International Research Journal of Advanced Engineering and Science
ISSN: 2455-9024

A Study on Safety & Modern-Anonymity

Gaurav Kumar Roy
BCA, C|EH, ECSA, CHFI, OWASP10, Diploma in DIS, Technical writer, New Delhi, India
Email address: gauravkxj62@gmail.com

Abstract*— *This research article convey the tricks & techniques of staying anonymous online using some special tools & programs.

Keywords*— *Protocols, security, anonymity, browser, server, downloads.

I. Introduction

Today, most of the computer users have the knowledge of using Internet, which is the global interconnection of computers that uses internet protocol suite such as TCP/IP protocols to connect billions of devices world-wide. These users share information, chat online, listens to songs, download files etc. But these users are not aware of the fact that they are under continuous surveillance, i.e. all of our online privacy is under inspection & supervision. Our ISP, advertisers, government of different countries, different intelligent agencies & hackers all around the world are eagerly in search of the facts that we are up to while browsing the web. So we have to maintain our anonymity. Anonymity with respect to internet can be defined as the condition of staying anonymous and protect yourself from being observed from strangers. There are plenty of tools and device used by government and agencies to pry eyes of your traffic. As we hear about NSA (National Security Agency), other government agencies and the hackers they hire skulk like a shadow and steal sensitive information regarding what we browse, what we need, what are our likes and dislikes. For some people, internet is an intimidating place. So I've made some research points on how to stay safe online without being afraid. Though complete anonymity is impossible for someone to build but there are some methods which can increase the online privacy of yours. Some methods are complicated, some require IT skills; but if you're serious about privacy then these methods will prove fruitful and will benefit you to stay anonymous in the open web.

II. Use of Antivirus & Firewall

Every user must protect their PC using famous and renowned antivirus & firewall as security. Users can use the best antivirus which mostly depends on user's choice. According to my survey & research, Kaspersky & Norton are the best. But Kaspersky has better facilities & provides an overall protection. Using either of them we can get spyware protection, live website protection, virus protection and protection from unsafe websites also. To make safety and security strong, users can buy hardware firewall at $50 and above. Hardware firewalls not only protect user's PCs but also protects all the networked devices that are connected to the internet. There are other small tricks that internet users must know to keep themselves safe from being hacked. These are:

i) Avoid using same password for all social media sites and email account sites.
ii) Download files from secure servers.
iii) Avoid clicking unknown links to stop spreading viruses on your computer.
iv) Try avoiding those shortened URLs which can be malicious.
v) Be cautious while shopping from online sites; check for https & SSL securities.

III. Anonymize Yourself

i) *TOR Browser*: If you want to browse anonymously, the best solution is the Onion Router. It uses a large collection of computer's network to route the internet sending & receiving through a number of encrypted layers to conceal the source of the traffic. So to download Tor Browser, follow the link:
https://www.torproject.org/download/download.html.en
The onion routing implies the encryption in the application layer of a communication protocol stack. This is named 'onion' because of the nesting of various layers of encryption including the source and destination IP addresses many times and then transfers it through a virtual circuit which randomly selects the Tor relays. Tor browser is the customized version of Firefox.

ii) *VPN*: If you are serious regarding anonymity and wants to keep your privacy to an optimum level, invest your money to buy a VPN (Virtual Private Network) solution. Two best VPNs are Private Internet Access and Tor Guard. These services promptly allows users to stay anonymize & disguise the traffic. These VPN provide advantages by hiding your IP and create an indecipherable traffic which your ISPs and government agencies cannot seize. VPN are by far the best tool used for bypassing censorship & snooping.

iii) *Testing the DNS Leak*: Even though users may use privacy services like VPN and Tor Browser, to hide the IP address, it may still be possible to get the identity via DNS Traffic. But there are tactics through which we can detect whether our configuration is leaking DNS information or not. Simply get to the link: www.DNSleaktest.com & run the test for checking DNS information leakage. If a result is showing a 3rd party program that the user is using such as Tor, VPN, proxies etc, then it is OK, else the ISP's DNS information will be shown which means that the user has a DNS leak. To fix this problem, use the software – 'DNSFix.exe' (download it from: https://dnsleaktest.com/dnsfixsetup.exe).

iv) *Use virtual machine*: It is to be noted that, your browser is not the only criterion for a 3rd party to invade your privacy.

Many files have a malicious program attach which infect the computer. So to prevent any sort of unintended breach of privacy users should open files in a virtual machine.

v) *Secure web mail with extension*: If you're use a popular webmail service such as yahoo mail, Gmail or Rediff mail & cannot switch to services which are more secure or with high privacy, then install the extension – 'Mailvelope'. It is an extension we can install in Mozilla and or Chrome which provides OpenPGP (Open Pretty Good Privacy) encryption to the web mail services. 'SecureGmail' is another such extension which provides encryption in emails send via Gmail. 'Hushmail' is another one which also provides private email account.

vi) *Incognito mode*: is the most basic & easy-to-use privacy mode. This option is available in most popular web browsers such as Internet Explorer, Google Chrome, Safari, Mozilla Firefox, Opera etc. Using this option of private browsing, the browser won't store browsing history or cookie. But this doesn't securely hide the identity or browsing activities.

vii) *Blocking 3rd party cookies:* These are the most common way of getting a track of your browsing habits. Every major web browsers offer the ability to turn-off tracking cookies. Otherwise it would be hard by advertisers to monitor which pages you visit.

viii) *Block & manage trackers*: The trackers are invisible and most people aren't aware that they're being tracked or their browsing habits are collected by unknown means. 'Ghostery' is a free extension available on all web browsers which you can install to reveal these trackers or web-bugs & can then block which ever seems uncomfortable.

ix) *Proxy server*: Online activities & browsing can be processed via proxy servers which act as an intermediary between your computer and the internet. This can be a good way to maintain the online anonymity to basically mask the IP address with its own. If the proxy is based from a different country then your own, you can easily trick advertisers & trackers from tracking the browsing contents.

x) *Use alternative search engines*: As most people use Google as their first preference in case of search engines. Though Google is undeniably the accurate, fast & efficient search engines, Google keeps a track of your search habits in various ways, including browser cookies. So, I prefer to use another search engine which is far efficient and fast plus emphasizes on protecting searches and maintain privacy & avoids filter bubble of personalized search results. It also provides searched information from the best sources rather than from the most sources. It also stops websites from delivering ads and useless links.

xi) *Security focus operating system*: 'Whonix' is an operating system which focuses on anonymity, security & privacy. It is an open source OS and is based on Tor network, and is too convenient for normal use with privacy. Whonix runs in 2 parts: - 1st one solely runs Tor & acts as gateway. The 2nd one is completely on an isolated network. Download this OS from whonix.org.

xii) *Make your own web browser*: By making your own browser, users can secure themselves from getting traced by advertisers and tracers.

To make your own browser, you need to have a programming knowledge. Since you have to create windows based application, take either C#, VB, VB.Net or other such programming language to develop a simple working web browser.

If you take Visual Basic (VB), it will be easier. Take a form and place a web browser control. Take a text-box to place the URL for searching which will act as your address bar. Take a progress bar to see the URL's browsing search progress.

A simple code is given: -

```
Private Sub vkCommand1_Click()
Me.WebBrowser1.Visible = True
Me.ProgressBar1.Value = 1
For i = 1 To 10000
Me.ProgressBar1.Value = i
Next
WebBrowser1.Navigate (Me.Text1.Text) &
(Me.Text2.Text)
End Sub
```

Gradually you can modify your browser by adding back and forward buttons also.

For back Button the code is: -

```
Private Sub vkCommand3_Click()
On Error GoTo noback
WebBrowser1.GoBack
Exit Sub
noback:
MsgBox "NO URL IN HISTORY LIST", vbCritical
End Sub
```

For forward button the code will be: -

```
On Error GoTo noF
WebBrowser1.GoForward
Exit Sub
noF:
MsgBox "NO URL IN HISTORY LIST", vbCritical
End Sub
```

IV. Conclusion

So, for every user–browsing anonymously and maintaining the privacy is important and for this, reason every users must know the interior corners of how to keep their privacy and personal information secure.

Acknowledgement

I would like to thank my parents & friends for supporting me to write this research paper.

References

[1] Anonymity on the Internet by Jacob Palme
[2] www.infoworld.com
[3] www.theguardian.com

[4] Managing anonymity and confidentiality in social research – by: G. Crow