

## **Data Security: Data Breach by Free Websites and Applications**

***Oseni Rayhanat Olatundun<sup>1\*</sup>, Oseni Abdul-Quadri Olayinka<sup>2</sup>***

<sup>1</sup>*M.Sc. IT Student, Gulzar Group of Institutes, Khanna, Ludhiana, Punjab, India.*

<sup>2</sup>*HND Graduate, Surveying and Geoinformatics, Federal School of Surveying, Oyo, Oyo State, Nigeria.*

***\*Corresponding Author***

***Email id: rooseni@student.lautech.edu.ng***

### **ABSTRACT**

*This paper talks about data security which is the protection of data from unauthorized access. It defines data insecurity as unauthorized access and collection of data with or without the users' knowledge. It explains how data are collected from the internet and through applications some of which are; Adware, Spyware, Browser Hijacking Software, Browsing History, In-Website Browsing History. It goes further to list what data can be collected by a website or an application with pictorial examples. This paper identifies the methods of preventing data breach, for example; Using internet anonymously, Authentication, Elimination of Third-Party Cookies, Use of Privacy Extensions or Add-Ons, Use of safe search engines, Encryption method and Firewall.*

***Keywords:*** Data security, Adware, Spyware, Browser Hijacking Software, Browsing History, In-Website Browsing History.

### **INTRODUCTION**

Information technology has made life a lot easier for people. It makes it easy to gain access to information that before would have been impossible. With information technology, came the internet. The Internet has affected our way of life both positively and negatively. It has made it easy for us to contact our loved ones through the use of social media, mobile phones, email, etc. It has virtually infiltrated every sector of our lives; the educational sector, the health sector, the food sector, the agricultural sector, engineering technology sector, etc. The internet makes use of the World Wide Web (WWW), one of the many utilities provided by the internet, to search, upload and gain access to information by the user. But because of that, personal data or data from databases have been compromised due to ease of access. The most common source of data insecurity is the internet because through the internet, you can gain authorized or unauthorized access to a person's data by collection the person's

browsing history, data uploaded on the web browser etc. using the internet, we download applications for various use in our laptops, mobile devices, desktop computers, etc. Data security is the protection of data whether it is personal data, company data or a country's data from unauthorized access by a person, organization or country. It can also be defined as keeping data stored in databases, computers or data of websites safe from cyber-attacks, data breach and loss. When data is security is breached, we say that our data has been compromised and our privacy has been invaded.

One of the fundamental human rights is the right to privacy. This right is enshrined in many constitutions across the globe. The United Nations (UN) Human Rights Committee saw the need for data protection laws as recognised by the International Covenant on Political and Civil Rights (ICCPR), fundamental rights to privacy, Article 17 (A Guide for Policy

Engagement on Data Protection. Privacy International August, 2018).[1]

The ICCPR states that *“The gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.”* [7]

This paper talks about the collection of user(s) data by websites or applications. It's understandable as human beings that we are attracted to free things because we don't have to pay for products and services provided. But unknown to us, most especially the laymen of the information technology world (IT), these free websites and applications are not really free. They gather user's data for sale to interested third party buyers with questionable intentions.

### **DATA SECURITY**

Data Security is the implementation of appropriate administrative, technical or physical means to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data.[3].

According to Techopedia (2019), "Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption." [2].

Data insecurity or data breach is a security incident whereby data from databases are accessed without authorization or knowledge of the data or system owner. A data breach can also be termed as data invasion whereby the privacy of the system owner is invaded upon because most breached data are made known to the public.

While it's true that data security is an unauthorized collection and access of our data, sometimes, we unknowingly give our consent to these information peddlers simply by agreeing to some terms and conditions given to us by websites we visit or some applications we want to download. In fact, some applications or websites make it so that without agreeing to these bogus conditions, you can not visit the websites nor download the desired applications.

### **INTERNET, SOFTWARE APPLICATIONS AND DATA COLLECTIONS**

As stated earlier, there are different ways data are collected and access via the web. According to [4], the following are some of the ways data can be accessed from the computer or database. These are:

- **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. Adware is financially supported by the organizations whose products are advertised.
- **Spyware:** This is a type of malware that is downloaded and installed on the target computer by downloading free application programs (games, movie apps, editing tools, web browser apps, social media apps, etc.) from the internet with the sole purpose of stealing sensitive information from the computer with or without the

permission of the user.

- **Browser hijacking software:** like spyware, these are also downloaded and installed from the internet along with free software. These are malicious software that are installed without the user consent and they change the settings of the user's browser and redirect links to other sites. The site the user is being redirected to might be an unsecured site which contains harmful contents.

Other forms of data collection are:

**Browsing History:** websites track the browsing history of users in various ways to gather information and the information are used for advertising purpose and often illegal purpose. Websites track history directly from the user's computer using tracking cookies that can be stored on the computer. If you do not want your history to be tracked through the cookies, all you have to do is to set your browser to reject the tracking cookies. You can also use privacy plug-ins to help you counter these cookies so that your information and browsing history is not stored.

**In-website browsing history:** This is another way of gathering information through websites that users have accounts with. For example, LinkedIn, Facebook, Quora, Instagram, E-mail, eBay, Amazon, Kindle, Harlequin, etc. where users have to create account to avail themselves of these websites' full functionalities for a better browsing experience. Some websites ask for users' locations and track the users' locations using this information.

### **INFORMATION A WEBSITE CAN COLLECT**

A website can use cookies to track your browsing history, ad preferences to let advertisers know:

- who you are,
- where you've been,
- who you've been talking to and,
- what you're interested in,
- the searches you make on Google,
- the places you check into on Facebook and
- the posts you share on Twitter (unless your profile is private and not public).
- Your Email address [5]

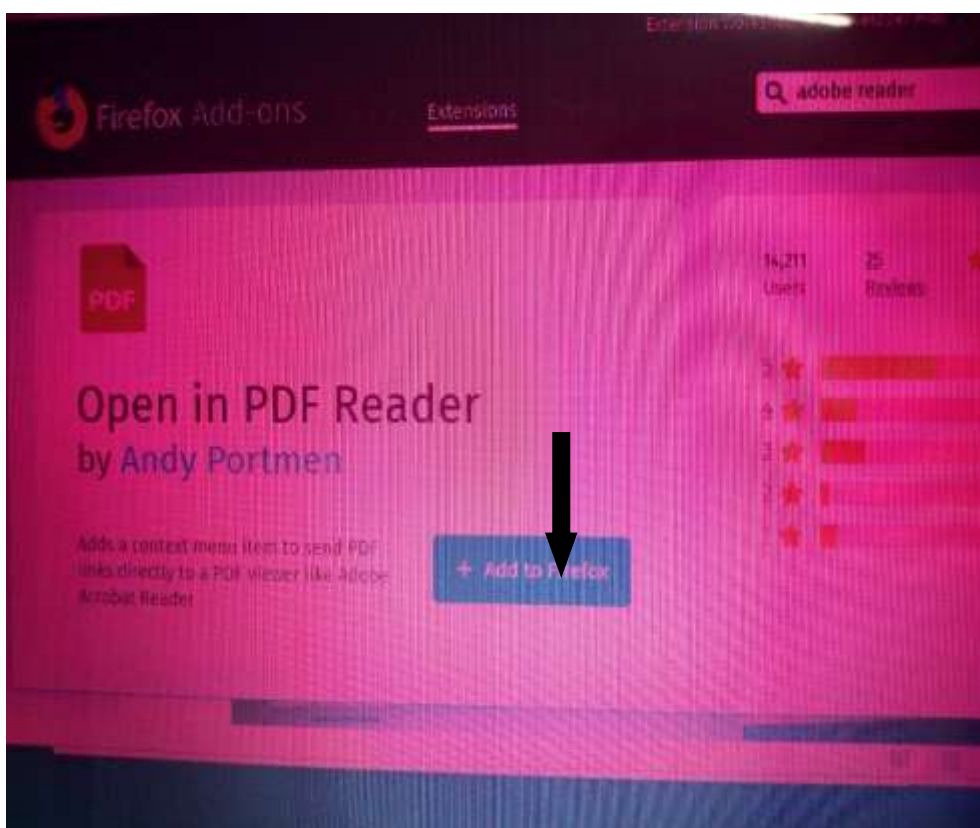
While downloaded Applications can access personal information when the user gives access permission:

- Your Email address(es)
- Your phone contacts and call records
- Your text messages (SMS)
- Your location
- Your Date of Birth, Height, Weight and Health Status
- Your social and educational backgrounds.

Even though there are terms, conditions and privacy policies the users can access at any time, they are sometimes not easy to understand by the users and this gives these websites and applications more loopholes to exploit on how to use the data collected.

Applications also exploit users trusts in a way that the users have to click on "I agree or Yes" before they are able to download the applications and users who are in need of said applications agree without second thought unless the user is someone who has an awareness about third party data collection, such a user will definitely click "I disagree or No". Free applications are notorious for these; they allow users to download or access their applications for free and in return, they collect users' data with or without the users' knowledge.

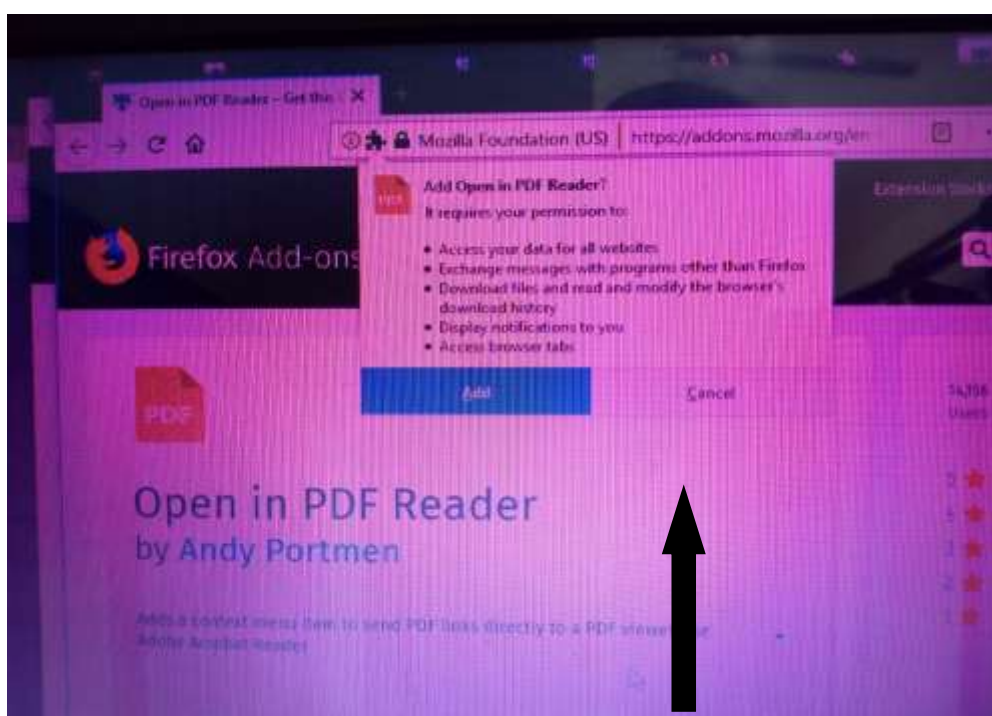
An example is shown below with the aid of two pictures:



**Fig.1:-** Webpage showing the “+ Add to Firefox” box.

In Figure 1, the user wanted to add a PDF Reader as an extension to the web browser Mozilla Firefox. There on the webpage is

the “+ Add to Firefox” box as indicated by the black arrow.



**Fig.2:-** Webpage indicating the black arrow above asking the user permission



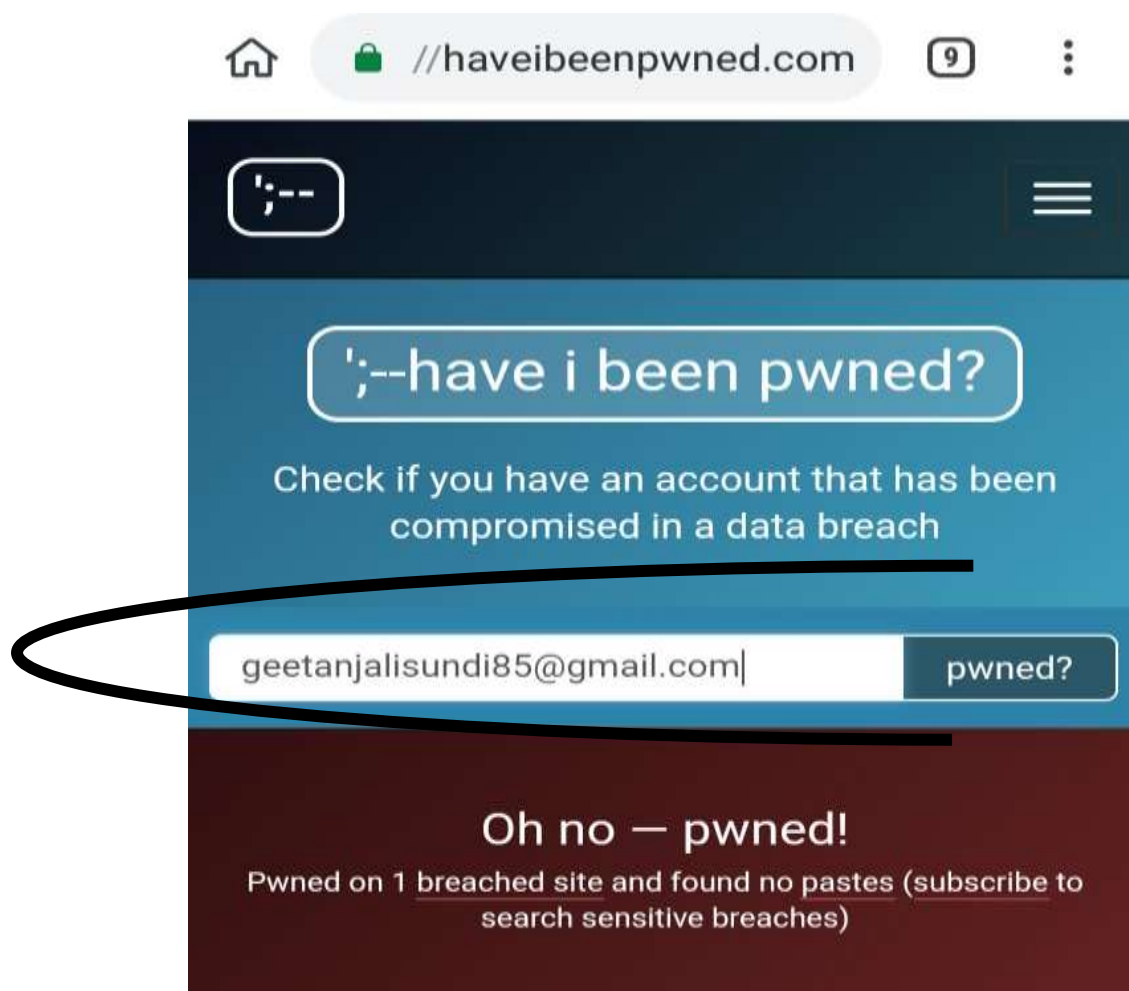
After clicking on the “+ Add to Firefox” box in figure 1, the webpage refreshed and a dialogue box appeared on the webpage as indicated by the black arrow above asking the user permission to:

- Access your data for all websites
- Exchange messages with programs other than Firefox
- Download files and read and modify the browser’s download history
- Display notifications to you
- Access browser’s tabs

If the user had clicked on Add, he/she would have given the App permission to

do all the aforementioned actions written above thereby granting third party access to private and personal information of the user. But when the user clicked “cancel”, the App didn’t add the PDF Reader extension to the browser.

Below are pictorial examples showing how some Email addresses with accompanying data have been sold illegally without the users’ consent or knowledge. It shows how the data of these emails have been compromised in a data breach. The samples are courtesy of “[haveibeenpwned.com](https://haveibeenpwned.com).”



**Fig.3:-**Showing user email id whose email address has been compromised

Figure 3 above shows user email id “[geetanjalisundi86@gmail.com](mailto:geetanjalisundi86@gmail.com)” whose email address has been compromised.

Below is Figure 4 which shows how her email address was breached and what data are compromised.



**Fig.4:-** The above figure shows "geetanjalisundi86@gmail.com" email account has been compromised by a travel and hotel booking website called "ixigo." The data Auth tokens, Device information, Email addresses, Genders, Names, Passwords, Phone numbers, Social media profiles, usernames.



**Fig.5:-** Club Penguin Rewritten data breach.



*Fig.6:-mySpace site data breach.*



*Fig.7:-LinkedIn data breach.*

## DATA BREACH INDICATORS OF COMPROMISE

- Pop-ups while surfing the internet, unwarranted or unexpected redirection to another site while browsing.
- Friends, family or contacts informing you or replying to unusual messages (most often graphic images) that supposedly came from you whereas, you never sent such messages. These messages can be sent via your email address, social media accounts or through your phone number(s).
- Unexpected changes in your browser and system configuration.
- Changes made to your accounts without your permission.
- Difficulty in logging into your social media or email accounts because your account Id and password has been hacked or compromised.
- Devices, System or application crashing repeatedly. The Devices, System or Apps might run sluggishly due to the presence of virus, spyware or malware.
- Warning alerts from firewalls to the network administrator or to the user when data or security has been compromised.

## WHAT TO DO WHEN DATA HAS BEEN COMPROMISED

When data has been breached and compromised, it is too late to prevent the leakage of data but here some steps to follow to minimize the damage.

- Do not change anything on the affected system(s) and isolate the affected system(s) or App(s) to reduce more exposure of data.
- Find out how and where the breach occurred. Was the breach intentional or not? Also, examine the repercussions.
- Gather evidence and note down every action in case you want to make a report about the incident. E.g., you can

take a screenshot of your compromised account, the alleged sent messages to contacts with date and time included.

- Revoke all access or permissions given to Apps, websites or third parties.
- If your social media account has been compromised, contact help and support and report the account for further actions.
- Send a message to your contacts to let them know you have been compromised and to distance yourself from any further incriminating actions that might occur.
- Contact an expert or service support for further assistance on your device or system.

## METHODS OF PREVENTING DATA BREACH

The following are the ways we can use to prevent data breach:

- **Using the internet anonymously:** users can hide their identities while surfing the internet. By hiding identities, it means hiding the Internet Protocol (IP) address which can be done by using proxy services and virtual private networks (VPNs).
- **Authentication:** It is a means of identifying an individual and ensuring that the individual is the same who he/she claims to be. It can be done by using username and password, biometrics (fingerprint, facial recognition, voice recognition), One Time Password (OTP), etc.
- **Elimination of third-party cookies:** Third-party cookies should be deleted to prevent or removed tracking of browsing history, browser tabs and user information by the third party.
- **Use of privacy extensions or add-ons:** users should add extensions that will keep out harmful or unsecured



websites and applications that might leak out user data.

- **Use of safe search engines:** users can use search engines that are private and do not collect personal information.
- **Encryption:** this is when data is kept in an encrypted (unreadable) or coded form before it is transmitted over the inter and only the person that has the key would be able to unlock and read the data.
- **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.[4]

## RECOMMENDATIONS

In order to prevent our data from theft or unauthorized access, the following actions are recommended.

- Be wary of downloading software from unknown or unreliable source.
- It is not every free Apps that is free in the true sense of the word. Some collect your data without permission as a form of payment.
- Read and understand privacy policies before agreeing. If it looks dubious, do not agree.
- Be cautious of giving permission to third-party cookies.
- Read and understand software permission control over your data and device carefully before agreeing to it.
- Always backup your data, device(s) and System.

## CONCLUSION

While the internet has many advantages, it also has its disadvantages and it is extremely important for us to be cautious of any website we visit and any applications we download most especially free applications. We must think twice before we agree to any privacy policies whenever we want to download an app or visit a website.

## REFERENCE

1. Privacy International (August, 2018), *A Guide for Policy Engagement on Data Protection: The Keys to Data Protection*. London, United Kingdom.
2. Techopedia.com. *What is Data Security?* Retrieved from: [www.techopedia.com/definition/26464/data-security](http://www.techopedia.com/definition/26464/data-security). Retrieved date: April 9, 2019.
3. Eric A. Hibbard. *SNIA; Data Storage Innovation (DSI) Conference: Privacy vs. Data Protection*. Hitachi Data Systems (2015).
4. Jeetendra Pande. *Introduction to Cyber Security*. Uttarakhand Open University, Haldwani (2017).
5. GlobalSign Blog. *What Data Is Collected About You Online and How to Stop It. GlobalSign GMO Internet Group*. Retrieved from: <https://www.globalsign.com/en/blog/what-data-is-collected-about-you-online/>. Retrieved date: April, 24, 2019.
6. Haveibeenpwned (2019) *Have I been pwned?*. Retrieved from: <https://haveibeenpwned.com>. Retrieved date: April 24, 2019.
7. UN Doc. HRI/GEN/1/Rev.9, General Comment No. 16: Article 17, paragraph 10.