Internet Privacy and Myths

Third Edition
About the Author

I am holder of Bachelor, Diploma, and Master degrees in the fields of Networking / Telecommunications, Computer Programming, and Technology Management, while I am holding various certificates in the fields of Information Technology and Cyber Security. My research areas are: Cyber Security, Networks, Privacy, Software Development and Social Media. My high education background along with my professional experience made me to write this book to inform the world about the truth, about what is right and wrong regarding internet privacy.

I hope you will enjoy reading my book, for more information about my self and my projects please visit my official web site: http://www.christosberetas.com
# Table of Contents

<table>
<thead>
<tr>
<th>Part</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>PART 1</td>
<td>WORLD WIDE WEB AND PRIVACY</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER 1</td>
<td>Introduction to WEB</td>
<td>2</td>
</tr>
<tr>
<td>CHAPTER 2</td>
<td>Web Surfing and Scripting</td>
<td>8</td>
</tr>
<tr>
<td>CHAPTER 3</td>
<td>Proxy Servers</td>
<td>12</td>
</tr>
<tr>
<td>PART 2</td>
<td>PRIVACY</td>
<td>16</td>
</tr>
<tr>
<td>CHAPTER 4</td>
<td>Phishing</td>
<td>17</td>
</tr>
<tr>
<td>CHAPTER 5</td>
<td>Wi-Fi Privacy</td>
<td>22</td>
</tr>
<tr>
<td>CHAPTER 6</td>
<td>Social Media</td>
<td>25</td>
</tr>
<tr>
<td>PART 3</td>
<td>GEOLOCATION</td>
<td>27</td>
</tr>
<tr>
<td>CHAPTER 7</td>
<td>Smart Phones and Meta Data</td>
<td>28</td>
</tr>
<tr>
<td>CHAPTER 8</td>
<td>GPS</td>
<td>31</td>
</tr>
<tr>
<td>CHAPTER 9</td>
<td>Roving Bug</td>
<td>34</td>
</tr>
<tr>
<td>PART 4</td>
<td>HACKING AND VIRUSES</td>
<td>36</td>
</tr>
<tr>
<td>CHAPTER 10</td>
<td>Keyloggers</td>
<td>37</td>
</tr>
<tr>
<td>CHAPTER 11</td>
<td>System Attacks</td>
<td>40</td>
</tr>
<tr>
<td>PART 5</td>
<td>SURVEILLANCE</td>
<td>43</td>
</tr>
<tr>
<td>CHAPTER 12</td>
<td>Honeypot Systems</td>
<td>44</td>
</tr>
<tr>
<td>CHAPTER 13</td>
<td>Monitoring</td>
<td>47</td>
</tr>
<tr>
<td>CHAPTER 14</td>
<td>Simple Wi-Fi Privacy Hole</td>
<td>50</td>
</tr>
<tr>
<td>APPENDIX</td>
<td>Useful Links and Bibliography</td>
<td>52</td>
</tr>
</tbody>
</table>
Introduction

I hope this book it will pleasant you while reading it. My aim is to inform all of you about the dangers of the internet and the violation of our privacy that happening by various ways everyday and certainly without our permission. Governments and private organizations around the world they would like to know what are you looking for, who you vote, why you bought this X product, what are your habits, what, what, what. Governments they are saying they doing this for security purposes while private organizations they are saying they are trying to “monitor” their visitors or customers for marketing reasons, but is this true?

Book Goals

In this book you will learn the following:

- You are not alone while browsing the web
- They know where are you located
- Anonymity is not always anonymity
- 24th Monitoring

…and many more

Secrets in this book

There are not secrets in this book, there is only one simple example at the end of this book, how easy is to break Wi-Fi privacy.
WORLD WIDE WEB AND PRIVACY

PART 1
**Introduction to Web**

The Internet is a worldwide computer network that consists mainly of Servers, Routers, Switches, other networking devices, and personal computers (picture 1.1 and 1.2).

As the Internet was spreading worldwide have created a standard for the smooth functioning of the world, thereby excludes any incompatibilities. Every computer connected to the Internet has a unique address called **IP ADDRESS** (Internet Protocol Address), picture 1.3 and 1.4, every server, personal computer and every device that connects to the network has a unique **IP ADDRESS** is either dynamic (the IP address is assigned automatically by the Internet service provider (ISP)), or static (the IP address is the same and never changes, after consultations between the client and the internet service provider).
The static IP address is like I know someone always where reside because it is permanent and never changes. But all this would not have any benefit if we do not had the Domain Name Servers (DNS), DNS is an index which undertakes to translate a domain name (for example, www.example.com to an IP address, for example 123.123.23.23 and vice versa), this way we are not obliged to remember always the IP ADDRESS of each Web page (picture 1.5 and 1.6).
An IP address can reveal the country, city and even the home address of the user (picture 1.7).
Also worth mentioning here the **MAC ADDRESS**, which is a unique number and is assigned by the manufacturer of the network adapter card, whether it is wireless or wired. This number is **unique** for each network adapter card and does not change (officially because unofficially can be spoofed) (picture 1.8).

### Internet Service Provider (ISP)

The Internet service providers create a history file for each of their users that is updated each time the user makes any activity on the Internet, this file is named **LOG file** and contains the **IP address** of the user, **MAC ADDRESS**, **time**, **user name**, **date**, and **duration** that have been visit the Web page as well any connections to third systems or networks (picture 1.9).
New versions of software may provide more information. The Government and the Internet Service Provider is given the possibility to request access to personnel file (LOG file) so they can easily know who did what, where and when, especially when involving illegal activities on the part of the user they are able to find very easily the user from the IP address of the computer, or the MAC ADDRESS so by sending the IP address of the computer's or the MAC ADDRESS to ISP asking who user had the specified address the specific time, the ISP will check for the user who is logged on the specific MAC ADDRESS, the ISP will respond with complete details of the user, the information details which have the ISP about the user is from the internet application which he/she made in one ISP to provide Internet connection.
Web Surfing and Scripting

CHAPTER 2
Web Surfing and Scripting

Surfing on the Internet, many people claim that they have not been registered to some online service, can not other people yet the companies and Governments to learn about their personal interests. This is a myth which is unfounded and is already collapsed. Companies, organizations and even Governments which engage in electronic marketing (e-marketing) or not, use their special code on Web pages to collect information from the user preferences, specifically this is accomplished primarily through the use of cookies (picture 2.1).

<table>
<thead>
<tr>
<th>Cookie</th>
<th>Name</th>
<th>Purpose</th>
<th>Further Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siteimprove</td>
<td>exist</td>
<td>This cookie is used to help record the visitor’s use of the website. It is used to collect statistics about site usage such as when the visitor last visited the site. This information is then used to improve the user experience on the website. The cookie contains no personal information and is used only for web analytics.</td>
<td>A persistent cookie, also called a session cookie, a cookie that is stored on a user’s hard drive until it expires or until the user deletes the cookie. Persistent cookies are used to collect identifying information about the user, such as Web surfing behavior or user preferences for a specific Web site.</td>
</tr>
<tr>
<td>Siteimprove</td>
<td>ASP.NET_SessionId</td>
<td>This cookie is used purely to track the sequence of pages a visitor looks at during a visit to the site. This information can be used to reduce user journeys, and enable visitors to find relevant information quicker.</td>
<td>These are session cookies (not persistent), and are cleared (erased) when you close your browser.</td>
</tr>
</tbody>
</table>

Certainly we all noticed and wondered how some days ago and while we looked for something specific on the Internet, and today in the form of a banner on one of the pages we visit which we had before some days informs us that today there is what we looked before few days a go. It is worth noting that the cost of creating a profile for each computer user is too small, the preferences and interests can be stored in a single CD. Certainly we all have noticed that by visiting some of Web pages they show
information about the name of the operating system, the version of web browser we use, what version of java is using our computer, the computer name, etc. this information may simply have informative character for the user about who visits the specific website, but cannot guarantee that the information is only informative and are not intended to create an online profile for users who visit the particular Web page, collecting whatever other information is freely available from the web browser or the operating system of the computer. However, I must point out here that some web pages applying the following 2 techniques, in addition using cookies, they use:

1. Code which during the loading of the Web page downloading files on the user's hard disk in order to gathering info.

2. When the Web page is loading runs a special code that collects user information.

Also when we surfing on Internet, the Internet Service Provider (ISP) is always know what Web pages we have been visit as well as any other computer networks we have been connected.

**Tracking Cookies**

This is the most dangerous issue regarding privacy, tracking cookies are those cookies who track web site visitor activities and send data back to the cookie author. The kind of collected data varied and depends from the cookie designer what kind of data wants to collect and analyze. This kind of cookies are installed on local hard disks of course without any user permission. Tracking cookies have the same logic as other “safe” non-tracking cookies but with an addition to log online activities and send them back to the author for analysis, this kind of data could be the IP Address, Computer Name, Username, etc.
To protect your self from tracking cookies, set your privacy policy about what kind of cookies you accept and clear web browser cookies frequently, I suggest to clear cookies every time the web browser is used and closed.
Proxy Servers

CHAPTER 3
**Proxy Servers (Anonymous Proxy Servers)**

By the use of a proxy server we can dispense the computer home or company network, to connect through our ISP on a third Server (Proxy Server) from which this server we will surf on the Internet and also to run various network applications, when we connect through proxy server maybe the proxy server needs user authorization or maybe is anonymous (not require user authorization), whatever website we visit through proxy server recorded in **log file** of the web server which hosts the web page we want to view the **IP ADDRESS** of the proxy server and not our real **IP ADDRESS** of our network, in this way we can achieve a certain degree of anonymity on the Internet (**picture 3.1**).

The ISP that provides us Internet connection knows that we are connected to Proxy Server but cannot know the activity we do after our connection to the proxy server, our activity as well as the actual real **IP ADDRESS** of the computer and the activities we do is recorded in the log file of the proxy server. The System Administrator who manages the proxy server is able to know the full activities. If the proxy server is claiming full anonymous, that means is **KA** (keep alive), (**pictures 3.2**) that means is not recorded anywhere visitor **IP ADDRESS** and there are not **log files**.
We cannot be sure for the following reasons:

1. There are anonymous proxy servers that appear as anonymous to attract hackers for easy identification. This proxy servers they are monitored by Governments and their services to prevent and detect electronic crimes.
2. There are anonymous proxy servers that belong to the companies, organizations, a court can reveal the true identity of the user who logged on.
3. We are not in a position to know the actual features of one anonymous proxy server, the policy applied by the system administrators, as well as the actual level of anonymity.
4. We do not know if the proxy server keep log file that contains personal data such as hostname, IP ADDRESS, MAC ADDRESS, etc.

**Transparent Proxy Servers**

This kind of Proxy Servers usually but not always listening on ports 80 and 443. It is called transparent because the client doesn’t know that there is a proxy server who mediates their requests. Usually this kind of proxy servers used:

- In ISP to reduce the bandwidth load.
- In Big organizations which the client configuration is complex.
- Their anonymity level depends by who configured the proxy server and its purpose.
**VPN**

A **VPN** network can provide important safety and anonymity because the data that is transferring they are encrypted.

In a **VPN** network we can know which user connected where, but we don’t know what data transferred, our **ISP** knows that we are connected to a **VPN**, but may not be familiar with the data we have been transfer or we will transfer, our ISP only knows that we connect to another network doesn't know beyond the activities with the **VPN** network. Despite the significant safety and anonymity a **VPN** network, the following points are hidden:

1. We do not know if **VPN** administrators have copies of data that we transfer.
2. We do not know if the data transfer to third parties organizations.
3. In the case of anonymous **VPN** network, we do not know if they are truly anonymous, whether a court may compel the organization to give personal information in this case means that the **VPN** organization keeping history.
4. Finally, we do not know if recorded info about our computer and our operating system.
PRIVACY

PART 2
Phishing

CHAPTER 4
**Phishing**

With the help of technology and Internet personal users or organizations trying to access as possible a user's personal data for two purposes:

1. For marketing purposes.
2. For illegal activities.

In the first case sent various e-mails which include links that clicking the user goes to a site depending on the issue of the email and the content and ask from the user while he/she is do click on the link which is included in the email to enter personal info or register in other company services, etc (picture 4.1).

First of all WELCOME to the only email list online that gives you the inside scoop on little-known methods to earn an extra income from home.

... And because you recently visited our website you are qualified as a ‘preferred’ member/visitor to see this...

**Picture 4.1**

So - we've secured permission for you to access this.

>> Click here and access it today.

Have A Great Day!

You need to read necessary the terms of use and if the website is the original and is legitimate before you enter personal info because your personal information, maybe will be distributing to other people or organizations without your permission for marketing or other illegal activities.
In the second case, someone sent fake e-mails that have altered the header from the attacker, the user seems sent it by official source as a serious organization, a Bank, etc (picture 4.2).

Dear customer,

We are glad to inform you that our bank has a new security system. The updated technology will ensure the security of your payments through our bank. Hoping you'll understand that we are doing this for your own safety, we suggest you to renew your account.

Once you have renewed your records, your session will be interrupted and you will have to log in again.

To renew your account information click on the following link:

http://pib-home?message=update_Aid

Note: If we do not receive the appropriate account verification within 48 hours, the account will be suspended. The purpose of this verification is to ensure that your bank account has not been fraudulently used and to combat the fraud from our community.

Best Regards,

Security Advisor

then encourage the user to click on a link contained in the e-mail to give personal information or to confirm his/her self in the system while the Web page being visited by clicking the user is not the official organization from which it appears the e-mail was sent, but it is a fake website which have caused some to collect personal information, such as name, credit card numbers, passwords, names from e-mails, etc. Usually not to suspect the candidate victims, they send an e-mail that appears to be sent from an official source, changing the header of the e-mail to ensure the user will be trust and open the email, when the user reply to this fake email, the email will be sent to a different address, and not the fake address that has the email as the sender, so they invite the candidate to respond to victims simply by e-mail by typing their personal info inside of the email as text and reply. The answer to this type of violation
is blocking real e-mail address that sent the fake email (open the e-mail header), blocking the e-mail address that they use for reply, and report spam. Never click on this links or respond back to this kind of e-mails for an important reason, with the answer we inform them that our email address is exist and used.

**Phishing Detection**

There is an easy way to detect if the e-mail you received is a phishing e-mail message or legitimate. There is a tool by name “Email Authenticator” who is developed by Christos Beretas and by copying the suspicious e-mail headers to this simple tool, it will tell you if the e-mail message is legitimate or not (remember nothing is 100% safe because new techniques are discovering by spammers daily), see the picture 4.3 below for the main tool GUI.

![Email Authenticator](image)
Report Phishing

There are many organizations world wide and federal agencies that you may report phishing activities. I suggest everyone who is received an phishing scam e-mail message to report that scam message to any available organization or federal agency, only by this way we will make a safer scam free world.

Another one option after reporting phishing scam e-mail messages to organizations and federal agencies, is to report also the phishing e-mail message to “Global Spam Tracking Project” (http://globalantispam.1apps.com) Global Spam Tracking Project is a project who is founded in 2014 by Christos Beretas and the purpose is to report hacking attacks and phishing scam messages, is FREE and you may report the activity anonymously.
**Wi-Fi – (Hot Spots)**

The wireless internet without cables offer much more flexibility which is exciting. But it is not as exciting as it sounds because ultimately the risk of data theft is greater than a wired network. An unlocked wireless router can access it by everyone detects the network, giving the possibility to the attacker to have wireless access to the network in conjunction with the wrong configuration of the computer can have access locally if the remote computer connect wired with the wireless router. Some argue that the free internet access via Wi-Fi hot spots offer anonymity and that can not be detected because no one of users accising the network have give persona info, whenever he/she wants to leave and go elsewhere, changing place regularly. This myth has been collapsed for the following reasons:

1. In free access to the Internet (Wi-Fi hot spots) areas usually there are security cameras, so the user is very easy to detect it.

2. Recorded on the wireless router or in another network device the computer components, such as hostname, MAC ADDRESS, username, IP ADDRESS. Etc.

When there is an illegal activity, the network administrator is able to know the above elements of the second (2) case, it is easy to make a cross-checking of information with the aid of the ISP, which will try to identify the MAC ADDRESS of the computer with the already recorded MAC ADDRESSES of all ISPs in the country to detect the attacker (picture 5.1).
<table>
<thead>
<tr>
<th>User</th>
<th>Device</th>
<th>IP</th>
<th>MAC</th>
<th>Log Time</th>
<th>Start</th>
<th>End</th>
<th>Last Activity</th>
<th>Timeout</th>
<th>Downloaded</th>
<th>Uploaded</th>
<th>Download Speed</th>
<th>Upload Speed</th>
</tr>
</thead>
</table>
Social Media

CHAPTER 6
**Social Media**

Most of us now a day we are members to various social media networks for various reasons, for communication, promotion, for fun, etc. All social media networks requires for registration full names, date of birth, location, even home address, then the most of them asking to upload personal pictures, videos, etc. Let’s consider below those things:

- People usually share more personal information in social media networks rather their personal life.
- People doing everything to improve their online reputation while they are not care for the information they are sharing.
- People they use third party applications who collect un-known information for them.
- Social Media Networks tracking customers online activities.
- The data that is entered by the user along with the data that are collected by the social media networks are NEVER deleted and stored permanently in data warehouses.
- Member data are used later for marketing purposes and further analysis.
- Location Tracking.
- Reduce anonymity level.
- Log files with member habits.

Now, what do you think?
GEOLOCATION

PART 3
CHAPTER 7
**Smart Phones and Geolocation**

Now a days everybody enjoying the use of smart phone and their applications, is something amazing to have access to any service from a mobile device and using services that before few years ago it was just a dream. Unfortunately, all this easiness that smart phones offer they have some disadvantages, for example:

- Some applications they are not behave the same as they behave on computer.
- They affecting from viruses, which sometimes they steal personal data or use hidden services with high cost in money for the phone owner.
- Use applications through Wi-Fi or while on the go is insecure because always exist the possibility someone else to steal information, always should do “log out” after completion.
- Some applications they are using by default the “geolocation” service that means while you are using the specific application is detected your current location.

Really, is that bad the geolocation service when using by default on some applications? The answer is YES, because:

- Everyone known where you are located.
- Someone may steal your home because he/she is known where you are.
- You want to have personal moments.
- You don’t want someone else to make a “personal profile” about your self regarding where are you going often and how long you stay there.
- Other people check you, where you are without your permission.
**Meta Data and Geolocation**

When people communicate electronically daily each other they send data that not include only the content but also provide “other data” that contain very useful information regarding the electronic communication. This kind of data may include:

- Physical Location.
- Home Address.
- IMEI.
- Unique Computer Data.
- Device Identification.
- The Message that was sent, and also the time and date.
- Recipient Information.
- ISP’s.
- How and When we check several Applications.

Governments and Organizations world wide they are interesting very much to collect metadata because is a reliable way to build an **e-profile** about people habits and what they like to do. Metadata also can be the key to predict future behaviour. We can not do much here to protect our privacy over metadata. There are some options available for example to Encrypt communication by custom encryption tools (useful for close communication, for example with friends or employees), the TOR project, VPN connections. We can not be sure 100% no one will still metadata or other information (is better to protect our privacy rather do nothing) because we don’t know the technological infrastructure of the other side and what kind of abilities they have.
GPS

CHAPTER 8
Smart Phone location through GPS

There are three ways to detect a smart phone location:

1. By using a radiogoniometer.
2. By using a GPS.
3. By using common cell phone data (without GPS).

In this chapter, I will examine the second option since this handbook base on technologies which they have directs relationship with internet.

Disable your GPS service on your smart phone when you are not use it.

There are three ways of smart phone detection via GPS:

1. When a legal application is installed on the smart phone and posts the location to a specific service.
2. When illegal software is installed on the smart phone and is post somewhere the current location, thus the smart phone is always traceable.
3. When your smart phone have enabled the GPS service for some reason.

In the first case, a legal software application is installed on the smart phone, and posts somewhere your current location or the smart phone respond on specific requests regarding the phone location via GPS. This kind of applications are used when the parents they want to know where they are their kids and install that type of applications on their smart phones.

In the second case, an illegal software application is installed on the smart phone, sometime without asking the smart phone owner if is agree or not for the installation, and send the smart phone location owner to un known servers, including some times other personal data that is collect from the affected smart phone. Usually this kind of applications they are running as “stealth mode”, because the smart phone owner
should not understand that this kind of software is installed and running on the smart phone.

In the third case, some smart phones by default they have active the GPS service, either some application keep it open or the smart phone operating system when it is loading activate the GPS service. But, how someone may find the smart phone location? The answer is following, if a smart phone has enabled the GPS service, by sending data from satellites to the smart phone, at this point it is easy to detect on a digital map the smart phone location, as many satellites send data to the smart phone via GPS service is easier to detect the accurate smart phone location.

In the picture 8.1 below is show how easy is to detect a device with enabled GPS service.
Roving Bug

CHAPTER 9
**Roving Bug**

Now a days almost all we have smartphones with various operating systems. We make phone calls, sharing pictures, listing music, browsing on internet, etc. The most people believe because their device is on their hands and the data are stored locally on the phone and because they have physical access to the phone this data are safe, but it is not.

Intelligence agencies world wide they knew very well that the smartphones will be the easiest way to track people, by tracking people I am not mean only their location, I mean access to your private data without any permission. Intelligence Agencies they can listen everything and they can access any cell phone in the world, but how? There are two ways:

1. Sending SMS message that automatically install spy software.
2. Embeded backdoor software in operating system kernel.

**In case 1:** someone is receiving an SMS message on smartphone the user is open it just to read it and possibly the message says something that you will think is a marketing offer or think is from wrong number or ask you to click on specific web link, by the time that the message is opened is automatically installed a spy software and opened a backdoor.

**In case 2:** There is pre-installed a software embedded at operating system by this way that is almost impossible to understand the code and this part of code is executed only when a unique “incident” will happen and it will activate that part of code.

In both of the above cases, intelligence agencies may access any smart phone and take pictures, record voice, access any data stored in the phone and of course track your current location.
HACKING AND VIRUSES

PART 4
CHAPTER 10

Keyloggers
KeyLoggers

When we sound the word “KeyLogger” is equal to word “break privacy”, a key logger software is the software which is installed on a computer and its purpose is to record each character, number, including any phrase is typed by the keyboard and recorded in log files. Then these data’s are sending to the key logger developer by email or other messaging service, usually this kind of software is installed without the user permission and is running as “stealth mode”. This software can be used everywhere, including in academia and in work places, some times this software is installed on computers that they use the employees of a company because the employers they should be sure their employees they are working or just browsing on internet. The legal way is only when for example a company known about the existence of this software on their systems and its purpose is only for tracking their employees if they are working or no and only for the company purposes, the illegal way is to install that kind of software without the user permission usually by the purpose to track the user personal life. Also, key loggers can be embedded in spyware thus make easy the information will transmitted in unknown third party. Undoubtedly, key loggers violate the user personal life and the privacy. In Picture 10.1 below you can see the key logger log file.
<table>
<thead>
<tr>
<th>Time</th>
<th>Process</th>
<th>Title</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:04:35</td>
<td>explorer.exe</td>
<td>Menu Démarrer</td>
<td>wordpad</td>
</tr>
<tr>
<td>00:04:47</td>
<td>wordpad.exe</td>
<td>Document - WordPad</td>
<td>i'm writing in wordpad</td>
</tr>
<tr>
<td>00:05:04</td>
<td>internet.exe</td>
<td>Internet Explorer ne peut...</td>
<td>revealer keylogger website</td>
</tr>
<tr>
<td>00:05:39</td>
<td>explorer.exe</td>
<td>Menu Démarrer</td>
<td>cmd</td>
</tr>
<tr>
<td>00:05:43</td>
<td>cmd.exe</td>
<td>C:\Windows\system32\cmd\c\</td>
<td>dir</td>
</tr>
<tr>
<td>00:05:48</td>
<td>cmd.exe</td>
<td>C:\Windows\system32\cmd\</td>
<td>dir</td>
</tr>
<tr>
<td>00:05:59</td>
<td>cmd.exe</td>
<td>C:\Windows\system32\cmd\</td>
<td>ipconfig /all</td>
</tr>
<tr>
<td>00:06:26</td>
<td>explorer.exe</td>
<td>Menu Démarrer</td>
<td>notepad</td>
</tr>
<tr>
<td>00:08:00</td>
<td>notepad.exe</td>
<td>Sans titre - Bloc-notes</td>
<td>les dead keys fonctionnent : âûèêà~yêç...</td>
</tr>
</tbody>
</table>
CHAPTER 11
**System Attacks**

Some organizations in the world they store personal and confidential information on the same server who run web server or any other kind of server system. They are applying security policies and they are trying to hide confidential data behind firewalls and vpn connections. THIS IS WRONG!

How many vpn systems compromised until now? Many! How many security policies have been compromised? Many! How many firewalls have been compromised? Many!

Imagine an organization who have 5 servers and 1 server who is the web server, the 6 servers communicate each other by VPN and behind firewall, do you believe is that network safe? If you believe that network is safe, then you should answer your self, how confidential information released until now which those information are not stored in the same web server but the web server was behing firewalls and VPN connections?

NOT connect the server who is the web server with other servers, and never store in that server who act as web server confidential documents. Neither firewalls and VPN may keep you safe, when a vulnerability will discovered no one will notify you and your confidential information will be on high risk.

The encryption is also an important part, it is very nice idea to use customized encryption tools to encrypt all sensitive data. Below are the three steps someone may follow:

1. Adoption of responsible and safe behaviour practices.
2. Provide guidelines and practices required to protect the IT infrastructure of the organization.
3. Creating a stronger safety culture, with broad understanding.
Below are my recommendations regarding security and privacy.

1. Systematic evaluation and assessment of the risks related to ensuring information accuracy.

2. Protection of resources and throughput information within and outside the organization (external organization services).

3. Development, maintenance – improvement, applications, systems and services.

4. Continuous updating of management and staff about information security issues and patches.

5. Control of information exchange and data.

6. Direct users support and identify security holes.

7. Strong data encryption by using customized encryption tools.

8. Commitment to the faithful implementation of Security Policies.

9. Frequently research for software or other services that may improve not only the quality of work but also the security.
Honeypot Systems

CHAPTER 12
**Honeypot Systems**

Don’t believe easy what other says and not follow them, trust yourself. This is my advice. Honeypot systems are this kind of systems who act as an extra layer of security, if we can say that. Their purpose is to track users activity of course without user permission, is similar like a trojan horse virus who might be a computer game and while someone is playing a backdoor is opened and the hacker have remote access to the computer.

I will mention one real life example, there are available world wide many anonymous proxy servers, with high anonymity, even they offer keep a live anonymity level, people world wide they use them because they believe their ISP or other intelligence agencies may not track their online behaviour, they are using those anonymous proxy servers to access their e-mails, to do banking transactions, to work remotely and to do other online activities. How many of those people do you think they know the proxy server who are connected is safe or honeypot? NONE!

An another personal example, one day I find a list of world wide anonymous keep a live proxy servers, I am just testing their ip addresses by using the network tool “Apokalypse” that is developed by Christos Beretas, I find a keep a live anonymous proxy server who responded back with name “honeypot-xxxxxx” replace xxxxxx with numbers.

I Don’t want to think how much is on risk the user who is used a honeypot proxy servers to have access to its bank account or to other sensitive data.

Proxy Servers which there are everywhere are unknown origin and we never known who is behind and the purposes.
Honeypot systems are also used as “virtual” systems to track attackers, an attacker may think is trying to hack a real system, but in reality is trying to hack a virtual honeypot system, some people also call that systems “Iron Boxes”. 
**Monitoring**

Governments and organizations they are monitoring people for different reasons. Governments monitoring people for security, they like to know who is that person, why buy this product, how much money spend and how much money earn. Organizations they are monitoring employees because they want to know if they are working, how fast they are working, where they are spending their time, also they like to collect personal data for example passwords for e-mails and other services, people usually at work they believe because there are many computers and many people, just there is an internet connection for the organization to just do the work and none care if someone is productive or not, of course not all companies are the same.

There are organizations who collect private information while someone is start browsing their website, and they collecting personal information such as how many minutes someone stayed on the website, how is came here, ip address, mac address, computer name, browser information, location, what is type for search, etc.

The history of monitoring is not recent, is began many years a go and started from the Governments who like to track their citizens behaviour and monitor their transactions. For example the “Carnivore” system who is installed in 2000 in USA in many Internet Service Providers to collect and analyze data.

**The PRISM project**

The PRISM project is the current surveilance project for resource collection and management. Its target is the American servers because the world traffic pass through the servers who are based in USA. Prism analysts they have full access to monitored data, and permit them to search data for specific period of time. I will not mention
much here about the PRISM project, the PRISM project possibly work as you can see in the example **picture 13.1** below.
**Wi-Fi Privacy Hole**

The incredibly rapid of technological developments in wireless networking, coupled with free wireless networks significantly decreased the level of security and Internet Privacy, as I mentioned above, the free wireless networks are attracting more and more computer users believing that Web surfing without anyone can detect them because they have not been registered in the system as users. In many areas of wireless free Internet access there are cameras, but not at all points. On subsequent rows I will describe a way you can with proper attention to browse the Internet through a free wireless network anonymously by 99%.

1. **Choosing a place where there are no cameras.**
2. **Change the computer name, changing user name, changing the geographical location on the computer.**
3. **Disable the existing on board wireless network adapter card.**
4. **Clear history and cookies from your Web Browser.**
5. **Use external (USB) wireless network adapter card that it is not used again (so that there is not somewhere else recorded the MAC ADDRESS).**
6. **Use of external (USB) wireless network adapter card to connect to the wireless network for free.**
7. **The external (USB) wireless network adapter card will be used only for free access and only to wireless networks.**
Useful Links

I am recommending some useful websites here that you can download usefull and freeware software applications that will help to do many tasks, but also you can keep learning more about information technology and cyber security.

3. http://independent.academia.edu/ChristosBeretas

For those who have LinkedIn and Twitter, and they are interesting to connect with Christos Beretas, they can visit his profile below:

- http://gr.linkedin.com/in/christosberetas
- https://twitter.com/c_beretas

Bibliography

- Jeffrey Hunker. 2010. Creeping Failure: How We Broke the Internet and What We Can Do to Fix It. McClelland & Stewart.