Identity Protection during the use of Internet

Navin Kumar Agrawal
Assistant Professor, GLA University Mathura, (U.P)

Email: navin.agrawal@gla.ac.in

Abstract. In today’s era, security become important concern. As we are moving towards the digitalization data protection is important issue. To make the data as well system safer we must follow some simple but important steps. These steps works just as safe guard. The concern regarding use of internet become more when we are making digital payment or sharing some useful information. More awareness is also required in case of non-technical person whenever use the internet. In this era technology is reachable to every person. We also execute many financial activities through our mobile / Computer. So many observers are there who are regularly keeping any eye on our activities and never miss our single loophole. Some simple Dos and Don’ts can make the difference and create awareness in the society.

Keywords: Cyber security, IP Address, HTTP, Cookies, Browsing.

1. Introduction

Every incident that effects in unauthorized access of data, software, system devices, networks such as routers and/or bypassing their underlying security mechanisms is a security breach.[1] A security breach arises as soon as an unauthorised person or applications illegally go into a logical IT range which is private, confidential, trusted or unauthorized.

To protect our identity on internet we must do following act on regular interval of time.

- Never enter your wealthy information on social sites.
- Make settings of your social media account(s) in a way so that except your friends no one would be able to see your personal information.
- Always check the website you are opening is secure (https://).
- Always sign out your account after completion work.
- Never create your account on unfaithful sites.

2. Many ways website track you

Generally, you do many things on internet and delete your search or browsing history from your computer system. By doing this you think that no one can track you but in this way you are absolutely wrong. There are following ways that a website can track you.

1. IP Address

Suppose your friend is working on your computer system and he forgets to log out his account and you do any unlawful act from his account [3]. Your each activity on internet is being recorded and can be tracked by a website very easily.

2. Cookies and tracking Scripts

Basically cookies are small data files, which is generated by a web page and sent to your browser. Private browsing will provide you control over which kind of cookies you will accept. If you don’t want to allow cookies then you may disable cookies.[2]
Tracking script is used to identify that how many people are using your site and their characteristics. Tracking scripts are designed in a way that they can be downloaded and cached safely in browser. There are so many built-in browser options which may safes us from tracking.

3. **HTTP Referrer**

HTTP (Hyper Text transfer Protocol) Referrer is an identifier. It records the information about the people visiting your website, from where they are coming. Basically, it is in the form of URL (Uniform Resource Locator). Suppose you are visiting a page and click a link that navigate to you on another site then that site (on which you are now) may record your original place of coming. Generally,

4. **Super Cookies**

Super cookies are different from general cookies. Super cookies are the type of browser cookies designed to be permanently stored in browser. Now technology has progressed and detection and deletion is being easier day by day. Super cookies perform same function like general cookies.

5. **User Agent**

We access internet through a browser and each browser works as an agent for us. When we access a web page through our browser then the information about browser and operating system is given to server [1]. A user agent header field contains information about the origination of request and provides it to server.

3. **We can do followings for safe browsing**

1. **Anonymous Browsing**

If you want that no one should gather information about you, then this a way for you. If a user wants to hide all these details then he may go for anonymous browsing [2]. Anonymous browsing can be achieved by using proxy server of VPN (Virtual Private Network) server.

2. **Private Browsing**

Mostly browsers allow private browsing. Private browsing allows you to browse the internet or visiting the websites without saving your history. In this mode of browsing no one would be able to track your page visited history. Private browsing never saves your password, cookies, and visited pages etc.

3. **Incognito Browsing**

Different browsers have different way to activate incognito mode. This mode of private browsing is good when you work on a sharable computer. Incognito mode will not save your cookies, your browsing history, and your entry details.

4. **Virtual Private Network**

It is a type of private network that is built over Public Network [6]. VPN allows user to send data privately over a public Network. VPN keeps your web browsing secure over public network.

4. **Confidentiality of information**

When we talk about the confidentiality of information that means we are talking about the protection of information from the unauthorized access only the person who has key would be able to access the information [5]. Vice versa of this, means conversion from cipher text to plain text is known as decryption.

5. **Online Safety**

We should always remember that minimization of risk maximize safety [6]. The meaning of online safety is to rescue from several frauds/Phishing. Risk to online safety may occur in various ways. To minimize the online risk you should do following things.

- Ensure that information is being forwarded to intended person only.
- Never make your information publicly.
- Alter your password on regular period of time.
- Restrict visitors to access information from your social networking sites.
- Use online transactions with trusted sites only.
- Pay special attention during the downloading from internet.
6. Damaged Caused by Malware
There may be different types of damaged caused by Malware. Followings are major damages that may occur in system due to Malware.

- Hardware Failure
- Corruption of Software
- Data Formatting

7. How to help protect yourself from a security breach
Your own data is in a great deal of spots, incorporating with government organizations, human services suppliers, budgetary establishments, and stores. There's very little you can do to forestall a security break at any of those spots. Be that as it may, you can do a few things to help ensure yourself when a break happens [4].

Here are a few points to remember,
- Use only website which having “Https”.
- Update device regularly.
- Stay informed in case of if required.
- Look Sign up/Sign in credentials

8. 3 Stages to better protect
1. Plan ahead.
Its value is your own information [8]. Help guard through as little sharing by way of conceivable. Watch for key values such as your SSN or aadhar number in case of India. Consider the offshoots of providing organizations, computer app makers and social media platforms with your personal data. Read privacy policies and seek assurances that they will protect your data [9].

2. Be proactive.
When a security breach happens, it is important to know what is being exposed to sensitive data and what you can do to better protect yourself. This could include changing your account passwords.

3. Follow up.
Here's the thing: If your personal information is compromised, you can face the short- or long-term consequences. Soon afterward, you can detect suspicious charges on a credit card. That could be easy to spot and be careful of. But information frequently stolen does not surface on the dark web for sale until months or years after a data breach.

Table 1. Reserve bank of India report

| Year | Cyber fraud cases |
|------|-------------------|
| 2016 | 1372              |
| 2017 | 2059              |
| 2018 | 5917              |

Figure 1: Cyber fraud cases in India
Table 2. Person Arrested by Age group Under Cyber Crime (IT Act + IPC Section)

| Crime                                                      | Age below 18 | Age 18 – 30 Years | Age 30 – 45 Years | Age 45 – 60 Years | Total (all age group) |
|------------------------------------------------------------|--------------|-------------------|------------------|------------------|----------------------|
| Hacking with Computer Systems                              | 2            | 24                | 20               | 2                | 48                   |
| Obscene publication/transmission in electronic form         | 0            | 61                | 18               | 7                | 86                   |
| licence or Digital Signature Certificate by misrepresentation/suppression of fact | 0            | 7                 | 4                | 0                | 11                   |
| Tampering computer source documents                        | 0            | 1                 | 1                | 0                | 2                    |
| Criminal Breach of Trust/Fraud                             | 1            | 13                | 49               | 22               | 85                   |

Figure 2 Person Arrested Under Cyber Crime (IT Act + IPC Section) By Age Group

9. Conclusion

After this study we can say that more awareness are required in terms of using technology, although sufficient provisions are available for punishment of cyber criminals. Data taken from National crime records bureau shows that more awareness are required. We must be aware with all and should spread awareness in society. Awareness is the only remedy to be safe in cyber world. That awareness may be
related to security tools or cyber laws. Every victim must complaint against crime to appropriate authority under defined rules/law in IT Act. Every Internet user should report to appropriate authority against any unlawful activity. Proper reporting of crime will also help to find motive behind that.

References
[1] R. M. Kamble, “cyber law and information technology” International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 789 ISSN 2229-5518.

[2] Agrawal, N.K., Kumar, A., Khatri, A., Gaur, G., “Facial image Classification based on Gender,” International Journal of Advanced Science and Technology, vol. 29, no. 3, pp. 3890-3896, 2020.

[3] N Agrawal, Arpit jain, ambuj agrawal, “Simulation of network on chip for 3D router architecture” International Journal of Recent Technology and Engineering, vol. 8, no.1C2, (2019), pp. 58-62.

[4] Agrawal, N.K., Singh, V.K., Parmar, Singh, D., Agrawal, M, “Design and Development of IoT based Robotic Arm by using Arduino” in Proceedings of the 4th International Conference on Computing Methodologies and Communication, ICCMC 2020., march, 202020, pp. 795–799.

[5] International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 06 | June -2017, A brief study on Cyber Crime and Cyber Laws of India

[6] Jigar Shah, “Study of Awareness about Cyber Laws for Indian Youth” International Journal of Trend in Scientific Research and Development, Volume 1(1), ISSN: 2456-6470, A.

[7] Navin Kumar Agrawal, Vinay Kumar Singh, Vinay Singh Parmar, Vijay Kumar Sharma, Dipti Singh, Muskan Ag,” Design and Development of IoT based Robotic Arm by using Arduino” 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)march 2020.

[8] Jadeja Prithviraj Manubha,” Cyber Crime and Cyber Law under Information Technology Act 2000 “ Research Review International Journal of Multidisciplinary, ISSN 2455-3085 (Online).

[9] M. Krishnasamy, Pradeep Kumar Verma, Vivek Mishra, Navin Kumar Agrawal, Garima Mathur, “A Novel Stochastic Model For Grouped Weighted Multilevel Space-Time Trellis Codes For Rayleigh Fading Channels” International Journal of Computer Networking, Wireless and Mobile Communications ISSN 2250-1568 Vol. 3, Issue 4, Oct 2013, 135-140.