAGER.....</b>	<b>55</b>
6.2.1 WHAT IS A PASSWORD MANAGER? .....	56
6.2.2 WHY YOU SHOULD USE IT? .....	56
6.2.3 HOW DOES IT WORK?.....	56
6.2.4 SOME POPULAR PASSWORD MANAGERS.....	56
<b>6.3 ENABLING TWO-STEP VERIFICATION .....</b>	<b>62</b>
<b>6.4 SECURING COMPUTER USING FREE ANTIVIRUS .....</b>	<b>72</b>
<b>7.1 CONFIGURING FIREWALL ON MAC COMPUTER .....</b>	<b>75</b>
7.1.1 TURNING ON AND CONFIGURING THE MAC OS X FIREWALL.....	75
<b>7.2 WORKING WITH WINDOWS FIREWALL IN WINDOWS .....</b>	<b>78</b>
7.2.1 FIREWALL IN WINDOWS 7 .....	78
7.2.2 CONFIGURING WINDOWS FIREWALL .....	79
7.2.3 HOW TO START & USE THE WINDOWS FIREWALL WITH ADVANCED SECURITY.....	83

7.2.3.1 How to Access the Windows Firewall with Advanced Security .....	83
7.2.3.2 What Are The Inbound & Outbound Rules?.....	84
7.2.3.3 What Are The Connection Security Rules?.....	86
7.2.3.4 What Does the Windows Firewall with Advanced Security Monitor? .....	87
<b>8.1 FINDING THE BEST BROWSER ACCORDING TO THE USERS REQUIREMENT .....</b>	<b>89</b>
<b>9.1 SAFE BROWSING .....</b>	<b>94</b>
9.1.1 HOW DO I KNOW IF A WEBSITE IS SECURE? .....	94
<b>9.2 TIPS FOR BUYING ONLINE.....</b>	<b>95</b>
<b>9.3 CLEARING CACHE FOR BROWSERS.....</b>	<b>96</b>
9.3.1 CLEARING CACHE FOR CHROME BROWSERS ABOVE VERSION 10.....	96
9.3.2 CLEARING CACHE FOR CHROME BROWSERS FROM VERSION 1 TO 9.....	99
9.3.3 CLEARING CACHE FOR SAFARI FOR IOS, IPHONE AND IPAD.....	102
9.3.4 CLEARING CACHE FOR SAFARI FOR MAC OS X.....	103
9.3.5 CLEARING CACHE FOR SAFARI FOR WINDOWS .....	104
9.3.6 CLEARING CACHE FOR INTERNET EXPLORER 9, 10 AND 11 .....	106
9.3.7 CLEARING CACHE FOR INTERNET EXPLORER 8.....	108
9.3.8 CLEARING CACHE FOR FIREFOX .....	111
9.3.9 CLEARING CACHE FOR FIREFOX 33 .....	112
9.3.10 CLEARING CACHE FOR OPERA .....	114
9.3.11 CLEARING CACHE FOR CCLEANER .....	115
<b>10.1 WHAT IS WIRELESS LAN? .....</b>	<b>117</b>
<b>10.2 MAJOR ISSUES WITH WLAN.....</b>	<b>118</b>
10.2.1 SECURE WLAN.....	118
10.2.2 WI-FI AT HOME.....	118
<b>11.1 SAFE BROWSING GUIDELINES FOR SOCIAL NETWORKING SITES .....</b>	<b>123</b>
11.1.1 GENERAL TIPS ON USING SOCIAL NETWORKING PLATFORMS SAFELY .....	124
11.1.2 POSTING PERSONAL DETAILS .....	125
11.1.3 FRIENDS, FOLLOWERS AND CONTACTS .....	125
11.1.4 STATUS UPDATES .....	126
11.1.5 SHARING ONLINE CONTENT .....	126
11.1.6 REVEALING YOUR LOCATION .....	126
11.1.7 SHARING VIDEOS AND PHOTOS .....	127
11.1.8 INSTANT CHATS.....	127
11.1.9 JOINING AND CREATING GROUPS, EVENTS AND COMMUNITIES .....	127

<b>11.2 EMAIL SECURITY TIPS .....</b>	<b>128</b>
<b>12.1 INTRODUCTION .....</b>	<b>130</b>
<b>12.2 SMARTPHONE SECURITY GUIDELINES.....</b>	<b>131</b>
12.2.1 PURSES, WALLETS, SMARTPHONES .....	131
12.2.2 PLATFORMS, SETUP AND INSTALLATION .....	132
12.2.2.1 <i>Platforms and Operating Systems</i> .....	132
12.2.2.2 <i>Feature Phones</i> .....	132
12.2.2.3 <i>Branded and locked smartphones</i> .....	133
12.2.2.4 <i>General Setup</i> .....	133
12.2.2.5 <i>Installing and updating applications</i> .....	133
12.2.3 COMMUNICATING SECURELY(THROUGH VOICE AND MESSAGES) WITH A SMARTPHONE .....	134
12.2.3.1 <i>Secure Voice Communication</i> .....	134
12.2.3.2 <i>Sending Messages Securely</i> .....	137
12.2.3.3 <i>Storing Information on your Smartphone</i> .....	138
12.2.3.4 <i>Sending Email from your Smartphone</i> .....	139
12.2.3.5 <i>Capturing Media with your Smartphone</i> .....	139
12.2.3.6 <i>Accessing the Internet Securely from your Smartphone</i> .....	140
12.2.3.7 <i>Advanced Smart Phone Security</i> .....	141
REFERENCES.....	144

# INTRODUCTION TO CYBER SPACE

## 1.1 INTRODUCTION

Internet is among the most important inventions of the 21<sup>st</sup> century which have affected our life. Today internet have crosses every barrier and have changed the way we use to talk, play games, work, shop, make friends, listen music, see movies, order food, pay bill, greet your friend on his birthday/ anniversary, etc. You name it, and we have an app in place for that. It has facilitated our life by making it comfortable. Gone are the days when we have to stand in a long queue for paying our telephone and electricity bills. Now we can pay it at a click of a button from our home or office. The technology have reached to an extent that we don't even require a computer for using internet. Now we have internet enabled smartphone, palmtops, etc. through which we can remain connected to our friends, family and office 24x7. Not only internet has simplified our life but also it has brought many things within the reach of the middle class by making them cost effective. It was not long back, while making an ISD or even a STD call, the eyes were stricken on the pulse meter. The calls were very costly. ISD and STD were used to pass on urgent messages only and the rest of the routine communication was done using letters since it was a relatively very cheap. Now internet have made it possible to not only talk but use video conference using popular applications like skype, gtalk etc. at a very low price to a level where a one hour video chat using internet is cheaper than the cost of sending a one page document from Delhi to Bangalore using speed-post or courier service. Not only this, internet has changed the use of the typical devices that were used by us. Television can be used not only for watching popular tv shows and movies but can be used for calling/ video chatting with friend using internet. Mobile phone is not only used for making a call but viewing a latest movie. We can remain connected to everyone, no matter what our location is. Working parents from office can keep eye on their children at home and help them in their homework. A businessman can keep eye on his staff, office, shop, etc with a click of a button. It has facilitated our life in more than one way. Have you ever wondered from where this internet came? Let us discuss the brief history of internet and learn how this internet was invented and how it evolved to an extent that now we cannot think of our lives without it.

### 1.1.1 History of Internet

I don't know what the cold war between USA and Russia gave to the world, but defiantly the internet is one of those very useful inventions whose foundation was laid during cold war

days. Russia Launched the world's first satellite, SPUTNIK into the space on 4<sup>th</sup> October, 1957. This was clearly the victory of Russia over the cyber space and as a counter step, Advanced Research Projects Agency, the research arm of Department of Defence, United States, declared the launch of ARPANET(Advanced Research Projects Agency NETwork) in early 1960's. This was an experimental network and was designed to keep the computers connected to the this network to communicate with each other even if any of the node, due to the bomb attack, fails to respond. The first message was sent over the ARPANET, a packing switching network, by Leonard Kleinrock's laboratory at University of California, Los Angeles (UCLA). You will be surprised to know that the fist message that was sent over internet was "LO". Actually they intended to send work "LOGIN" and only the first two letters reached its destination at second network node at Stanford Research Institute (SRI) and before the last three letters could reach the destination the network was down due to glitch. Soon the error was fixed and the message was resent and it

The major task that ARPANET have to play is to develop rules for communication i.e. protocols for communicating over ARPANET. The ARPANET in particular led to the development of protocols for internetworking, in which multiple separate networks could be joined into a network of networks. It resulted in the development if TCP/IP protocol suite, which specifies the rules for joining and communicating over APRANET.

Soon after, in 1986 NSF(national Science Foundation) backbone was created to and five US universities' computing centres were connected to form NSFnet. The participating Universities were:

- Princeton University -- John von Neumann National Supercomputer Center, JvNC
- Cornell University -- Cornell Theory Center, CTC
- University of Illinois at Urbana-Champaign -- National Center for Supercomputing Applications, NCSA
- Carnegie Mellon University -- Pittsburgh Supercomputer Center, PSC
- General Atomics -- San Diego Supercomputer Center, SDSC

NFSnet, the successor of ARPAnet, become popular by 1990 and ARPANET was decommissioned. There were many parallel networks developed by other Universities and other countries like United Kingdom. In 1965, National Physical Laboratory(NPL) proposed a packing switching network. Michigan Educational Research Information Triad formed MERIT network in 1966 which was funded and supported by State of Michigan and the

National Science Foundation (NSF). France also developed a packet switching network, known as CYCLADES in 1973.

Now there were many parallel systems working on different protocols and the scientist were looking for some common standard so that the networks could be interconnected. In 1978, TCP/IP protocol suits were ready and by 1983, the TCP/IP protocol were adopted by ARPANET.

In 1981, the integration of two large network took place. NFS developed Computer Science Network(CSNET) and was connected to ARPANET using TCP/IP protocol suite. Now the network was not only popular among the research community but the private played also took interest in the network. Initially NFS supported speed of 56 kbit/s. It was upgraded to 1.5 Mbit/s in 1988 to facilitate the growth of network by involving merit network, IBM, MCA and the state of Michigan.

After the corporates took realized the strength and merit of this network, they participated in the development of the network to ripe its benefits. By late 1980s many Internet Service Providers(ISPs) emerged to provide the backbone for carrying the network traffic. By 1991, NFSNET was expanded and was upgraded to 45Mbit/s. Many commercial ISPs provided backbone service and was popular among the corporate. To facilitate the commercial use of the network, NFSNET was decommissioned in 1995 and now the Internet could carry commercial traffic.

Now more and more Universities and research centres throughout the world connected to it. Now this network was very popular among the research community and in 1991 National Research and Education Network (NREN) was founded and the World Wide Web was released. Initially the role of internet was only limited to file transfer. The credit of internet what we see it today goes to Tim Berners-Lee who introduced www. With the advent of www, there was a transformation on how the network was used. Now this web of information can be used to retrieve any information available over the internet. Software called, browser was developed to browse the internet. It was developed by researchers at University of Illinois in 1992 and named as Mosaic. This browser enables to browse the internet the way we browse it today.

### **1.1.1.1 Internet Addresses**

With so many devices connected to the internet, we require some mechanism to uniquely identify every device that is connected to the internet. Also we require some centralized

system which takes care of this mechanism so that the signs which are used to identify each device are not duplicate; else the whole purpose is defeated. To take care of this, we have a centralized authority known as Internet Assigned Numbers Authority (IANA), which is responsible for assigning a unique number known as IP(Internet Protocol) address. An IP address is a 32-bit binary number which is divided into four octets and each octet consists of 8 binary digits and these octet are separated by a dot(.). An example of an IP address is

**11110110.01011010.10011100.1111100**

Each 8-bits in an octet can have two binary values i.e. 0 and 1. Therefore, each octet can have minimum value 0. i.e. 00000000 to maximum value 256 i.e. 11111111 and in total have  $2^8 = 256$  different combinations.

Again to remember this 32-bit address in binary is bit difficult, so for the better understanding of the human being, it is expressed in a decimal format. But this decimal format is for human understanding only and the computer understands it in binary format only. In decimal, the above IP address is expressed as 123.45.78.125

These octets are used to create and separate different classes. An IP address consists of two parts viz. **Network** and **Host**. Network part identifies the network different network and the host part identifies a device of a particular network.

This address uniquely identifies a devices connected to the internet similar to the postal system where we identify any house by fist identifying the county, then state, district, post office, cluster/block and finally the house number. These IP addresses are classified into five categories based on the availability of IP range. These categories/classes are:

*Table 1: IP Address Classes*

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

IANA decentralises that task of assigning the IP addresses by allocating the large chunk of IP addresses to five Regional Internet Registries (RIRs), which are further responsible to

allocate the IP addresses in their zone. These RIRs along with their area of operations are listed below:

- APNIC- This RIR is responsible for serving the Asia Pacific region
- AfriNIC- This RIR is responsible for serving the African region
- ARIN- This RIR is responsible for serving North America and several Caribbean and North Atlantic islands
- LACNIC- This RIR is responsible for serving Latin America and the Caribbean, and
- RIPE NCC- This RIR is responsible for serving Europe, the Middle East, and parts of Central Asia

For liaison and coordinating between these five RIRs, there is an organization called Number Resource Organization(NRO). These organizations are

#### **1.1.1.2 DNS**

Whenever we browse any website in the internet, we type name something like www.uou.ac.in and we rarely deal with IP address like 104.28.2.92 but the fact is even if we type http:\| 104.28.2.92 in the URL, it will land us to the same webpage. The fact is we are very comfortable using and remembering the names instead of a number. Moreover, these IP address changes over time and some of the sites have multiple IP address. Also, the transfer of the data over internet is only possible using IP addresses because the routing of the packet of data sent over internet is done using IP address. There is a server called **Domain Name System(DNS)** which takes care of this translation job to simplify and to save us from remembering these changing IP address numbers, the DNS. Whenever you type an address like http:\|www.uou.ac.in, there is a process called DNS name resolution, takes place in the background. The computer keeps the track of recently visited sites and locally maintains a database in DNS cache. In case, the IP address of the site you have requested for is not found in the DNS cache of your local computer, then the next probable place to find it is DNS server of your Internet Service Provider(ISP). These DNS servers of ISP also maintain the cache of the recently visited pages. Just in case, the information is not found here also, the DNS server of the ISP forward the query to the root nameservers. The root name servers publish the root zone file to other DNS servers and clients on the Internet. The root zone file describes where the authoritative servers for the DNS top-level domains (TLD) are located. There are currently 13 rootname servers. They are:

- A - VeriSign Global Registry Services

- B - University of Southern California - Information Sciences Institute
- C - Cogent Communications
- D - University of Maryland
- E - NASA Ames Research Center
- F - Internet Systems Consortium, Inc.
- G - U.S. DOD Network Information Center
- H - U.S. Army Research Lab
- I - Autonomica/NORDUnet
- J - VeriSign Global Registry Services
- K - RIPE NCC
- L - ICANN
- M - WIDE Project

These root nameservers directs the query to the appropriate Top-Level Domain(TLD) nameservers by reading the last part of the URL first. In our example the url was <http://www.uou.ac.in>. The last part is .in. Some of the examples of TLD name servers are .com, .biz, .org, .us, .in, etc. These TLD nameservers acts as a switchboard and direct the query to the appropriate authoritative nameserver maintained by each domain. These authoritative nameserver maintains DNS records along with other useful information. This address record is returned back to the requesting host computer via TLD nameservers, nameservers, ISP's DNS server. These intermediatly server keeps the record of this IP address in their DNS cache, so that if the same request is encountered again , they don't have to go through this process again. If the same URL is requested again, the DNS cache of the local host computer will return the IP address of the URL.

### **1.1.1.3 Internet Infrastructure**

Internet, as the name suggests, in a network of network i.e. it is a collection of several small, medium and large networks. This clearly indicates to one fact, nobody is a single owner of the internet and it is one of the proven example of collaborative success. Now you must be surprised how such a large network which is spread across the continents can run without the any problem. Yes it is correct that to monitor such a large network, we require an international body which can frame the rules, regulation and protocols to join and use this network. Therefore, an international organization, known as “The Internet Society” was formed in 1992 to take care of such issues.

Let us now discuss, how this internet works? How the email you sent to your friend is received by your friend's computer located at another country/continent. When you are working in your laptop/desktop in your home without connecting to the internet, your computer is a standalone system. But, whenever you connect to the internet by dialling to your Internet Service Provider(ISP) using your modem, you become the part of the network. The ISP is the link between the internet backbone, through which the entire data route, and the user. The ISP connects to the internet backbone at Network Access Points(NAP). These NAPs are provided by the large telecommunication companies at various regions. These large telecommunication companies connect the countries and the continents by building and maintaining the large backbone infrastructure to route data from NAP to NAP. ISPs are connected to this backbone at NAP and are responsible for building and managing network locally. So when you dial internet through modem, you first become part of the local ISP, which in turn connects to the internet backbone through NAP. The data is routed through this backbone and sent to the destination NAP, where the ISP of your friend's network is located. As soon as your friend dials his modem to connect to the internet, the data is delivered to your friend's computer.

#### **1.1.4 World Wide Web**

Sometimes we interchangeably use the term internet and world wide web or simply the web, as it is popularly known as. But web is only one of the several utilities that internet provides. Some of the popular services that internet provides other than web are e-mail, Usenet, messaging service, FTP, etc. The web uses HTTP protocol to communicate over internet and to exchange information. The web was developed at CERN (European de Recherches Nucléaires), Switzerland by a UK scientist Tim Berners-Lee in 1989. It consists of all the public web sites and all the devices that access the web content. WWW is an information sharing model which is developed to exchange information over the internet. There are plenty of public websites, which is a collection of web pages, available over the internet. These web-pages contain plenty of information in a form of text, videos, audio and picture format. These web pages are accessed using an application software called a web browser. Some of the examples of the popular web browser are: Internet Explorer, Chrome, Safari, Firefox, etc.

So this was a little introduction about internet and how it functions. Now let us discuss about cyber crime.

## 1.2 INTRODUCTION TO CYBER CRIME

The internet was born around 1960's where its access was limited to few scientist, researchers and the defence only. Internet user base have evolved exponentially. Initially the computer crime was only confined to making a physical damage to the computer and related infrastructure. Around 1980's the trend changed from causing the physical damaging to computers to making a computer malfunction using a malicious code called virus. Till then the effect was not so widespread because internet was only confined to defence setups, large international companies and research communities. In 1996, when internet was launched for the public, it immediately became popular among the masses and they slowly became dependent on it to an extent that it has changed their lifestyle. The GUIs were written so well that the user doesn't have to bother how the internet was functioning. They have to simply make a few clicks over the hyper links or type the desired information at the desired place without bothering where this data is stored and how it is sent over the internet or whether the data can be accessed by another person who is connected to the internet or whether the data packet sent over the internet can be snooped and tampered. The focus of the computer crime shifted from merely damaging the computer or destroying or manipulating data for personal benefit to financial crime. These computer attacks are increasing at a rapid pace. Every second around 25 computers become victim to cyber attack and around 800 million individuals are affected by it till 2013. CERT-India have reported around 308371 Indian websites to be hacked between 2011-2013. It is also estimated that around \$160 million are lost per year due to cyber crime. This figure is very conservative as most of the cases are never reported.

According to the 2013-14 report of the standing committee on Information Technology to the 15th Lok Sabha by ministry of communication and information technology, India is the third largest number of Internet users throughout the world with an estimated 100 million internet users as on June, 2011 and the numbers are growing rapidly. There are around 22 million broadband connections in India till date operated by around 134 major Internet Service Providers(ISPs).

Before discussing the matter further, let us know what the cyber crime is?

The term **cyber crime** is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity. It is often

committed by the people of destructive and criminal mindset either for revenge, greed or adventure.

### 1.2.1 Classification of Cyber Crimes

The cyber criminal could be internal or external to the organization facing the cyber attack.

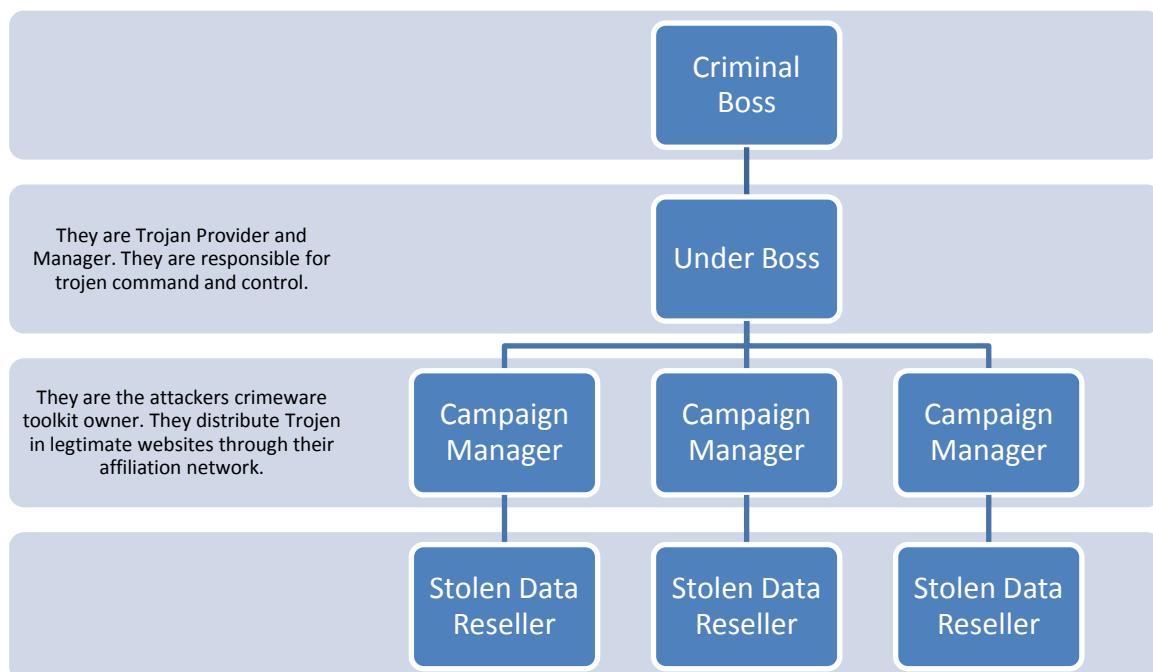
Based on this fact, the cyber crime could be categorized into two types:

- **Insider Attack:** An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparatively easy for an insider to perform a cyber attack as he is well aware of the policies, processes, IT architecture and weakness of the security system. Moreover, the attacker have an access to the network. Therefore it is comparatively easy for a insider attacker to steal sensitive information, crash the network, etc. In most of the cases the reason for insider attack is when a employee is fired or assigned new roles in an organization, and the role is not reflected in the IT policies. This opens a vulnerability window for the attacker. The insider attack could be prevented by planning and installing an Internal intrusion detection systems (IDS) in the organization.
- **External Attack:** When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber attack not only faces financial loss but also the loss of reputation. Since the attacker is external to the organization, so these attackers usually scan and gathering information. An experienced network/security administrator keeps regular eye on the log generated by the firewalls as external attacks can be traced out by carefully analysing these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks.

The cyber attacks can also be classified as structured attacks and unstructured attacks based on the level of maturity of the attacker. Some of the authors have classified these attacks as a form of external attacks but there is precedence of the cases when a structured attack was performed by an internal employee. This happens in the case when the competitor company wants the future strategy of an organization on certain points. The attacker may strategically gain access to the company as an employee and access the required information.

- **Unstructured attacks:** These attacks are generally performed by amateurs who don't have any predefined motives to perform the cyber attack. Usually these amateurs try to test a tool readily available over the internet on the network of a random company.
- **Structure Attack:** These types of attacks are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind. They have access to sophisticated tools and technologies to gain access to other networks without being noticed by their **Intrusion Detection Systems(IDSs)**. Moreover, these attacker have the necessary expertise to develop or modify the existing tools to satisfy their purpose. These types of attacks are usually performed by professional criminals, by a country on other rival countries, politicians to damage the image of the rival person or the country, terrorists, rival companies, etc.

Cyber crimes have turned out to be a low-investment, low-risk business with huge returns. Now-a-days these structured crimes are performed are highly organized. There is a perfect hierarchical organizational setup like formal organizations and some of them have reached a level in technical capabilities at par with those of developed nation. They are targeting large financial organizations, defence and nuclear establishments and they are also into online drugs trading.



*Figure 1 : Hierarchical Organisational Structure*

The role of all the people in the hierarchy remain changing and it is based on the opportunity. If a hacker who have hacked sensitive data from an organization may use it for financially exploiting the organisation himself. In case, the hacker himself have the technical expertise for it, he will do it himself, otherwise he may find a buyer who is interested in that data and have the technical expertise.

There are some cyber criminals offers on-demand and service. The person, organization or a country may contact these cyber criminals for hacking an organization to gain access to some sensitive data , or create massive denial-of –service attack on their competitors. Based on the demand of the customer the hackers write malware, virus, etc to suit their requirements. An organization effected by a cyber attack, not only faces financial loss, but its reputation is also adversely affected, and the competitor organization will definitely benefit by it.

### **1.2.2 Reasons for Commission of Cyber Crimes**

There are many reasons which act as a catalyst in the growth of cyber crime. Some of the prominent reasons are:

- a. *Money*: People are motivated towards committing cyber crime to make quick and easy money.
- b. *Revenge*: Some people try to take revenge with other person/organization/society/ caste or religion by defaming its reputation or bringing economical or physical loss. This comes under the category of cyber terrorism.
- c. *Fun*: The amateur do cyber crime for fun. They just want to test the latest tool they have encountered.
- d. *Recognition*: It is considered to be pride if someone hack the highly secured networks like defense sites or networks.
- e. *Anonymity*- Many times the anonymity that a cyber space provides motivates the person to commit cyber crime as it is much easier to commit a cyber crime over the cyber space and remain anonymous as compared to real world.  
It is much easier to get away with criminal activity in a cyber world than in the real world. There is a strong sense of anonymity than can draw otherwise respectable citizens to abandon their ethics in pursuit of personal gain.
- f. *Cyber Espionage*: At times the government itself is involved in cyber trespassing to keep eye on other person/network/country. The reason could be politically, economically or socially motivated.

## **1.3 MALWARE AND ITS TYPE**

Malware stands for “*Malicious Software*” and it is designed to gain access or installed into the computer without the consent of the user. They perform unwanted tasks in the host computer for the benefit of a third party. There is a full range of malwares which can seriously degrade the performance of the host machine. There is a full range of malwares which are simply written to distract/annoy the user, to the complex ones which captures the sensitive data from the host machine and send it to remote servers. There are various types of malwares present in the Internet. Some of the popular ones are:

### **1.3.1 Adware**

It is a special type of malware which is used for forced advertising. They either redirect the page to some advertising page or pop-up an additional page which promotes some product or event. These adware are financially supported by the organizations whose products are advertised.

### **1.3.2 Spyware**

It is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine. Mostly it gathers the browsing habits of the user and the send it to the remote server without the knowledge of the owner of the computer. Most of the time they are downloaded in to the host computer while downloading freeware i.e. free application programmes from the internet. Spywares may be of various types; It can keeps track of the cookies of the host computer, it can act as a keyloggers to sniff the banking passwords and sensitive information, etc.

### **1.3.3 Browser hijacking software**

There is some malicious software which are downloaded along with the free software offered over the internet and installed in the host computer without the knowledge of the user. This software modifies the browsers setting and redirect links to other unintentional sites.

### **1.3.4 Virus**

A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, occupy memory space of the computer by replicating the copy of the code, slow down the performance of the computer, format the host machine, etc. It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc. A virus may be present in a computer but it cannot activate itself without the human intervention.

Until and unless the executable file(.exe) is execute, a virus cannot be activated in the host machine.

### 1.3.5 Worms

They are a class of virus which can replicate themselves. They are different from the virus by the fact that they does not require human intervention to travel over the network and spread from the infected machine to the whole network. Worms can spread either through network, using the loopholes of the Operating System or via email. The replication and spreading of the worm over the network consumes the network resources like space and bandwidth and force the network to choke.

### 1.3.6 Trojan Horse

Trojan horse is a malicious code that is installed in the host machine by pretending to be useful software. The user clicks on the link or download the file which pretends to be a useful file or software from legitimate source. It not only damages the host computer by manipulating the data but also it creates a backdoor in the host computer so that it could be controlled by a remote computer. It can become a part of *botnet*(robot-network), a network of computers which are infected by malicious code and controlled by central controller. The computers of this network which are infected by malicious code are known as zombies.

Trojens neither infect the other computers in the network nor do they replicate.

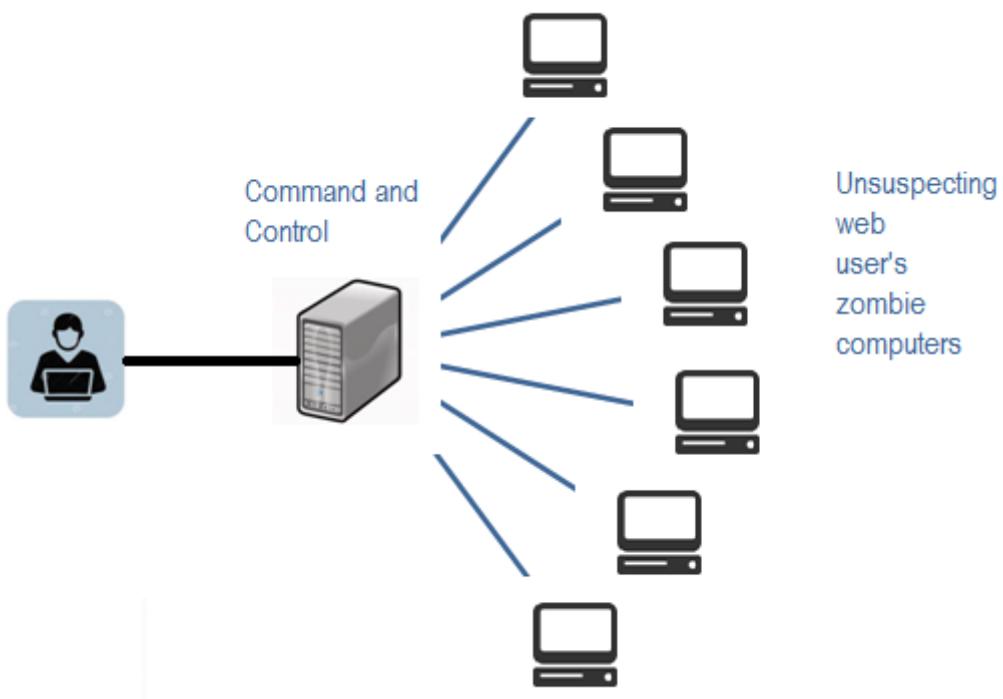


Figure 2: A typical botnet

### 1.3.7 Scareware

Internet has changed how we talk, shop, play etc. It has even changed the way how the criminal target the people for ransom. While surfing the Internet, suddenly a pop-up alert appears in the screen which warns the presence of dangerous virus, spywares, etc. in the user's computer. As a remedial measure, the message suggests the user download the full paid version of the software. As the user proceeds to download, a malicious code, known as scareware is downloaded into the host computer. It holds the host computer hostage until the ransom is paid. The malicious code can neither be uninstalled nor can the computer be used till the ransom is paid. A sample message alert of a scareware is shown below in Fig 3<sup>1</sup>



Figure 3: Sample Warning Message of a Scareware<sup>1</sup>

## 1.4 KINDS OF CYBER CRIME

Various types of cyber crimes are:

### 1.4.1 Cyber Stalking

It is an act of stalking, harassing or threatening someone using Internet/computer as a medium. This is often done to defame a person and use email, social network, instant messenger, web-posting, etc. as a medium as it offers anonymity. The behaviour includes false accusations, threats, sexual exploitation to minors, monitoring, etc.

<sup>1</sup> Image courtesy: <https://www.flickr.com/photos/alamagordo/2372928527>

#### **1.4.2 Child Pornography**

It is an act of possessing image or video of a minor (under 18), engaged in sexual conduct.

#### **1.4.3 Forgery and Counterfeiting**

It is a use of computer to forgery and counterfeiting is a document. With the advancement in the hardware and the software, it is possible to produce counterfeit which matches the original document to such an extent that it is not possible to judge the authenticity of the document without expert judgement.

#### **1.4.4 Software Piracy and Crime related to IPRs**

Software piracy is an illegal reproduction and distribution for personal use or business. It comes under crime related to IPR infringement. Some of the other crimes under IPR infringement are: download of songs, downloading movies, etc.

#### **1.4.5 Cyber Terrorism**

It is defined as the use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives.

#### **1.4.6 Phishing**

It is a process of acquiring personal and sensitive information of an individual via email by disguising as a trustworthy entity in an electronic communication. The purpose of phishing is identity theft and the personal information like username, password, and credit card number etc. may be used to steal money from user account. If a telephone is used as a medium for identity theft, it is known as *Vishing* (voice phishing). Another form of phishing is *Smishing*, in which sms is used to lure customers.

#### **1.4.7 Computer Vandalism**

It is an act of physical destroying computing resources using physical force or malicious code.

#### **1.4.8 Computer Hacking**

It is a practice of modifying computer hardware and software to accomplish a goal outside the creator's original purpose. The purpose of hacking a computer system may vary from simply demonstrations of the technical ability, to sealing, modifying or destroying information for social, economic or political reasons. Now the corporate are hiring hackers, a person who is engaged in hacking computers, to intentionally hack the computer of an organization to find and fix security vulnerabilities.

The hackers may be classified as:

- White Hat: white hat hackers are the persons who hack the system to find the security vulnerabilities of a system and notify to the organizations so that a preventive action can be taken to protect the system from outside hackers. White hat hackers may be paid employee of an organization who is employed to find the security loop-holes, or may be a freelancer who just wants to prove his mantle in this field. They are popularly known as ethical hackers.
- Black Hat: in contrast to the white hat, the black hat hack the system with ill intentions. They may hack the system for social, political or economically motivated intentions. They find the security loopholes in the system, and keep the information themselves and exploit the system for personal or organizational benefits till the organization whose system is compromised is aware of this, and apply security patches. They are popularly known as crackers.
- Grey Hat: Grey hat hackers find out the security vulnerabilities and report to the site administrators and offer the fix of the security bug for a consultancy fee.
- Blue hat: A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed.

#### **1.4.9 Creating and distributing viruses over internet**

The spreading of an virus can cause business and financial loss to an organization. The loss includes the cost of repairing the system, cost associated with the loss of business during downtime and cost of loss of opportunity. The organization can sue the hacker, if found, for the sum of more than or equivalent to the loss borne by the organization.

#### **1.4.10 Spamming**

Sending of unsolicited and commercial bulk message over the internet is known as spamming.

An email can be classified as spam, if it meets following criteria:

- a. Mass mailing:- the email is not targeted to one particular person but to a large number of peoples.
- b. Anonymity:- The real identify of the person not known
- c. Unsolicited:- the email is neither expected nor requested for the recipient.

These spams not only irritate the recipients and overload the network but also waste the time and occupy the valuable memory space of the mailbox.

#### **1.4.11 Cross Site Scripting**

It is an activity which involves injecting a malicious client side script into a trusted website. As soon as the browser executes the malicious script, the malicious script gets access to the cookies and other sensitive information and sent to remote servers. Now this information can be used to gain financial benefit or physical access to a system for personal interest.

#### **1.4.12 Online Auction Fraud**

There are many genuine websites who offers online auction over internet. Taking the advantage of the reputation of these websites, some of the cyber criminals lure the customers to online auction fraud schemes which often lead to either overpayment of the product or the item is never delivered once the payment is made.

#### **1.4.13 Cyber Squatting**

It is an act of reserving the domain names of someone else's trademark with intent to sell it afterwards to the organization who is the owner of the trademark at a higher price.

#### **1.4.14 Logic Bombs**

These are malicious code inserted into legitimate software. The malicious action is triggered by some specific condition. If the conditions holds true in future, the malicious action begins and based on the action defined in the malicious code, they either destroy the information stored in the system or make system unusable.

#### **1.4.15 Web Jacking**

The hacker gain access to a website of an organization and either blocks it or modify it to serve political, economical or social interest. The recent examples of web jacking are some of the websites of the educational institutes were hacked by Pakistani hackers and an animation which contains Pakistani flags were flashed in the homepage of these websites. Another example is Indian hackers hacked website of Pakistani railways and flashed Indian flag in the homepage for several hours on the occasion of Independence Day of India in 2014.

#### **1.4.16 Internet Time Thefts**

Hacking the username and password of ISP of an individual and surfing the internet at his cost is Internet Time Theft.

#### **1.4.17 Denial of Service Attack**

It is a cyber attack in which the network is chocked and often collapsed by flooding it with useless traffic and thus preventing the legitimate network traffic.

#### **1.4.18 Salami Attack**

It is an attack which proceeds with small increments and final add up to lead to a major attack. The increments are so small that they remain unnoticed. An example of salami attack is gaining access to online banking of an individual and withdrawing amount in such a small amounts that it remains unnoticed by the owner. Often there is default trigger set in the banking website and transactions below say, Rs. 1000 withdrawal are not reported to the owner of the account. Withdrawing amount of Rs. 1000 over a period of time will lead to total withdrawal of a large sum.

#### **1.4.19 Data Diddling**

It is a practice of changing the data before its entry into the computer system. Often, the original data is retained after the execution on the data is done. For example, DA or the basic salary of the person is changed in the payroll data of an individual for pay calculation. Once the salary is calculated and transferred to his account, the total salary is replaced by his actual salary in the report.

#### **1.4.20 Email Spoofing**

It is a process of changing the header information of an e-mail so that its original source is not identified and it appears to an individual at the receiving end that the email has been originated from source other than the original source.

# CYBER SECURITY TECHNIQUES

There are many cyber security techniques to combat the cyber security attacks. The next section discusses some of the popular techniques to counter the cyber attacks.

## 2.1 AUTHENTICATION

It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be. A typical method for authentication over internet is via username and password. With the increase in the reported cases of cyber crime by identity theft over internet, the organizations have made some additional arrangements for authentication like *One Time Password*(OTP), as the name suggest it is a password which can be used one time only and is sent to the user as an *SMS* or an email at the mobile number/email address that he have specified during the registration process. It is known as two-factor authentication method and requires two type of evidence to authentication an individual to provide an extra layer of security for authentication. Some other popular techniques for two-way authentication are: biometric data, physical token, etc. which are used in conjunction with username and password.

The authentication becomes more important in light of the fact that today the multinational organizations have changed the way the business was to be say, 15 years back. They have offices present around the Globe, and an employee may want an access which is present in a centralized sever. Or an employee is working from home and not using the office intranet and wants an access to some particular file present in the office network. The system needs to authenticate the user and based on the credentials of that user, may or may not provide access to the used to the information he requested. The process of giving access to an individual to certain resources based on the credentials of an individual is known as authorization and often this process is go hand-in-hand with authorization. Now, one can easily understand the role of strong password for authorization to ensure cyber security as an easy password can be a cause of security flaw and can bring the whole organization at high risk. Therefore, the password policy of an organization should be such that employees are forced to use strong passwords (more than 12 characters and combination of lowercase and uppercase alphabets along with numbers and special characters) and prompt user to change their password frequently. In some of the bigger organizations or an organization which deals in sensitive information like defence agencies, financial institutions, planning commissions, etc. a hybrid authentication

system is used which combines both the username and password along with hardware security measures like biometric system, etc. Some of the larger organizations also use VPN(Virtual Private Network), which is one of the method to provide secure access via hybrid security authentication to the company network over internet.

## 2.2 ENCRYPTION

It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it. Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key. The decoding of the complex code to original text using key is known as decryption. If the same key is used to lock and unlock the data, it is known as symmetric key encryption.

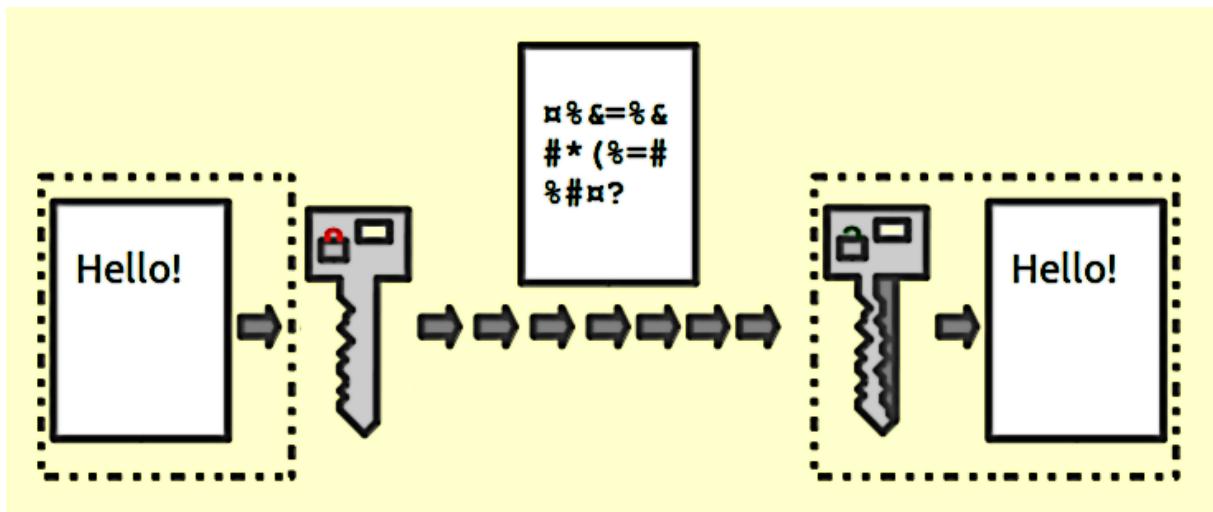


Figure 4: Encryption<sup>2</sup>

In symmetric key encryption, the after coding of data, the key is sent to the destination user via some other medium like postal service, telephone, etc. because if the key obtained by the hacker, the security of the data is compromised. Key distribution is a complex task because the security of key while transmission is itself an issue. To avoid the transfer of key a method called asymmetric key encryption, also known as public key encryption, is used. In

<sup>2</sup> Image courtesy: [https://upload.wikimedia.org/wikipedia/commons/b/bc/Public\\_key\\_encryption\\_keys.png](https://upload.wikimedia.org/wikipedia/commons/b/bc/Public_key_encryption_keys.png)

asymmetric key encryption, the key used to encrypt and decrypt data are different. Every user posse's two keys viz. public key and private key. As the name suggest, the public key of every user is known to everyone but the private key is known to the particular user, who own the key, only. Suppose sender A wants to send a secret message to receiver B through internet. A will encrypt the message using B's public key, as the public key is known to everyone. Once the message is encrypted, the message can safely be send to B over internet. As soon as the message is received by B, he will use his private key to decrypt the message and regenerate the original message.

## **2.3 DIGITAL SIGNATURES**

It is a technique for validation of data. Validation is a process of certifying the content of a document. The digital signatures not only validate the data but also used for authentication. The digital signature is created by encrypting the data with the private key of the sender. The encrypted data is attached along with the original message and sent over the internet to the destination. The receiver can decrypt the signature with the public key of the sender. Now the decrypted message is compared with the original message. If both are same, it signifies that the data is not tempered and also the authenticity of the sender is verified as someone with the private key(which is known to the owner only) can encrypt the data which was then decrypted by his public key. If the data is tempered while transmission, it is easily detected by the receiver as the data will not be verified. Moreover, the massage cannot be re-encrypted after tempering as the private key, which is posses only by the original sender, is required for this purpose.

As more and more documents are transmitted over internet, digital signatures are essential part of the legal as well as the financial transition. It not only provides the authentication of a person and the validation of the document, it also prevents the denial or agreement at a later stage. Suppose a shareholder instructs the broker via email to sell the share at the current price. After the completion of the transaction, by any chance, the shareholder reclaims the shares by claiming the email to be forge or bogus. To prevent these unpleasant situations, the digital signatures are used.

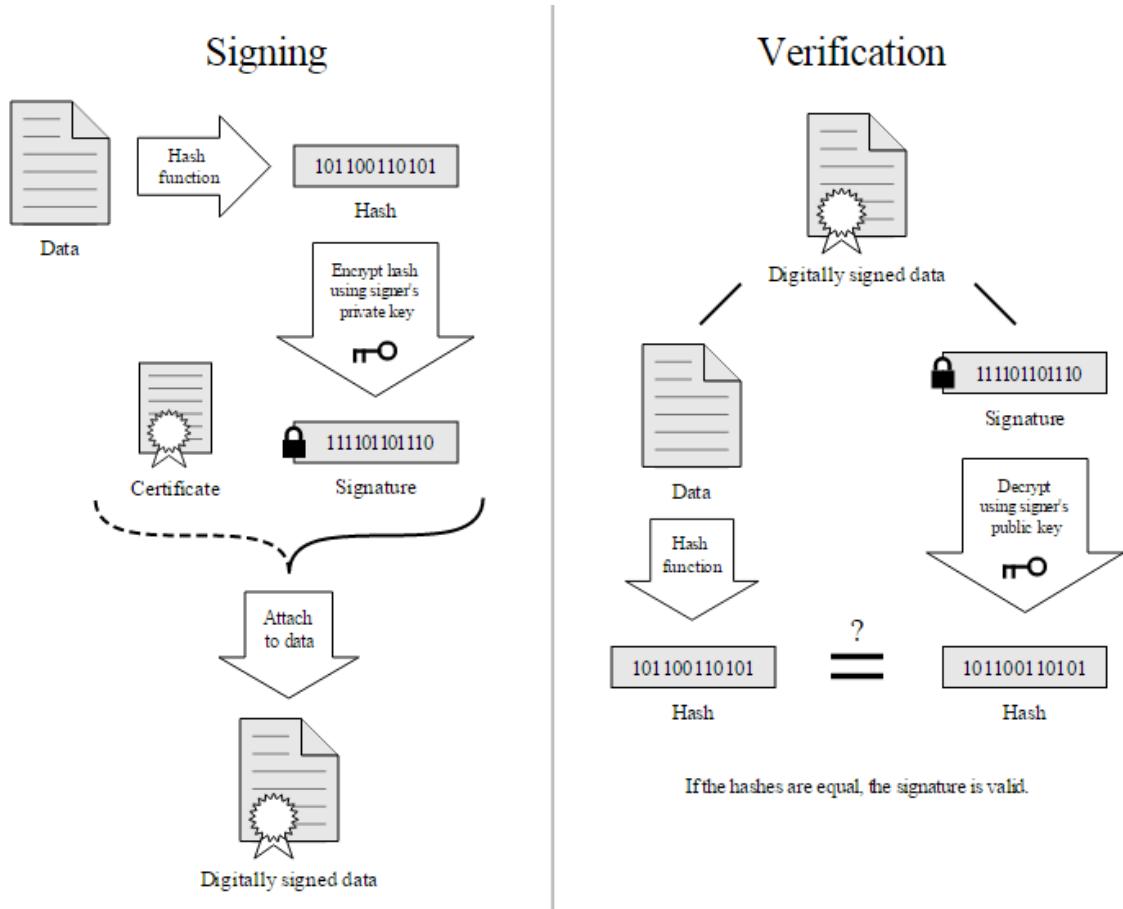


Figure 5: Digital signature<sup>3</sup>

## 2.4 ANTIVIRUS

There are verities of malicious programs like virus, worms, trojan horse, etc that are spread over internet to compromise the security of a computer either to destroy data stored into the computer or gain financial benefits by sniffing passwords etc. To prevent these malicious codes to enter to your system, a special program called an anti-virus is used which is designed to protect the system against virus. It not only prevents the malicious code to enter the system but also detects and destroys the malicious code that is already installed into the system. There are lots of new viruses coming every day. The antivirus program regularly updates its database and provides immunity to the system against these new viruses, worms, etc.

---

<sup>3</sup> Image courtesy: [https://upload.wikimedia.org/wikipedia/commons/2/2b/Digital\\_Signature\\_diagram.svg](https://upload.wikimedia.org/wikipedia/commons/2/2b/Digital_Signature_diagram.svg)



Figure 6: Different antivirus available on the market<sup>4</sup>

## 2.5 FIREWALL

It is a hardware/software which acts as a shield between an organization's network and the internet and protects it from the threats like virus, malware, hackers, etc. It can be used to limit the persons who can have access to your network and send information to you.

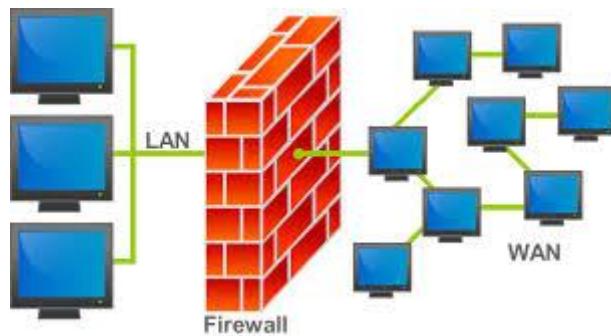


Figure 7: Firewall<sup>5</sup>

There are two type of traffic in an organization viz. inbound traffic and outbound traffic. Using firewall, it is possible to configure and monitor the traffic of the ports. Only the packets from trusted source address can enter the organization's network and the sources which are blacklisted and unauthorized address are denied access to the network. It is important to have firewalls to prevent the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly. A firewall can be implemented using hardware as well as software or the combination of both.

<sup>4</sup> Image courtesy: <https://www.flickr.com/photos/thomasguest/3027199004>

<sup>5</sup> Image courtesy: <https://upload.wikimedia.org/wikipedia/commons/5/5b/Firewall.png>

- Hardware Firewalls: example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet.
- Software Firewalls: These firewalls are installed and installed on the server and client machines and it acts as a gateway to the organizations' network.

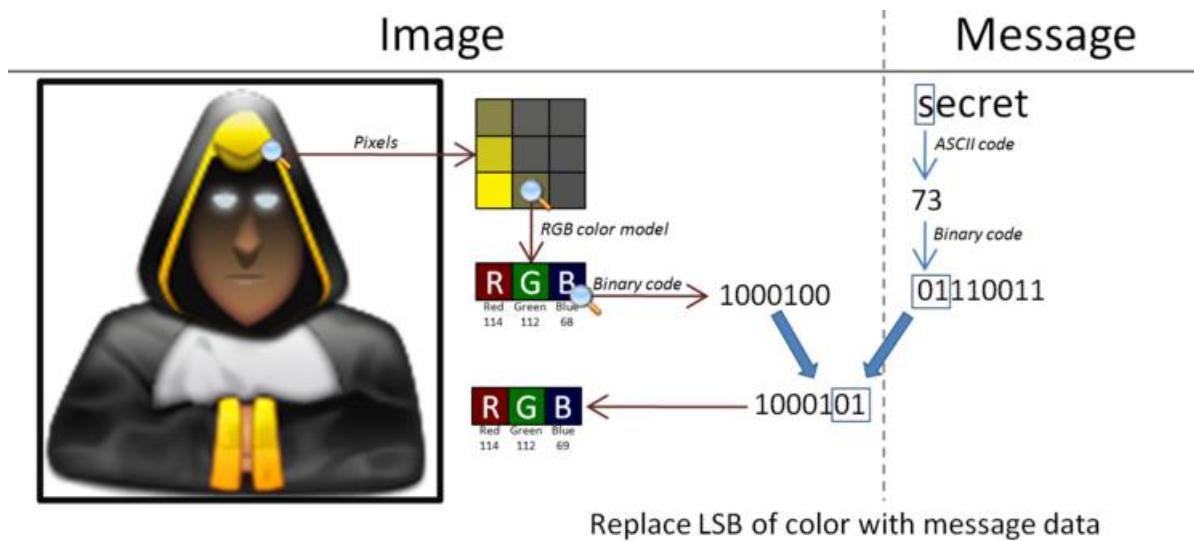
In the operating system like Windows 2003, Windows 2008 etc. it comes embedded with the operating system. The only thing a user need to do is to optimally configure the firewall according to their own requirement. The firewalls can be configured to follow “rules” and “policies” and based on these defined rules the firewalls can follow the following filtering mechanisms.

- Proxy- all the outbound traffic is routed through proxies for monitoring and controlling the packet that are routed out of the organization.
- Packet Filtering- based on the rules defined in the policies each packet is filtered by their type, port information, and source & destination information. The example of such characteristics is IP address, Domain names, port numbers, protocols etc. Basic packet filtering can be performed by routers.
- Stateful Inspection: rather than going through all the field of a packet, key features are defined. The outgoing/incoming packets are judged based on those defined characteristics only.

The firewalls are an essential component of the organizations' network. They not only protect the organization against the virus and other malicious code but also prevent the hackers to use your network infrastructure to launch DOS attacks.

## **2.6 STEGANOGRAPHY**

It is a technique of hiding secret messages in a document file, image file, and program or protocol etc. such that the embedded message is invisible and can be retrieved using special software. Only the sender and the receiver know about the existence of the secret message in the image. The advantage of this technique is that these files are not easily suspected.



*Figure 8: Steganography<sup>6</sup>*

There are many applications of steganography which includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access and theft , digital watermarks for IPR issues, etc.

Let us discuss how the data is secretly embeded inside the cover file( the medium like image, video, audio, etc which is used for embed secret data) without being noticed. Let us take an example of an image file which is used as a cover mediem. Each pixel of a high resolution image is represented by 3 bytes(24 bits). If the 3 least significant bits of this 24 bits are altered and used for hiding the data, the resultant image, after embeded the data into it, will have unnoticeable change in the image quality and only a very experienced and tranined eyes can detect this change. In this way, evcery pixel can be used to hide 3 bits of information.

Similerly, introducing a white noise in an audio file at regular or random interval can be used to hide data in an audio or video files. There are various free softwares available for Steganography. Some of the popular ones are: QuickStego, Xiao, Tucows, OpenStego, etc.

---

<sup>6</sup> Image courtesy: [https://upload.wikimedia.org/wikipedia/commons/b/b8/Seformatbmp-embedding\\_full.png](https://upload.wikimedia.org/wikipedia/commons/b/b8/Seformatbmp-embedding_full.png)

# INVESTIGATING CYBER CRIMES: INTRODUCTION TO CYBER FORENSIC

In the preceding chapters, we have discussed the prevention techniques for cyber attack. What if one has encountered cyber attack? What Next? The next step is to report the cyber crime. But if a person is exposed to cyber forensic principles, the chances that the person accidentally destroys the vital cyber evidences are minimized.

## 3.1 COMPUTER FORENSICS

Cyber forensic is a branch of science which deals with tools and techniques for investigation of digital data to find evidences against a crime which can be produced in the court of law. It is a practice of preserving, extracting, analyzing and documenting evidence from digital devices such as computers, digital storage media, smartphones, etc. so that they can be used to make expert opinion in legal/administrative matters.

The computer forensic plays a vital role in an organization as our dependency on computing devices and internet is increasing day-by-day. According to a survey conducted by University of California<sup>7</sup>, 93% of all the information generated during 1999 was generated in digital form, on computers, only 7% of the remaining information was generated using other sources like paper etc. It is not always easy to collect evidences as the data may be tampered, deleted, hidden or encrypted. Digital forensic investigation is a highly skilled task which needs the expertise of various tools, techniques and guidelines for finding and recovering the digital evidences from the crime scene or the digital equipments used in the crime. With digital equipments like smartphone, tablets, palmtops, smart tv, etc having increasing processing capabilities and computation speed, the possibility of use of these devices in cyber crime cannot be ruled out. A forensic investigator must not only have deep understanding of the working of these devices and also hands-on exposure to the tools for accurate data retrieval so that the value and integrity of the data is preserved.

---

<sup>7</sup> [http://www.isfs.org.hk/publications/ComputerForensics\\_part1.pdf](http://www.isfs.org.hk/publications/ComputerForensics_part1.pdf)

A computer can be used intentionally or unintentionally to cyber crime. The intentional use is to use your computer to send hate mails or installing cracked version of an otherwise licenced software into your computer. Unintentional use is the computer you are using contains virus and it is spread into the network and outside the network causing major loss to someone in financial terms. Simillerly a computer can be directly used to commit a digital crime. For example, your computer is used to access the sensitive and classified data and the data is sent someone inside/outside the network who can use this data for him own benefit. The indirect use of computer is when while downloading a crack of a software, a trojan horse is stored in the computer, while creates a backdoor in the network to facilitate hacker. Now the hacker logs into your computer and use it for committing cyber crime. An experienced computer forensic investigator plays a crucial role in distinguishing direct and indirect attack. Computer forensic experts are also useful for recovery of accidental data loss, to detect industrial espionage, counterfeiting, etc.

In large organization, as soon as a cyber crime is detected by the incident handling team, which is responsible for monitoring and detection of security event on a computer or computer network, initial incident management processes are followed<sup>8</sup>. This is an in-house process. It follows following steps:

1. *Preparation:* The organization prepares guidelines for incident response and assigns roles and the responsibilities of each member of the incident response team. Most of the large organizations earn a reputation in the market and any negative sentiment may negatively affect the emotions of the shareholders. Therefore, an effective communication is required to declare the incident. Hence, assigning the roles based on the skill-set of a member is important.
2. *Identification:* based on the traits the incident response team verifies whether an event had actually occurred. One of the most common procedures to verify the event is examining the logs. Once the occurrence of the event is verified, the impact of the attack is to be assessed.
3. *Containment:* based on the feedback from the assessment team, the future course of action to respond to the incident is planned in this step.

---

<sup>8</sup> <http://countuponsecurity.com/2012/12/21/computer-security-incident-handling-6-steps/>

4. *Eradication*: In this step, the strategy for the eradication or mitigate of the cause of the threat is planned and executed.
5. *Recovery*: it is the process of returning to the normal operational state after eradication of the problem.
6. *Lesson Learned*: if a new type of incident is encountered, it is documented so that this knowledge can be used to handle such situations in future.

The second step in the process is forensic investigation is carried out to find the evidence of the crime, which is mostly performed by 3<sup>rd</sup> party companies. The computer forensic investigation involves following steps:

1. *Identify incident and evidence*: this is the first step performed by the system administrator where he tries to gather as much information as possible about the incident. Based on this information the scope and severity of the attack is assessed. Once the evidence of the attack is discovered, the backup of the same is taken for the investigation purpose. The forensic investigation is never performed on the original machine but on the data that is restored from the backup.
2. *Collect and preserve evidence*: Various tools like Helix, WinHex, FKT Imager, etc. are used to capture the data. Once the backup of the data is obtained, the custody of the evidence and the backup is taken. MD5(message digest) hash of the backup is calculated and matched with the original one to check the integrity of the data. Other important sources of information like system log, network information, logs generated by Intrusion Detection Systems(IDS), port and process information are also captured.
3. *Investigate*: The image of the disk is restored from the backup and the investigation is performed by reviewing the logs, system files, deleted and updates files, CPU uses and process logs, temporary files, password protected and encrypted files, images, videos and data files for possible steganographic message, etc.
4. *Summarize and Presentation*: The summary of the incident is presented in chronological order. Based on the investigation, conclusions are drawn and possible cause is explained.

While carrying out the digital forensic investigation, rules and procedure must be applied. Specially while capturing the evidence. It should be ensured that the actions that are taken for capturing the data do not change the evidence. The integrity of the data should be maintained. It must be ensured that the devices used for capturing the backup are free from contamination.

Moreover, all the activities related to seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review<sup>9</sup>. Prevention is always better than cure. It is always recommended to fine tune your intrusion detection system like firewall occasionally perform penetration tests on your network to avoid pray to hacker. Last but not the least, report the crime.

### **3.2 WHY SHOULD WE REPORT CYBER CRIME?**

Some of the companies do not report a cyber crime incident because they fear this will harm their reputation amongst its shareholders. Some of the data are very sensitive and its disclosure may impact their business negatively. But, the fact is until and unless a cyber crime incident is reported, the cyber criminals will never be crabbed by the law enforcement agencies. This will further worsen the conditions and encourage the criminals to repeat these types of incidents with the same or the other organizations. So it is very important to identify and prosecute them. This will help not only to identify the existing threats to the economy and the infrastructure but also new threats are identified. Depending on the scope of a cyber crime, the cyber crime should be reported to nearest cyber cell of your locality, state cyber cell, central investigating agencies like CBI, IB or the international bodies like Interpol.

Some of the addresses of the cyber coordinating units are:

<b>Assam</b> <b>Address:</b> CID HQ,Dy.SP., Assam Police <b>Contact Details:</b> Ph: +91-361-252-618, +91 9435045242 <b>E-mail id:</b> ssp_cod@assampolice.com	<b>Haryana</b> <b>Address:</b> Cyber Crime and Technical Investigation Cell, Joint Commisioner of Police, Old S.P.Office complex,Civil Lines, Gurgaon <b>E-mail:</b> jtcp.ggn@hry.nic.in
<b>Mumbai</b> <b>Address:</b> Cyber Crime Investigation Cell, Office of Commissioner of Police office,Annex -3 Building, 1st floor, Near Crawford Market, Mumbai-01.	<b>Chennai</b> <b>Address:</b> Asst. Commr. of Police, Cyber Crimes Cell, Vepery, Chennai <b>Contact Details:</b> 04423452348, 04423452350

<sup>9</sup> <http://www.isfs.org.hk/publications/011009/Collins-CIO&CeO.pdf>

<p><b>Contact Details:</b> +91-22-22630829, +91-22-22641261</p> <p><b>Web site:</b> <a href="http://www.cybercellmumbai.com">http://www.cybercellmumbai.com</a></p> <p><b>E-mail id:</b> officer@cybercellmumbai.com</p> <p><b>Thane</b></p> <p><b>Address:</b> 3rd Floor, Police Commissioner Office, Near Court Naka, Thane West, Thane 400601.</p> <p><b>Contact Details:</b> +91-22-25424444</p> <p><b>Web site:</b> <a href="http://www.thanepolice.org">www.thanepolice.org</a></p> <p><b>E-Mail:</b> police@thanepolice.org</p>	<p><b>E-mail id:</b> cybercrimechn@yahoo.com</p> <p><b>For Rest of Tamil Nadu,</b></p> <p><b>Address:</b> A-Wing, III rd Floor, Rajaji Bhawan, Besant Nagar, Chennai-600090</p> <p><b>Contact Details:</b> 044-24461959, 24468889, 24463888</p> <p><b>E-mail id:</b> hobeochn@cbi.gov.in</p>
<p><b>Bangalore</b> (for whole of the Karnataka)</p> <p><b>Address:</b> Cyber Crime Police Station, C.O.D Headquarters, Carlton House, # 1, Palace Road, Bangalore - 560 001</p> <p><b>Contact Details:</b> +91-80-2220 1026, +91-80-2294 3050, +91-80-2238 7611 (FAX)</p> <p><b>Web site:</b> <a href="http://www.cyberpolicebangalore.nic.in">http://www.cyberpolicebangalore.nic.in</a></p> <p><b>Email-id:</b> ccps@blr.vsnl.net.in, ccps@kar.nic.in</p>	<p><b>Hyderabad</b></p> <p><b>Address:</b> Cyber Crime Police Station, Crime Investigation Department, 3rd Floor, D.G.P. office, Lakdikapool, Hyderabad – 500004</p> <p><b>Contact Details:</b> +91-40-2324 0663, +91-40-2785 2274, +91-40-2785 2040, +91-40-2329 7474 (Fax)</p> <p><b>Website:</b> <a href="http://www.cidap.gov.in/cybercrimes.aspx">http://www.cidap.gov.in/cybercrimes.aspx</a></p> <p><b>E-mailid:</b> cidap@cidap.gov.in, info@cidap.gov.in, cybercell_hyd@hyd.appolice.gov.in</p>
<p><b>Delhi</b></p> <p><b>CBI Cyber Crime Cell:</b> Superintendent of Police, Cyber Crime Investigation Cell, Central Bureau of Investigation, 5th Floor, Block</p>	<p><b>Pune</b></p> <p><b>Address :</b> Deputy Commissioner of Police(Crime), Office of the Commissioner Office, 2, Sadhu Vaswani Road, Camp,Pune 411001</p>

<p>No.3, CGO Complex, Lodhi Road, New Delhi – 3</p> <p><b>Contact Details:</b> +91-11-4362203, 011-26851998 011-26515229, +91-11-4392424</p> <p><b>Web site:</b> <a href="http://cbi.nic.in">http://cbi.nic.in</a></p> <p><b>Asst. Commissioner of Police,</b> Cyber Crime Cell, EOW, Crime Branch, 2nd Floor, Police Training School, Malaviya Nagar, New Delhi-110 017</p> <p><b>E-Mail:</b> cbiccic@bol.net.in, dcp-eow-dl@nic.in</p>	<p><b>Contact Details:</b> +91-20-26123346, +91-20-26127277 +91-20-2616 5396, +91-20-2612 8105 (Fax)</p> <p><b>Website:</b> <a href="http://www.punepolice.gov.in">www.punepolice.gov.in</a></p> <p><b>E-Mail:</b> crimecomp.pune@nic.in, punepolice@vsnl.com</p>
<p><b>Himachal Pradesh</b></p> <p><b>Address :</b> CID Office ,Dy.SP, Himachal Pradesh</p> <p><b>Contact Details:</b> +91-94180 39449</p> <p><b>E-mail:</b> soodbrijesh9@gmail.com</p>	<p><b>Gujarat</b></p> <p>DIG, CID, Crime and Railways. Fifth Floor, Police Bhavan Sector 18, Gandhinagar 382 018</p> <p><b>Contact Details:</b> +91-79-2325 4384, +91-79-2325 0798, +91-79-2325 3917 (Fax)</p>
<p><b>Jharkhand</b></p> <p><b>Address:</b> IG-CID,Organized Crime, Rajarani Building, Doranda Ranchi – 834002</p> <p><b>Contact Details::</b> +91-651-2400 737, +91-651-2400 738</p> <p><b>E-mail:</b> a.gupta@jharkhandpolice.gov.in</p>	<p><b>Kerala</b></p> <p><b>Address :</b> Hitech Cell, Police Head Quarters, Thiruvananthapuram</p> <p><b>Contact Details:</b> +91-471 272 1547, +91-471 272 2768</p> <p><b>E-mail:</b> hitechcell@keralapolice.gov.in</p>
<p><b>Jammu</b></p> <p><b>Address:</b> SSP-Crime, CPO Complex,Panjtirthi, Jammu-180004</p> <p><b>Contact Details:</b> +91-191-257-8901</p>	<p><b>Orissa</b></p> <p><b>Address:</b> CID,Crime Branch, Orissa</p> <p><b>Contact Details:</b> +91 94374 50370</p> <p><b>E-mail:</b> splcidcb.orpol@nic.in</p>

<b>E-mail:</b> <a href="mailto:sspcrmjmu-jk@nic.in">sspcrmjmu-jk@nic.in</a>	
<b>Meghalaya</b> <b>Address:</b> SCRB,Superintendent of Police Meghalaya <b>Contact Details:</b> +91 98630 64997 <b>E-mail:</b> scrb-meg@nic.in	<b>Punjab</b> <b>Address:</b> Cyber Crime Police Station, DSP Cyber Crime, S.A.S Nagar, Patiala, Punjab <b>Contact Details:</b> +91 172 2748 100
<b>Bihar</b> <b>Address:</b> Cyber Crime Investigation Unit, Dy.S.P.Kotwali Police Station, Patna <b>Contact Details:</b> +91 94318 18398 <b>E-mail:</b> cciu-bih@nic.in	<b>West Bengal</b> <b>Address:</b> CID, Cyber Crime, West Bengal <b>Contact Details:</b> +9133 24506163 <b>E-mail:</b> occyber@cidwestbengal.gov.in
<b>Uttar Pradesh</b> <b>Address:</b> Cyber Complaints Redressal Cell, Nodal Officer Cyber Cell Agra, Agra Range 7,Kutchery Road, Baluganj,Agra-232001, Uttar Pradesh <b>Contact Details:</b> +919410837559 <b>E-mail:</b> info@cybercellagra.com	<b>UttaraKhand</b> <b>Address:</b> Special Task Force Office Sub Inspector of Police, Dehradoon <b>Contact Details:</b> +91 135 264098, +91 94123 70272 <b>E-mail:</b> dgc-police-us@nic.in

# SOME RECENT CYBER SECURITY ATTACKS

## 4.1 INTRODUCTION

The proliferation of Internet amongst the population is getting deep day-by-day. This not only increase the scope of e-governance and e-commerce in the area of healthcare, banking, power distribution, etc. but also expose these sectors to cyber threats like hacking, credential thefts, data tempering, account hijacking, etc. According to a report, there were around 62,189 cyber security incidents, originating mainly from Countries including US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE, in the period from Jan-May, 2014. Also, around 10,000 Indian government sites were compromised in this period. India has a serious shortage of IT Security professional to deal with such threats in effective manner. According to a report, India needs around one million cyber security professionals to deal with cyber threats effectively.

## 4.2 SOME RECENT CYBER CRIME INCIDENTS

In the current section, we will discuss some of the common cyber crimes and frauds incidents over internet so that you could appreciate how these little ignorance could lead to a big disaster.

1. Paypal, an international online money transfer service, which allows you to safely transfer money through an Internet using various encryption techniques and provides an alternative to other traditional payment methods like cheques, money orders, etc. It has an active user base of over 100 million active users in 190 countries and performs over 9 million payments daily. It is one of the popular medium of payment over online auction sites like ebay etc. It is a convenient medium for trading particularly if the buyers and sellers are from different countries and have different currencies.

Romanian Hacker TinKode aka Razvan Cernaianu, exploited a loophole in the code of the chargeback process of PayPal. Due to this, a user can double its money on every attempt. Suppose the user has Rs.1000, then using this loophole, the amount will be doubled to Rs.2000 in the first attempt. Now this Rs. 2000 will be doubled to Rs. 4000 in the second attempt. Further Rs. 4000 will be doubled to Rs. 8000. Like wise this process will continue endlessly.

2. In Australia, a website called MP3/WMA Land, which offers a large number of pirated songs, music video clips for free download to its users. This resulted in heavy financial losses to the artists and the producers of those songs. The complain was loudeged by an organizations called Music Industry Piracy Investigations.

The owners of the website, Ng, Tran and Le, who were the students of Australian University, were framed for Australia's largest copyright infringement case(Urbas, 2012).

3. One of the intresting case of online stalking was registered by Mrs. Ritu Kohli at Delhi Police (Kaur, 2013). She reported that someone is using her identity over the Internet in the website [www.mirc.com](http://www.mirc.com) for chatting, and distributed her address and phone number. As a result she received a large number of phone calls from all over including Dubai, Ahemdabad, Mumbai, etc. at odd hours. This caused a lot of mental frustration and she decided to report the case. Based on her complain, Delhi Police traced the IP address and finally traced the address of accused, Manish Kathuria and arrested him.

A Dubai based NRI was blackmailed, and by the time the case was reported, he had already approximatly 1.25 crore to the accused (Madhya Pradesh State Cyber Police, 2013). The NRI met a girl over Internet and after a series of long chatting sessions, the girl won the love and trust of the NRI. In the meantime, she introduces him with several of her friends. Due to some reasons, the relation could not last long. After some time, one of the girl's friend, who was introduced to him by the girl, reports him that due to the mental stress of the broken relationship, the girl have committed sucide and police is investigating the case. Many fake copies of the letters from CBI, High Court of Calcutta, New York police and Punjab University etc. were also sent to the NRI. The NRI seeked help from the girl's friend, who in turn introduced her with a law firm based at Kolkata. The owner of the law firm agreed to take this case. A huge some of money was demanded by the law firm and a total of more than 1.26 crore were transferred on different occassions and he still demamded more money. The NRI smell something fishy and reported the case to Mumbai Police. The NRI forwarded all the email that he recieived from the girl, her friend and the owner of the law firm. After the foransic invertigation for the email, the IP address of all the three persons were found to be originated from the same source. After investigation, it was found that the identity of the girl and her friends were all virtual i.e. they does not exist. The owner of the law firm was the mastermind who assumed false identity of all the persons and created this false story to blackmail the NRI.

4. Iran's nuclear facility at Natanz was attacked by virus, *Stuxnet* which is believed to be developed by US (Shubert, 2011). It was not possible to inject the virus through the Internet as the network of the the Iran's nuclear facility is a private network and was isolated from rest of the world. The virus first infected the third party utility which is used by Natanz facility and gained access to the network. The virus was designed to attack a specific system software which controls the operation of Siemens controllers. The virus speeds up or slow down the centrifuges and thus wearing them out prematurely. Moreover, it hijacked the system and send false signals about the health and status of the nuclear plant. Therefore, by the time the effect of the virus was detected, it was too late and the virus have done much harm to the nuclear facility.
5. A trojan mail was used to hack the user name and the password of the current account of Mumbai based firm RPG Group and siphoned off Rs. 2.41 crore by Real Time Gross Settlement(RTGS) (Narayan, 2013). The bank officials suspected when they notice the huge amount of money transfer. They confirmed they came from the company's officials who denied the transfer of the money to the designated accounts. Based on the names and the address of the account holders who have received the money, the police came to know that the account holders have permitted the main accused to use their account in return of huge commission.
6. Chennai police cracked a case of credit card fraud, where two BPO employees with the help of the son of the accused, increased the credit card limit and the communication address of the credit card owner (Madhya Pradesh State Cyber Police, 2013). They illegally hacked into their company's computer to find out the details of the credit card owner. The credit card company was cheated for about 7 lakhs before the incident was noticed. Due to the change of the communication address, the owner of credit card could not receive monthly statements generated at the month's end. The case was registered with the Chennai police. After the digital forensic investigation of the BPO's computer system, it was found that its two employees have illegally accessed to the computer to steal the customer record.
7. A case of copyright infringement was lodged in Andhra Pradesh (Nandanwar, 2013). A well known mobile service operator company launched a promotional campaign, in which it offered a mobile phone at a very low cost to its customers with a lock-in period of 3-years. The software of the phone was configured in such a way that, in the lock-in period the sim of any other company cannot work with the handset. A competitor of that company lured the existing customers of the company which gave

the mobile phone to “unlocked” the phone by cracking the software of the mobile so that any other sim can be used with the handset. The company reported the crime and the case were registered under copyright infringement u/s 63 of copyrights act.

8. A gang of criminals is active over the cyber space, which steals the credit card data of the cardholders from the POS at shopping malls, petrol pumps, resturents, hotels, etc. and use these cards to book air tickets online. According to the reports, over 15000 credit cards were fraudulently used by these criminals to book online tickets which account for approximatly Rs. 17 crore revenue loss. These criminals use public infrastructure like cyber cafe, etc. to book these tickets so that it is difficult to trace them. The fraud came to the notice when the customers who were charged for booking an airticket and these customers reported at the card issuing banks claming that these tickets were never booked by them.
9. In the year 2000, a worm known as Love Bug worm or VBS/Loveletter, which specially target Windows operating system based computer system, caused damage costing approx. Rs. 22,000 crore. An spam mail containing “ILOVEYOU” in the subject line and LOVE-LETTER-FOR-YOU.TXT.vbs as an attachment is received. If the user clicked the attachment, the machine gets infacted and the worm start searching all the drive of the computer and start currupting the files. It also start forwarding the copies of the email to all the outlook contacts added in the addressbook of the user. Nearly 10% machines connected to the Internet were infacted within no time (Madhya Pradesh State Cyber Police, 2013). Many large organizations which includes British parliament, Pentagon have to shut down the email system to stop this worm spreading into their network.
10. Online degree fraud are very popular these days over internet where accredited online degrees are offered by fake Universities (Gollin, 2003). These diploma mills offer to turn your work experience into a degree in exchange of money. The transcripts are also issued to the students on the basis of self evaluation. Its only when the students is rejected on account of fake degree, he realize that he fell pray to online fraud.
11. Can you belive a fake tweet message can cost \$136 billlion loss within seconds (Fisher, 2013). The US stock markets crashed in response to a fake twitter message send via hacked twitter account of Associated Press, USA which reported two explosions in the White House and that President Barack Obama had been injured. Later, Syrian Electronic Army, a terrorist group claimed responsibility on its own Twitter feed for the AP hack. The hacking was performed by sending a phishing e-

mail. As soon as the link in the phishing e-mail was clicked, a spyware was installed in the computer and the information stored in the system were sent to remote servers. Using this information the account of AP was hacked and the hoax was created which effected sentiments of the invester of NY Stock Exchange and resulted in heavy loss.

12. Recently a new virus, which infects the Point of Sale(POS) machines and steals the payment record of credit card of the customers. These confidential data like PIN codes, credit card numbers, expiration date, CCV number, etc. are tracked and sent to the hackers so that this information can be misused for committing financial frauds (US-CERT, 2014).
13. The people with ill intentions are not only looking for your private and confidential data, but are in search of your communication infrastructure so that your identity can be used for hiding their identity so that they are not caught after creating neusence. The terrorist outfit Indian Mujahideen(IM) used the unprotected wi-fi network of a Mumbai based US citizen, Kenneth Haywood. They hacked his wi-fi network used send an e-mail, which contains his IP address, to a news agency just 5 minutes before the Ahemdabad blast (Chowdhury, Nair, & Johnson, 2008).
14. The terrorist used open wi-fi network of Matunga's Khalsa College of Arts, Science and Commerce, Mumbai to send a terror mail to media house (The Indian Express, 2008). The terrorists remotely access the router and deleted the system logs after using the network so that it becomes difficult for the investigating to trace the origin of the email.
15. Pune based software engineer, Asma Sandip Thorve was arrested by economic offences wing of Pune police for illegally steeling source code of the software product and other confidential information of Brainvisa Technologies due to which the company lost Rs. 46.5 crores (Times of India, 2009).
16. There is a new type of crime evolving over internet where a prospective business partner will offer you a homebased business oppourtunity with no investment and very lucrative commission (Castillo, 2007). Once the person agrees to work with the company, the prospective business partner will ask for the details like address, phone numbers, photo identity, date of birth, etc. After some time, the person will receive parcel at the address with repackging instructions along with the list of addresses where these parcels are to be dispatched abroad. Actually these goods are purchased using stolen credit cards and the goods are delivered at the address provided by the person. The person will be held responsible if address of the delivery of the goods is

traced by the investigators. The real trouble begins when your commision arrives. It is in the form of third party cheque and is of the higher amount then you expected. Some days latter an instruction to return the excess amount electronically is received. Once the excess fund is electronically transferred, the bank will discover that the cheque is fake and the person will be help responsible for this act.

17. Some of the customers of ICICI bank were victim phishing attack (Nair, 2009). Some of the customers received an email from a person who claimed to be an official of ICICI bank. He asked the customers to update their account information using a link which redirects the customers to a page which is very similler to ICICI bank's webpage. The case was registered by the bank officials when this fraud came to the knowledge of the bank when some of the customers got suspecious and informed the IT department of the bank to verify the source of such email. The bank officials were suprized to find out that the website, which was very closely resembling the bank's official website. If the customer used that link to update his account credentials by logging into the fake website using their user id and the password, these details would reached the hackers and they can later use this information to login into the customer's account and transfer money aur pruchase goods online.
18. The cyber criminals have targeted the gas filling station in the US to skim the credit card and debit card data. The hacker planted bluetooth enabled credit card skimmers in most of the gas stations locted in the Southern United States. The customer data which includes information like account number, PIN, CVV, etc eas used by the hackers to withdraw more than \$2 million from the ATM mostly located at Manhattan.
19. The hackers used the tools used by the law enforcement agencies to parse data from iPhones to steel the private photographs of female celebreties in the US (Hazen, 2014). The hackers are belived to be using software called Elcomsoft Phone Password Breaker and iBrute to log into apple's site and download the backupfiles into their machines.
20. There are many incidents were non- friendly countries launch cyber attacks to gain access to the sensitive information. One such event is Russia is suspected for his involvement in hacking of US financial system (Farberov, 2014). One of the leading banks JPMorgan Chase was reported to be attacked by Russian hackers. The hackers were successful in steeling the sensitive data from the bank's server.
21. Recently, a Chinese mobile company, Xiaomi was found guilty for sending the sensitive data to Chinese servers (Kumar, 2014). This information includes sms,

photographs, contact list, etc. without the knowledge of the users. It's not the first time that a Chinese company was help suspected for espionage and US government have banned the use of Chinese equipments in some of its major establishments.

# CYBER SECURITY INITIATIVES IN INDIA

## 5.1 INTRODUCTION

With the growth of internet, the dependence on computers has increased exponentially. The challenge is to protect critical information infrastructure, like civil aviation sector, Railways' passenger reservation system and communication network, port management, companies and organisations in power, oil and natural gas sectors, banking and finance, telecom sector, etc. from cyber attacks. India is ranked fourth among the top 50 countries in terms of the number of cyber crime complaints reported to the Internet Crime Complaint Centre (IC3), preceded only by the US, Canada and the UK based on the 2014 IC3 annual report (The Telegraph, 2015).

Shortage of trained cyber security workforce is of serious concern to India. In comparison to China, US and Russia that have 125000, 91080 and 7300 trained cyber experts respectively; India has merely 556 cyber experts deployed in various government agencies (Joshi, 2013). India is considered an IT superpower that is a major exporter of software and hosts major ITES-based outsourced businesses. Therefore, IT constitutes a major share of Indian economy. Recently, European Union has picked holes in India's data security system and suggested that a joint expert group be set up to propose ways on how the country should tighten measures for qualifying as a data secure nation (Sen, 2013). Therefore, India needs look seriously into upgrading its Information Security infrastructure and reframe cyber policies to get data secure status from EU. This is crucial for India to retain high-end outsourced business, which has a potential of increasing from the existing \$20 billion to \$50 billion.

## 5.2 COUNTER CYBER SECURITY INTIATIVES IN INDIA

To counter cyber security attacks, Government of India have taken some initiatives which are listed below:

1. **National Counter Terrorism Center(NCTC):** After 26/11 attack in 2008, suddenly the Indian government realized the importance of Counter terrorism initiatives and proposed National Counter Terrorism Center(NCTC) to provide intelligence inputs to the decision makers to plan for counter terrorist activities. The NCTC is supposed to coordinate between various State and Central govt. agencies and serve as a single and

effective point of control and coordination of all counter terrorism measures. It is modeled on the American NCTC and Britain's Joint Terrorism Analysis Centre and will derive its powers from the Unlawful Activities Prevention Act, 1967 (Mrunal, 2012).

2. **National Information Security Assurance Programme (NISAP):** To create the awareness among the people in the government and critical sector organization, CERT-In has taken an initiative called National Information Security Assurance Programme (NISAP), to develop and implement information security policy and information security best practices based on ISO/IEC 27001 for protection of their infrastructure. CERT-in has established the facility for Computer Forensics for investigation of cyber crimes and to provide hands on training to the law enforcement agencies and judiciary. This infrastructure is being augmented to include network forensics and mobile forensics investigation facility. CERT-In is cooperating with defence, banks, judiciary and law enforcement agencies in training their officials as well as extending the support in investigation of cyber crimes (Srinath, 2006).
3. **Computer Emergency Response Team-India(CERT-In):** The Indian Computer Emergency Response Team was created in 2004 by Department of Information Technology. The purpose of creating CERT-In was to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country and is also responsible for overseeing administration of the IT act (CERT-In, 2014).
4. **Indo US Cyber Security Forum (IUSCSF):** The India-US Cyber Security Forum was established in 2001 and is dedicated to protecting the critical infrastructure of the knowledge-based economy. The members of the forum are various government and private sector organizations, both from India and the United States, working under the Forum's auspices, have identified risks and common concerns in cyber security and crafted an action-oriented work plan on securing networked information systems. The Forum focuses on cyber-security, cyber-forensics and related research and works towards enhancing co-operation among law enforcement agencies on both sides in dealing with cyber crime. Defence services of both the countries will enhance their interaction through exchange of experience in organizational, technological, and procedural aspects. Ongoing co-operation between India's STQC and the US National Institute of Standards and Technology (NIST) will expand to new areas including harmonization of standards. CII and their US counterpart have decided to set up an

India Information Sharing and Analysis Centre (ISAC) and India Anti-Bot Alliance ('bot' refers to software that can be tasked to invade computers and undertake malicious activities remotely on behalf of hackers) (Press Information Bureau, 2006).

5. **National Critical Information Infrastructure Protection Centre (NCIIPC) of India:** It is declared as a nodal agency for the protection of critical information infrastructure of India and is responsible for all measures including R&D for protection of critical information infrastructure. Some of the activities that NCIIPC performs are (Chander, 2013):
  - a. Identification of Critical Sub-sectors
  - b. Study of Information Infrastructure of identified critical sub-sectors
  - c. Issue of Daily / Monthly cyber alerts / advisories
  - d. Malware Analysis
  - e. Tracking zombies and Malware spreading IPs
  - f. Cyber Forensics activities
  - g. Research and Development for Smart and Secure Environment.
  - h. Facilitate CII owners in adoption of appropriate policies, standards, best practices for protection of CII.
  - i. Annual CISO Conference for Critical Sectors.
  - j. Awareness and training
  - k. 24X7 operation and helpdesk
6. **National Intelligence Grid (Natgrid) project of India:** It is the integrated intelligence grid developed by C-DAC-Pune connecting databases of core security agencies of the Government of India (C-DAC, 2014). It is a counter terrorism measure that collects and collates a host of information from government databases including tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel (Yasmeen, 2013). This combined data will be made available to 11 central agencies, which are: Research and Analysis Wing, the Intelligence Bureau, Central Bureau of Investigation, Financial intelligence unit, Central Board of Direct Taxes, Directorate of Revenue Intelligence, Enforcement Directorate, Narcotics Control Bureau, Central Board of Excise and Customs and the Directorate General of Central Excise Intelligence.
7. **Crime and Criminal Tracking Networks and Systems (CCTNS) project of India:** It is a project under National e-Governance Plan(NeGP) covering all 28 States and 7

UTs which aims at creation of a nation-wide networking infrastructure for evolution of IT-enabled sophisticated tracking system around 'investigation of crime and detection of criminals (PTI, 2013). The goals of the CCTNS are to facilitate collection, storage, retrieval, analysis, transfer and sharing of data and information at the police station and between the police station and the State Headquarters and the Central Police Organizations. CCTNS would provide a comprehensive database for crimes and criminals, and it would be easier for the law enforcement agencies to track down a criminal moving from one place to another.

8. **National Cyber Coordination Centre (NCCC):** National Cyber Coordination Centre is a proposed cyber security and e-surveillance agency in India. It is intended to screen communication metadata and co-ordinate the intelligence gathering activities of other agencies. Some of the components of NCCC include a cyber attack prevention strategy, cyber attack investigations and training, etc.
9. **Botnet Cleaning Center:** As a part of the Digital India programme, the Government is setting up a centre that will detect malicious programmes like 'botnets' and help people remove such harmful softwares from their devices. "The Government is setting up 'botnet' cleaning and malware analysis centre" according to media reports. Botnet is a network of malicious software. It can steal information, take control of device function and carry out cyber attacks like Distributed Denial-of-Service (DDoS).
10. **E-mail policy of Government of India:** In present date Email is considered to be as the major source of communication between individuals and organization as well. The same applies to Govt. of India (GOI) as well. E-mail has become major mode of communications for the entire government. With the increasing use of Emails to communicate among different Govt. Agencies, the Email Policy was laid down by Government of India (GOI) in October 2013. Here we will cover some of the important clause of policy, readers are advised to download policy from Department of Electronics and IT website.
11. **Ministry of Home Affairs (MHA):** The Ministry of Home Affairs (MHA) is a ministry of the Government of India. An interior ministry, it is mainly responsible for the maintenance of internal security and domestic policy. Readers are advised to read annual report of the Ministry of Home Affairs. The Ministry of Home Affairs (MHA) has multifarious responsibilities, the important among them being-internal security, border management, CentreState relations, administration of Union Territories, management of Central Armed Police Forces, disaster management, etc.

**12. National Crime Records Bureau (NCRB):** NCRB shall endeavour to empower Indian Police with Information Technology and Criminal Intelligence to enable them to effectively & efficiently enforce the law & improve public service delivery. This shall be achieved through coordination with police forces at National & International level, upgradation of crime analysis technology, developing IT capability & IT enabled solutions.

**13. Data Security Council of India (DSCI):** Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together national governments and their agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives. To further its objectives, DSCI engages with governments, regulators, industry associations and think tanks on policy matters. To strengthen thought leadership in cyber security and privacy, DSCI develops best practices and frameworks, publishes studies, surveys and papers. It builds capacity in security, privacy and cyber forensics through training and certification program for professionals and law enforcement agencies and engages stakeholders through various outreach initiatives including events, awards, chapters, consultations and membership programs. DSCI also endeavours to increase India's share in the global security product and services market through global trade development initiatives. These aim to strengthen the security and privacy culture in the India.

# GUIDELINES FOR SECURE PASSWORD, TWO STEP VERIFICATION AND USING FREE ANTIVIRUS

## 6.1 GENERATING SECURE PASSWORD

### 6.1.1 Guideline for setting secure Password<sup>10</sup>

Choosing the right password is something that many people find difficult, there are so many things that require passwords these days that remembering them all can be a real problem. Perhaps because of this a lot of people choose their passwords very badly. The simple tips below are intended to assist you in choosing a good password.

#### Basics

- ✓ Use at least eight characters, the more characters the better really, but most people will find anything more than about 15 characters difficult to remember.
- ✓ Use a random mixture of characters, upper and lower case, numbers, punctuation, spaces and symbols.
- ✓ Don't use a word found in a dictionary, English or foreign.
- ✓ Never use the same password twice.

#### Things to avoid

- ✓ Don't just add a single digit or symbol before or after a word. e.g. "apple1"
- ✓ Don't double up a single word. e.g. "appleapple"
- ✓ Don't simply reverse a word. e.g. "elppa"
- ✓ Don't just remove the vowels. e.g. "ppl"
- ✓ Key sequences that can easily be repeated. e.g. "qwerty", "asdf" etc.
- ✓ Don't just garble letters, e.g. converting **e** to **3**, **L** or **i** to **1**, **o** to **0**. as in "z3r0-10v3"

#### Tips

- ✓ Choose a password that you can remember so that you don't need to keep looking it up, this reduces the chance of somebody discovering where you have written it down.
- ✓ Choose a password that you can type quickly, this reduces the chance of somebody discovering your password by looking over your shoulder.

#### Bad Passwords

---

<sup>10</sup> [http://www.lockdown.co.uk/?pg=password\\_guide](http://www.lockdown.co.uk/?pg=password_guide)

- ✓ Don't use passwords based on personal information such as: name, nickname, birthdate, wife's name, pet's name, friends name, home town, phone number, social security number, car registration number, address etc. This includes using just part of your name, or part of your birthdate.
- ✓ Don't use passwords based on things located near you. Passwords such as "computer", "monitor", "keyboard", "telephone", "printer", etc. are useless.
- ✓ Don't ever be tempted to use one of those oh so common passwords that are easy to remember but offer no security at all. e.g. "password", "letmein".
- ✓ Never use a password based on your username, account name, computer name or email address.

## **Choosing a password**

- ✓ Use good password generator software.
- ✓ Use the first letter of each word from a line of a song or poem.
- ✓ Alternate between one consonant and one or two vowels to produce nonsense words. eg. "taupouti".
- ✓ Choose two short words and concatenate them together with a punctuation or symbol character between the words. eg. "seat%tree"

## **Changing your password**

- ✓ You should change your password regularly, I suggest once a month is reasonable for most purposes.
- ✓ You should also change your password whenever you suspect that somebody knows it, or even that they may guess it, perhaps they stood behind you while you typed it in.
- ✓ Remember, don't re-use a password.

## **Protecting your password**

- ✓ Never store your password on your computer except in an encrypted form. Note that the password cache that comes with windows (.pwl files) is NOT secure, so whenever windows prompts you to "Save password" don't.
- ✓ Don't tell **anyone** your password, not even your system administrator
- ✓ Never send your password via email or other unsecured channel
- ✓ Yes, write your password down but don't leave the paper lying around, lock the paper away somewhere, preferably off-site and definitely under lock and key.
- ✓ Be very careful when entering your password with somebody else in the same room.

## **Remembering your password**

Remembering passwords is always difficult and because of this many people are tempted to write them down on bits of paper. As mentioned above this is a very bad idea. So what can you do?

- ✓ Use a secure password manager, see the downloads page for a list of a few that won't cost you anything.
- ✓ Use a text file encrypted with a strong encryption utility.
- ✓ Choose passwords that you find easier to remember.

## **Bad Examples**

- ✓ "fred8" - Based on the users name, also too short.
- ✓ "christine" - The name of the users girlfriend, easy to guess
- ✓ "kciredref" - The users name backwards
- ✓ "indescribable" - Listed in a dictionary
- ✓ "iNdesCriBaBle" - Just adding random capitalisation doesn't make it safe.
- ✓ "gandalf" - Listed in word lists
- ✓ "zeolite" - Listed in a geological dictionary
- ✓ "qwertyuiop" - Listed in word lists
- ✓ "merde!" - Listed in a foreign language dictionary

## **Good Examples**

None of these good examples are actually good passwords, that's because they've been published here and everybody knows them now, always choose your own password don't just use somebody else's.

- ✓ "mItWdOtW4Me" - **Monday is the worst day of the week for me.**

## **How would a potential hacker get hold of my password anyway?**

There are four main techniques hackers can use to get hold of your password:

1. **Steal it.** That means looking over your shoulder when you type it, or finding the paper where you wrote it down. This is probably the most common way passwords are compromised, thus it's very important that if you do write your password down you keep the paper extremely safe. Also remember not to type in your password when somebody could be watching.
2. **Guess it.** It's amazing how many people use a password based on information that can easily be guessed. Psychologists say that most men use 4 letter obscenities as passwords and most women use the names of their boyfriends, husbands or children.
3. **A brute force attack.** This is where every possible combination of letters, numbers and symbols in an attempt to guess the password. While this is an extremely labour intensive task, with modern fast processors and software tools this method is not to be underestimated. A Pentium 100 PC might typically be able to try 200,000 combinations every second this would mean that a 6 character password containing just upper and lower case characters could be guessed in only 27½ hours.
4. **A dictionary attack.** A more intelligent method than the brute force attack described above is the dictionary attack. This is where the combinations tried are first chosen from words available in a dictionary. Software tools are readily available that can try every word in a dictionary or word list or both until your password is found. Dictionaries with hundreds of thousands of words, as well as specialist, technical and foreign language dictionaries are available, as are lists of thousands of words that are often used as passwords such as "qwerty", "abcdef" etc.

## 6.2 USING PASSWORD MANAGER<sup>11</sup>

We use passwords to ensure security and the confidentiality of our data. One of the biggest modern day crimes is identity theft, which is easily accomplished when passwords are compromised. The need of the hour is good password management. Have you ever thought of an alternative to remembering your passwords and not repeatedly entering your login credentials? Password managers are one of the best ways to store, back up and manage your passwords. A good password is hard to remember and that's where a password manager

---

<sup>11</sup> <http://opensourceforu.efytimes.com/2015/01/peek-top-password-managers/>

comes in handy. It encrypts all the different passwords that are saved with a master password, the only one you have to remember.

### **6.2.1 What is a password manager?**

A password manager is software that helps a user to manage passwords and important information so that it can be accessed any time and anywhere. An excellent password manager helps to store information securely without compromising safety. All the passwords are saved using some kind of encryption so that they become difficult for others to exploit.

### **6.2.2 Why you should use it?**

If you find it hard to remember passwords for every website and don't want to go through the 'Forgot password?' routine off and on, then a password manager is what you are looking for. These are designed to store all kinds of critical login information related to different websites.

### **6.2.3 How does it work?**

Password managers may be stored online or locally. Online password managers store information in an online cloud, which can be accessed any time from anywhere. Local password managers store information on the local server, which makes them less accessible. Both have their own advantages, and the manager you use would depend on your need.

Online password managers use browser extensions that keep data in a local profile, syncing with a cloud server. Some other password managers use removable media to save the password so that you can carry it with you and don't have to worry about online issues. Both these options can also be combined and used as two-factor authentication so that data is even more secure.

### **6.2.4 Some popular Password managers**

The passwords are saved using different encryptions based on the services that the companies provide. The best password managers use a 256-bit (or more) encryption protocol for better security, which has been accepted by the US National Security Agency for top secret information handling. If you have considered using a password manager and haven't decided on one, this section features the top five.

1. **KeePassX:** KeePassX is an open source, cross-platform and light weight password management application published under the terms of the GNU General Public License. It was built based on the Qt Libraries. KeePassX stores information about user names, passwords and other login information in a secure database. KeePassX uses its own random password generator, which makes it easier to create strong

passwords for better security. It also includes a powerful and quick search tool with which a keyword of a website can be used to find login credentials that have been stored in the database. It allows users to customise groups, making it more user friendly. KeePassX is not limited to storing only usernames and passwords but also free-form notes and any kind of confidential text files.

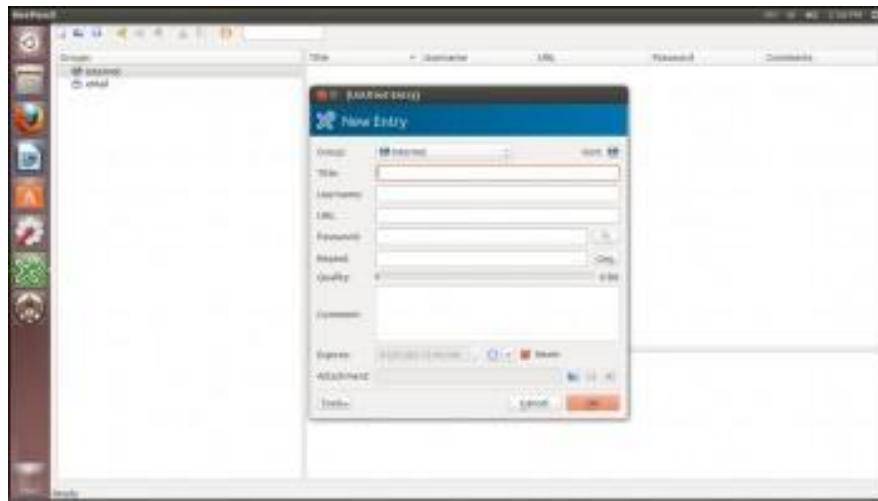


Figure 9: KeePassX

### Features

- *Simple user interface:* The left pane tree structure makes it easy to distinguish between different groups and entries, while the right pane shows more detailed information.
- *Portable media access:* Its portability makes it easy to use since there's no need to install it on every computer.
- *Search function:* Searches in the complete database or in every group.
- *Auto fill:* There's no need to type in the login credentials; the application does it whenever the Web page is loaded. This keeps it secure from key loggers.
- *Password generator:* This feature helps to generate strong passwords that make it difficult for dictionary attacks. It can be customised.
- *Two factor authentication:* It enables the user to either unlock the database by a master password or by a key from a removable drive.
- *Adds attachments:* Any type of confidential document can be added to the database as an attachment, which allows users to secure not just passwords.

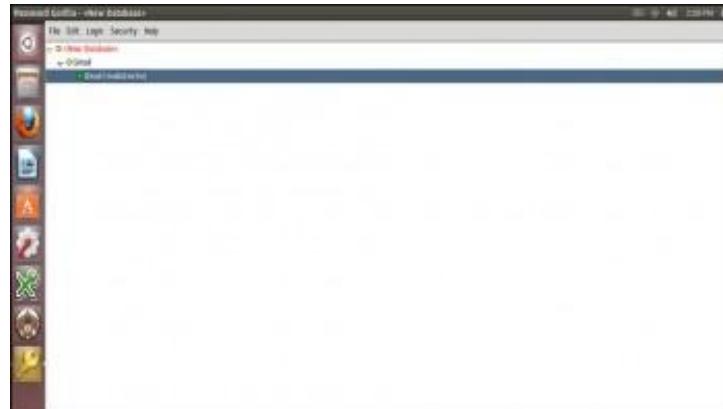
- *Cross-platform support:* It works on all supported platforms. KeePassX is an open source application, so its source code can be compiled and used for any operating system.
  - *Security:* The password database is encrypted with either the AES encryption or the Twofish algorithm, which uses 256-bit key encryption.
  - *Expiration date:* The entries can be expired, based on a user defined date.
  - *Import and export of entries:* Entries: from PwManager or Kwallet can be imported, and entries can be exported as text files.
  - *Multi-language support:* It supports 15 languages.
2. **Clipperz:** Clipperz is a Web-based, open source password manager built to store login information securely. Data can be accessed from anywhere and from any device without any installation. Clipperz also includes an offline version when an Internet connection is not available.
- 

Figure 10: Clipperz

### Features

- *Direct login:* Automatically logs in to any website without typing login credentials, with just one click.
- *Offline data:* With one click, an encrypted local copy of the data can be created as a HTML page.
- *No installation:* Since it's a Web-based application, it doesn't require any installation and can be accessed from any compatible browser.

- *Data import*: Login data can be imported from different supported password managers.
  - *Security*: The database is encrypted using JavaScript code on the browser and then sent to the website. It requires a passphrase to decrypt the database without which data cannot be accessed.
  - *Support*: Works on any operating system with a major browser that has JavaScript enabled.
3. Password Gorilla: Password Gorilla is an open source, cross-platform, simple password manager and personal vault that can store login information and notes. Password Gorilla is a Tcl/Tk application that runs on Linux, Windows and Mac OS X. Login information is stored in the database, which can be accessed only using a master password. The passwords are SHA256 protected and the database is encrypted using the Twofish algorithm. The key stretching feature makes it difficult for brute force attacks.



*Figure 11: Password Gorilla*

### *Features*

- *Portable*: Designed to run on a compatible computer without being installed.
- *Import of database*: Can import the password database saved in the CSV format.
- *Locks the database when idle*: It automatically locks the database when the computer is idle for a specific period of time.
- *Security*: It uses the Twofish algorithm to encrypt the database.
- *Can copy credentials*: Keyboard shortcuts can be used to copy login credentials to the clipboard.

- *Auto clear:* This feature clears the clipboard after a specified time.
  - *Organises groups:* Groups and sub-groups can be created to organise passwords for different websites.
4. **Gpassword Manager:** Gpassword Manager is a simple, lightweight and cross-platform utility for managing and accessing passwords. It is published under the terms of the Apache License. It allows users to securely store passwords/URLs in the database. The added entries can be marked as favourites, which then can be accessed by right-clicking the system tray icon. The passwords and other login information shown in the screen can be kept hidden based on user preferences.



*Figure 12: Gpassword manager*

#### *Features*

- *Access to favourite sites:* A list of favourite Web pages can be accessed quickly from the convenient ‘tray’ icon.
  - *Quick fill:* Passwords and other information can be clicked and dragged onto forms for quick filling out.
  - *Search bar:* The quick search bar allows users to search passwords that are needed.
  - *Password generator:* Passwords with user-defined options can be generated with just a click.
  - *Quick launch:* Favourite websites can be launched by right-clicking the tray icon.
5. **Password Safe:** Password Safe is a simple and free open source application initiated by Bruce Schneier and released in 2002. Now Password Safe is hosted on

SourceForge and developed by a group of volunteers. It's well known for its ease of use. It is possible to organise passwords based on user preference, which makes it easy for the user to remember. The whole database backup and a recovery option are available for ease of use. Passwords are kept hidden, making it difficult for shoulder surfing. Password Safe is licensed under the Artistic licence.



Figure 13: Password Safe

### Features

- *Ease of use:* The GUI is very simple, enabling even a beginner to use it.
- *Multiple databases:* It supports multiple databases. And different databases can be created for each category.
- *Safe decryption:* The decryption of the password database is done in the RAM, which leaves no trace of the login details in the hard drive.
- *Password generator:* Supports the generation of strong, lengthy passwords.
- *Advanced search:* The advanced search function allows users to search within the different fields.
- *Security:* Uses the Twofish algorithm to encrypt the database.

## 6.3 ENABLING TWO-STEP VERIFICATION<sup>12</sup>

Every day, tens of thousands of personal accounts are hacked. Personal information is compromised, passwords are cracked, and lives are put in jeopardy. If you ever use one password for multiple accounts, you are exponentially increasing your vulnerability to being hacked. Thankfully, Google has launched its **2-step verification system**: anytime an unknown device is used to sign into your Google account, the user has to provide a verification code *in addition* to the password. So it's not enough for hackers to just get your password; they'll also need physical control of your phone or computer to access your account.

**Step 1:** Sign into your Gmail account. Click on a thumbnail of your avatar on the right side of the top menu bar, and then click "Account" to update your settings.

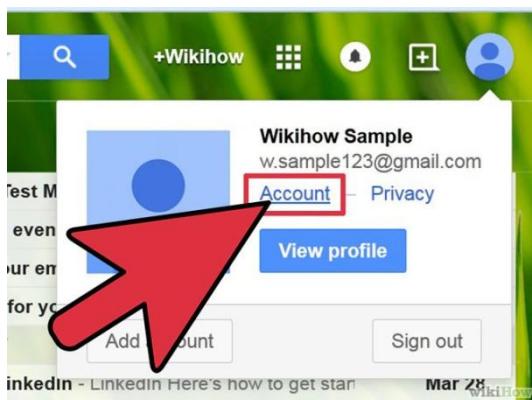


Figure 14: Account setting

**Step 2:** You will land on your Account Settings page. Scroll down until you find a blue bar that says "signing in".

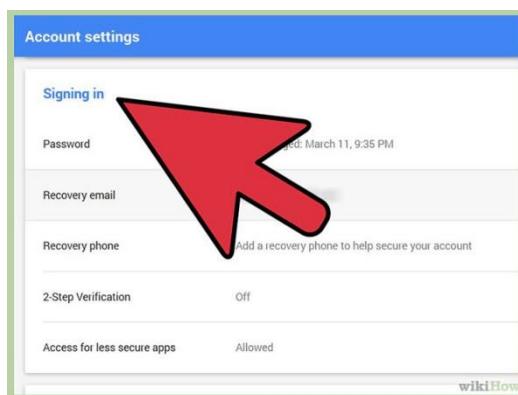


Figure 15: Signing in

<sup>12</sup> <http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License

**Step 3:** In the 2-step verification section, you'll see if you already have 2-step verification turned on. If it says "OFF," click "Edit" to set the feature up.

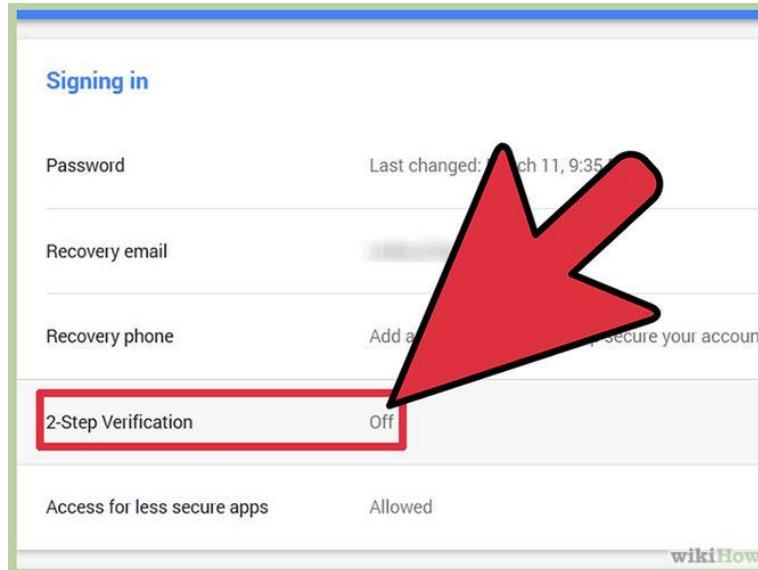


Figure 16: Turning on two steps verification<sup>13</sup>

**Step 4:** You'll see a page that briefly walks through the steps of setting up 2-step verification. Hover over the steps for more detail. Once you're ready, click "Start setup."

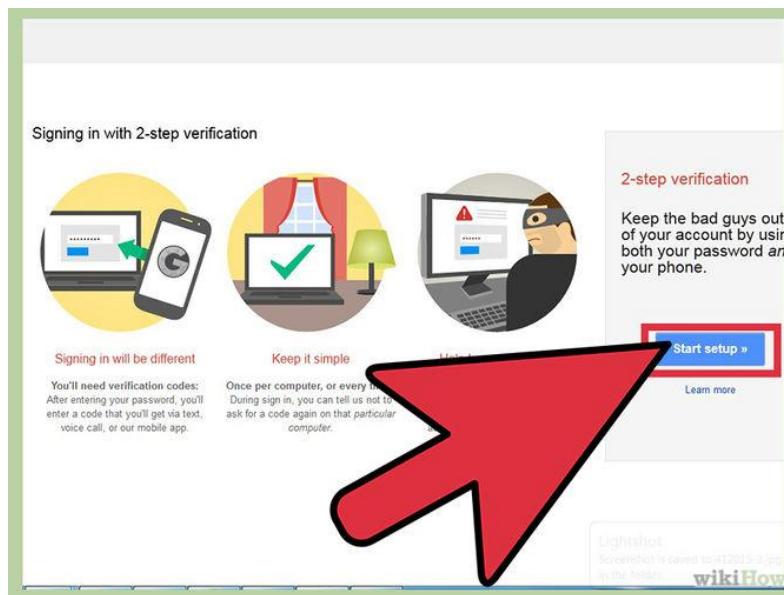


Figure 17: Start setup

**Step 5:** Type in your cell phone number. This will be the phone associated with your Google account. Anytime you sign into your Google account from an unknown device (e.g., a public

<sup>13</sup> Image courtesy: Figure 14 to 30 are adopted from <http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License.

computer), Google will send a verification code to your phone and you will need to enter that before you can sign in.

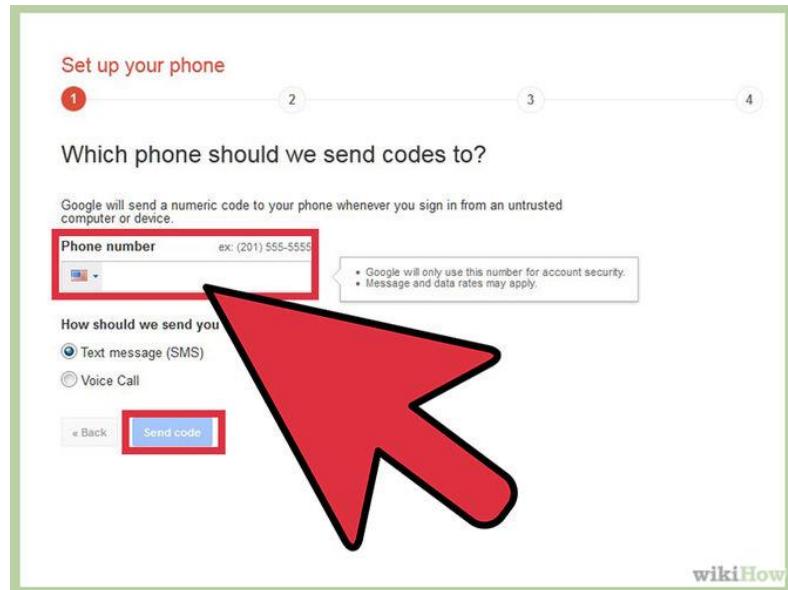


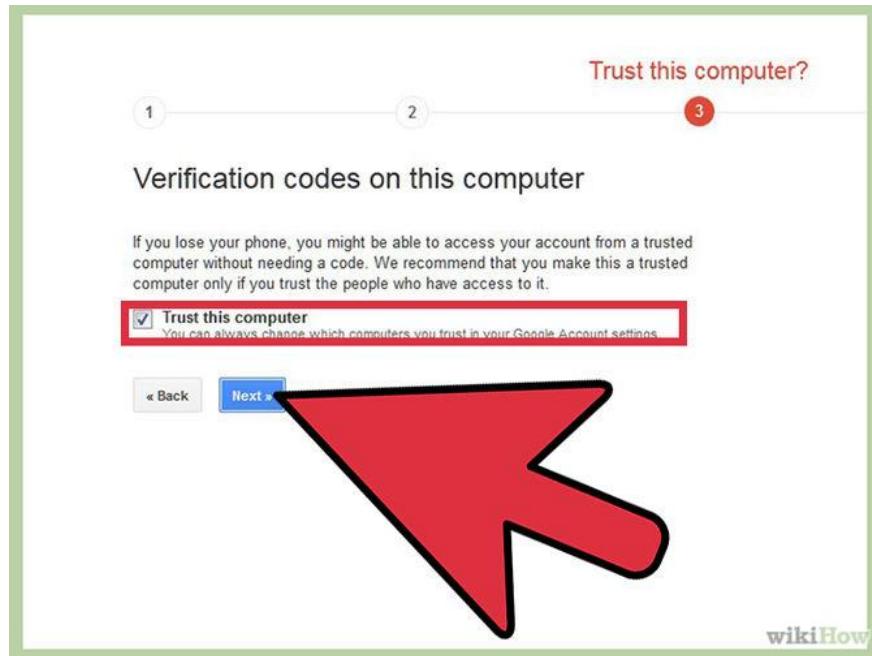
Figure 18: Entering mobile number for verification

**Step 6:** Select whether you'd like to receive a text message or Google Voice call with your verification code. Press submit. Then wait for the code to arrive to your phone and enter it in.



Figure 19: Entering varification code

**Step 7: Decide whether to trust this device.** If you are turning on 2-step verification from a personal computer or trusted device, check the "trust this device" box. You will only be asked to enter a verification code when you sign into this account once per 30 days.



*Figure 20: Setting up trust setting of the computer*

**Step 8:** Press OK, and you have just set up 2-step verification for your Google account! Skip any additional steps that seem unfamiliar or confusing for now -- we will address all of them in successive sections of this article.

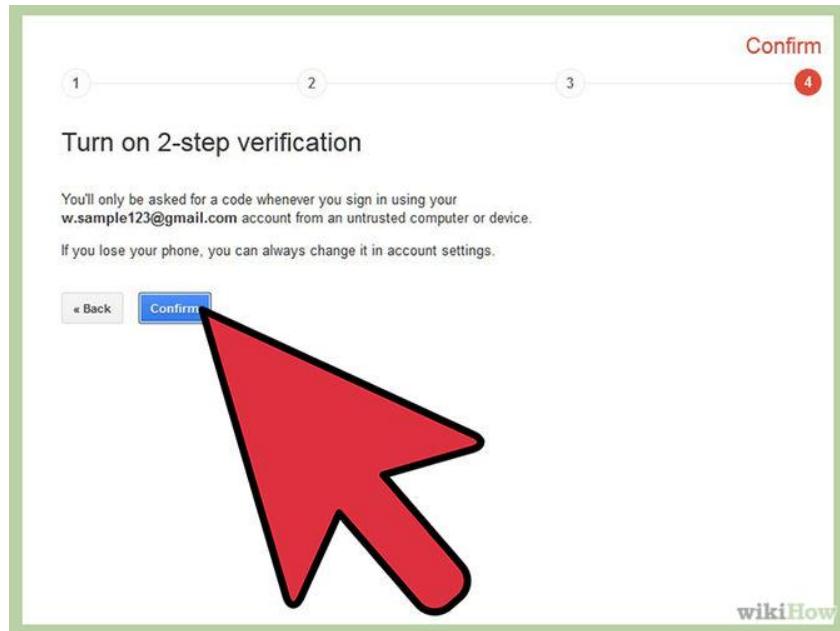


Figure 21: Confirmation

**Step 9:** Print a list of backup verification codes and store it in a secure but accessible place, like your wallet. If you ever need to sign into your Google account but don't have your primary phone with you, you can enter one of these codes instead.

- Go to your 2-step verification settings page.
- Under "How to receive codes," click on the "Show backup codes" link. Print this page.

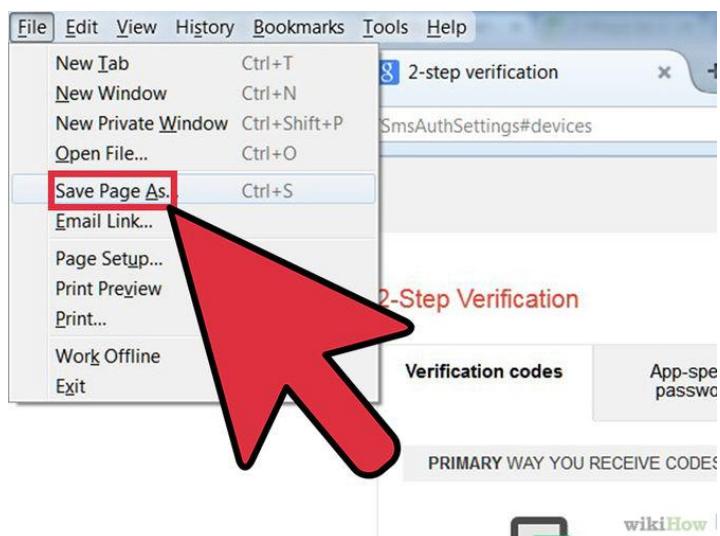


Figure 22: Saving the page

### Method 1 of 2: Application-Specific Passwords

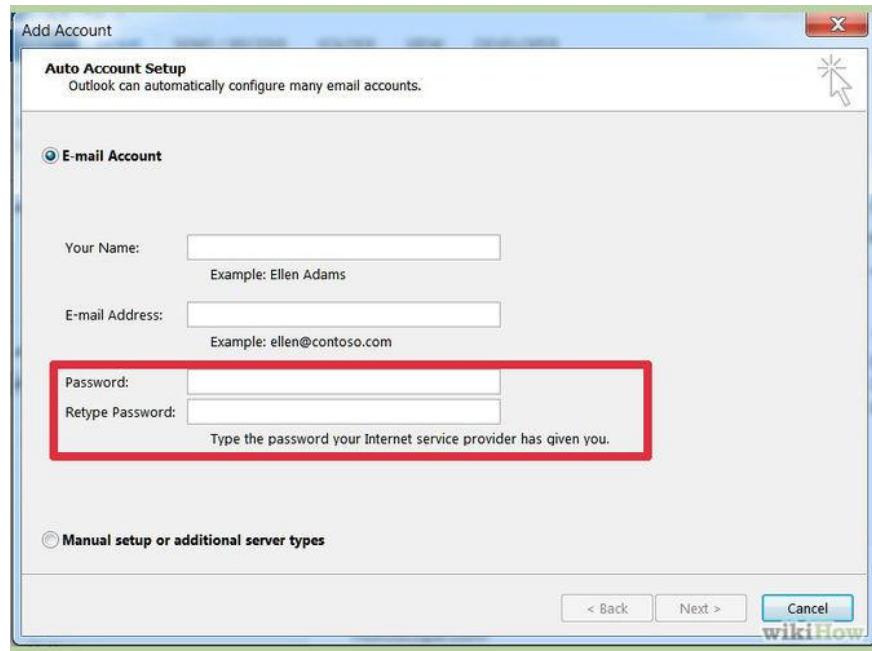


Figure 23: Setting up application specific password

**Step 1:** Understand the need for application-specific passwords. With 2-step verification, Google has you covered every time you sign into your account from a web browser. However, if you use your Google account with other applications, such as Microsoft Outlook or a mobile device's mail application, those systems cannot ask you for a verification code. Therefore, you will need to sign into those systems *once* with an application-specific password. You will only need to re-enter an application-specific password if you choose to reset it and generate a new one for that device.

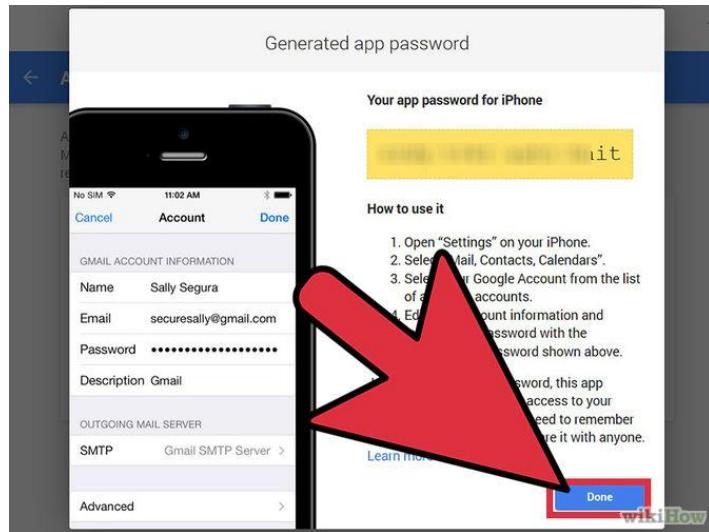


Figure 24: Generating app password

**Step 2:** Generate application-specific passwords for your devices. Go to your 2-step verification settings page or click "Edit" next to 2-step verification on the Security Account Settings page (steps 1-3 above). Scroll down and click on "Manage application-specific passwords."

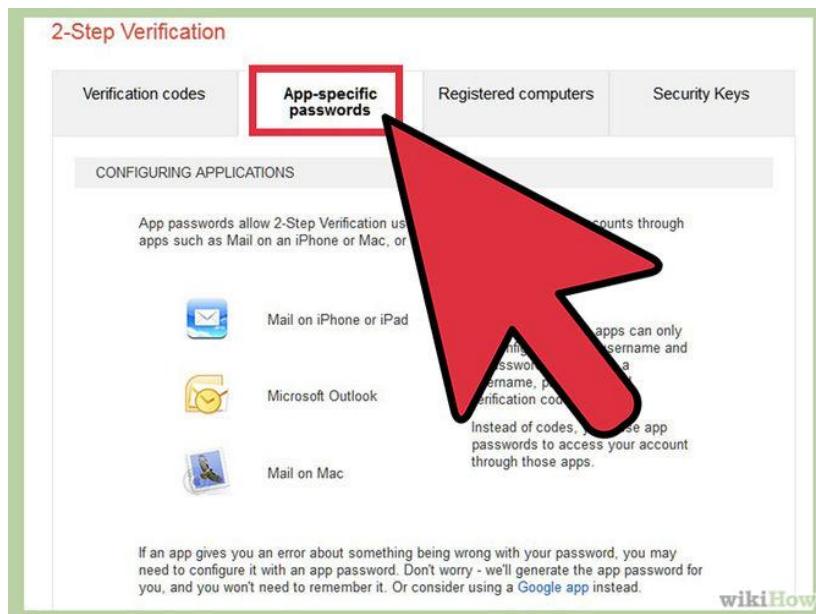


Figure 25: Managing application specific passwords

**Step 3:** At the top of the page, you will see a list of sites, applications and devices to which you have granted some level of access to your account. If you allowed a third-party website (e.g., LinkedIn, Twitter, Foursquare) to comb your Gmail Contacts to find friends, for example, you will see that listed. If you use other Google applications, you will also see those listed. Feel free to revoke access to any site or program you no longer wish to use.

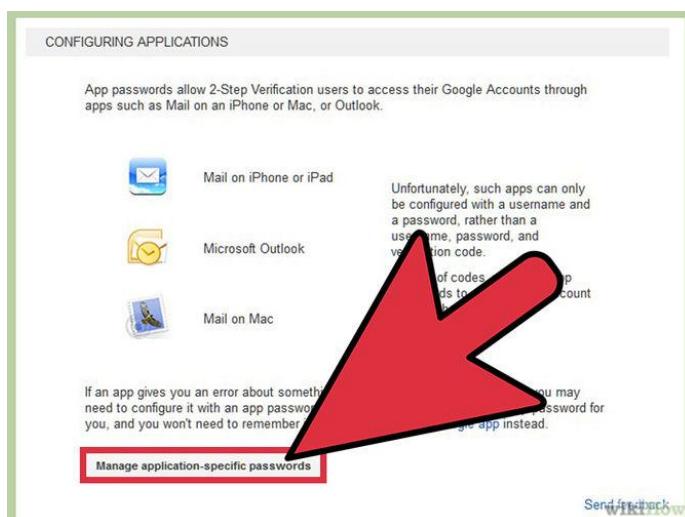


Figure 26: Configuring applications

**Step 4:** Scroll down to the field at the bottom for entering the name of a device. Enter in something that will help you remember what this application-specific password is for -- e.g., Mail App on iPhone, Google App on iPhone, Chrome Sync, Outlook, Thunderbird, or whatever describes your application. Click "Generate password". You should generate a new application-specific password for *each* application.

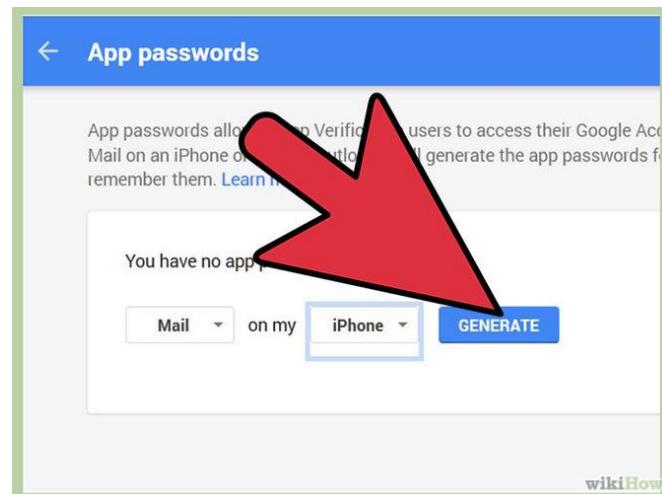


Figure 27: Generating app password

**Step 5:** Open up the application. Go to the settings page where you enter in your Google Account information. Type in your Google account name as usual. Now instead of your account password, type in the application-specific password in the password field. You have now granted this application full access to your Google account. You will only need to enter this password once. There is no need to write it down or memorize it, and it will not be displayed by Google again.

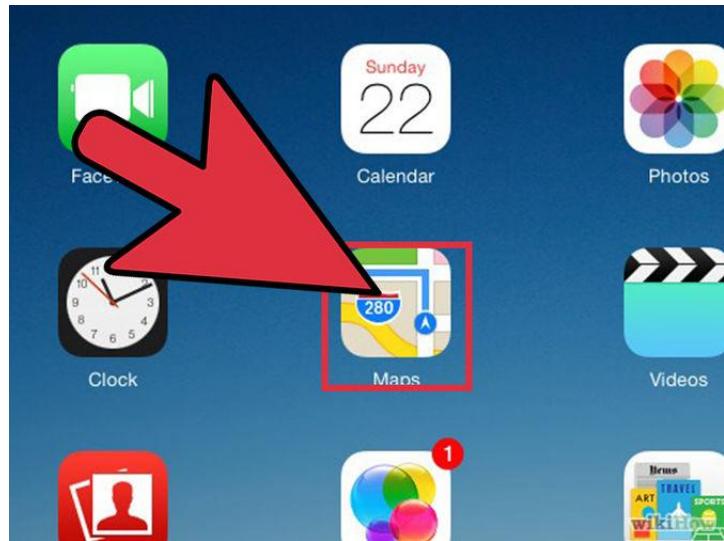


Figure 28: Testing the password

**Step 6:** Click "Done" on your web browser once you have successfully entered the application-specific password.

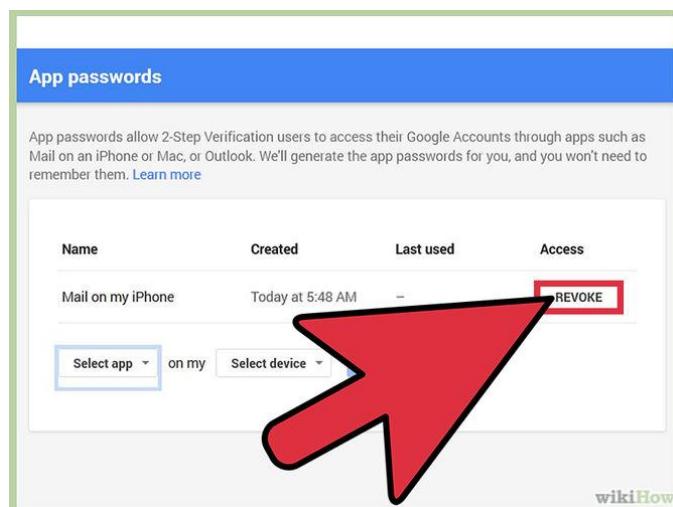


Figure 29: Revoke the password

**Step 7:** Know how to revoke an app's access to your Gmail account. If you don't want to use an app anymore, or you lost your phone and want to stop anyone who has it from accessing your Gmail, simply click on the "Revoke" button in your application-specific password settings page.

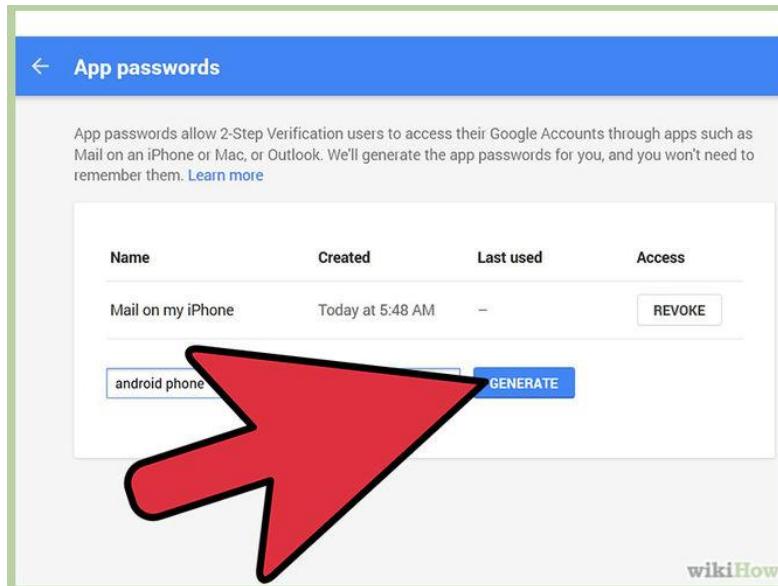


Figure 30: Generating password for android phone

**Step 8:** Create new application-specific passwords for *each* application that you connect your Google Account to! This means if you sync your Google Account to two mail apps and a chat client, you should have *three* application-specific passwords.

### Method 2 of 2: If You Lose Your Phone

If you lose your phone and have 2-step verification turned on, you *can* still access your Gmail account. You also can and should follow these steps to stop strangers from gaining access to your Google accounts.

**Step 1:** Revoke your current application-specific passwords. If you have a smartphone with apps linked to your Google account, they will automatically be signed out. When you get a new phone, you can generate new application-specific passwords (see previous section) and enter them into your new devices.

**Step 2:** Change your Gmail password. Even if someone else has your verification code, they can't get into your Gmail account without your new password. While it's unlikely that the person who has your phone also has cracked your Gmail password, you can never be too sure. If you are logged into Google from any web browser on your mobile device, you'll now also automatically be signed out.

**Step 3:** Add a backup phone number if you have a second mobile device. Go to your 2-step verification settings page and click "Add a phone number" in the "Backup phones" section.

**Step 4:** If you don't have a backup phone, use your list of printable backup codes to access your account. On your 2-step verification settings page, click "Show backup codes". If you haven't done so already, print out this page and keep it in a safe but accessible place -- such as your wallet.

**Step 5:** If you get phone and change your phone number, be sure to revoke access to your previous number on the 2-step verification settings page.

## **6.4 SECURING COMPUTER USING FREE ANTIVIRUS<sup>14</sup>**

As computers become more and more integrated in to our lives, we end up leaving many sensitive data on our computer-from passwords, official email id, bank account to personal notes, business plans and other confidential information. So, good security software is a must for everyone. Here is a list of 11 free anti-virus software and its common features which you can select (home users) for your online security. All are listed in alphabetical order

**1. Avast Antivirus**— Avast is one of the best free anti-virus software available that provides a complete protection against security threats. This full-featured antivirus package has the following feature: Built in Anti-spyware, Anti-Rootkit, Web shield, Strong self protection, P2P and IM shield, Anti-Virus kernel, resident protection, Network shield, Automatic update, System integration, Windows 64 bit support, Integrated Virus Cleaner. It can be downloaded from <https://www.avast.com/index>

**2. AVG Antivirus** – AVG anti-virus free edition provides basic antivirus and anti-spyware protection for Windows. Following features included in the free edition: Anti-virus , anti-spyware and Safe surf feature. It can be downloaded from <http://free.avg.com/>

**3. Avira AntiVir Personal** - Avira is a comprehensive, easy to use antivirus program, designed to reliable free of charge virus protection to home-users. Features included are: Protection from virus worms and Trojans, Anti-rootkit, Anti-fishing, Anti dialers. It can be downloaded from <http://www.free-av.com/>

**4. BitDefender** - Free Edition uses the same ICSA Labs certified scanning engines found in Pro version of BitDefender , allowing you to enjoy basic virus protection for no cost at all. Features includes: On demand Virus Scanner and Remover and Scheduled scanning. It can be downloaded from <http://www.bitdefender.com/PRODUCT-14-en--BitDefender-Free-Edition.html>

---

<sup>14</sup> [http://shaifulaueo.blogspot.in/p/free-antivirus\\_13.html](http://shaifulaueo.blogspot.in/p/free-antivirus_13.html)

- 5. Blink Personal** – An all-in one security suite with antivirus limited for one year. Blink personal Security suite features – Antivirus and Anti spyware, Anti root kit, Built-in Firewall protection and Identity protection. It can be downloaded from <http://free-antivirus.eeye.com/>
- 6. Calmwin antivirus**–An open source, free Antivirus program for Windows 98/Me/2000/XP/2003 and Vista. Features include - high detection rates for viruses and spyware; automatic downloads of regularly updated Virus Database, Standalone virus scanner. It does not include an on-access real-time scanner. It can be downloaded from <http://www.calmwin.com/>
- 7. Comodo Antivirus** - has all the functionality of a paid AV without the price – Features includes- Detects and remove viruses from computers and networks. On Access Scanning conducts a real-time, scheduled virus scan. Host Intrusion Detection allows you to Intercept viruses, spyware, and other malware before they infect your computer.Get updates of the latest virus definitions everyday so you can stay protected against the latest threats. It can be downloaded from <http://antivirus.comodo.com/>
- 8. Moon Secure Antivirus** - Aims to be the best Free Antivirus for Windows under GPL license. It offers multiple scan engines, Net shield, Firewall, On access, on Exec scanner and rootkits preventions plus features from Commercial Antivirus applications. It can be downloaded from <http://sourceforge.net/projects/moonav/>
- 9. PCTools Antivirus**- with PC Tools AntiVirus Free Edition you are protected against the most nefarious cyber-threats attempting to gain access to your PC and personal information. It protects you from Virus, worm, Trojan and has Smart Updates, IntelliGuard Protection, file guard and email guard. It can be downloaded from <http://www.pctools.com/free-antivirus/>
- 10. Rising Antivirus** – Rising Antivirus Free Edition is a solution with no cost to personal users for the life of the product while still provides the same level of detection and protection capability as RISING Antivirus . It protects your computers against all types of viruses, Trojans, worms, rootkits and other malicious programs. Ease of use and Smartupdate technology make it an "install and forget" product and entitles you to focus on your own jobs with your computer. It can be downloaded from <http://www.freerav.com/>
- 11. Threatfire Lite** – Provides Comprehensive protection against viruses, worms, Trojans, spyware, rootkits, keyloggers & buffer overflows. And have Real-time behavior-based malware detection, malware quarantine & removal, etc. It can be downloaded from <http://www.threatfire.com/download/>

## **ACTIVITY**

1. Compare the feature of some of the popular free antivirus.
2. What is the difference between free antivirus and paid antivirus? Is it safe to use free antivirus in your machine?
3. Use the guidelines to for generating secure passwords and evaluate whether your current passwords can be considered as safe or unsafe passwords.
4. Based on the above guidelines, change your unsafe passwords to safe ones.
5. Find out some popular password managers and evaluate them based on their characteristics'.
6. Based on the above comparison, choose one of the best password managers for yourself.
7. Create two step verification for your Gmail account.
8. Find out how many sites, other than Gmail provide two steps verification.

## **RECOMENDED VIDEOS**

<https://www.youtube.com/watch?v=WprjZyY8ZuY>

<https://www.youtube.com/watch?v=mYhJyVKjai4>

<https://www.youtube.com/watch?v=MFyPg2Flf8s>

<https://www.youtube.com/watch?v=iNWUtj9qhPo>

<https://www.youtube.com/watch?v=A9O0zYv-5d0>

[https://www.youtube.com/watch?v=cdRbvO\\_MXh4](https://www.youtube.com/watch?v=cdRbvO_MXh4)

[https://youtu.be/Xhmae4\\_fG2o](https://youtu.be/Xhmae4_fG2o)

<https://youtu.be/COU5T-Wafa4>

<https://youtu.be/cUH3tQbGj4A>

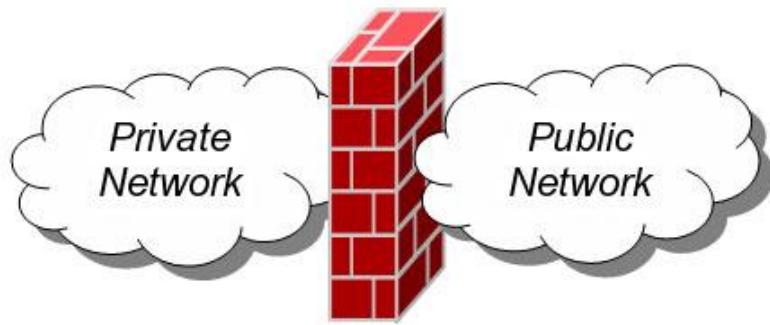
<https://youtu.be/hYyWgPXfx9U>

Configuring Firewall in your computer

## 7.1 CONFIGURING FIREWALL ON MAC COMPUTER<sup>15</sup>

Every Mac ships with a built-in firewall - a service that can be configured to disallow information from entering your Mac. But what is a firewall, and why do you need to use it on your Mac?

Every time you request information from the Internet, such as a web page or email message, your Mac sends data packets to request the information. Servers receive the packets, and then send other packets back to your Mac. This all happens in a matter of seconds. Once your Mac has reassembled the packets, you'll see something, like an email message or web page.



*Figure 31: Firewall*

A firewall can help prevent bad packets from entering your Mac. Hackers love to run automated applications that can scan thousands of computers (including your Mac) for open ports that can be exploited. To ensure that random individuals do not gain unauthorized access to your Mac, you should enable Mac OS X's built-in firewall. It will close your Mac's open ports and disallow random network scans.

### 7.1.1 Turning on and Configuring the Mac OS X Firewall

Here's how to turn on and configure your Mac's built-in firewall:

1. From the Apple menu, select **System Preferences**. The window shown below appears.

---

<sup>15</sup> Content and image courtesy(figure 31 to 35): <http://www.macinstruct.com/node/165> available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License



Figure 32: System preference dashboard

2. Select **Security & Privacy**.
3. Click the **Firewall** tab.
4. Click the lock icon and authenticate with your administrator username and password.

The window shown below appears.

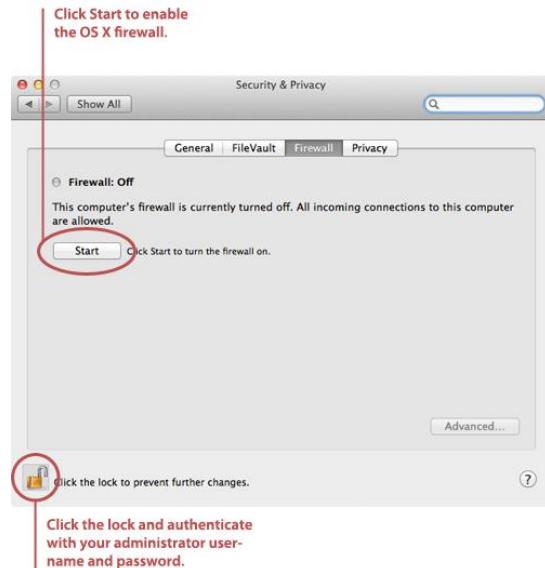


Figure 33: Security and privacy dashboard

5. Click **Start**. The firewall turns on - you'll know it's enabled when you see the green light and the **Firewall: On** message, as shown below.



Figure 34: Turning on firewall

6. Click **Advanced**. The window shown below appears.

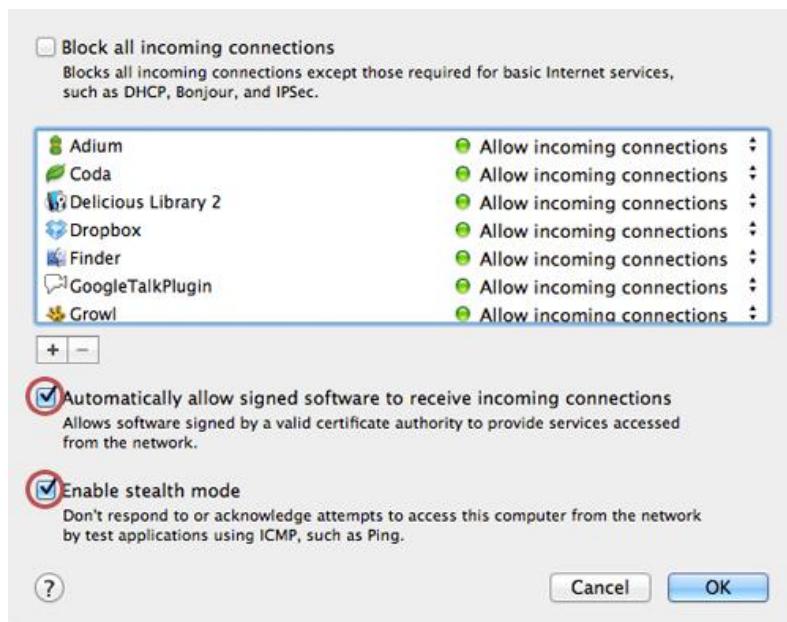


Figure 35: Configuring firewall

7. Select the **Automatically allow signed software to receive incoming connections** checkbox. This allows the applications on your Mac to communicate with the outside world.
8. Select the **Enable stealth mode** checkbox. This prevents your Mac from responding to port scans and ping requests.
9. Click **OK** to close the *Advanced* settings.
10. Close System Preferences. Your Mac is now protected by the built-in firewall!

## 7.2 WORKING WITH WINDOWS FIREWALL IN WINDOWS7<sup>16</sup>

### 7.2.1 Firewall in Windows 7

Windows 7 comes with two firewalls that work together. One is the **Windows Firewall**, and the other is **Windows Firewall with Advanced Security (WFAS)**. The main difference between them is the complexity of the rules configuration. Windows Firewall uses simple rules that directly relate to a program or a service. The rules in WFAS can be configured based on protocols, ports, addresses and authentication. By default, both firewalls come with predefined set of rules that allow us to utilize network resources. This includes things like browsing the web, receiving e-mails, etc. Other standard firewall exceptions are File and Printer Sharing, Network Discovery, Performance Logs and Alerts, Remote Administration, Windows Remote Management, Remote Assistance, Remote Desktop, Windows Media Player, Windows Media Player Network Sharing Service.

With firewall in Windows 7 we can configure inbound and outbound rules. By default, all outbound traffic is allowed, and inbound responses to that traffic are also allowed. Inbound traffic initiated from external sources is automatically blocked.

Sometimes we will see a notification about a blocked program which is trying to access network resources. In that case we will be able to add an exception to our firewall in order to allow traffic from the program in the future.

Windows 7 comes with some new features when it comes to firewall. For example, "full-stealth" feature blocks other computers from performing operating system fingerprinting. OS fingerprinting is a malicious technique used to determine the operating system running on the host machine. Another feature is "boot-time filtering". This feature ensures that the firewall is working at the same time when the network interface becomes active, which was not the case in previous versions of Windows.

When we first connect to some network, we are prompted to select a network location. This feature is known as Network Location Awareness (NLA). This feature enables us to assign a network profile to the connection based on the location. Different network profiles contain different collections of firewall rules. In Windows 7, different network profiles can be

---

<sup>16</sup> Contents and image courtesy( Figure 31 o 43):<http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security> available under Creative Commons Attribution-Noncommercial-Share Alike 4.0 International.

configured on different interfaces. For example, our wired interface can have different profile than our wireless interface. There are three different network profiles available:

- Public
- Home/Work - private network
- Domain - used within a domain

We choose those locations when we connect to a network. We can always change the location in the Network and Sharing Center, in Control Panel. The Domain profile can be automatically assigned by the NLA service when we log on to an Active Directory domain. Note that we must have administrative rights in order to configure firewall in Windows 7.

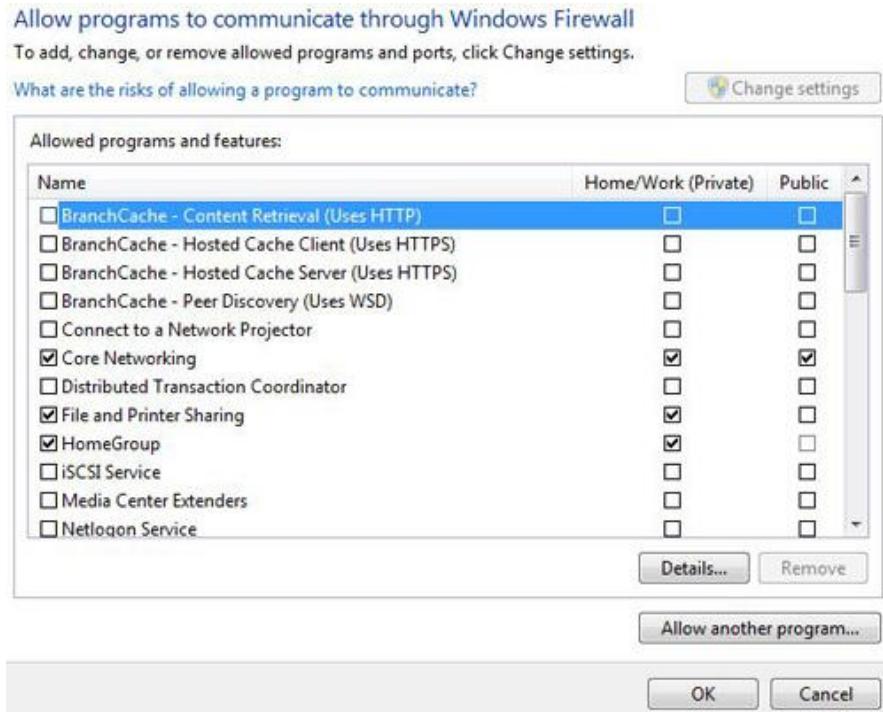
### 7.2.2 Configuring Windows Firewall

To open Windows Firewall we can go to **Start > Control Panel > Windows Firewall**.



Figure 36: Control panel dashboard on Windows machine

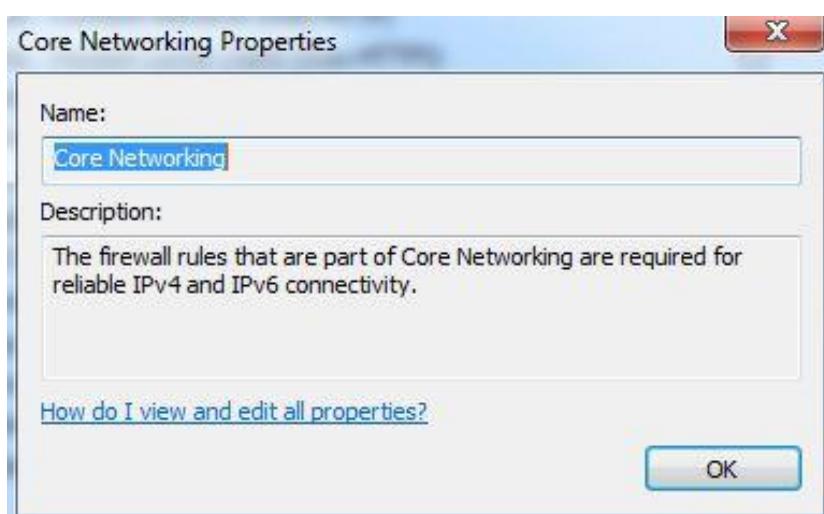
By default, Windows Firewall is enabled for both private (home or work) and public networks. It is also configured to block all connections to programs that are not on the list of allowed programs. To configure exceptions we can go to the menu on the left and select "Allow a program or feature through Windows Firewall" option.



*Figure 37: Configuring firewall setting*

### Exceptions

To change settings in this window we have to click the "Change settings" button. As you can see, here we have a list of predefined programs and features that can be allowed to communicate on private or public networks. For example, notice that the Core Networking feature is allowed on both private and public networks, while the File and Printer Sharing is only allowed on private networks. We can also see the details of the items in the list by selecting it and then clicking the Details button.



*Figure 38: Setting exceptions*

## Details

If we have a program on our computer that is not in this list, we can manually add it by clicking on the "Allow another program" button.



Figure 39: Selecting programs not present in the list

## Add a Program

Here we have to browse to the executable of our program and then click the Add button. Notice that we can also choose location types on which this program will be allowed to communicate by clicking on the "Network location types" button.



Figure 40: Adding a program

## Network Locations

Many applications will automatically configure proper exceptions in Windows Firewall when we run them. For example, if we enable streaming from Media Player, it will automatically configure firewall settings to allow streaming. The same thing is if we enable Remote Desktop feature from the system properties window. By enabling Remote Desktop feature we actually create an exception in Windows Firewall.

Windows Firewall can be turned off completely. To do that we can select the "Turn Windows Firewall on or off" option from the menu on the left.

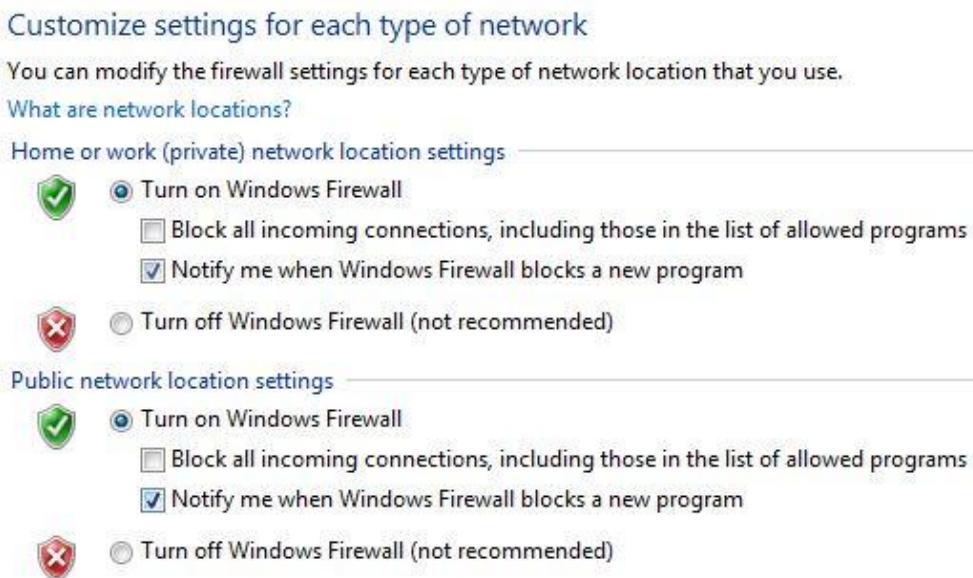


Figure 41: Customize settings

## Firewall Customization

Note that we can modify settings for each type of network location (private or public). Interesting thing here is that we can block all incoming connections, including those in the list of allowed programs.

Windows Firewall is actually a Windows service. As you know, services can be stopped and started. If the Windows Firewall service is stopped, the Windows Firewall will not work.

Windows Firewall	This service ...	Started	Automatic
Windows Event Log	This service ...	Started	Automatic
Windows Firewall	Windows Fi...	Started	Automatic
Windows Font Cache S...	Optimizes p...	Started	Automatic (D...
Windows Image Acquisi...	Provides im...		Manual

Figure 42: Enabling firewall from Windows services

## Firewall Service

In our case the service is running. If we stop it, we will get a warning that we should turn on our Windows Firewall.



Figure 43: Firewall notification

### Warning

Remember that with Windows Firewall we can only configure basic firewall settings, and this is enough for most day-to-day users. However, we can't configure exceptions based on ports in Windows Firewall any more. For that we have to use Windows Firewall with Advanced Security, which will be covered in next section.

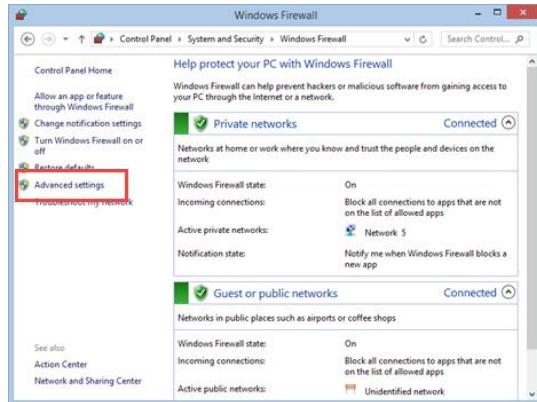
## 7.2.3 How to Start & Use the Windows Firewall with Advanced Security<sup>17</sup>

The *Windows Firewall with Advanced Security* is a tool which gives you detailed control over the rules that are applied by the *Windows Firewall*. You can view all the rules that are used by the *Windows Firewall*, change their properties, create new rules or disable existing ones. In this tutorial we will share how to open the *Windows Firewall with Advanced Security*, how to find your way around it and talk about the types of rules that are available and what kind of traffic they filter.

### 7.2.3.1 How to Access the Windows Firewall with Advanced Security

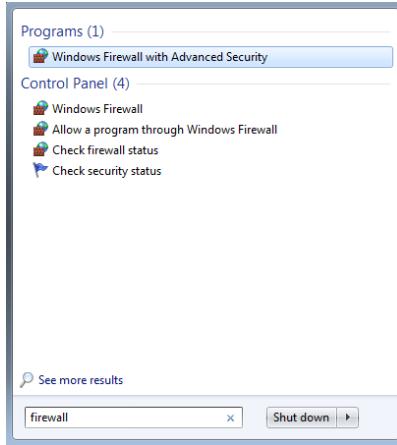
You have several alternatives to opening the *Windows Firewall with Advanced Security*:

One is to open the standard Windows Firewall window, by going to "*Control Panel -> System and Security -> Windows Firewall*". Then, click or tap *Advanced settings*.



<sup>17</sup> <http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security>

In Windows 7, another method is to search for the word *firewall* in the *Start Menu* search box and click the "*Windows Firewall with Advanced Security*" result.



In Windows 8.1, *Windows Firewall with Advanced Security* is not returned in search results and you need to use the first method shared above for opening it.

The *Windows Firewall with Advanced Security* looks and works the same both in Windows 7 and Windows 8.1. To continue our tutorial, we will use screenshots that were made in Windows 8.1.



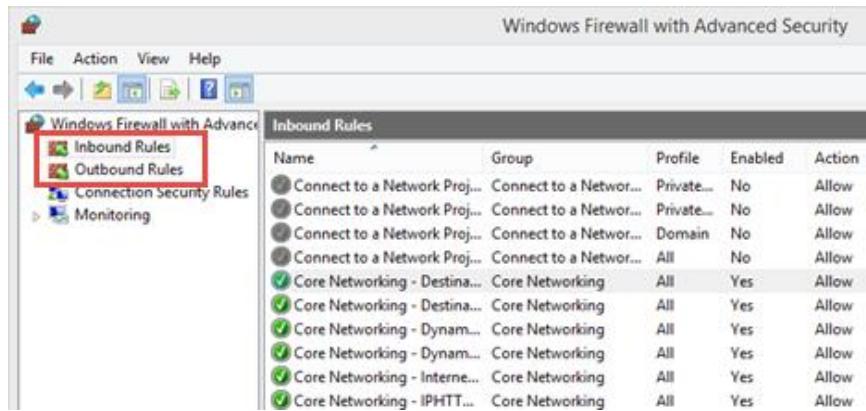
### 7.2.3.2 What Are The Inbound & Outbound Rules?

In order to provide the security you need, the *Windows Firewall* has a standard set of inbound and outbound rules, which are enabled depending on the location of the network you are

connected to. Inbound rules are applied to the traffic that is coming from the network and the Internet to your computer or device. Outbound rules apply to the traffic from your computer to the network or the Internet.

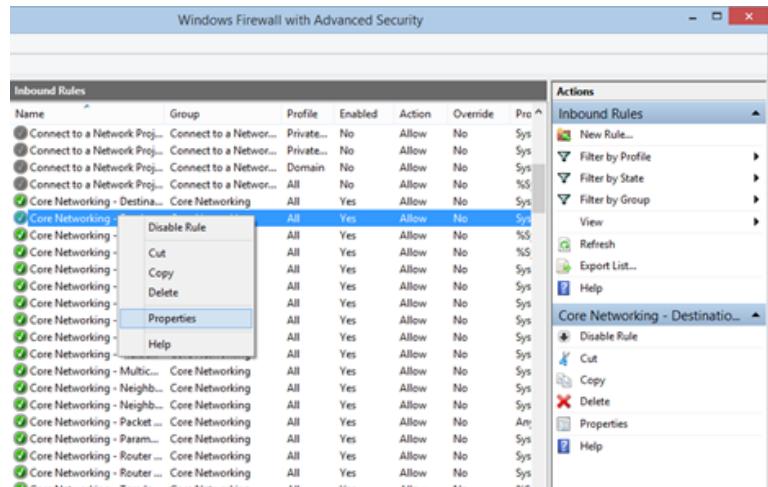
These rules can be configured so that they are specific to: computers, users, programs, services, ports or protocols. You can also specify to which type of network adapter (e.g. wireless, cable, virtual private network) or user profile it is applied to.

In the *Windows Firewall with Advanced Security*, you can access all rules and edit their properties. All you have to do is click or tap the appropriate section in the left-side panel.

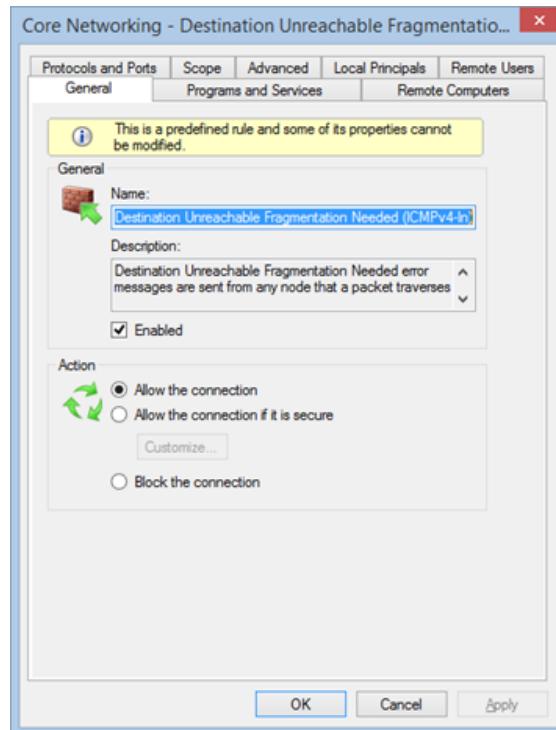


The rules used by the *Windows Firewall* can be enabled or disabled. The ones which are enabled or active are marked with a green check-box in the *Name* column. The ones that are disabled are marked with a gray check-box.

If you want to know more about a specific rule and learn its properties, right click on it and select *Properties* or select it and press *Properties* in the column on right, which lists the actions that are available for your selection.



In the *Properties* window, you will find complete information about the selected rule, what it does and in when it is applied. You will also be able to edit its properties and change any of the available parameters.

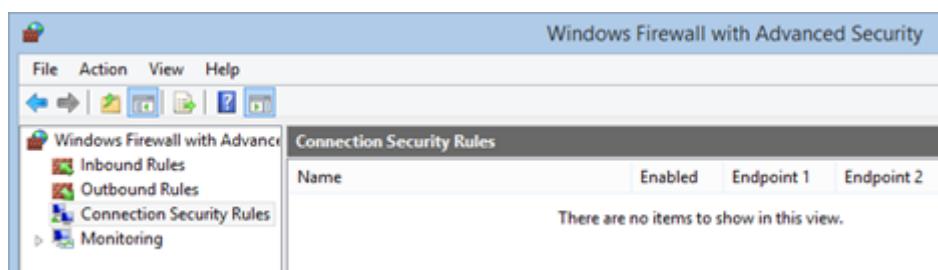


#### 7.2.3.3 What Are The Connection Security Rules?

Connection security rules are used to secure traffic between two computers while it crosses the network. One example would be a rule which defines that connections between two specific computers must be encrypted.

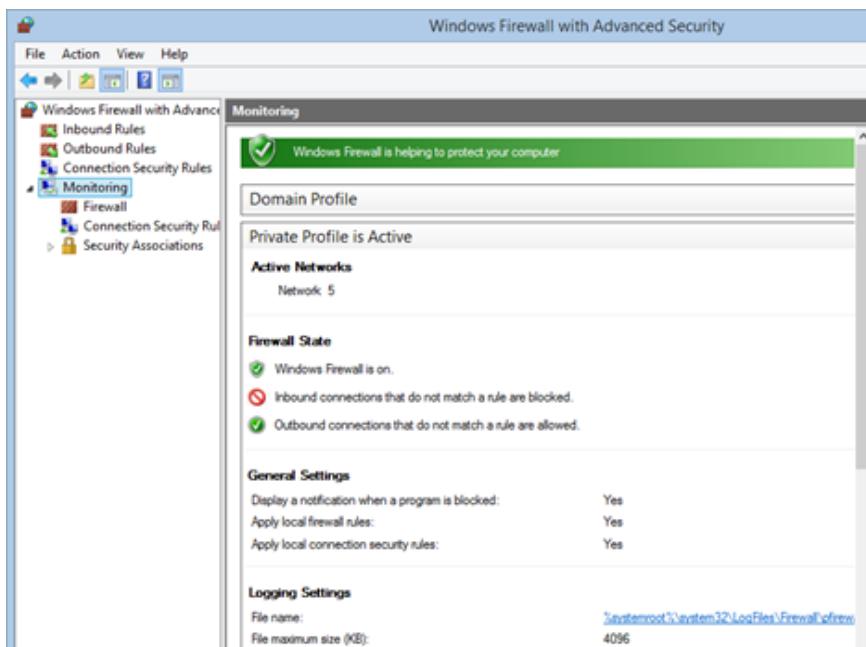
Unlike the inbound or outbound rules, which are applied only to one computer, connection security rules require that both computers have the same rules defined and enabled.

If you want to see if there are any such rules on your computer, click or tap "*Connection Security Rules*" on the panel on the left. By default, there are no such rules defined on Windows computers and devices. They are generally used in business environments and such rules are set by the network administrator.



#### **7.2.3.4 What Does the Windows Firewall with Advanced Security Monitor?**

The *Windows Firewall with Advanced Security* includes some monitoring features as well. In the *Monitoring* section you can find the following information: the firewall rules that are active (both inbound and outbound), the connection security rules that are active and whether there are any active security associations.



You should note that the *Monitoring* section shows only the active rules for the current network location. If there are rules which get enabled for other network locations, you will not see them in this section.

The above section discussed on how to setup a firewall on two Operating Systems viz. Windows and Mac. Linux have many variants therefore it is not possible to discuss how to configure firewall on Linux. There are some links in the Recommended Videos section which discuss the procedure of setting up firewall in various variant of Linux.

#### **Activity**

1. Setup and configure a firewall in your system.
2. Find some some of the free and commercially available firewalls over internet.

#### **RECOMENDED VIDEOS**

<https://www.youtube.com/watch?v=krbivwp4t3U>

<https://www.youtube.com/watch?v=H0g8xJMnT68>

**For linux**

<https://www.youtube.com/watch?v=hkzHtEnFZpc>

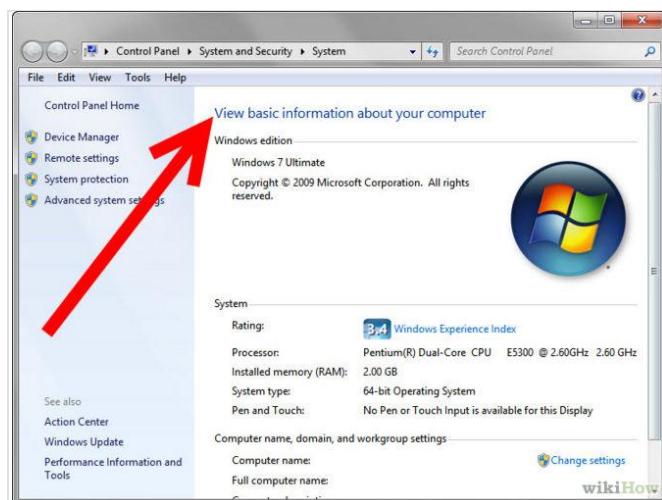
[https://www.youtube.com/watch?v=o0a09CQi\\_48](https://www.youtube.com/watch?v=o0a09CQi_48)

<https://www.youtube.com/watch?v=wbzP2-qvc4o>

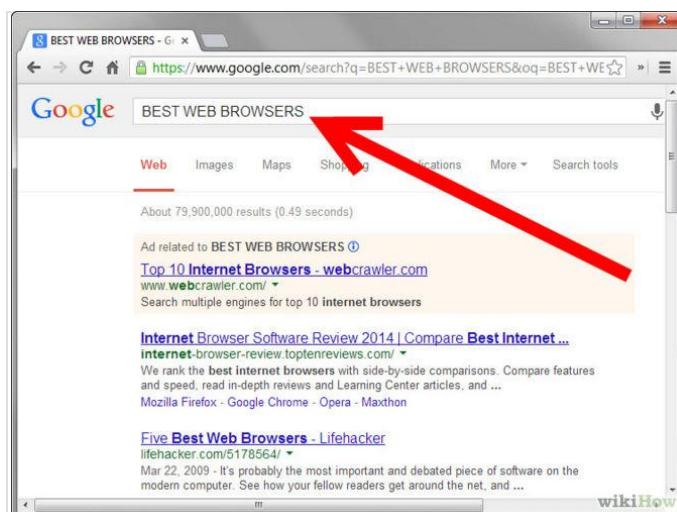
# CHOOSING BEST BROWSER TO SUIT YOUR REQUIREMENTS

## 8.1 FINDING THE BEST BROWSER ACCORDING TO THE USERS REQUIREMENT<sup>18</sup>

Browsers are the key to the Internet these days, at least for most tasks. There are many, many browsers for every platform and operating system, so the choice can be tough. However, this should help narrow the search.

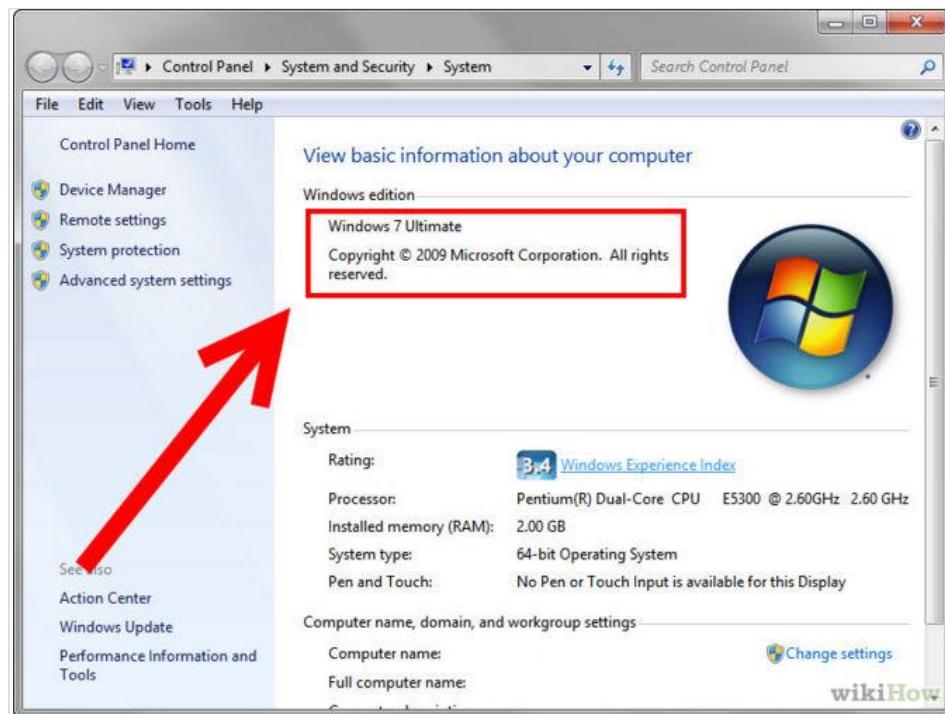


**Step 1:** Determine the age of your computer. How old is your computer? Is it a mobile device? Know your systems specifications as this may be more suited to some browsers than others.

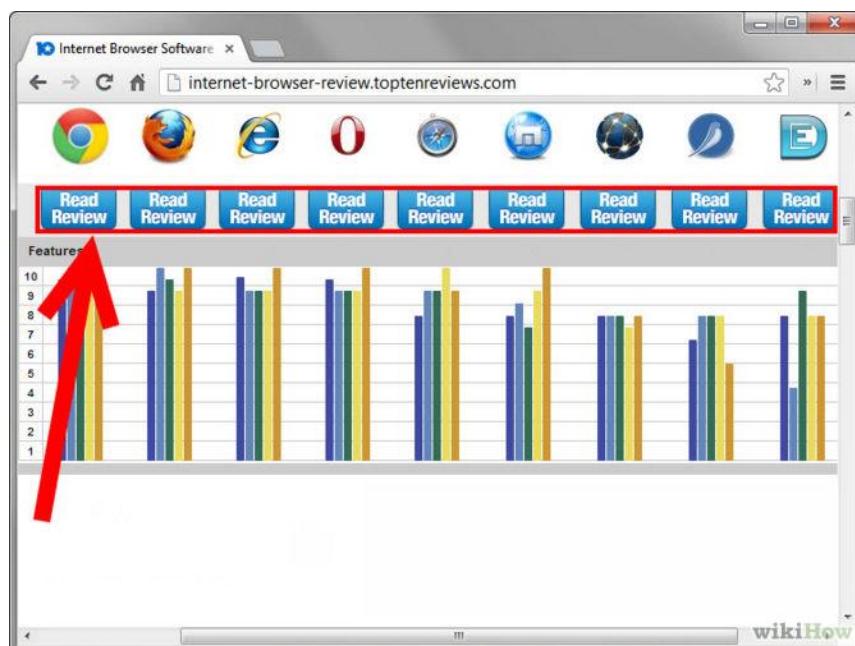


<sup>18</sup> <http://www.wikihow.com/Choose-an-Internet-Browser>

**Step 2:** Think about your ideal browser; what would it be able to do? You may want it to be quite simple, handling only the bare necessities. You may want some basic features like web feed reading, bookmarking (favorites), or search boxes. Some browsers have a lot more, and that's where it starts to get confusing.



**Step 3:** Make sure you know what platform you are on. Some browsers are only available to a certain operating system, or not available to one operating system.



**Step 4:** Research browsers. Tabbed browsers include Safari (runs on OS X, iPhone and is new to Windows), Firefox (general purpose with the most plug-ins), Opera(supports torrents, handles e-mail and runs on mobile devices), Konqueror (dual purpose file manager), Seamonkey (includes HTML editor and e-mail client), Off By One (tiny) and Flock (social networking).

The screenshot shows a comparison chart of different web browsers across various metrics. A red arrow points to the 'Features' section of the chart.

	Google Chrome	Firefox	Internet Explorer	Opera	Konqueror	Flock	Seamonkey
<b>Speed</b>							
Initial Startup Time	4	6.3	4.3	5.1	4.2	8	9
Average Startup Time	4.3	6.3	4	4.4	3.7	6.9	4
Navigation Time	4.4	6.7	4.5	4.6	3.8	3.2	11
<b>Features</b>							
Tabbed Browsing	✓	✓	✓	✓	✓	✓	✓
Add-ons	✓	✓	✓	✓	✓	✓	✓
Integrated Search Engine	✓	✓	✓	✓	✓	✓	✓
Save Tabs	✓	✓	✓	✓	✓	✓	✓
Customization Options	✓	✓	✓	✓	✓	✓	✓
Bookmarks	✓	✓	✓	✓	✓	✓	✓
RSS Feeds	✓	✓	✓	✓	✓	✓	✓
Zoom	✓	✓	✓	✓	✓	✓	✓
Find-On Page Function	✓	✓	✓	✓	✓	✓	✓
Password Manager	✓	✓	✓	✓	✓	✓	✓
Autofill	✓	✓	✓	✓	✓	✓	✓
Automatic Updates	✓	✓	✓	✓	✓	✓	✓

**Step 5:** See the features of all browsers you have found, and compare with what you want.

The screenshot shows the homepage of the Off By One Web Browser. A red arrow points to the top banner.

**Off By One** Yes, Another Free Web Browser

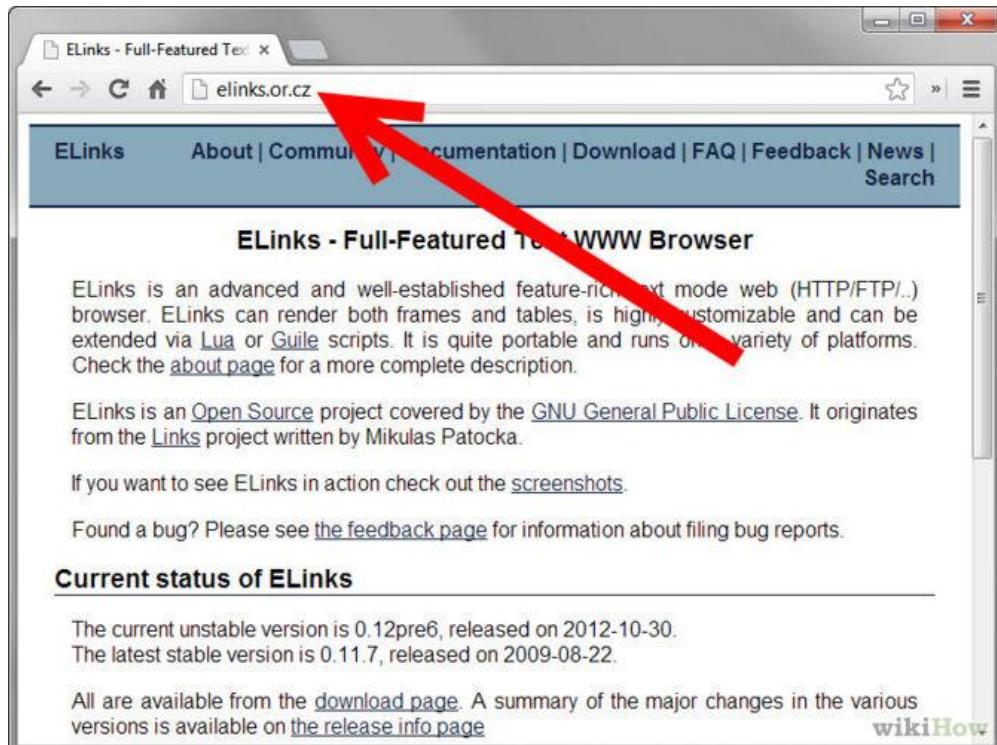
**The Browser Has Landed**  
The **Off By One Web Browser** may be the world's smallest and fastest web browser with full HTML 3.2 support. It is a completely self-contained, stand-alone 1.2 MB application with no dependencies on any other browser or browser component. For Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000 and Windows XP.

**New!** Now, with a tabbed browsing interface.  
[Click here to download the Off By One Browser Setup kit or ZIP file package](#), posted January 2, 2006.

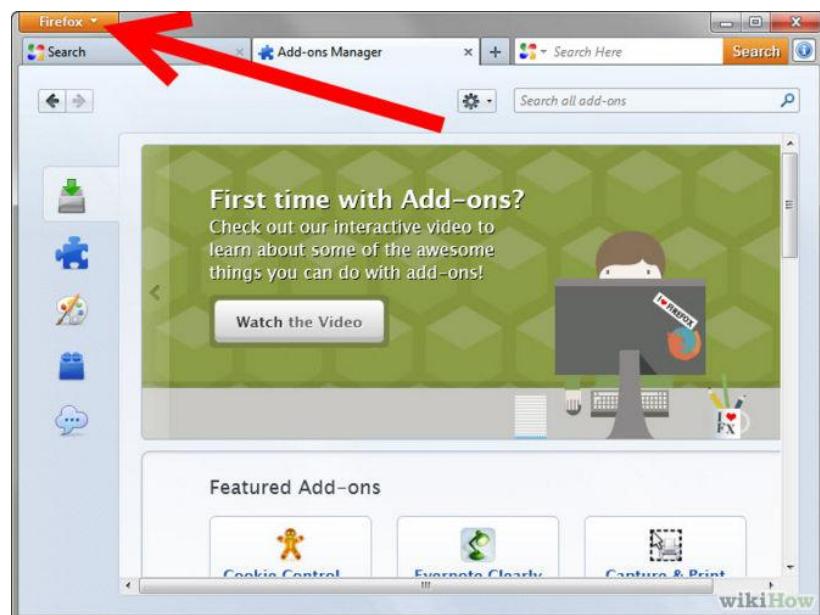
**Also available as a component for Windows developers**

The Off By One Web Browser was created to demonstrate the

**Step 6:** Consider alternative lower-memory browsers, if you have low computer memory. Consider Off by One, Dillo, SkipStone and NetSurf.



**Step 7:** Consider a text-based browser, if you want an even faster-than-fast(maximum speed/hyperdrive) experience. Consider ELinks.



**Step 8:** Find out if you can add features you may want or if there is an easy method to doing so such as an existing plugin or extension in the case of Firefox.



**Step 9:** Download and install your new browser!

### Activity

1. Compare the various browsers based on their characteristics'.

### RECOMMENDED VIDEOS:

<https://www.youtube.com/watch?v=sr7mgYD2tAc>

<https://www.youtube.com/watch?v=-jHs-RYD7gc>

<https://www.youtube.com/watch?v=gNiz4kfSZnw>

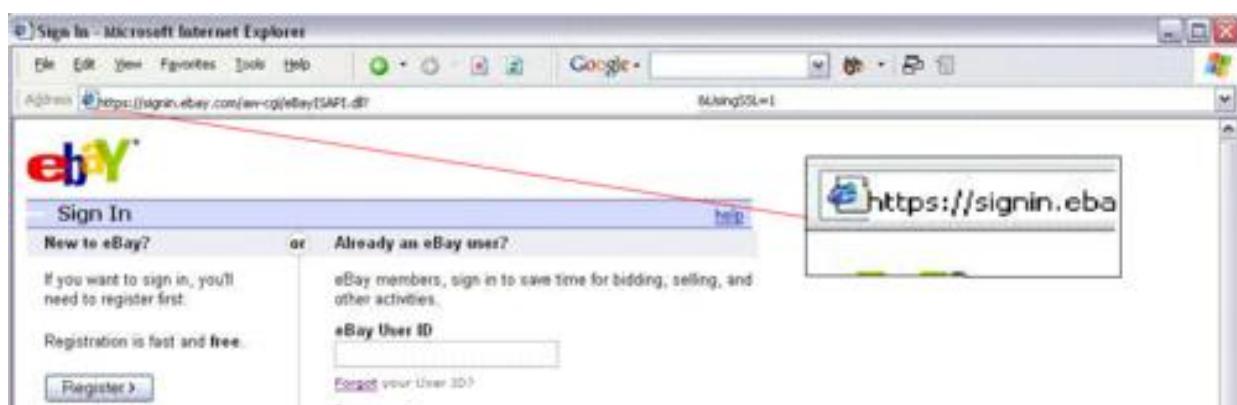
# GUIDELINES FOR SAFE INTERNET BROWSING

## 9.1 SAFE BROWSING

Internet security is a matter of great concern for internet users. It is important to **know if a website is secure** or not while surfing the internet<sup>19</sup>. A **secure website** creates a safe connection between the website and the web browser so that entered data, such as personal information, credit card details, banking information, etc, is not accessible to unauthorized entities. When the browser opens a secured connection, "https" can be seen in the URL instead of just http. To **know if a website is secure** or not, look for the locked yellow colour padlock symbol on the lower right corner of the browser window.

### 9.1.1 How do I know if a website is secure?

Some web sites use a secure connection between the web site and your browser. This may be important to you, for instance, if you want to pay online for a product or a service and have to enter credit card information or other personal information. To know if your browser is viewing a secure web site, you can look in the lower right part of the window. There is a small box in the frame of the window to the left of the area that describes which zone you are in (usually the Internet zone, with a globe icon). If you see a yellow padlock icon, the web site you are viewing is a "secure web site." If the box is empty, the web site does not have a secure connection with your browser.



<sup>19</sup> <http://ccm.net/faq/2-how-do-i-know-if-a-website-is-secure>

## **9.2 TIPS FOR BUYING ONLINE<sup>20</sup>**

Shopping online can be cheaper and more convenient for you and for businesses. However, make sure you understand your rights and the risks before you shop online or bid in an online auction.

**I. Pay securely:** Don't make any payment unless:

- You are on a secure website, and
- You can make a secure payment.

This will protect you against fraud and unauthorised credit card transactions. A secure website address will always:

- begin with 'https://', not 'http://'
- display the image of a closed padlock (usually in the bottom right corner of your browser window).

**Only make a payment if you can see both of these things.** Never give out your bank account details, credit card number or other personal details if you are not certain that the business is a reputable trader.

**II. Know the business:** Only buy from websites you know and trust. Check that the company has a physical street address and landline phone number. If the company operates from overseas, you might have trouble getting a refund or repair.

**III. Know the product:** Make sure you check whether:

- the product is legal
- the product will work in Australia
- any warranties or guarantees offered are valid in Australia
- the product has an authorised repairer nearby.

**IV. Check the contract:** Make sure you read and understand:

- the terms and conditions of sale
- the refund policy
- the delivery details
- returns and repairs policies, including any associated costs.

**V. Check the full cost:** Be aware of the full cost of your purchase. Additional costs may include:

- currency conversion
- taxes

---

<sup>20</sup> <https://www.qld.gov.au/law/your-rights/consumer-rights-complaints-and-scams/consumer-advice-rights-and-responsibilities/tips-to-become-a-smarter-shopper/tips-for-buying-online/>

- postage and delivery fees
- packaging.

It might end up being cheaper to buy the product at a local shop.

VI. **Protect your privacy:** Only buy online if you are comfortable with a business's privacy policy. Do not give out information unless they require it to complete the sale. Remember, if a deal sounds too good to be true, it probably is.

VII. **Keep records:** Always write down any reference numbers and print out copies of:

- the order form (both before and after you confirm the order)
- receipts (can come by email or in a pop-up window).

Always make sure all charges are correct by checking the receipt against your:

- credit card statement
- merchant account statement (such as PayPal)
- bank statement.

The charges may be converted from another currency.

VIII. **Online auction sites:** Most online auction sites (like eBay) offer a dispute resolution process for buyers and sellers. This should be your first step to resolve a dispute if:

- you did not receive the items you bought
- you did not receive payment for items you sold
- you received items that were significantly different from their description.

The eBay website has an example of this facility.

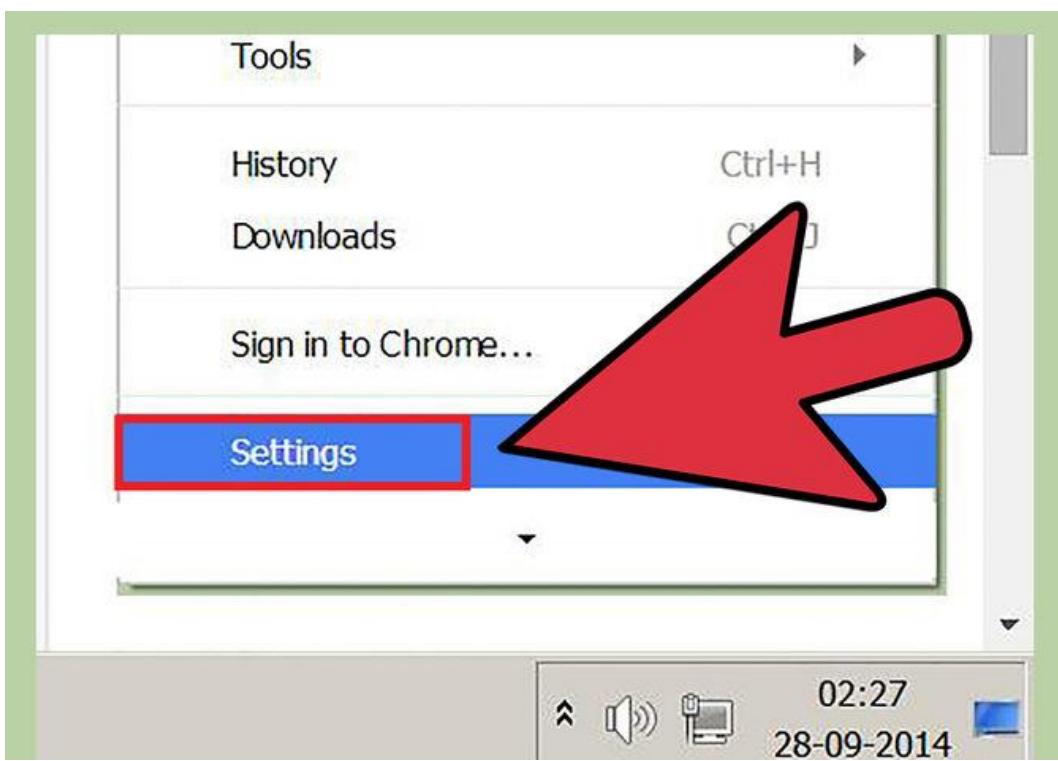
## 9.3 CLEARING CACHE FOR BROWSERS

Your internet browser's cache stores certain information (snapshots) of webpages you visit on your computer or mobile device so that they'll load more quickly upon future visits and while navigating through websites that use the same images on multiple pages so that you do not download the same image multiple times<sup>21</sup>. Occasionally, however your cache can prevent you from seeing updated content, or cause functional problems when stored content conflicts with live content. You can fix many browser problems simply by clearing your cache. This article contains instructions with screenshots on how to clear the cache for all major browsers.

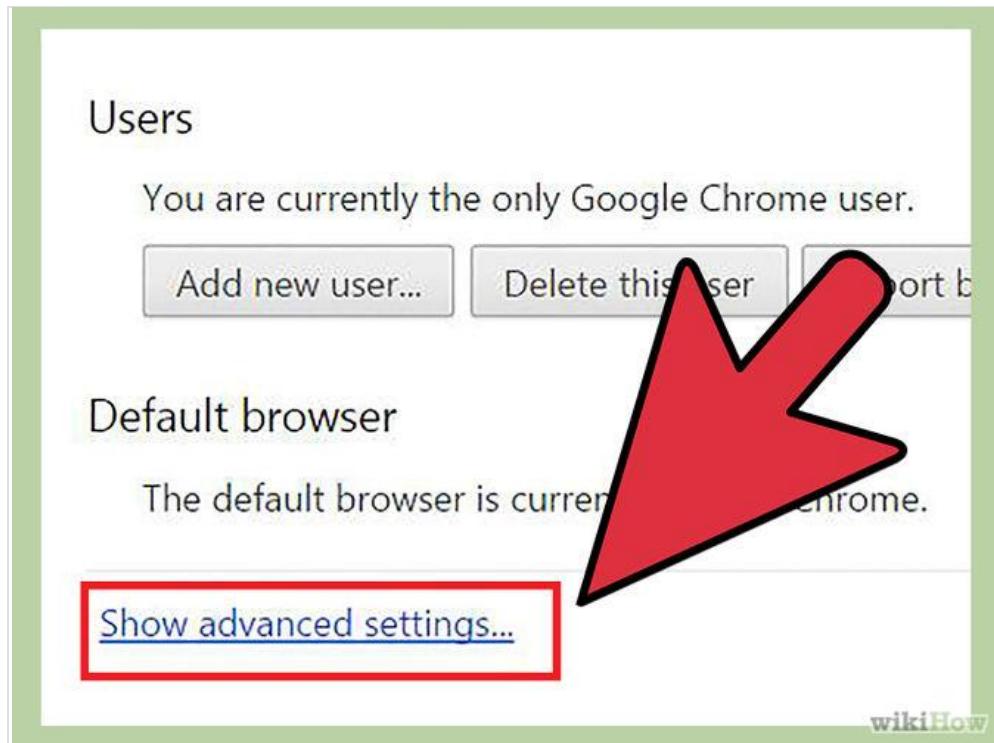
### 9.3.1 Clearing cache for Chrome Browsers above version 10

---

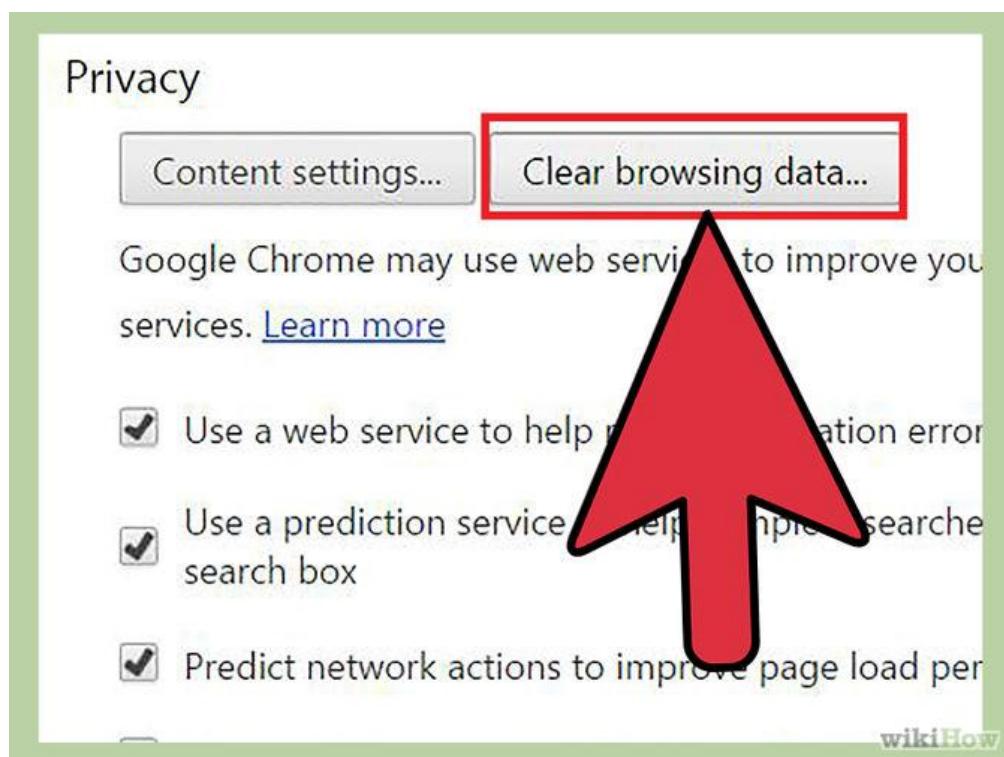
<sup>21</sup> <http://www.wikihow.com/Clear-Your-Browser%27s-Cache>



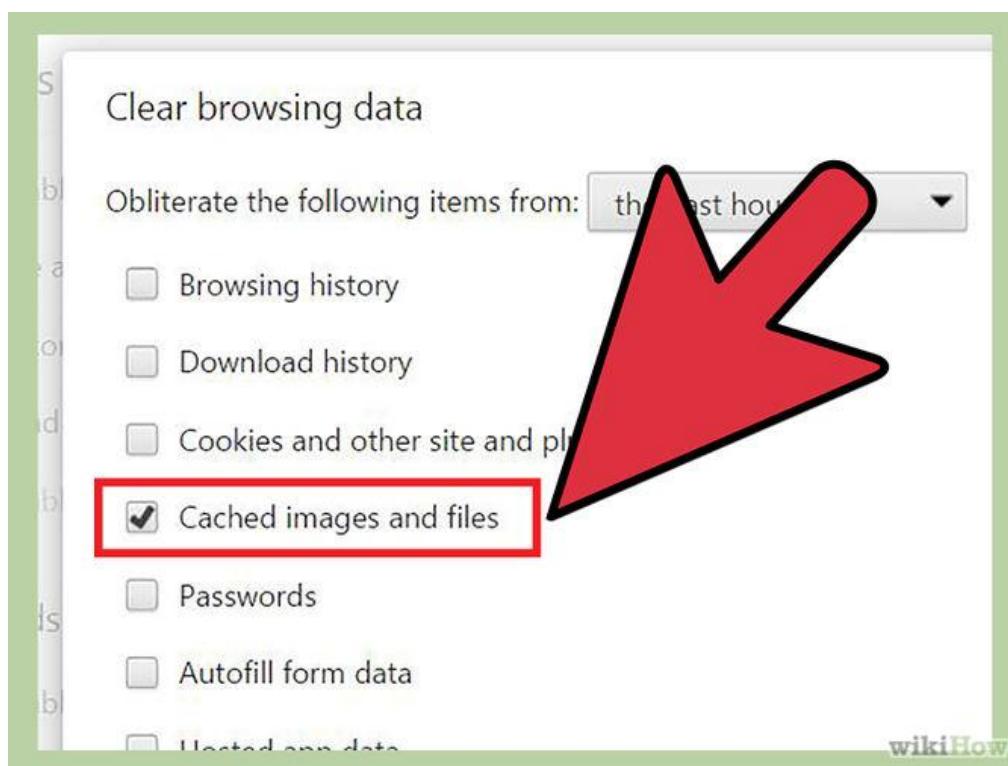
**Step 1:** Open the settings on Chrome. Click the menu icon in the upper right corner of the browser to the right. Click settings on the bottom of the menu.



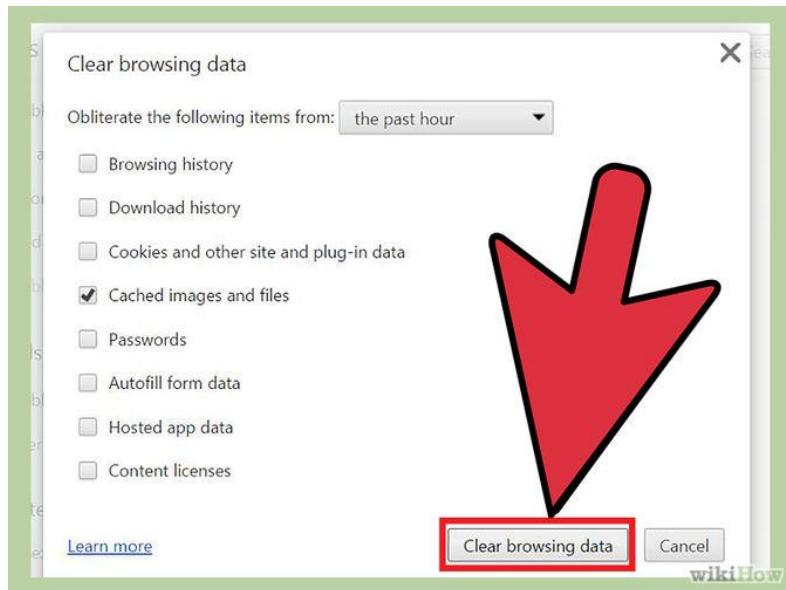
**Step 2:** From settings, click "Show advanced settings. It's located at the very bottom of the settings section.



**Step 3:** Scroll to the privacy section and click "Clear browsing data."

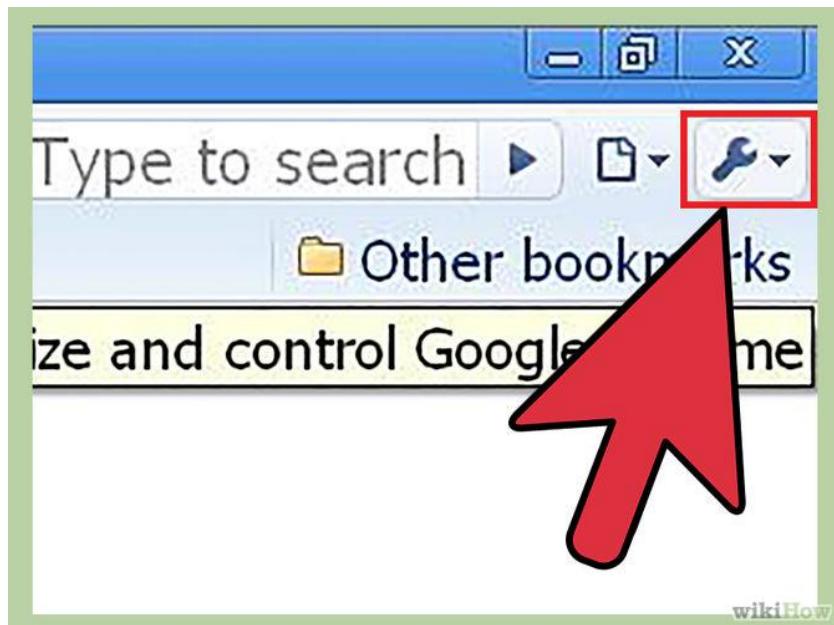


**Step 4:** Select "Cached images and files". Uncheck all other options to avoid deleting browser history, cookies and other things you may wish to retain. Change "Obliterate the following items from" to "the beginning of time".

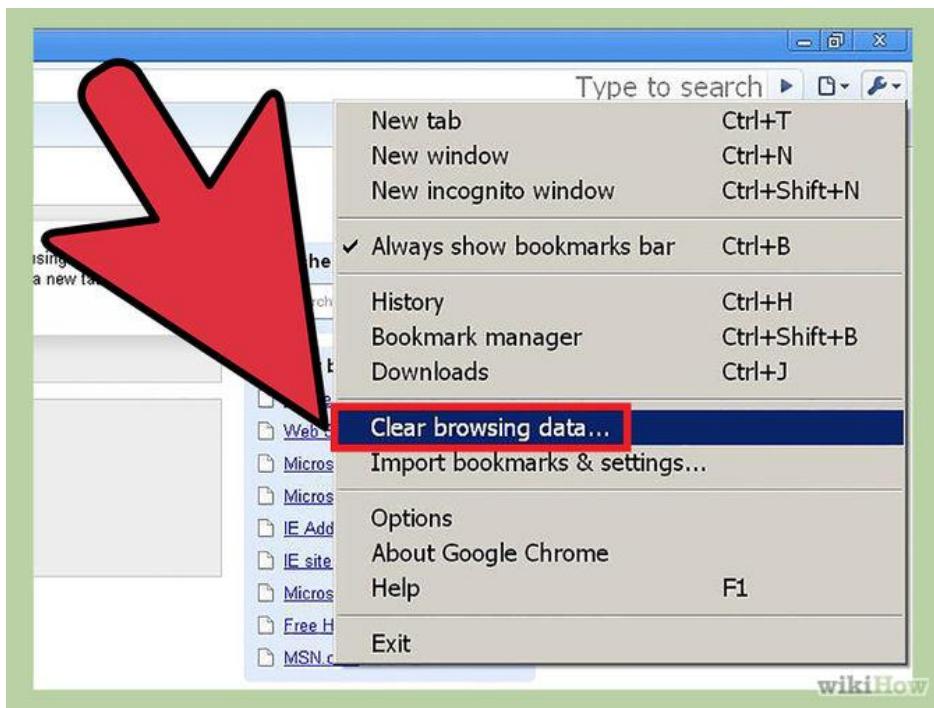


**Step 5:** Press "Clear browsing data". You are done!

### 9.3.2 Clearing cache for Chrome Browsers from version 1 to 9



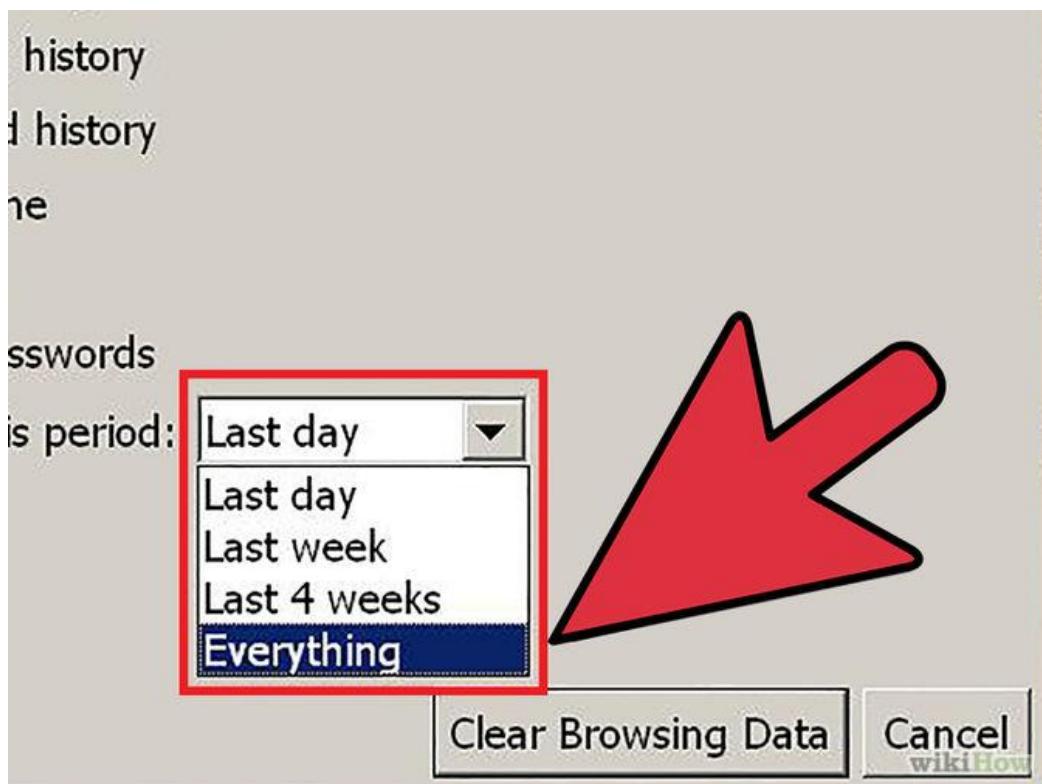
**Step 1:** Once your browser is open, select the Tools menu (the wrench in the upper-right corner) and select Options (Preferences on Mac).



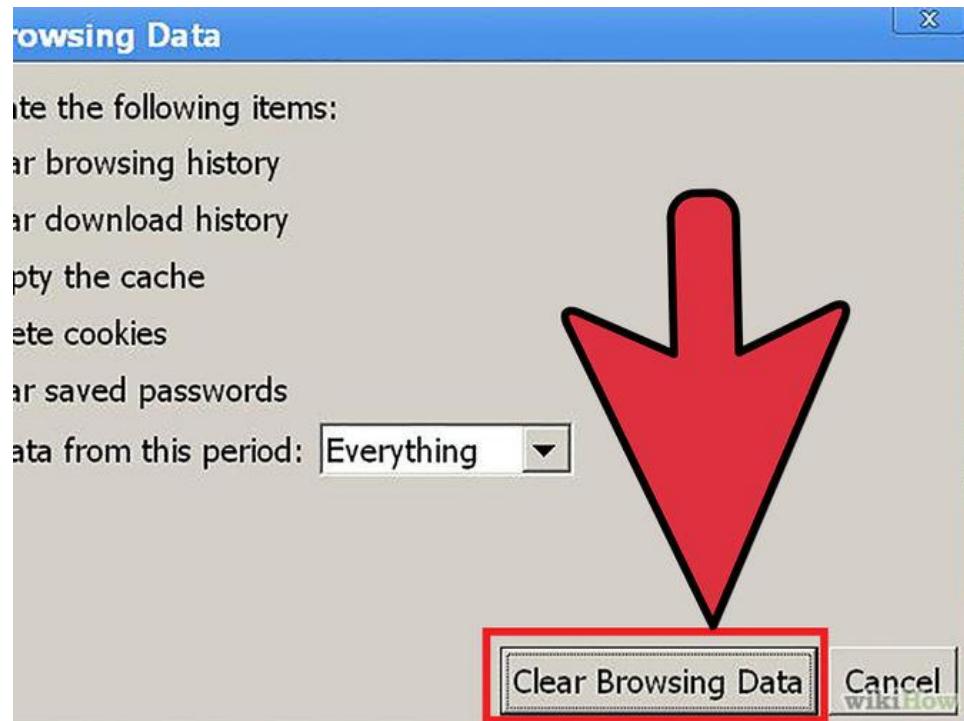
**Step 2:** On the Under the Hood tab, click the **Clear Browsing data** button.



**Step 3:** Select the **Empty the cache** check-box.



**Step 4:** You can also choose the period of time you wish to delete cached information using the Clear data from this period dropdown menu.

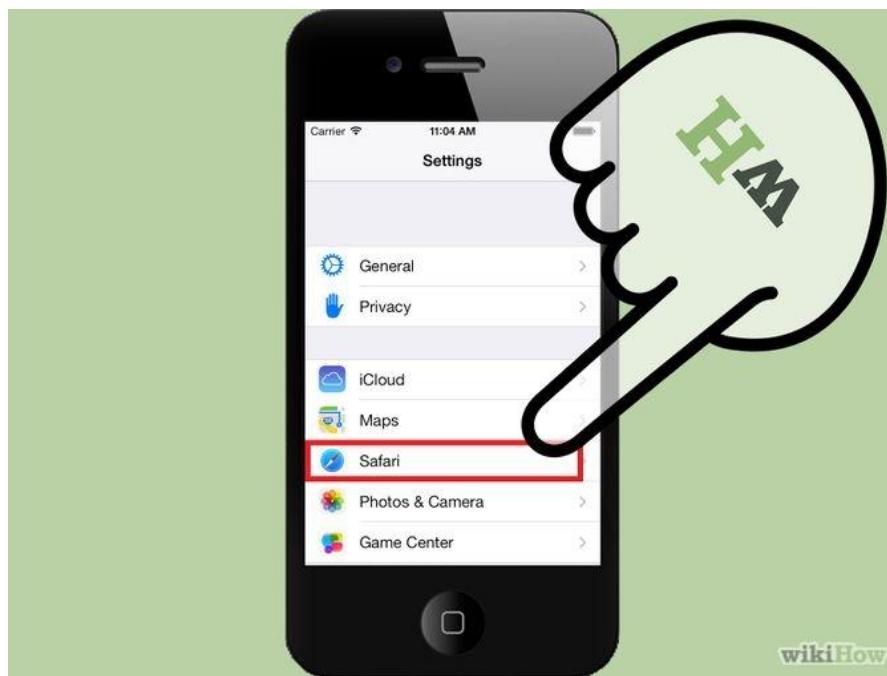


**Step 5:** Click the Clear Browsing Data button.

### 9.3.3 Clearing cache for Safari for iOS, iPhone and iPad



**Step 1:** Click on Settings from the home page.

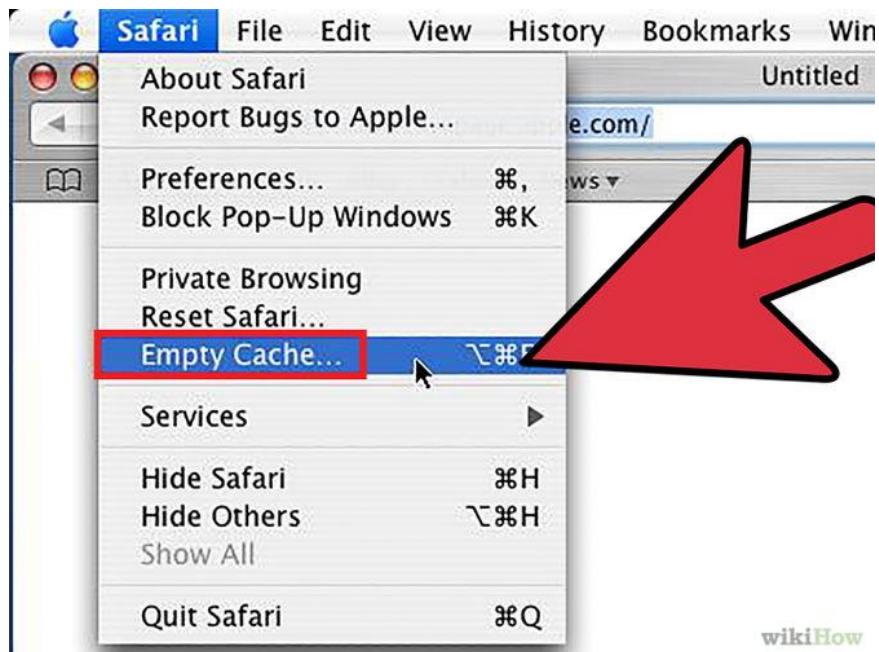


**Step 2:** Scroll down until you see "Safari." Click on it to bring up the option page.

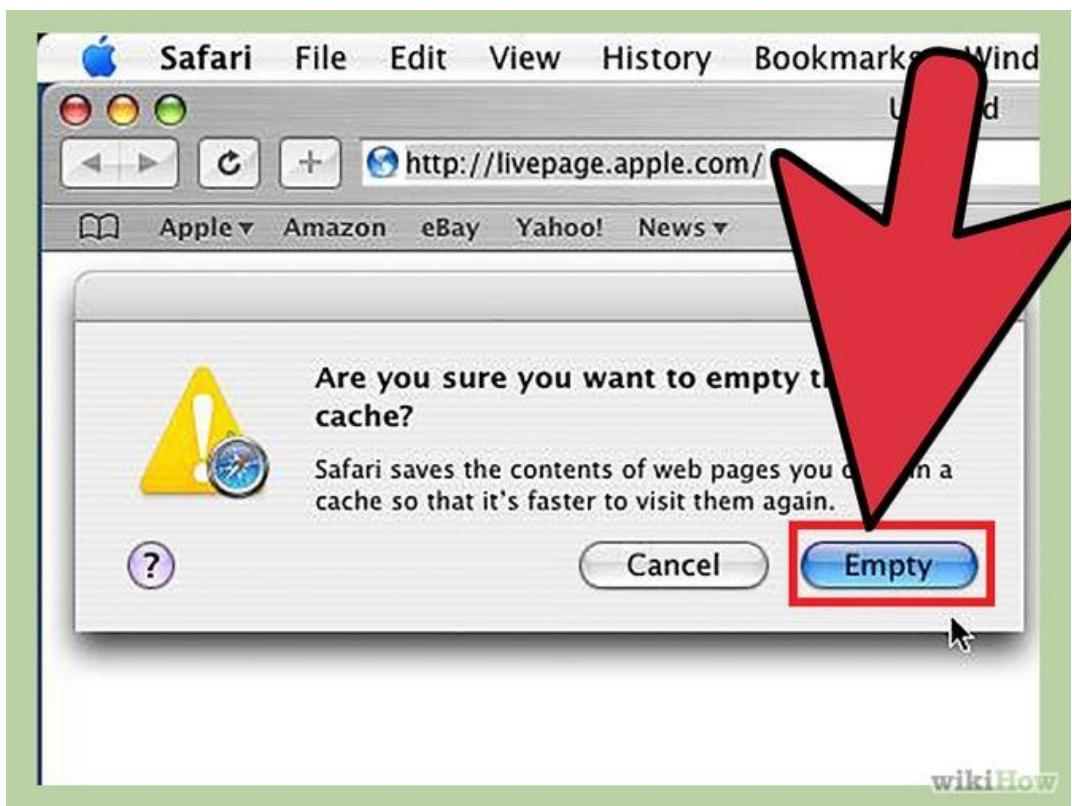


**Step 3:** Click "Clear Cookies and Data". A popup box will appear. Click "Clear Cookies and Data" again to confirm your choice.

#### 9.3.4 Clearing cache for Safari for Mac OS x

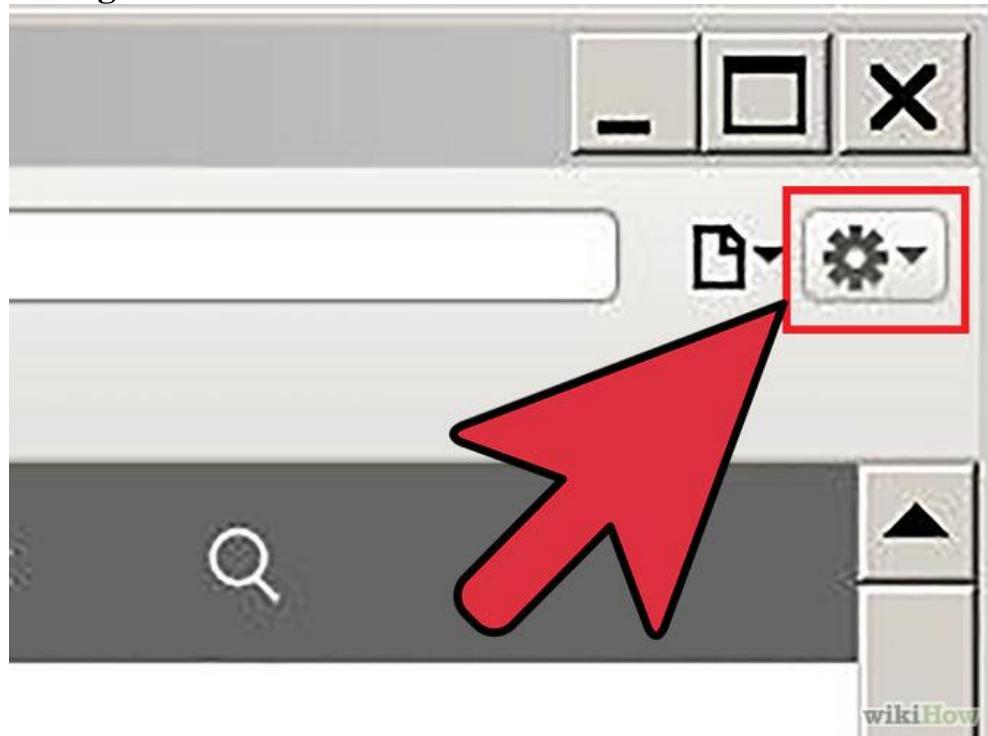


**Step 1:** Once your browser is open, click the Safari menu and select Empty Cache.

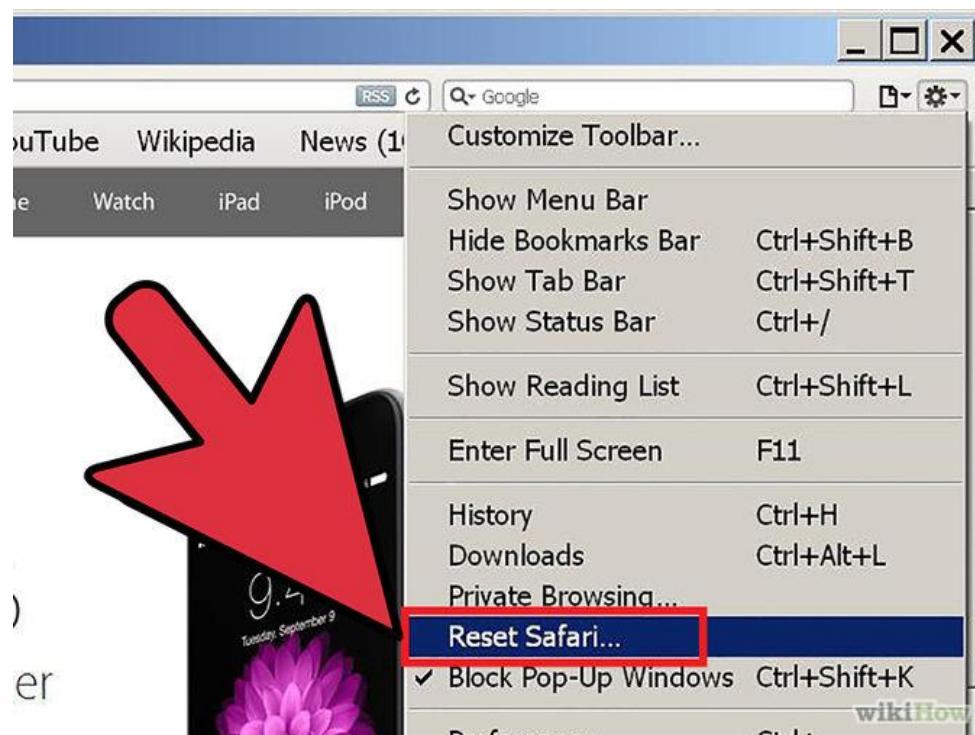


**Step 2:** Click Empty.

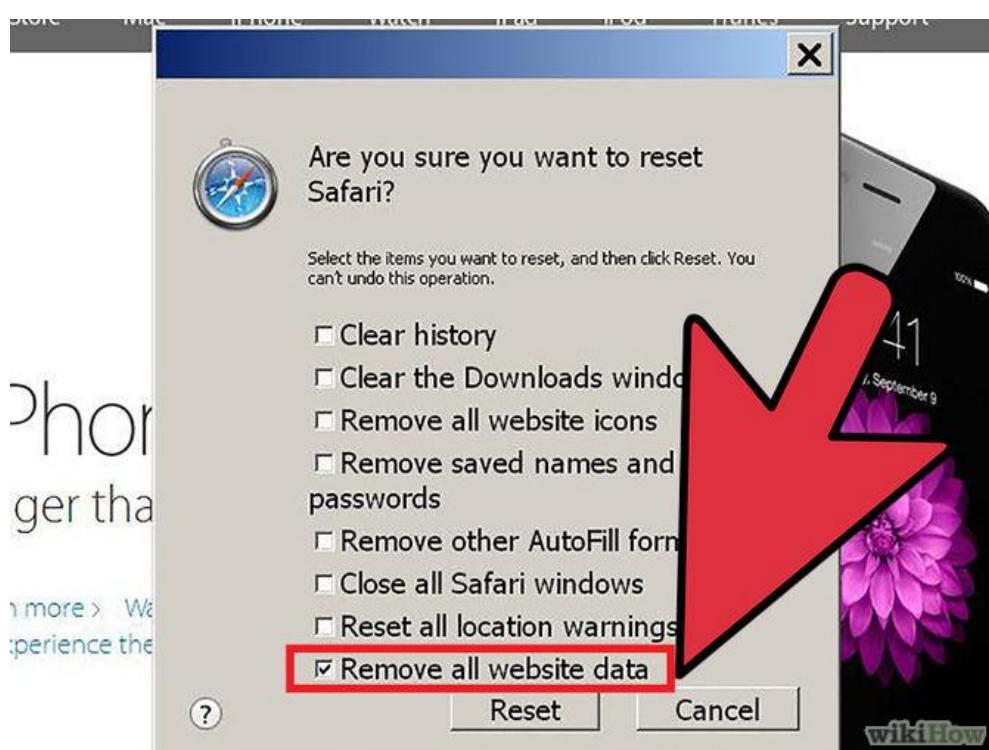
### 9.3.5 Clearing cache for Safari for windows



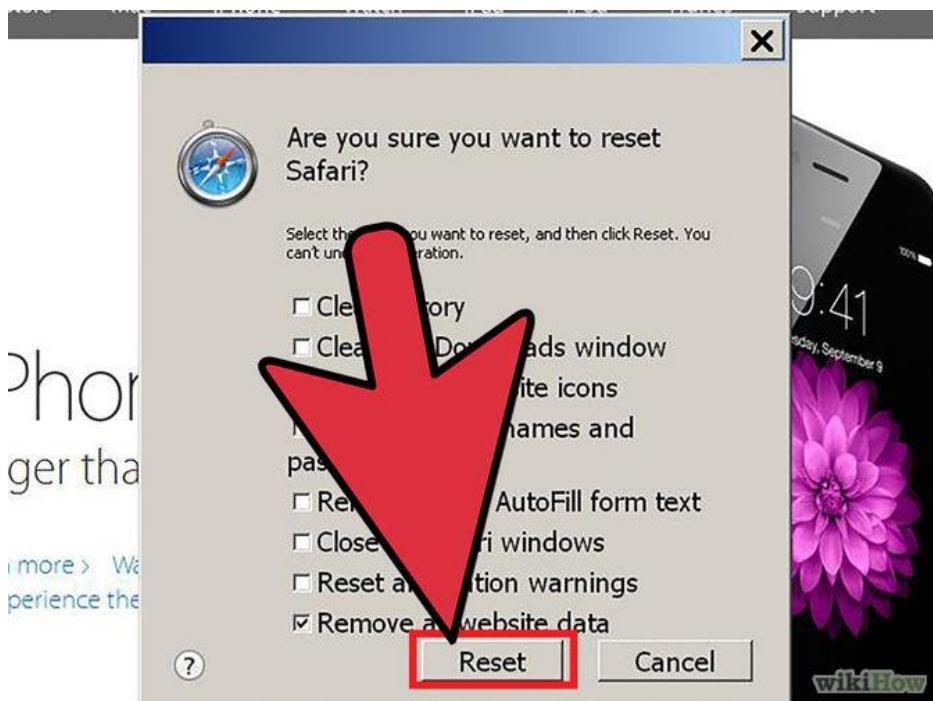
**Step 1:** Once your browser is open, click the gear icon on the top right.



**Step 2:** Select "Reset Safari..." This will prompt a screen to open.

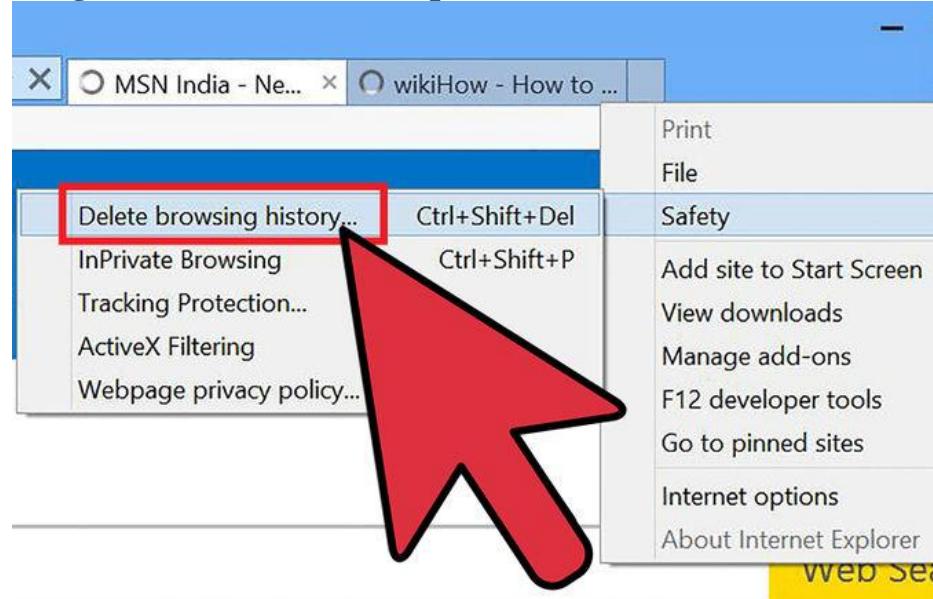


**Step 3:** Select "**Remove all website data**" at the very bottom of the prompt. Check or uncheck any other categories you want reset.

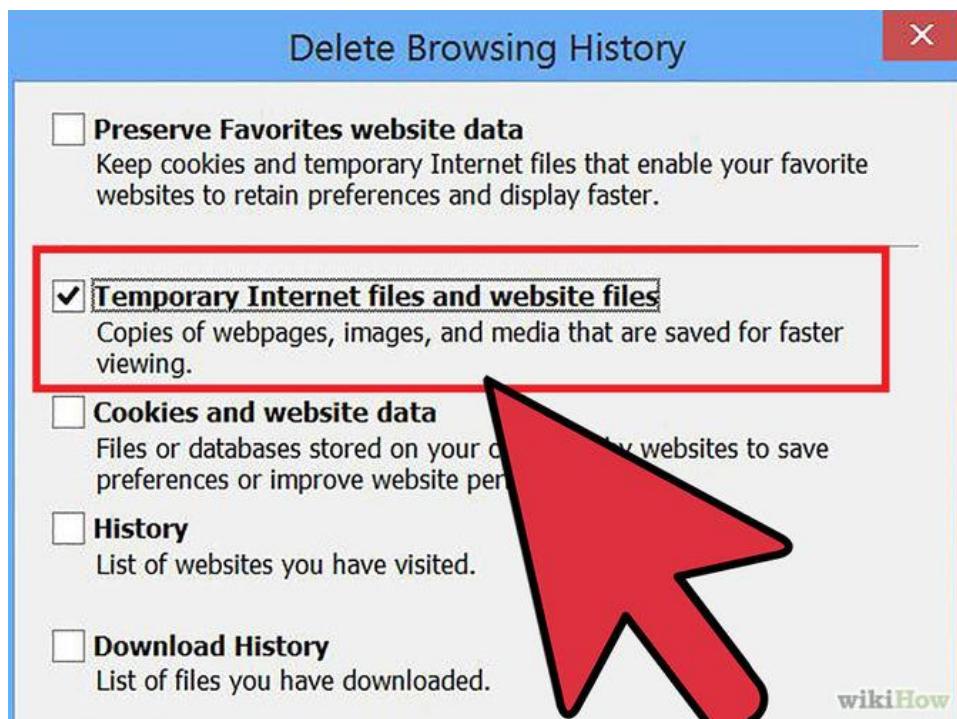


**Step 4:** Click “Reset”.

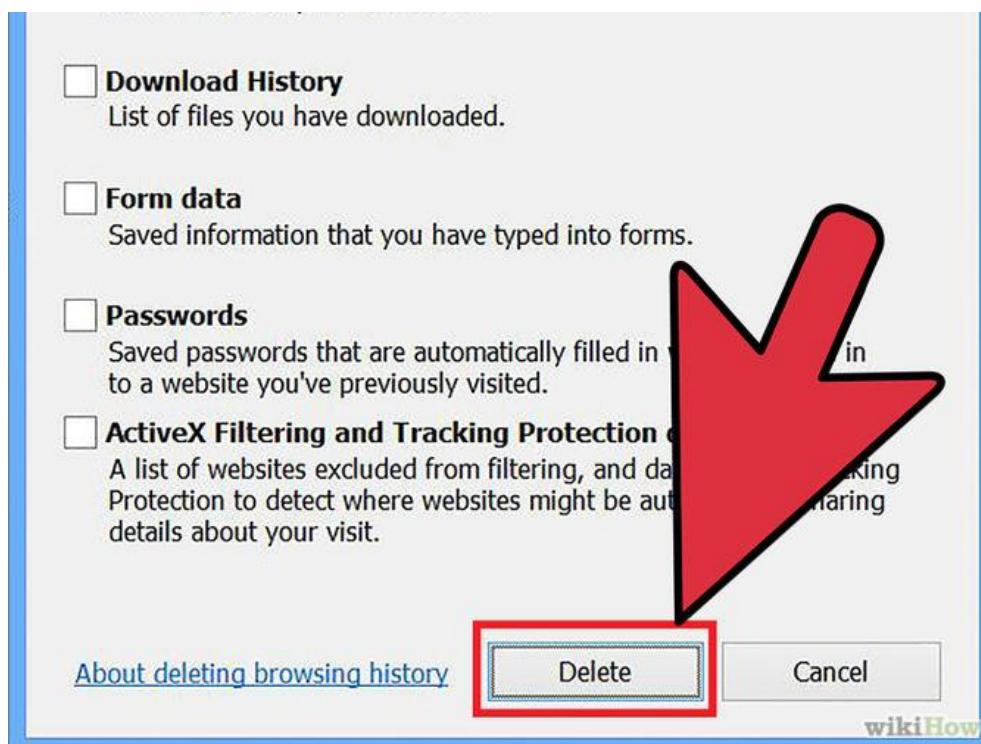
### 9.3.6 Clearing cache for Internet explorer 9, 10 and 11



**Step 1:** Once your browser is open, click the gear icon at the top right to open the **Settings** menu. Then, select **Safety** and **Delete Browsing History**.

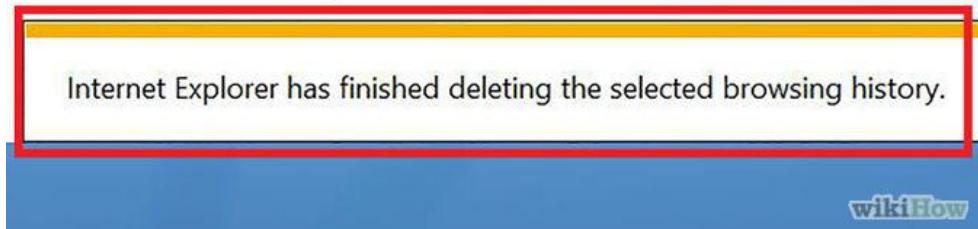
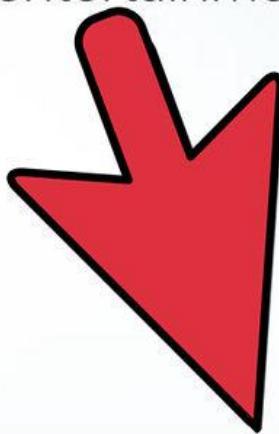


**Step 2:** Select Temporary Internet Files. You will also need to uncheck all of the other boxes, especially Preserve Favorites website data. This option makes the window also delete objects from websites in your Favorites folder, which is necessary to completely clear your cache.



**Step 3:** Click the Delete button near the bottom of the window to perform the operations (i.e. clear your cache by deleting temporary files).

; entertainment lifestyle shopping

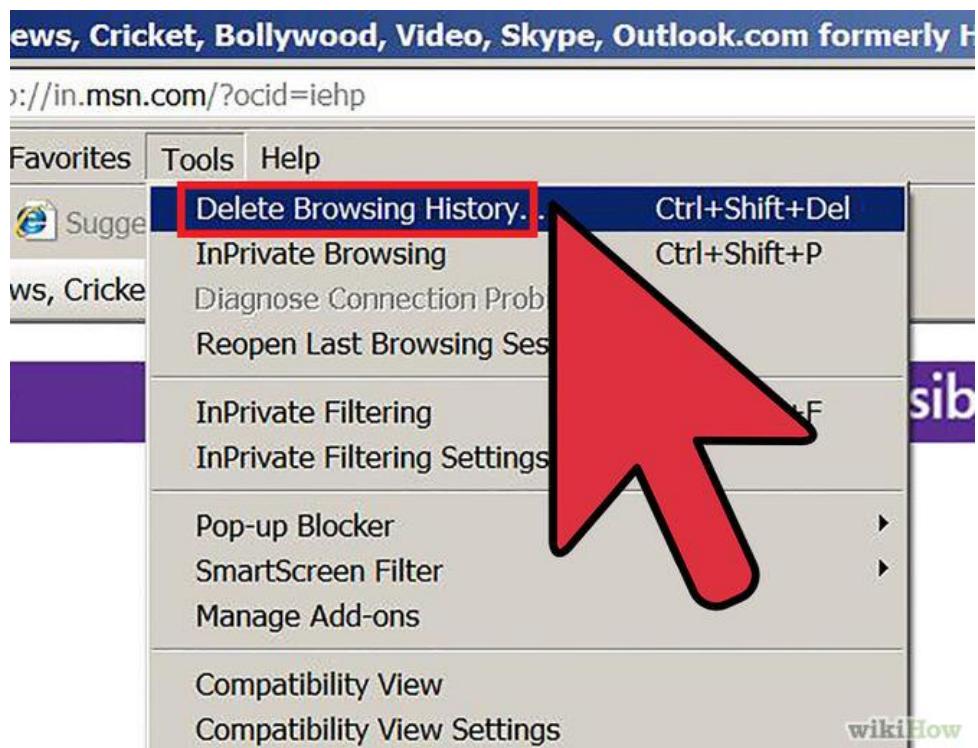


**Step 4:** Your computer will work for a moment, and then the process will be complete. You've successfully cleared Internet Explorer 9's Cache!

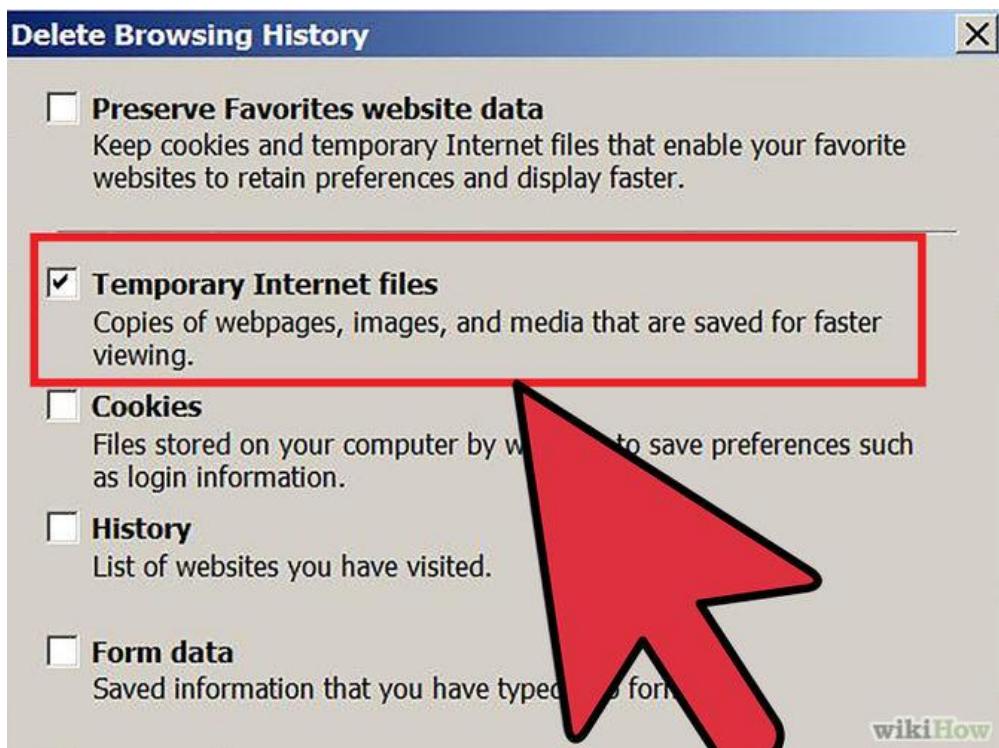
### 9.3.7 Clearing cache for Internet explorer 8



**Step 1:** Once your browser is open, click the **Tools** menu.



**Step 2:** Click on **Delete Browsing History**.



**Step 3:** Select **Temporary Internet Files**.



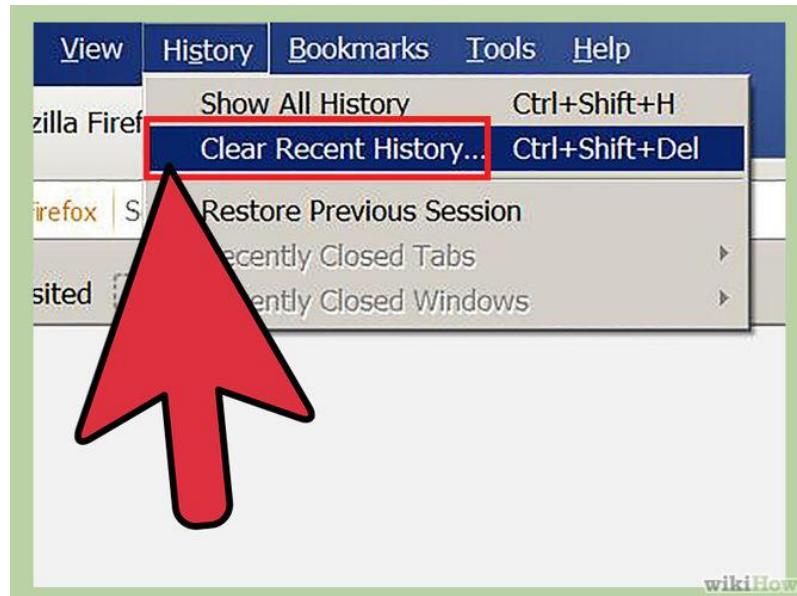
**Step 4:** Click the **Delete** button near the bottom of the window to delete your temporary files (i.e. clear your cache).



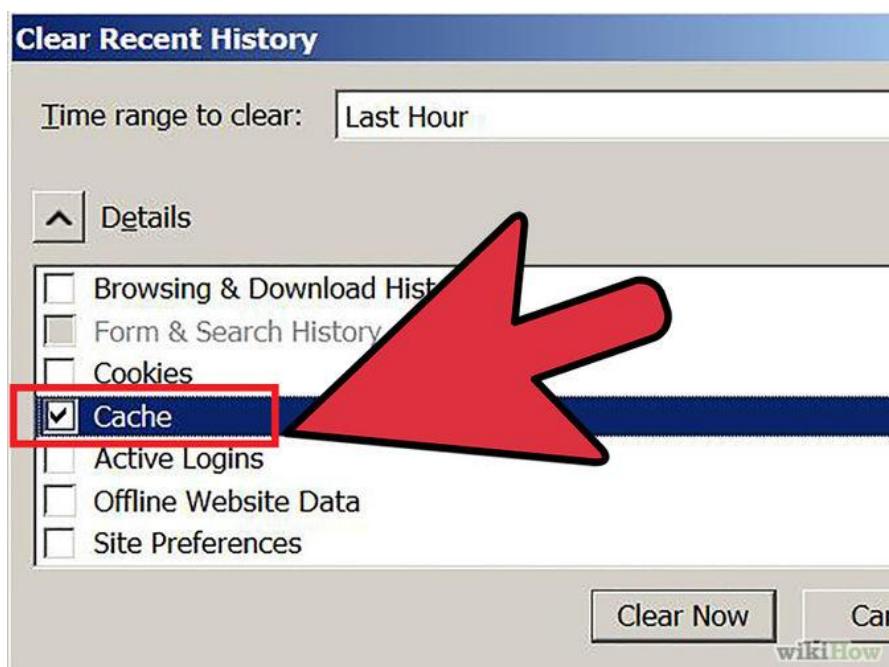
**Step 5:** Set your cache to delete every time you close Internet Explorer. If you want the browser to automatically clear the cache whenever you close it, close the 'Delete Browsing History' window, select '**Internet Options**' from the Tools menu, and check the '**Delete Browsing history on exit**' checkbox.

*Note:* IE8 has a "feature" which retains some cookies even after you clear your cache if you do not UNCHECK the "Preserve Favorites Website Data." If you truly need to clear your cache, you will want to uncheck this!

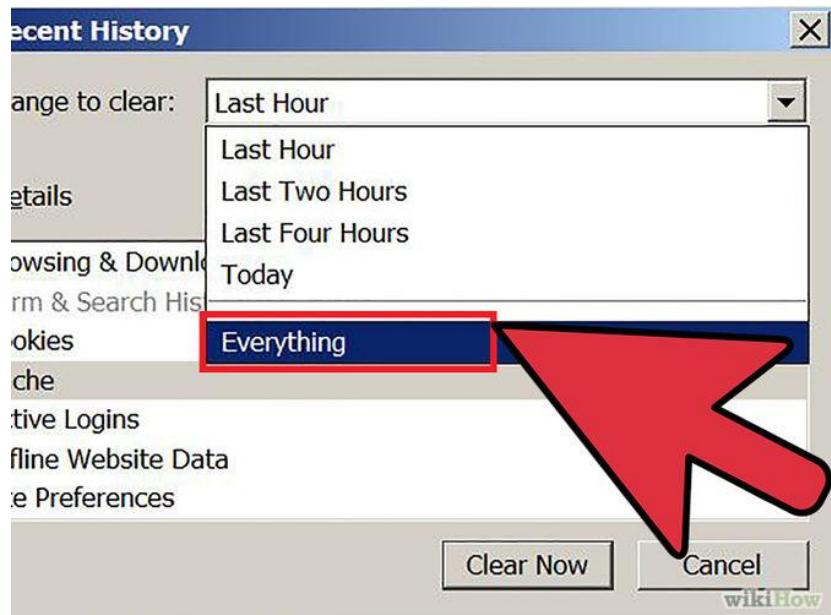
### 9.3.8 Clearing cache for Firefox



**Step 1:** On a PC, click the "Firefox" menu in the top left corner. Next, select the right arrow next to "**History >**", and click "**Clear Recent History**".



**Step 2:** Make sure "**Details**" is expanded, then select "**Cache**" from the list. Uncheck everything else.

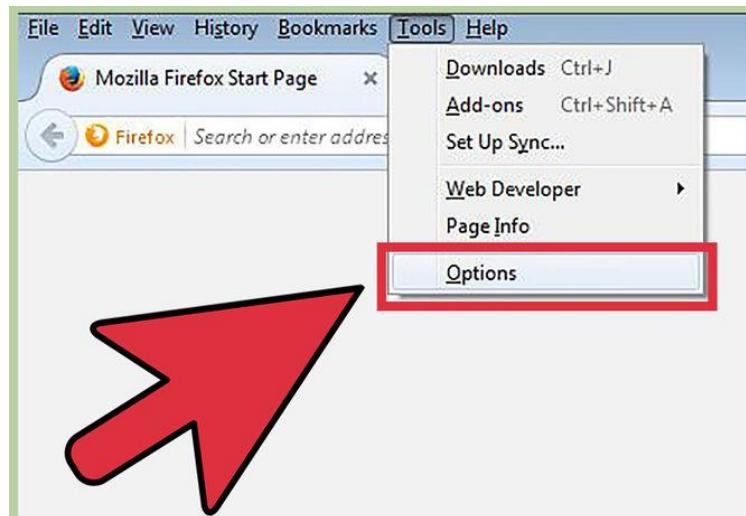


**Step 3:** In the "Time Range to Clear" drop down, select "**Everything**".

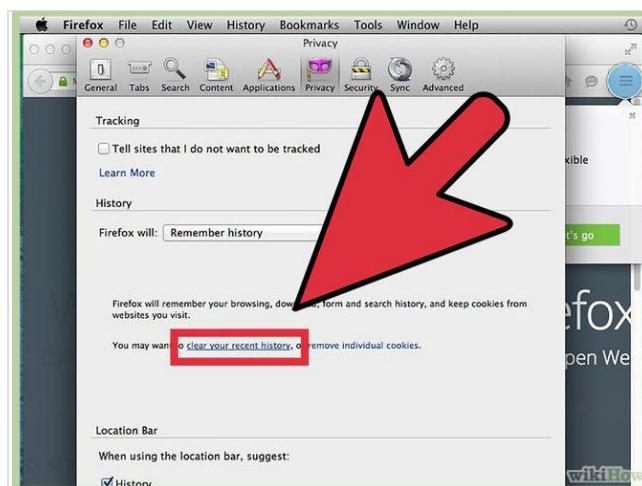


**Step 4:** Select "**Clear Now**". Your computer will work for a moment, and the process will be complete. You've successfully cleared Firefox's Cache!

### 9.3.9 Clearing cache for Firefox 33



**Step 1:** Click the Menu button ("hamburger button" - the one with three horizontal lines) and then choose Options.

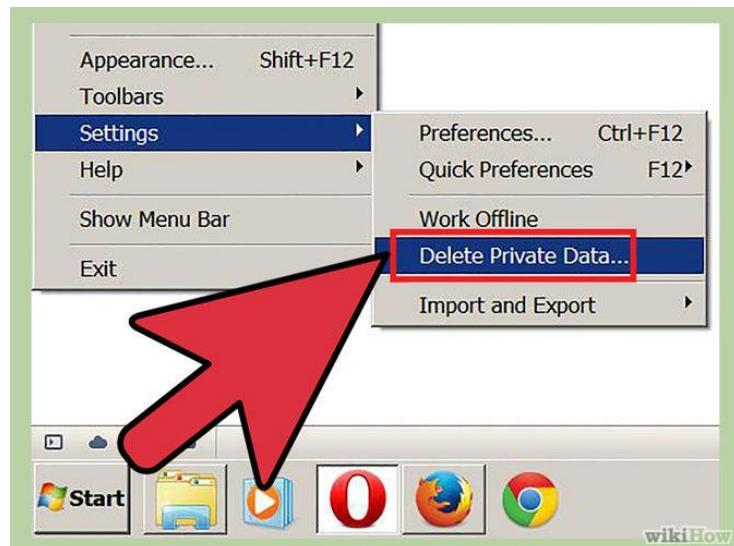


**Step 2:** Firefox for Mac: On a Mac, choose Preferences from the Firefox menu and then continue as instructed below. With the Options window now open, click the Privacy tab. In the History area, click the clear your recent history link.

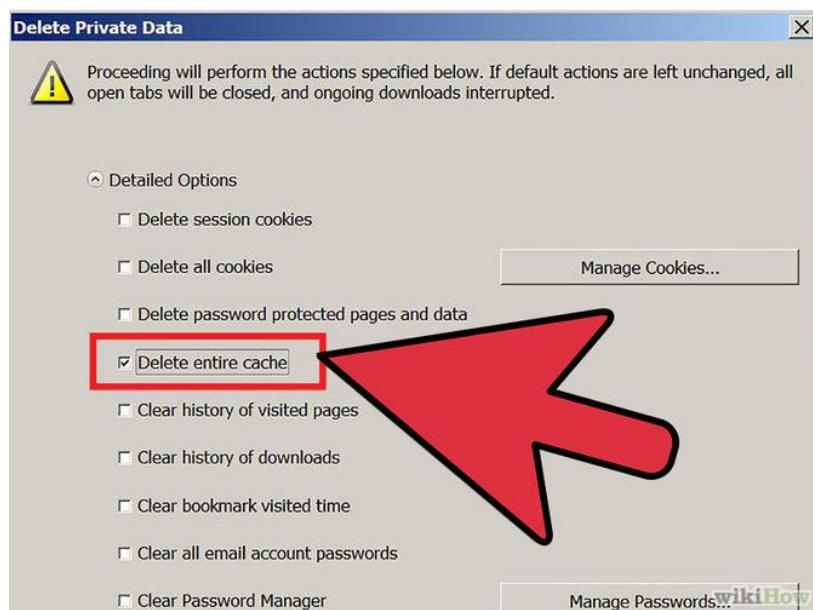


**Step 3:** If you wish to clear other kinds of stored data, feel free to check the appropriate boxes. They will be cleared with the cache in the next step.

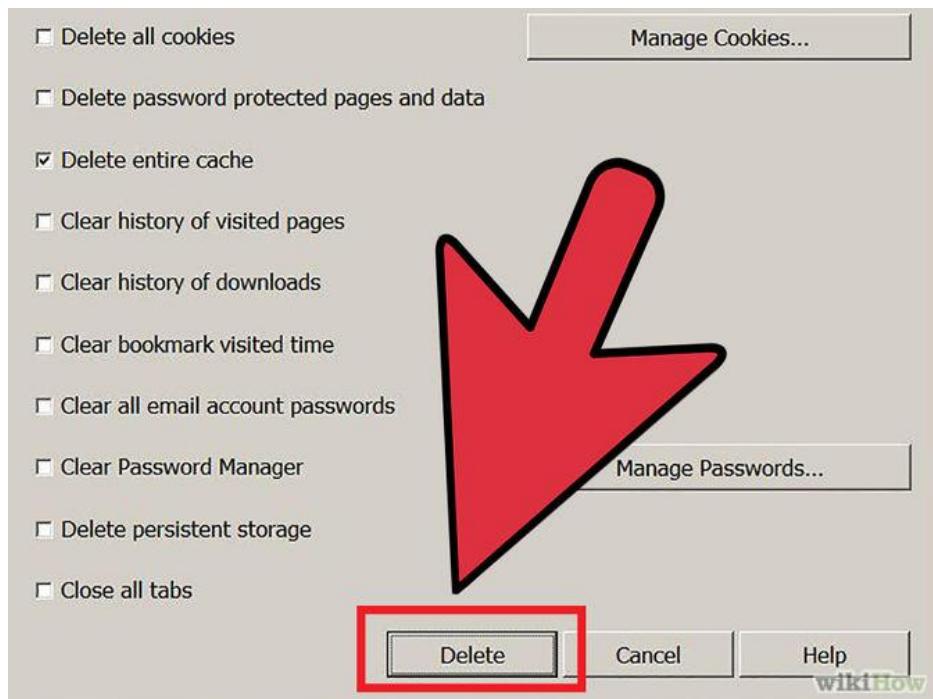
### 9.3.10 Clearing cache for opera



**Step 1:** Once your browser is open, select the "Settings" menu and click "Delete private data".

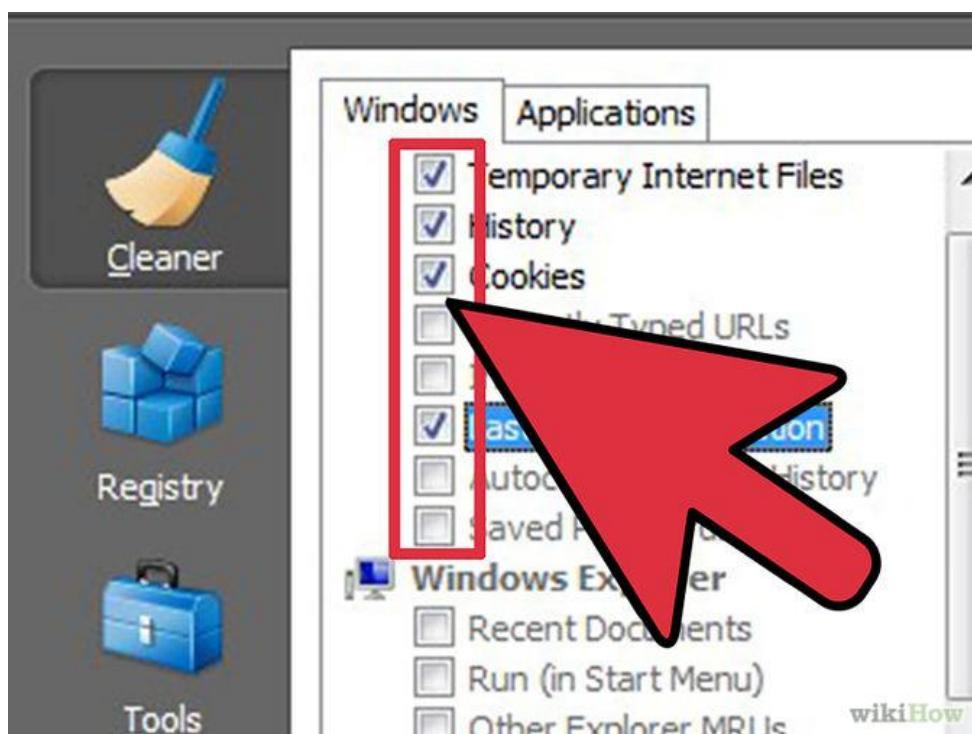


**Step 2:** Make sure the "Delete entire cache" box is checked. Make sure any unwanted categories are left **unchecked**.



**Step 3:** Press “Delete”.

### 9.3.11 Clearing cache for Ccleaner



**Ccleaner-** This is a computer maintenance tool that lets you scan and delete browser cache and cookies. Launch it, go to Cleaner tab and make sure to check the Temporary internet files for the browser you have.

## **Activity**

- a. Perform the cache clearing operation on your system browser.
- b. Perform the cache clearing operation on the browser of your smartphone.
- c. Install CCleaner in your system and use it to perform cache clearing operation.
- d. Find out whether the popular websites you visit daily are secure or not.
- e. Can you find any banking site that does not use https://
- f. Can you find some social networking site that does not use https://
- g. Can you list down some important points that should be kept in mind before going for online shopping.

# WIRELESS SECURITY

This chapter is about different kind of Best Practices that should be followed when using Wireless LAN.

## 10.1 WHAT IS WIRELESS LAN?

The Wireless LAN or WLAN is becoming a popular way to connect devices such as computers these days. In offices and homes, WLAN has become an alternative way of communication compared to wired LAN. The convenience to connect different devices is both cost effective and easily maintainable. The Wikipedia says: “Wireless LANs have become popular in the home due to ease of installation, and the increasing to offer wireless access to their customers; often for free.”

The other factors why WLANs are becoming more acceptable are:

1. No need to be connected physically with each other through any medium such as cables.  
You can roam around freely in office premises, home or around.
2. WLANs are cost effective. Cabling all the way in the offices, hotels etc are not needed.  
So it's cheap and provides same quality of service.
3. Unreachable spots where a cable is hardly accessible, WLAN signals can reach out such as big installations like airports. Also surfing outdoors is also convenient. Just install the device called Access Points (AP) and you are done.
4. Less interruption and easy trouble shooting in case of failures as compared to cabled networks.
5. More secure as most of APs support best encryption methods which protect them from sniffing and other attacks.



Figure 44: A typical Wireless network

## **10.2 MAJOR ISSUES WITH WLAN**

Having said that, WLAN are also as prone to various attacks as their counterpart wired LANs are. Actually WLANs are easier to hack as compared to wired LANs, if not properly configured, due to its easy accessibility around the installation. No need to be in contact of physical wires to hack can be done from anywhere. Its convenience can turn into serious risk to the organization if not configured properly. Major attacks include such as, Sniffing, Key cracking, DoS (Denial of Service), Deauthentication attacks, War driving etc. This chapter is not focused on attacks, we shall mainly concentrate on best practices- how to install and use WLAN securely which can thwart a number of above mentioned attacks.

### **10.2.1 Secure WLAN**

Wireless Security mainly depends on these 3 factors:

- How much is your wireless network secured in terms of encryption being used.
- Monitoring for suspicious and unusual activities.
- User awareness and education.

These are the combination of various approaches ranging from corporate to home networks.

These are also for users how to remain safe while surfing.

### **10.2.2 Wi-Fi at home**

Using a Wi-Fi at home is not a luxury anymore it has become a necessity. However, when the question of security comes into the scene, the first thought that would arise in my mind is how you can protect something which you cannot see, neither can you feel it? Protecting a home wireless network is altogether a different side of the coin as compared to wired networks. Most of wireless network device vendor's and Internet Service provider do not provide any security settings by default and leave the customer to fend for herself. So make sure, your network is secured from being maliciously used.

There is no silver bullet that will protect your wireless network infrastructure. These are, however, some countermeasures listed below that should be used in conjunction with each other to secure your wireless network to the highest level:

**1. Use most secure possible encryption:** The first and most necessary step- use industry standard encryptions. The old (however generally used) WEP-Wired Equivalent Privacy, has been known to be broken. Even you use complex passwords it can be broken and decrypted within minutes or hours. WEP uses 40 bit or 128 bits RC4 ciphers to encrypt the channel.

Instead use secure protocols such as WPA 2 – Wi-Fi Protected Access- 2, which uses strong 128 bits AES ciphers and is typically considered more robust encryption strategy available.

**Attacks mitigated:** WEP Key cracking, Sniffing, Capturing/Eavesdropping

**2. Use Firewall:** All the wireless routers come with built-in firewalls. Enable them with all the security features. You should block any anonymous ping requests and place restrictions on website browsing, if required. Define additional security policies and apply them.

**Attacks mitigated:** Fingerprinting, System compromise

**3. Have a monitoring system in place:** There's a saying- prevention is better than a cure. If you are able to detect some suspicious activities before it penetrates your network, you can block them or take precautionary measures. Deploy WIPS/WIDS for monitoring suspicious activities.

**Attacks mitigated:** Scanning, DoS

**4. Don't use default credentials:** Every wireless router comes with a set of default username/password. Sometimes, people don't change them and keep using them for long time. Username and passwords are used by computers or other devices to connect to wireless router. If any hacker is able to guess them, he can connect to your network easily. Studies show that majority of users use the same combination of username/passwords as set by manufacturers. Some default username combinations are: admin/admin, admin/password or admin/ “ “.

**Attacks mitigated:** Unauthorized access, War driving

**5. Disable Auto-connect feature:** Some devices or the computers/laptops have ‘Let this tool manage your wireless networks’ or ‘Connect automatically to available network’. Such users having this auto-connect feature enabled are prone to Phishing attack or Rogue AP attack. Attackers keep their APs alive and kicking for such kind of unsuspecting users. They also use luring names as ‘HotSpot’, ‘SecureConnect’, ’GovtNetworks’ etc. The user will never suspect them and keep surfing the wireless network happily. Also if you have not changed the default password of your router, the attacker will try to use this feature on their machine and automatically connect using the easily guessable default passwords.

**Attacks mitigated:** Phishing, Sniffing, Rouge AP association

**6. Don't use public Wi-Fi spots to surf sensitive websites:** Free and open wireless networks available on airports, cafes, railway stations are not very secure by nature. They do

not use any encryption to secure the channel between your laptop to the router. So any information which is not by default going on HTTPS from your laptop/smart phone is susceptible to sniffing and even more your session could be hijacked because the unencrypted channel may leak the active session ID used by your website. Recently to demonstrate these types of attacks one researcher developed a tool Firesheep [<http://codebutler.github.com/firesheep/>]. All the attacker needs to do is to just install this tool in Firefox and start sniffing the communications on a public unencrypted Wi-Fi. Some applications like Facebook encrypts the login page [HTTPS] but internal pages are served on unencrypted [HTTP] channel so your session ID can be leaked.

**Attacks mitigated:** Sniffing, Session Hijacking

**7. Change the default SSID:** Although this will not prevent hackers breaking into a network, using a default SSID acts as an indication that the user is careless. So he may be an obvious target to explore further to see if he still uses the default passwords as well?

**Attacks mitigated:** War driving

**8. Restrict access by assigning static IP addresses and MAC filtering:** Disable automatic IP assigning feature and use private static IPs to the legitimate devices you want to connect. This will help you in blocking unwanted devices from being connected to your network. Also, enable MAC filtering- router remembers MAC of each and every device connected to it and saves it as list. You can use this facility to restrict access. Only a set of trusted devices can be allowed to connect. However MAC spoofing is still possible but it raises an extra bar for your wireless network.

**9. Turn off your router when not in use:** Last but not least, a little obvious, but it will save your network from all the attacks for that time period.

#### 1.7.2.3 Wi-Fi in a Corporate/Enterprise Network

Due to the nature of activity and criticality of information, it is very important that Corporate / Enterprise networks have a higher degree of security.

The following are good to have:

- Defining an adequate organization wide Information Security policy & procedures for wireless network

- SSID's should not be associated with the organization, AP vendor or any other related information which would be easy to guess or associate with the current organization
- Enable WPA2 Enterprise encryption with RADIUS authentication and use of EAP protocol like EAP-TTLS, TLS etc.
- Implementation of PKI infrastructure. CA signed certificates to authenticate the server to client and vice versa
- Filtering of clients based on unique identifier like MAC Address
- Isolated 'Guest' wireless network with no interface / connection to the corporate network
- Limiting the radius of Wi-Fi network by reducing the power output of the AP
- Allocating IP Address to the employee and guest machines only after successful authentication
- Periodically changing the keys & passwords
- Use of VPN while accessing corporate information from Public Wi-Fi network
- Client side utilities like DecaffeintIDcan help in detecting changes in ARP table and serve as common man's IDS to protect against attacks like 'hole196' and DoS.
- Implementation of Wireless IDS. Wireless IDS is a new concept. The key features of Wireless IDS are:
  - Prevention against Rogue AP's
  - Detection & prevention against DoS attacks
  - Assistance in locating the approximate physical location of the attacker
  - Assistance in enforcing the Organization's Information Security policy on wireless networks
  - Detection of use of scanning tools like Kismet & NetStumbler

## **ACTVITY**

1. What are the precautions one should take using a wi-fi network at public place?
2. How to secure home network?
3. How to secure enterprise network?
4. Find more about the terms over internet:
  - IDS
  - DOS
  - Kismet
  - NetStumbler

## **RECOMENDED VIDEOS**

[https://www.youtube.com/watch?v=\\_WHynHcXm7c](https://www.youtube.com/watch?v=_WHynHcXm7c)

[https://www.youtube.com/watch?v=Jmszt\\_\\_J204](https://www.youtube.com/watch?v=Jmszt__J204)

<https://www.youtube.com/watch?v=aktovPyT0iM>

[https://www.youtube.com/watch?v=CStMHLQWa\\_8](https://www.youtube.com/watch?v=CStMHLQWa_8)

<https://www.youtube.com/watch?v=a9q-tDRCTtc>

<https://www.youtube.com/watch?v=xex1h93fnI8>

<https://www.youtube.com/watch?v=a9q-tDRCTtc>

# EMAIL AND SOCIAL MEDIA SECURITY

## 11.1 SAFE BROWSING GUIDELINES FOR SOCIAL NETWORKING SITES<sup>22</sup>

Online communities have existed since the invention of the internet. First there were bulletin boards and email lists, which gave people around the world opportunities to connect, to communicate and to share information about particular subjects. Today, social networking websites have greatly expanded the range of possible interactions, allowing you to share messages, pictures, files and even up-to-the-minute information about what you are doing and where you are. These functions are not new or unique – any of these actions can also be performed via the internet without joining a social networking site.

Although these networks can be very useful, and promote social interaction both online and offline, when using them you may be making information available to people who want to abuse it. Think of a social networking site as being like a huge party. There are people there that you know, as well as some that you don't know at all. Imagine walking through the party with all your personal details, and up-to-the-minute accounts of what you are thinking, written on a big sign stuck on your back so that everyone can read it without you even knowing. Do you really want everyone to know all about you?

Remember that social networking sites are owned by private businesses, and that they make their money by collecting data about individuals and selling that data on, particularly to third party advertisers. When you enter a social networking site, you are leaving the freedoms of the internet behind and are entering a network that is governed and ruled by the owners of the site. Privacy settings are only meant to protect you from other members of the social network, but they do not shield your data from the owners of the service. Essentially you are giving all your data over to the owners and trusting them with it.

If you work with sensitive information and topics, and are interested in using social networking services, it is important to be very aware of the privacy and security issues that they raise. Human rights advocates are particularly vulnerable to the dangers of social networking sites and need to be extremely careful about the information they reveal about themselves AND about the people they work with.

---

<sup>22</sup> <https://securityinabox.org/en/guide/social-networking>

Before you use any social networking site it is important to understand how they make you vulnerable, and then take steps to protect yourself and the people you work with. This guide will help you understand the security implications of using social networking sites.

### **11.1.1General Tips on using Social Networking platforms safely**

Social media have become an evident part of our life. We share out updates with our friends, family and anyone who is concerned using social media. But the hackers can use this information to steal sensitive data and hack your account. Given below are some of the general tips on using social media.

➤ **Always ask the questions:**

- ✓ Who can access the information I am putting online?
- ✓ Who controls and owns the information I put into a social networking site?
- ✓ What information about me are my contacts passing on to other people?
- ✓ Will my contacts mind if I share information about them with other people?
- ✓ Do I trust everyone with whom I'm connected?

- Always make sure you use **secure passwords** to access social networks. If anyone else does get into your account, they are gaining access to a lot of information about you and about anyone else you are connected to via that social network. Change your passwords regularly as a matter of routine.
- Make sure you understand the default **privacy settings** offered by the social networking site, and how to change them.
- Consider using **separate accounts/identities**, or maybe different pseudonyms, for different campaigns and activities. Remember that the key to using a network safely is being able to trust its members. Separate accounts may be a good way to ensure that such trust is possible.
- Be careful when accessing your social network account in public internet spaces. **Delete your password and browsing history** when using a browser on a public machine.
- **Access social networking sites using https://** to safeguard your username, password and other information you post. Using https:// rather than http:// adds another layer of security by encrypting the traffic from your browser to your social networking site.
- Be careful about putting too much information into **your status updates** – even if you trust the people in your networks. It is easy for someone to copy your information.

- Most social networks allow you to integrate information with other social networks. For example you can post an update on your Twitter account and have it automatically posted on your Facebook account as well. Be particularly **careful when integrating your social network accounts!** You may be anonymous on one site, but exposed when using another.
- Be cautious about how safe your content is on a social networking site. **Never rely on a social networking site as a primary host for your content** or information. It is very easy for governments to block access to a social networking site within their boundaries if they suddenly find its content objectionable. The administrators of a social networking site may also decide to remove objectionable content themselves, rather than face censorship within a particular country.

### **11.1.2 Posting Personal Details**

Social networking sites ask you for a good deal of data about yourself to make it easier for other users to find and connect to you. Perhaps the biggest vulnerability this creates for users of these sites is the possibility of identity fraud, which is increasingly common. In addition, the more information about yourself you reveal online, the easier it becomes for the authorities to identify you and monitor your activities. The online activities of diaspora activists from some countries have led to the targeting of their family members by the authorities in their homelands.

Ask yourself: is it necessary to post the following information online?

- ✓ birth dates
- ✓ contact phone numbers
- ✓ addresses
- ✓ details of family members
- ✓ sexual orientation
- ✓ education and employment history

### **11.1.3 Friends, Followers and Contacts**

The first thing you will do after filling in your personal details with any social networking application is establish connections to other people. Presumably these contacts are people you know and trust – but you may also be connecting to an online community of like-minded individuals that you have never met. The most important thing to understand is what information you are allowing this online community to have.

When using a social network account such as Facebook, where a lot of information about yourself is held, consider only connecting to people you know and trust not to misuse the information you post.

#### **11.1.4 Status Updates**

On Twitter and Facebook and similar networks, the status update answers the questions: What am I doing right now? What's happening? The most important thing to understand about the status update is who can actually see it. The default setting for the status update on most social networking applications is that anyone on the internet can see it. If you only want your contacts to see the updates, you need to tell the social networking application to keep your updates hidden from everyone else.

To do this in Twitter, look for “Protect Your Tweets”. In Facebook, change your settings to share your updates with “Friends Only”. Even if you switch to those settings, consider how easy it is for your information to be reposted by followers and friends. Agree with your network of friends on a common approach to passing on the information posted in your social networking accounts. You should also think about what you may be revealing about your friends that they may not want other people to know; it's important to be sensitive about this, and to ask others to be sensitive about what they reveal about you.

There have been many incidents in which information included in status updates has been used against people. Teachers in the US have been fired after posting updates about how they felt about their students; other employees have lost their jobs for posting about their employers. This is something that nearly everyone needs to be careful about.

#### **11.1.5 Sharing Online Content**

It's easy to share a link to a website and get your friend's attention. But who else will be paying attention, and what kind of reaction will they have? If you share (or "like") a site that opposes some position taken by your government, for example, agents of that government very might well take an interest and target you for additional surveillance or direct persecution.

If you want your contacts (and of course the administrators of the social networking platform you use) to be the only ones who can see the things you share or mark as interesting, be sure to check your privacy settings.

#### **11.1.6 Revealing your Location**

Most social networking sites will display your location if that data is available. This function is generally provided when you use a GPS-enabled phone to interact with a social network, but don't assume that it's not possible if you aren't connecting from a mobile. The network your computer is connected to may also provide location data. The way to be safest about it is to double-check your settings.

Be particularly mindful of location settings on photo and video sharing sites. Don't just assume that they're not sharing your location: double-check your settings to be sure.

### **11.1.7 Sharing Videos and Photos**

Photos and videos can reveal people's identities very easily. It's important that you have the consent of the subject/s of any photo or video that you post. If you are posting an image of someone else, be aware of how you may be compromising their privacy. Never post a video or photo of anyone without getting their consent first.

Photos and videos can also reveal a lot of information unintentionally. Many cameras will embed hidden data (metadata tags), that reveal the date, time and location of the photo, camera type, etc. Photo and video sharing sites may publish this information when you upload content to their sites.

### **11.1.8 Instant Chats**

Many social networking sites have tools that allow you to have discussions with your friends in real time. These operate like Instant Messaging and are one of the most insecure ways to communicate on the internet, both because they may reveal who you are communicating with, and what you are communicating about.

*Connecting to the site via https is a minimum requirement for secure chatting, but even this is not always a guarantee that your chat is using a secure connection. For example, Facebook chat uses a different channel to HTTPS (and is more prone to exposure).*

It is more secure to use a specific application for your chats, such as Pidgin with an Off-the-record plugin, which uses encryption. Read the 'Pidgin – secure instant messaging' hands-on guide.

### **11.1.9 Joining and Creating Groups, Events and Communities**

What information are you giving to people if you join a group or community? What does it say about you? Alternatively, what are people announcing to the world if they join a group or community that you have created? How are you putting people at risk?

When you join a community or group online it is revealing something about you to others. On the whole, people may assume that you support or agree with what the group is saying or doing, which could make you vulnerable if you are seen to align yourself with particular political groups, for example. Also if you join a group with a large number of members that you don't know, then this can compromise any privacy or security settings that you have applied to your account, so think about what information you are giving away before joining. Are you using your photo and real name so strangers can identify you?

Alternatively, if you set up a group and people choose to join it, what are they announcing to the world by doing so? For example, perhaps it is a gay and lesbian support group that you have set up to help people, but by joining it people are openly identifying themselves as gay or gay-friendly, which could bring about dangers for them in the real world.

## 11.2 EMAIL SECURITY TIPS<sup>23</sup>

1. Don't open email attachments that you are not expecting, or which have come from someone you do not know. When you open such an email, make sure that your anti-virus software is up-to-date and pay close attention to any warnings from your browser or email program.
2. You can use anonymity software which can help you hide your chosen email service from anyone who might be monitoring your internet connection. A good, free software programme to do this is *Tor* (Find out more about Tor browser using Google). If you don't want to give away information about your identity through your email, do not register a username or 'Full Name' that is related to your personal or professional life.
3. You can avoid getting spam (unwanted or junk email) by guarding your email address and distributing it sparingly. Also, never open or reply to any emails you consider to be spam, because spammers will take this as a proof of the legitimacy of the address and will just send you more spam. Consider using a spam filter, but remember that it needs to be monitored as it may mistake a genuine email for spam.
4. You should try to avoid your emails being mistaken for spam by the recipients. Spam filters will block messages with certain words in the subject heading. It is worth scanning your spam folder for subject lines that are getting blocked.

---

<sup>23</sup> <https://survival.tacticaltech.org/internet/email/tips>

5. Beware of email scams. Many scam emails pretend to come from a bank, Ebay, Paypal, or other online shops. If you get an email telling you that your account is in danger of being shut down, or that you need to take immediate action by updating your account information, be very suspicious: these messages are usually scams. Another frequent scam has you receiving an email from someone you know which says that they have had an emergency and asks you to send them money. This person's email account is likely to have been compromised by a scammer.
6. Pay close attention if your browser suddenly gives you messages about invalid security certificates when you attempt to access a secure webmail account. It could mean that someone is tampering with the communication between your computer and the server in order to intercept your messages.

## **ACTIVITY**

1. What are anonymous accounts? Find some browsers which supports anonymity.
2. After going though the above section, find out whether you were following the above safe practices while handling your social medial account? Find the gaps?
3. Based on the above recommendations, adjust your social media account settings.

## **RECOMENDED VIDEOS**

<https://www.youtube.com/watch?v=EFHfg1bfgVc>

<https://www.youtube.com/watch?v=tkgLHoafeFk>

[https://www.youtube.com/watch?v=QUyla\\_nMJis](https://www.youtube.com/watch?v=QUyla_nMJis)

<https://www.youtube.com/watch?v=-CeuqCHX7tE>

<https://www.youtube.com/watch?v=xCHTmzfsGmI>

# SMARTPHONE SECURITY

## 12.1 INTRODUCTION<sup>24</sup>

Advances in technology now mean that mobile phones can provide services and features similar to desktop or laptop computers. These Smartphones offer many new ways to communicate and capture and disseminate media. To provide these new functionalities, the smartphones not only use the mobile network, but also connect to the internet either via a wi-fi connection (similar to a laptop at an internet cafe) or via data connections through the mobile network operator.

So while you can, of course, make phone calls with a smartphone, it is better to view smartphones as small computing devices. This means that the other material in this toolkit is relevant to your use of your smartphone as well as your computer.

Smartphones usually support a wide range of functionality – web browsing, email, voice and instant messaging over the internet, capturing, storing and transmitting audio, videos and photos, enabling social networking, multi-user games, banking and many other activities. However, many of these tools and features introduce new security issues, or increase existing risks. For instance, some smartphones have built-in geo-location (GPS) functionality, which means they can provide your precise location to your mobile network operator by default, and to many applications you use on your phone (such as social networking, mapping, browsing and other applications). As mentioned before, mobile phones already relay your location information to your mobile network operator (as part of the normal functions of the phone). However, the additional GPS functionality not only increases the precision of your location information, it also increases the amount of places where this information might be distributed.

It's worth reviewing all the risks associated with mobile phones discussed in our guide How to use mobile phones as securely as possible as all of them are also relevant to smartphone use. That guide also covers issues of eavesdropping, interception of SMS or phone calls, SIM card related issues, and best practices.

In this guide we'll take a look at the additional security challenges posed by smartphones.

---

<sup>24</sup> <https://securityinabox.org/en/guide/smartphones>

## 12.2 SMARTPHONE SECURITY GUIDELINES

### 12.2.1 Purses, Wallets, Smartphones

We have an intuitive understanding of the value of keeping our purse or wallet safe, because so much sensitive information is stored in them, and losing them will compromise our privacy and safety. People are less aware of the amount of personal information being carried in their smartphones, and consider losing a phone a nuisance rather than a risk. If you also think that a smartphone is a computing device which is always connected to a network and is continually carried around, it also highlights the important difference between a holder of discrete, passive information (like a wallet), and an active and interactive item like a smartphone.

*A simple exercise can help illustrate this:*

Empty the content of your wallet or purse, and take account of sensitive items. Typically you may find:

- Pictures of loved ones (~5 pictures)
- Identification cards (driver's license, membership cards, social security cards)
- Insurance and health information (~2 cards)
- Money (~5 bills)
- Credit/Debit cards (~3 cards)

Now, examine the contents of your smartphone. A typical smartphone user may find some of the above in higher quantities, and in some cases much more valuable items:

- Pictures of loved ones (~100 pictures)
- Email applications and their passwords
- Emails (~500 emails)
- Videos (~50 videos)
- Social networking applications and their passwords
- Banking applications (with access to the bank accounts)
- Sensitive documents
- Sensitive communication records
- A live connection to your sensitive information

The more you use smartphones, the more you need to become aware of the associated risks and take appropriate precautions. Smartphones are powerful amplifiers and distributors of your personal data. They are designed to provide as much connectivity as possible and to link to social networking services by default. This is because your personal data is valuable information that can be aggregated, searched and sold.

It can be disastrous if you lose your phone without having a backup of your most important data (such as your contacts) in a secure location. Besides backing up your data, make sure you also know how to restore the data. Keep a hard copy of the steps you need to take so you can do it quickly in an emergency.

In this chapter we'll start by introducing some smartphone basics – a description of various platforms and some basic setup procedures for securing your information and communication. The remaining parts of this chapter will cover specific precautions related to common uses of smartphones.

## **12.2.2 Platforms, Setup and Installation**

### **12.2.2.1 Platforms and Operating Systems**

At the time of writing, the most common smartphones in use are Apple's iPhone and Google's Android, followed by Blackberry and Windows phones. The key difference between Android and other operating systems is that Android is, mostly, an Open Source (*FOSS*) system, which allows the operating system to be audited independently to verify if it properly protects users' information and communication. It also facilitates development of security applications for this platform. Many security-aware programmers develop Android applications with user safety and security in mind. Some of these will be highlighted later in this chapter.

Regardless what type of smartphone you are using, there are issues that you should be aware of when you use a phone which connects to the internet and comes with features such as *GPS* or wireless networking capacities. In this chapter we focus on devices with the Android platform, because, as mentioned above, it's easier to secure data and communications. Nonetheless, basic setup guides and some applications for devices other than Android phones are provided, too. Blackberry phones have been presented as "secure" messaging and email devices. This is because messages and emails are securely channeled through Blackberry servers, out of the reach of potential eavesdroppers. Unfortunately, more and more governments are demanding access to these communications, citing need for guarding against potential terrorism and organised crime. India, United Arab Emirates, Saudi Arabia, Indonesia and Lebanon are examples of governments which have scrutinized the use of Blackberry devices and demanded access to user data in their countries.

### **12.2.2.2 Feature Phones**

Another category of mobiles are often called 'feature phones'. Recently, feature phones have increased their functionalities to include those of some smartphones. But generally, feature phones' operating systems are less accessible, therefore there are limited opportunities for

security applications or improvements. We do not specifically address feature phones, although many measures discussed here make sense for feature phones too.

#### **12.2.2.3 Branded and locked smartphones**

Smartphones are usually sold branded or locked. Locking smartphones means that the device can only be operated with one carrier, whose SIM card is the only one that will work in the device. Mobile network operators usually brand a phone by installing their own firmware or software. They may also disable some functionalities or add others. Branding is a means for companies to increase revenue by channelling your smartphone use, often also collecting data about how you are using the phone or by enabling remote access to your smartphone.

For these reasons, we recommend that you buy an unbranded smartphone if you can. A locked phone poses a higher risk since all your data is routed through one carrier, which centralises your data streams and makes it impossible to change SIM cards to disseminate the data over different carriers. If your phone is locked, ask someone you trust about unlocking it.

#### **12.2.2.4 General Setup**

Smartphones have many settings which control the security of the device. It is important to pay attention to how your smartphone is set up. In the Hands-on Guides below we will alert you to certain smartphone security settings that are available but not active by default, as well as those which are active by default and make your phone vulnerable.

#### **12.2.2.5 Installing and updating applications**

The usual way to install new software on your smartphone is to use the iPhone Appstore or Google Play store, log in with your user credentials, and download and install a desired application. By logging-in you associate your usage of the online store with the logged-in user account. The owners of the application store keep records of this user's browsing history and application choices.

The applications which are offered in the official online store are, supposedly, verified by store owners (Google or Apple), but in reality this provides weak protection against what applications will do after being installed on your phone. For example, some applications may copy and send out your address book after you install them on your phone. On Android phones each application needs to request, during the installation process, what it will be permitted to do when it is in use. You should pay close attention to what permissions are requested, and if these permissions make sense for the function of the app you are installing. For example, if you are considering a "news reader" application and you find out that it requests the rights to send your contacts over a mobile data connection to a third party, you

should look for alternative applications with appropriate access and rights. )ites. Some users may want to consider these alternative sites to minimize online contact with Google. One of the alternative store is **F-Droid** ('Free Droid'), which only provides *FOSS* applications. However please remember that you should trust the site before you download any apps from it. For inexperienced users we recommend that you use Google Play store.

If you don't want to (or are unable to) go online to access apps, you can transfer apps from someone else's phone by sending *.apk* files (short for 'android application package') via bluetooth. Alternatively you could download the .apk file to your device's Micro SD card or use a usb cable to move it there from a PC. When you have received the file, simply long tap on the filename and you will be prompted to install it. (**Note:** be especially careful while using Bluetooth.

### **12.2.3 Communicating Securely(Through Voice and Messages) with a Smartphone**

#### **12.2.3.1 Secure Voice Communication**

##### *Basic telephony*

In order to send or receive any calls or communications to your phone, the signal towers nearest you are alerted by your phone of its presence<sup>25</sup>. As a result of those alerts and communications the network service provider knows the precise geographic location of your mobile phone at any given time.

**About Anonymity:** If you are conducting sensitive phone conversations or sending sensitive SMS messages, beware of the above tracking 'feature' of all mobile phones. Consider adopting the steps below:

- Make calls from different locations each time, and choose locations that are not associated with you.
- Keep your phone turned off, with the battery disconnected, go to the chosen location, switch your phone on, communicate, switch the phone off and disconnect the battery. Doing this habitually, each time you have to make a call, will mean that the network cannot track your movements.
- Change phones and SIM cards often. Rotate them between friends or the second-hand market.

---

<sup>25</sup> <https://securityinabox.org/en/guide/mobile-phones>

- Use unregistered pre-paid SIM cards if this is possible in your area. Avoid paying for a phone or SIM cards using a credit card, which will also create a connection between these items and you.

**About eavesdropping:** Your phone can be set to record and transmit any sounds within the range of its microphone without your knowledge. Some phones can be switched on remotely and brought into action in this way, even when they look as though they are switched off.

- Never let people whom you don't trust get physical access to your phone; this is a common way of installing spying software on your phone.
- If you are conducting private and important meetings, switch your phone off and disconnect the battery. Or don't carry the phone with you if you can leave it where it will be absolutely safe.
- Make sure that any person with whom you communicate also employs the safeguards described here.
- In addition, don't forget that using a phone in public, or in places that you don't trust, makes you vulnerable to traditional eavesdropping techniques, or to having your phone stolen.

**About interception of calls:** Typically, encryption of voice communications (and of text messages) that travel through the mobile phone network is relatively weak. There are inexpensive techniques which third parties can use to intercept your written communications, or to listen to your calls, if they are in proximity to the phone and can receive transmissions from it. And of course, mobile phone providers have access to all your voice and text communications. It is currently expensive and/or somewhat technically cumbersome to encrypt phone calls so that even the mobile phone provider can't eavesdrop – however, these tools are expected to become cheaper soon. To deploy the encryption you would first have to install an encryption application on your phone, as well as on the device of the person with whom you plan to communicate. Then you would use this application to send and receive encrypted calls and/or messages. Encryption software is currently only supported on a few models of so-called 'smart' phones.

Conversations between Skype and mobile phones are not encrypted either, since at some point, the signal will move to the mobile network, where encryption is NOT in place<sup>26</sup>. Using Internet through your Smartphone over mobile data connections or WiFi can provide more secure ways to communicate with people, namely by using VoIP and employing means to secure this channel of communication. Some smartphone tools can even extend some of this security beyond VoIP, to mobile phone calls as well (See **Redphone** below).

*Here we list a few tools and their pros and cons:*

### **Skype**

The most popular commercial VoIP application, Skype, is available for all smartphone platforms and works well if your wireless connectivity is reliable. It is less reliable on mobile data connections.

Skype is a non Open-Source software what makes it very difficult to independently confirm its level of security. Additionally, Skype is owned by Microsoft, which has a commercial interest in knowing when you use Skype and from where. Skype also may allow law enforcement agencies retrospective access to all your communications history.

### **Other VoIP tools**

Using VoIP is generally free (or significantly cheaper than mobile phone calls) and leaves few data traces. In fact, a secured VoIP call can be the most secure way to communicate.

**RedPhone** is a Free and Open-Source Software application that encrypts voice communication data sent between two devices that run this application. It is easy to install and very easy to use, since it integrates itself into your normal dialing and contact scheme. But people you want to talk to also need to install and use RedPhone. For ease of use, RedPhone uses your mobile number as a way to identify you to your contacts. Unfortunately, this makes it more difficult to use RedPhone without a functioning mobile service plan, even on devices capable of using WiFi to connect to the Internet. RedPhone also uses a central server, which puts the administrators of the service in a powerful position by allowing them to see much of the meta-data related to your encrypted VoIP calls.

**CSipSimple** is a powerful VoIP client for Android phones that is well maintained and comes with many easy set-up wizards for different VoIP services.

---

<sup>26</sup> <https://securityinabox.org/en/guide/smartphones>

**Open Secure Telephony Network (OSTN)** and the server provided by the Guardian project, **ostel.co**, currently offers one of the most secure means to communicate via voice. Knowing and trusting the entity that operates the server for your VoIP communication needs is an important consideration.

When using CSipSimple, you never directly communicate with your contact, instead all your data is routed through the Ostel server. This makes it much harder to trace your data and find out who you are talking to. Additionally, Ostel doesn't retain any of this data, except the account data that you need to log in. All your speech is securely encrypted and even your meta data, which is usually very hard to disguise, is blurred since traffic is proxied through the ostel.co server. If you download CSipSimple from ostel.co it also comes preconfigured for use with ostel, which makes it very easy to install and use.

*Tool Guides* for CSipSimple and Ostel.co are forthcoming. In the meantime, more information can be found by following the links above.

#### **12.2.3.2 Sending Messages Securely**

You should use precautions when sending SMS and using instant messaging or chatting on your smartphone.

##### **SMS**

SMS communication is insecure by default. Anyone with access to a mobile telecommunication network can intercept these messages easily and this is an everyday occurrence in many situations. Don't rely on sending unsecured SMS messages in critical situations. There is also no way of authenticating SMS messages, so it is impossible to know if the contents of a message was changed during delivery or if the sender of the message really is the person they claim to be.

##### **Securing SMS**

**TextSecure** is a *FOSS* tool for sending and receiving secure SMS on Android phones. It works both for encrypted and non-encrypted messages, so you can use it as your default SMS application. To exchange encrypted messages this tool has to be installed by both the sender and the recipient of a message, so you will need to get people you communicate with regularly to use it as well. TextSecure automatically detects when an encrypted message is received from another TextSecure user. It also allows you to send encrypted messages to more than one person. Messages are automatically signed making it nearly impossible to tamper with the contents of a message. In our TextSecure hands-on guide we explain in detail the features of this tool and how to use it.

## **Secure Chat**

Instant messaging and chatting on your phone can produce a lot of information that is at risk of interception. These conversations might be used against you by adversaries at a later date. You should therefore be extremely wary about what you reveal when you are writing on your phone while instant messaging and chatting.

There are ways to chat and instant message securely. The best way is to use end-to-end encryption, as this will enable you to make sure the person on the other end is who you want.

We recommend ChatSecure as a secure text chat application for the Android phones. ChatSecure offers easy and strong encryption for your chats with *Off-the-Record* Messaging protocol. This encryption provides both authenticity (you can verify that you are chatting with the right person) and the independent security of each session so that even if the encryption of one chat session is compromised, other past and future sessions will remain secure.

ChatSecure has been designed to work together with Orbot, so your chat messages can be routed through the *Tor* anonymizing network. This makes it very hard to trace it or even find out that it happened.

For iPhones, the **ChatSecure** client provides the same features, although it is not easy to use it with the *Tor* network.

Whichever application you will use always consider which account you use to chat from. For example when you use Google Talk, your credentials and time of your chatting session are known to Google. Also agree with your conversation partners on not saving chat histories, especially if they aren't encrypted.

### **12.2.3.3 Storing Information on your Smartphone**

Smartphones come with large data storage capacities. Unfortunately, the data stored on your device can be easily accessible by third parties, either remotely or with physical access to the phone. You can take steps to encrypt any sensitive information on your phone by using specific tools.

#### ***Date Encryption Tools***

The **Android Privacy Guard (APG)** allows OpenGPG encryption for files and emails. It can be used to keep your files and documents safe on your phone, as well when emailing.

#### ***Recording Password Securely***

You can keep all your needed passwords in one secure, encrypted file by using **Keepass**. You will only need to remember one master password to access all the others. With Keepass you

can use very strong passwords for each account you have, as KeePass will remember them for you, and it also comes with a password generator to create new passwords. You can synchronise KeePass password databases between your phone and your computer. We recommend that you synchronise only those passwords that you will actually use on your mobile phone. You can create a separate smaller password database on the computer and synchronise this one instead of coping an entire database with all the passwords that you use to your smartphone. Also, since all the passwords are protected by your master password, it is vital to use very strong password for your KeePass database.

#### **12.2.3.4 Sending Email from your Smartphone**

In this section we will briefly discuss the use of email on smartphones. In the first instance, consider if you really need to use your smartphone to access your email. Securing a computer and its content is generally simpler than doing so for a mobile device such as a smartphone. A smartphone is more susceptible to theft, monitoring and intrusion.

If it is absolutely vital that you access your email on your smartphone, there are actions you can take to minimize the risks.

- Do not rely on smartphone as your primary means for accessing your email. Downloading (and removing) emails from an email server and storing them only on your smartphone is not advised. You can set up your email application to use only copies of emails.
- If you use email encryption with some of your contacts, consider installing it on your smartphone, too. The additional benefit is that encrypted emails will remain secret if the phone falls into wrong hands.

Storing your private encryption key on your mobile device may seem risky. But the benefit of being able to send and store emails securely encrypted on the mobile device might outweigh the risks. Consider creating a mobile-only encryption key-pair (using **APG**) for your use on your smartphone, so you do not copy your encryption private key from your computer to the mobile device. Note that this requires that you ask people you communicate with to also encrypt emails using your mobile-only encryption key.

#### **12.2.3.5 Capturing Media with your Smartphone**

Capturing pictures, video or audio with your Smartphone can be a powerful means to document and share important events. However, it is important to be careful and respectful of privacy and safety of those pictured, filmed or recorded. For example, if you take photos or record video or audio of an important event, it might be dangerous to you or to those who

appear in the recordings, if your phone fell into the wrong hands. In this case, these suggestions may be helpful:

- Have a mechanism to securely upload recorded media files to protected online location and remove them from the phone instantly (or as soon as you can) after recording.
- Use tools to blur the faces of those appearing in the images or videos or distort the voices of audio or videos recordings and store only blurred and distorted copies of media files on your mobile device.
- Protect or remove meta information about time and place within the media files.

**Guardian Project** has created a *FOSS* app called **ObscuraCam** to detect faces on photos and blur them. You can choose the blurring mode and what to blur, of course. Obscuracam also deletes the original photos and if you have set up a server to upload the captured media, it provides easy functionality to upload it.

#### **12.2.3.6 Accessing the Internet Securely from your Smartphone**

As discussed in our guide **How to keep your Internet communication private** and our guide **How to remain anonymous and bypass censorship on the Internet**, access to content on the Internet, or publishing material online such as photos or videos, leaves many traces of who and where you are and what you are doing. This may put you at risk. Using your smartphone to communicate with the Internet magnifies this risk.

##### ***Through Wi-Fi or Mobile Data***

Smartphones allow you to control how you access the Internet: via a wireless connection provided by an access point (such as an internet cafe), or via a mobile data connection, such as GPRS, EDGE, or UMTS provided by your mobile network operator.

Using a WiFi connection reduces the traces of data you may be leaving with your mobile phone service provider (by not having it connected with your mobile phone subscription). However, sometimes a mobile data connection is the only way to get online. Unfortunately mobile data connection protocols (like EDGE or UMTS) are not open standards. Independent developers and security engineers cannot examine these protocols to see how they are being implemented by mobile data carriers.

In some countries mobile access providers operate under different legislation than internet service providers, which can result in more direct surveillance by governments and carriers.

Regardless of which path you take for your digital communications with a smartphone, you can reduce your risks of data exposure through the use of anonymising and encryption tools.

### ***Anonymity of your Smartphone***

To access content online anonymously, you can use an Android app called **Orbot**. Orbot channels your internet communication through Tor's anonymity network.

Another app, Orweb, is a web browser that has privacy enhancing features like using proxies and not keeping a local browsing history. Orbot and Orweb together circumvent web filters and firewalls, and offer anonymous browsing.

### ***Proxies***

The mobile version of *Firefox* – **Firefox mobile** can be equipped with proxy add-ons, which direct your traffic to a proxy server. From there your traffic goes to the site you are requesting. This is helpful in cases of censorship, but still may reveal your requests unless the connection from your client to the proxy is encrypted. We recommend the **Proxy Mobile** add-on (also from **Guardian Project**, which makes proxying with Firefox easy. Is also the only way to channel Firefox mobile communications to Orbot and use the *Tor* network.

### **12.2.3.7 Advanced Smart Phone Security**

#### ***Get Full Access to your Smartphone***

Most Smartphones are capable of more than their installed operating system, manufacturers' software (firmware), or the mobile operators' programmes allow. Conversely, some functionalities are 'locked in' so the user is not capable of controlling or altering these functions, and they remain out of reach. In most cases those functionalities are unnecessary for smartphone users. There are however, some applications and functionalities that can enhance the security of data and communications on a smartphone. Also there are some other existing functionalities that can be removed to avoid security risks.

For this, and other reasons, some smartphone users choose to manipulate the various software and programs running the smartphone in order to gain appropriate privileges to allow them to install enhanced functionalities, or remove or reduce other ones.

The process of overcoming the limits imposed by mobile carriers, or manufacturers of operating systems on a smartphone is called rooting (in case of Android devices), or jailbreaking (in case of iOS devices, like iPhone or iPad). Typically, successful rooting or jailbreaking will result in your having all the privileges needed to install and use additional

applications, make modifications to otherwise locked-down configurations, and total control over data storage and memory of the smartphone.

**WARNING:** Rooting or jailbreaking may not be a reversible process, and it requires experience with software installation and configuration. Consider the following:

- There is a risk of making your smartphone permanently inoperable, or 'bricking' it (i.e. turning it into a 'brick').
- The manufacturer or mobile carrier warranty may be voided.
- In some places, this process maybe illegal.

But if you are careful, a rooted device is a straightforward way to gain more control over your smartphone to make it much more secure.

### ***Alternative Firmwares***

Firmware refers to programmes that are closely related to the particular device. They are in cooperation with the device's operating system and are responsible for basic operations of the hardware of your smartphone, such as the speaker, microphone, cameras, touchscreen, memory, keys, antennas, etc.

If you have an Android device, you might consider installing a firmware alternative to further enhance your control of the phone. Note that in order to install alternative firmware, you need to root your phone.

An example of an alternative firmware for an Android phone is **Cyanogenmod** which, for example, allows you to uninstall applications from the system level of your phone (i.e. those installed by the phone's manufacturer or your mobile network operator). By doing so, you can reduce the number of ways in which your device can be monitored, such as data that is sent to your service provider without your knowledge.

In addition, Cyanogenmod ships by default with an OpenVPN application, which can be tedious to install otherwise. VPN (Virtual Private Network) is one of the ways to securely proxy your internet communication (see below).

Cyanogenmod also offers an Incognito browsing mode in which history of your communication is not recorded on your smartphone.

### ***Full Device Encryption***

If your phone is rooted you may consider encrypting its entire data storage or creating a volume on the Smartphone to protect some information on the phone.

**Luks Manager** allows easy, on-the-fly strong encryption of volumes with an user-friendly interface. We highly recommend that you install this tool before you start storing important data on your Android device and use the Encrypted Volumes that the Luks Manager provides to store all your data.

### ***Virtual Private Network(VPN) Security***

A VPN provides an encrypted tunnel through the internet between your device and a VPN server. This is called a tunnel, because unlike other encrypted traffic, like https, it hides all services, protocols, and contents. A VPN connection is set up once, and only terminates when you decide.

Note that since all your traffic goes through the proxy or VPN server, an intermediary only needs to have access to the proxy to analyze your activities. Therefore it is important to carefully choose amongst proxy services and VPN services. It is also advisable to use different proxies and/or VPNs since distributing your data streams reduces the impact of a compromised service.

## **ACTIVITIES**

1. Find out more about jailbreaking over internet.
2. Find and use the feature of “off-the –record” option in your chat application and observe what difference it makes.
3. Download and use Skype to make a video call to your friend.
4. Find out more about ***ObscuraCam*** over internet.

## **RECOMENDED VIDEOS**

<https://www.youtube.com/watch?v=KCObM4PBTVk>

<https://www.youtube.com/watch?v=V8bCyRCqK0k>

## References

- Barry M. Leiner, V. G. (s.j.). *Brief History of the Internet*. Onttrek Dec. 20, 2015 uit <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet> available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.
- Bunting, S., & Wei, W. (2006). *The Official EnCE: EnCase Certified Examiner Study Guide*. Wiley Publishing Inc.
- Castillo, F. (2007). *Reshipping Fraud - A Home Business Con*.
- C-DAC. (2014). *National Intelligence Grid : NATGRID*.
- CERT-In. (2014). *Indian Computer Emergency Response Team*.
- Chander, M. (2013). *National Critical Information Infrastructure Protection Centre (NCIIPC): Role, Charter & Responsibilities*.
- Chowdhury, S., Nair, S., & Johnson. (2008). *The curious case of Ken Haywood*. The Indian Express.
- Cone, M. (2011, Dec. 17). *How to Configure Your Mac's Firewall*. Onttrek Oct. 24, 2015 uit MACINSTRUCT: <http://www.macinstruct.com/node/165> available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.
- Cyber Crime Investigation Cell, Mumbai.* (s.j.). Onttrek Dec. 20, 2015 uit <http://cybercellmumbai.gov.in/>
- (2014). *CYBER CRIME, CYBER SECURITY AND RIGHT TO PRIVACY*. New Delhi: LOK SABHA SECRETARIAT.
- CYBER SECURITY MANIFESTO 2.0.* (2012, Oct. 01). Onttrek Sep. 26, 2015 uit cybersecuritymanifesto: <http://cybersecuritymanifesto.com/>
- Email tips.* (s.j.). Onttrek Oct. 29, 2015 uit Digital Survival: <https://survival.tacticaltech.org/internet/email/tips> available under a Creative Commons Attribution-Share Alike 3.0 Unported License.

Farberov, S. (2014). *Russian hackers attacked US financial system stealing gigabytes of data in suspected retaliation for Ukraine sanctions*. Mail Online.

Fisher, M. (2013). *Syrian hackers claim AP hack that tipped stock market by \$136 billion. Is it terrorism?* The Washington Post.

Gallagher, S. (2013, Oct. 02). *We are not who we are*. Onttrek Sep. 26, 2015 uit Security Blog: <https://securityblog.redhat.com/tag/two-factor-authentication/> available under a Creative Commons Attribution-ShareAlike 3.0 Unported License.

Glass, E. (2003). *The NTLM Authentication Protocol and Security Support Provider*. Onttrek Sep. 26, 2015 uit Sourceforge: <http://davenport.sourceforge.net/ntlm.html> available under permission by the owner to use, copy, modify, and distribute this document for any purpose and without any fee.

Gollin, G. (2003). *Unconventional University Diplomas from Online Vendors: Buying a Ph.D. University That Doesn't Exist*.

Gonsalves, A. (2014). *How hackers used Google to steal corporate data*. [www.infoworld.com](http://www.infoworld.com).

Gordon, S., & Ford, R. (2003). *Cyberterrorism?* Onttrek Dec. 20, 2015 uit <http://www.symantec.com/avcenter/reference/cyberterrorism.pdf>

(1998). How Email Works. In P. Grall, *How Internet Works* (bl. 85). Que Corporation.

Gupta, A. (2011, March 01). *Digital Forensic Analysis Using BackTrack, Part 1*. Onttrek Sep. 26, 2015 uit opensourceforu: <http://opensourceforu.efytimes.com/2011/03/digital-forensic-analysis-using-backtrack-part-1/> available under Creative Commons Attribution-NonCommercial 3.0 Unported License.

*Hacker (computer security)*. (Nov.). Onttrek Dec. 20, 2015 uit 2015: [http://en.wikipedia.org/wiki/Hacker\\_\(computer\\_security\)](http://en.wikipedia.org/wiki/Hacker_(computer_security)) available under the Creative Commons Attribution-ShareAlike License.

Havercan, P. (2015, July 17). *A plain person's guide to Secure Sockets Layer*. Onttrek Sep. 26, 2015 uit <http://peter.havercan.net/computing/plain-persons-guide-to-secure-sockets-layer.html> available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Hazen, S. (2014). *Hackers Used Police Tool to Steal Celeb Photos*. NEWSER.

*How do I know if a website is secure?* (2015, Oct.). Onttrek Oct. 29, 2015 uit ccm.net: <http://ccm.net/faq/2-how-do-i-know-if-a-website-is-secure> available under the Creative Commons Attribution - NonCommercial - ShareAlike 3.0 France license.

*How it works.* (2010, Jan. 17). Onttrek Sep. 26, 2015 uit Wikidot: <http://pychatter.wikidot.com/how-it-works> available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License.

*How to Choose an Internet Browser.* (s.j.). Onttrek Oct. 29, 2015 uit WikiHow: <http://www.wikihow.com/Choose-an-Internet-Browser> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License

*How to Clear Your Browser's Cache.* (s.j.). Onttrek Oct. 29, 2015 uit WikiHow: <http://www.wikihow.com/Clear-Your-Browser%27s-Cache> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License

*How to Reveal a Fake Facebook Account.* (s.j.). Onttrek Sep. 27, 2015 uit www.wikihow.com: <http://www.wikihow.com/Reveal-a-Fake-Facebook-Account> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License

*How to Set up 2 Step Verification in Gmail.* (s.j.). Onttrek Oct. 24, 2015 uit WikiHow: <http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License

*How to Set up 2 Step Verification in Gmail.* (s.j.). Onttrek Oct. 29, 2015 uit <http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License.

*Introduction to Digital Forensics.* (2011, Nov. 16). Onttrek Sep. 28, 2015 uit Wikibooks: [https://en.wikibooks.org/wiki/Introduction\\_to\\_Digital\\_Forensics](https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics) available under the Creative Commons Attribution-ShareAlike License

ISFS. (2004, April). *Computer Forensics.* Onttrek Dec. 20, 2015 uit [http://www.isfs.org.hk/publications/ComputerForensics\\_part1.pdf](http://www.isfs.org.hk/publications/ComputerForensics_part1.pdf)

Kaur, R. P. (2013). Statistics of Cyber Crime in India: An Overview. *International Journal Of Engineering And Computer Science*, 2 (8).

*Kerberos Authentication.* (s.j.). Onttrek Sep. 26, 2015 uit Interactiva: <http://computers.interactiva.org/Security/Authentication/Kerberos/> available under a Creative Commons Attribution-ShareAlike 3.0 Unported License

Kessler, G. C. (2001, Sep.). *Steganography: Hiding Data Within Data*. Onttrek Dec. 20, 2015 uit <http://www.garykessler.net/library/steganography.html>

Kessler, G. C. (2005, Dec.). *The Role of Computer Forensics in Law Enforcement*. Onttrek Dec. 20, 2015 uit [http://www.garykessler.net/library/role\\_of\\_computer\\_forensics.html](http://www.garykessler.net/library/role_of_computer_forensics.html)

Kumar, M. (2014). *Xiaomi Phones Secretly Sending Users' Sensitive data to Chinese Servers*. The Hacker News.

Leung, C. (s.j.). *Binding a Corporate Information Protection Strategy*. Onttrek Dec. 20, 2015 uit <http://www.isfs.org.hk/publications/011009/Collins-CIO&CeO.pdf>

Lucas, I. (2009, July 10). *Password Guidelines*. Onttrek Oct. 24, 2015 uit Lockdown.co.uk: [http://www.lockdown.co.uk/?pg=password\\_guide](http://www.lockdown.co.uk/?pg=password_guide) available under a Creative Commons Attribution-ShareAlike 2.0 License

Madhya Pradesh State Cyber Police. (2013). *Recent Examples of Cyber Crime & E-Commerce Fraud Related Investigations in India*.

Mcafee. (2014). *Net Losses: Estimating the Global Cost of Cybercrime*. Santa Clara.

Mehnle, J. (2010, April 17). *Sender Policy Framework*. Onttrek Sep. 28, 2015 uit Openspf: <http://www.openspf.org/Introduction> available under Creative Commons CC BY-SA 2.5

Mrunal. (2012). *National Counter Terrorism Center (NCTC): Meaning, functions, Controversy*.

Nair, S. (2009). *Selected Case Studies on Cyber Crime*.

Nandanwar, R. (2013). *Case Study of Recent Examples of Cyber Crime and E-Commerce Fraud related Investigations involving IPR and Copyright Act*.

Narayan, V. (2013). *Mumbai bank hacked, Rs 2.4 crore siphoned off in 3 hours*. Mumbai: The Economic Times.

Nelson, B., Phillips, A., & Steuart, C. (2009). *Guide to Computer Forensics and Investigations*. Cengage Learning.

*Networking in Windows 7*. (s.j.). Onttrek Oct. 24, 2015 uit <http://www.utilizewindows.com/>: <http://www.utilizewindows.com/7/networking/452-working-with-windows-firewall-in-windows-7> available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

NK, V. (2015, Jan. 24). *A Peek into the Top Password Managers*. Onttrek Oct. 24, 2015 uit opensourceforu.com: <http://opensourceforu.efytimes.com/2015/01/peek-top-password-managers/> available under Creative Commons Attribution-NonCommercial 3.0 Unported License.

Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). *First Responders guide to Computer Forensic*. CERT Training and Education.

*Password Authentication Protocol*. (2015, July 17). Onttrek Sep. 26, 2015 uit WIKIPEDIA: [https://en.wikipedia.org/wiki/Password\\_Authentication\\_Protocol](https://en.wikipedia.org/wiki/Password_Authentication_Protocol) available under the Creative Commons Attribution-ShareAlike License.

Press Information Bureau. (2006). *India-US cyber security Forum - Fact Sheet*.

*PROTECT THE SENSITIVE FILES ON YOUR COMPUTER*. (s.j.). Onttrek Oct. 29, 2015 uit SECURITY IN-A-BOX: <https://securityinabox.org/en/guide/secure-file-storage> available under a Creative Commons Attribution-Share Alike 3.0 Unported License.

*PROTECT YOURSELF AND YOUR DATA WHEN USING SOCIAL NETWORKING SITES*. (s.j.). Onttrek Oct. 29, 2015 uit securityinabox.org: <https://securityinabox.org/en/guide/social-networking> available under a Creative Commons Attribution-Share Alike 3.0 Unported License.

PTI. (2013). <http://www.thehindu.com/news/national/govt-launches-crime-tracking-pilot-project/article4272857.ece>. The Hindu.

Quirk, S. (2014, Mar. 13). *Concordia Password Security Policy*. Onttrek Sep. 26, 2015 uit <http://kb.cu-portland.edu/Password+Security> available under a Creative Commons Attribution 3.0 License.

Ranger, S. (2014, June 09). *Organised cybercrime groups are now as powerful as nations*. Onttrek Dec. 20, 2015 uit <http://www.zdnet.com/organised-cybercrime-groups-are-now-as-powerful-as-nations-7000030323/>

*Recognise scam or hoax emails and websites.* (s.j.). Onttrek Sep. 27, 2015 uit <https://www.communications.gov.au/what-we-do/internet/stay-smart-online/your-identity/recognise-scam-or-hoax-emails-and-websites> available under a Creative Commons Attribution 3.0 International License.

Rocha, L. (2012, Dec. 21). *COMPUTER SECURITY INCIDENT HANDLING – 6 STEPS*. Onttrek Dec. 20, 2015 uit Count Upon Security: <http://countuponsecurity.com/2012/12/21/computer-security-incident-handling-6-steps/>

Rusen, C. A. (2014, Sep. 09). *How to start & use the Windows firewall with advance security*. Onttrek Oct. 24, 2015 uit DigitalCitizen: <http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security> available under Creative Commons Attribution-Noncommercial-Share Alike 4.0 International.

Rusen, C. A. (2014, Sep. 26). *How to Start & Use The Windows Firewall with Advanced Security*. Onttrek Oct. 29, 2015 uit <http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security> available under Creative Commons Attribution-Noncommercial-Share Alike 4.0 International.

*Selecting a strong password.* (2015, Sep. 10). Onttrek Sep. 26, 2015 uit Wordpress: <https://en.support.wordpress.com/selecting-a-strong-password/> available under a Creative Commons Sharealike license.

Shubert, A. (2011). *Cyber warfare: A different way to attack Iran's reactors*. CNN.

Singh, G., Sharma, A., Rampal, K., Kular, R., Gupta, S., Sarita, R., et al. (2013). *India Risk Survey 2013*. Pinkerton and Federation of Indian Chambers of Commerce and Industry (FICCI).

Srinath, B. J. (2006). *Cyber Security Awareness for Protection of National Information Infrastructure*. Dept. of Information Technology. Ministry of Communication & Information Technology, Govt. of India.

Stewart, W. (2000, Jan. 07). *How Email Works*. Onttrek Sep. 28, 2015 uit <http://www.livinginternet.com/>: <http://www.livinginternet.com/e/ew.htm> available under a Creative Commons Attribution Share Alike License

Swain, B. (2009, July). *What are malware, viruses, Spyware, and cookies, and what differentiates them?* Onttrek Dec. 20, 2015 uit <http://www.symantec.com/connect/articles/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them>

Talukder, M. i. (s.j.). *Free Antivirus*. Onttrek Oct. 29, 2015 uit [http://shaifulaueo.blogspot.in/p/free-antivirus\\_13.html](http://shaifulaueo.blogspot.in/p/free-antivirus_13.html) available under a Creative Commons Attribution 3.0.license.

*The Home Computer Security Centre*. (2009, july 10). Onttrek Oct. 29, 2015 uit <http://www.lockdown.co.uk>: [http://www.lockdown.co.uk/?pg=password\\_guide](http://www.lockdown.co.uk/?pg=password_guide) available under a Creative Commons Attribution-ShareAlike 2.0 License.

The Indian Express. (2008). *Latest terror mail traced to Mumbai college*. Mumbai: The Indian Express.

*The Invention of Internet*. (s.j.). Onttrek Dec. 20, 2015 uit <http://www.history.com/topics/inventions/invention-of-the-internet>

*The Telegraph*. (2015, Dec. 06). Onttrek Dec. 17, 2015 uit [http://www.telegraphindia.com/1151207/jsp/business/story\\_57045.jsp#.VnJcINJ95dg](http://www.telegraphindia.com/1151207/jsp/business/story_57045.jsp#.VnJcINJ95dg)

Times of India. (2009). *Another techie held for duping Brainvisa*. Pune: Times of India.

*Tips for buying online*. (2015, Oct. 02). Onttrek Oct. 29, 2015 uit Tips for buying online: <https://www.qld.gov.au/law/your-rights/consumer-rights-complaints-and-scams/consumer-advice-rights-and-responsibilities/tips-to-become-a-smarter-shopper/tips-for-buying-online/> available under a Creative Commons Attribution 3.0 Australia (CC BY) licence.

*Understanding Authentication*. (2008, Feb. 14). Onttrek Sep. 26, 2015 uit Go4Experts: <http://www.go4expert.com/articles/understanding-authentication-t8842/> available under Creative Commons with Attribution Required.

Urbas, G. (2012). Copyright, Crime and Computers: New Legislative Frameworks for Intellectual Property Rights Enforcement. *Journal of International Commercial Law and Technology*, 7 (1), 11-26.

US-CERT. (2014). *Backoff Point-of-Sale Malware:Alert (TA14-212A)*. United States Computer Emergency Readiness Team.

US-CERT. (2008). *Computer Forensics*. Onttrek Dec. 20, 2015 uit <https://www.us-cert.gov/sites/default/files/publications/forensics.pdf>

*USE MOBILE PHONES AS SECURELY AS POSSIBLE*. (s.j.). Onttrek Oct. 29, 2015 uit <https://securityinabox.org/en/guide/smartphones> available under a Creative Commons Attribution-Share Alike 3.0 Unported License.

Verma, D. (2012, Nov. 05). *How To Identify Fake EMail And Trace Sender's Location*. Onttrek Sep. 27, 2015 uit <http://www.usethistip.com>: <http://www.usethistip.com/2012/11/how-to-identify-fake-email-and-trace.html> available under a Creative Commons Attribution 3.0 License.

*What Is A Software Patch?* (2013, Nov. 08). Onttrek oct. 29, 2015 uit OSSWATCH: <http://oss-watch.ac.uk/resources/softwarepatch> available under a Creative Commons Attribution-ShareAlike 4.0 International License.

*Working With Windows Firewall in Windows 7*. (s.j.). Onttrek Oct. 29, 2015 uit <http://www.utilizewindows.com>: <http://www.utilizewindows.com/7/networking/452-working-with-windows-firewall-in-windows-7>

Yasmeen, A. (2013). *Natgrid will deter terror*. The Hindu dated 15 Dec. 2013.

