As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 7(02): 133-139, 2021

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0702023
Available online at: http://www.ijmtst.com/vol7issue02.html

Data Breaches - Staying safe online in 21st Century

Prakarsh Kaushik[1] | Devang Pratap Singh[1]| Sai Sri Nandan Challapalli[1]

[1]Student of Computer Science and Engineering, Amity University, Greater Noida, India

To Cite this Article
Prakarsh Kaushik, Devang Pratap Singh AND Sai Sri Nandan Challapalli, "Data Breaches - Staying safe online in 21st Century", *International Journal for Modern Trends in Science and Technology*, Vol. 07, Issue 02, February 2021, pp: 133-139.

Article Info
Received on 18-January-2021, Revised on 17-February-2021, Accepted on 21-February-2021, Published on 26-February-2021.

ABSTRACT

A breach of data is a reported occurrence where private, sensitive, or covered records have been compromised and/or released unlawfully mostly due to cyber attacks or theft. Breach of data can include personal health records, personal information, travel information, trade secrets, intellectual property, or information you provided to or is stored on a platform. Data revealed to breaches pose a security and privacy risk to Users around the world. Despite these, guidelines on how organizations can react to breaches, or how to manage information securely once it has leaked, still haveto be established. More than 3 billion people suffered and became victims of data breaches and cyber attacks in the last two decades leading to loss of personal data as well as monetary loss. This research paper conducts real time research about awareness of data privacy, kind of data/ information that needs to be protected, basic protocols for staying safe online, and some of the biggest corporate data breaches that happened in this century. We bring people from different cities of India in this study through a survey and use the data provided by these 150 participants to examine their understanding of data privacy, their concern regarding their online data and the practices they follow in their daily life to keep their online data safe in this age of computers and internet.

KEYWORDS:*Breach, Data, Cyber attacks, Data Privacy, Cyber theft.*

I. INTRODUCTION

We often hear about massive data breaches in the news these days. But it shouldn't be all that surprising. With the implementation of new platforms and technology, most of our information is being shifted online, be it travel information, insurances, bank details, or other personal details. As a result, data breaches and cyber attacks are becoming increasingly common and costly. Multi national companies and firms are incredibly attractive targets for cyber attackers, merely because of the large volumes of information stored under a single roof (here, a data server), that can be nicked in one fell swoop. There are several reasons why data breaches occur? Sometimes it's accidental but it is also extremely rare. Most of the time targeted attacks are carried out in different ways to steal data.

In the last two decades, more than 3 billion people have been victims of online data breach and theft across the globe. In the year 2017 alone, Account information and data of 150 million Uber users were stolen and around 2.5 billion users of Yahoo suffered also suffered a similar data breach case. Once stolen, all this data is auctioned or sold on online black markets to the highest bidder. This stolen data is then used to target audience for selling products/services, identity theft or cyber extortion, or even worse. Stolen credit/debit card

details are used to carry out financial transactions without the user's authorization.

Various practices to stay safe in the digital world, Handling data once it is exposed, different practices and concerns of survey participants of different age and place of residence regarding their data and its privacy is further discussed in this report.

INCIDENT OF DATA BREACHES IN RECENT YEARS

In Even after tightening security measures and hiring the best cybersecurity professionals to prevent their data from getting exposed, some well known companies like eBay, Quora, Uber, Dropbox, Apollo, Adobe, Badoo, Tumblr, Equifax were also victims of a data breach which led to data of millions of users getting exposed. Not only these companies but Palo Alto Networks, a multinational cybersecurity company acknowledged that they had experienced a severe breach of data that resulted in online leaking/publishing of personals as well as professional information of both former and current employees.

Apart from the above mentioned companies, we compiled a list of some of the biggest data breaches affecting MNC's that happened in the 21st century in order of the users affected. The list consists of 7 well know companies who became victims of the data breach and monetary loss.

YAHOO

In August 2013, data like name, date of birth, password, email, etc. of more than 3 billion Yahoo users were compromised as a result of cyber attack. Even the security questions and its answer, which are used for the security purpose of the user's account were compromised.

The following year in 2014, Yahoo again became a victim of the data breach. This time data of 500 million users was compromised. Though Yahoo claimed than more than half of the passwords were encrypted. Yahoo acknowledged and disclosed about this breach two years after in December 2016. This was the biggest known data breach in history.

AADHAR(UIDAI)

Aadhar is a proof of identity and address valid across India which is a 12 digit unique identification number issued by the Unique Identification Authority of India (UIDAI) on behalf of the Government of India.

UIDAI disclosed that in March 2018, data and information such as name, date of birth, bank details, biometrics, photograph, 12 digit unique identification number of more than 1.1 billion Indian citizens were compromised due to a data leak on a system run by a state owned utility company. This was the second biggest known data breach in history.

FACEBOOK

Facebooks IDs, comments, likes, reactions, account name, personal information, etc. of more than 540 million users were exposed on the public Internet as a result of a data breach in one of the world's most famous social media platform Facebook.

This breach occurred and was disclosed in April 2019. The data exposed due to breach was posted publicly on an online database and was easily accessible by anyone Not only this but it is assumed that similar breach with users account

information has also happened in the previous year (i.e. 2018)

MARIRIOTT INTERNATIONAL

Marriott International is a hospitality company that announced in November 2018 that more than data of 500 million customers of Starwood Hotels have been stolen after a cyberattack. It is assumed that the attacks found a backdoor into the database and system of Starwood hotels and manage to stay untraceable. Marriot unaware of this breach acquired Starwood in 2016.

The breach not only exposed personal information like name, age,contact, passport information but also credit/debit card information to the attackers. It is also assumed that attackers were able to decrypt financial information like the expiration date and CVV of debit/credit card of customers.

MYSPACE

Myspace, once used to be the world's largest social networking site. More than 360 million users' account were compromised in an attack which happened in 2013. This data breach was disclosed publicly by Myspace three years after its occurrence in 2016. Data that was compromised included name, date of birth, email, and password of the user's account. During these three years, all the accounts created in or before 2013 could easily be accessed via that data exposed from the breach. Myspace invalidated all the password created before 2013 and asked its user to update them.

TWITTER

In May 2018, Twitter discovered a bug in its system, which enabled the user's password to be stored in an internal network without encryption.

More than 300 million Twitter users were asked to change their password. This social media giant ensured its users that though their data was exposed for several months, there hasn't been any breach or theft of data.

LINKEDLN

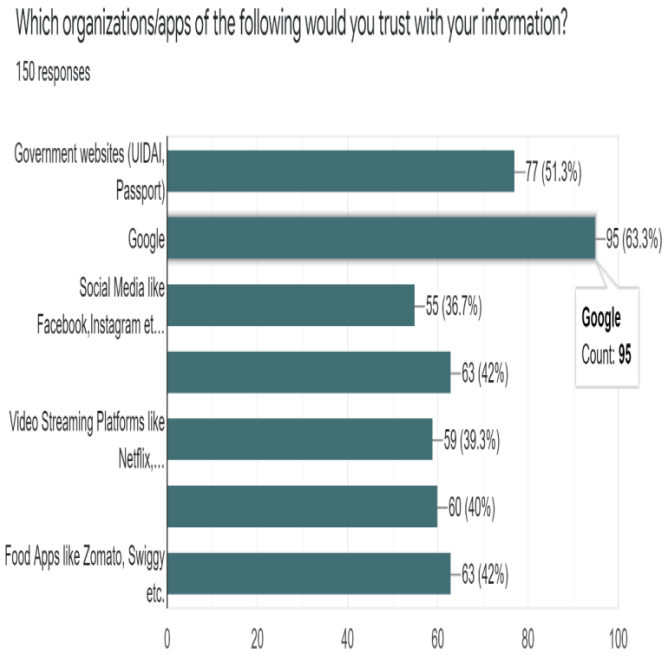
LinkedIn also suffered a data breach that compromised account as well as personal information of 165 million LinkedIn users. This breach was disclosed publicly by the company in June 2012. The encryption of stored password was weak and thus the attackers were able to decrypt a password of 117 million users. The company immediately sent password reset notification to its users.

II. PRACTICES TO STAY SAFE ONLINE

While the concerned companies have very many ways to deal with data breaches, as a user, an individual can put in very simple efforts to keep him and his data safe.

In our daily activities, we may overlook some common practices to make things/tasks simpler. Just like not setting up a password for our mobile because it is tedious to enter it every single time. But such small daily habits can make the difference in instances like data breaches and cyberattacks that were discussed in the previous section. The setting of a password, for example, can stop misuse of data in case the phone is lost or stolen. Also, it can directly prevent juice jacking, i.e. theft of data through USB cables disguised as charging ports at public places like shopping malls and airports.

It always makes sense to assume that data/money that is lost in a data breach or cyber attack is cannot be recovered without due harm. And that is why an individual must regularly follow some practices. Like setting up strong passwords. As simple as it is said. This makes breaking into your device/account rather difficult. The best password is one with a combination of alpha number characters with special characters and minimum eight characters in length. One should refrain from keeping names, date of birth and phone numbers as passwords. We should also be careful whom we trust with our data and money. Companies tend to build goodwill for many years and it must be considered. It is astonishing to find by the means of a survey, that people tend to trust a Non Indian private company over Indian agencies.



We must keep a regular track of our bank accounts, credit card bills, and other financial accounts to keep any fraud at bay. In this way, anything suspicious will easily come to our notice and necessary action can be taken. Use of reliable security software (either paid/free) for all electronic devices is also helpful in protecting your data. Checking the URL of sites while entering sensitive information and prefer sites with prefix https:// as 's' indicates an additional layer of security. Be informed about customer care contact details of payment apps and bank services so that we don't fall prey to fraudsters.

These may seem very common. Also, these find mention in various places like newspapers. But the idea behind this report is to reiterate the need to follow them.

III. SURVEY PARTICIPANTS DEMOGRAPHICS

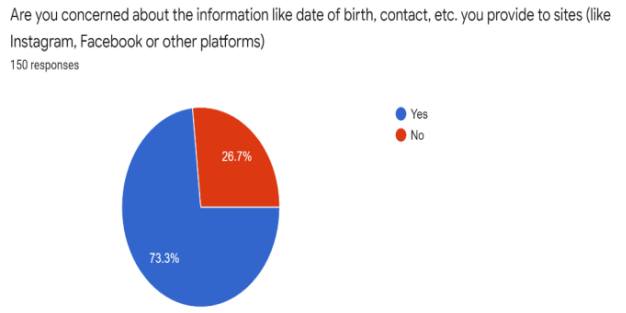
In the 7 day survey we conducted, 150 people participated and contributed to the successful completion of this project. The participants of the survey were from a variety of categories based on age, place of residence, and their understanding of data and its privacy. Among 150 participants, 34% were living in metropolitan cities, 44% were living in an urban area and 22% in a rural area. Roughly 1.3% were below 18 in age, 36% were in the age group of 18 to 25, 41.3% between 26 to 35 of age group, 18% between 36 to 50 and 3.3% above the age of 50 years. 90% of 150 participants responded to the question that they understand the term data privacy and are aware of the consequences of data theft.

IV. PRACTICES ADOPTED BY SURVEY PARTICIPANTS TO STAY SAFE ONLINE

Securing the company's as well as user data is one of the most important processes in running a successful business and to keep thriving against its competitors almost every company is tightening its security measures and updating its system with the latest technologies. However, users shouldn't ever depend entirely on companies to keep their data safe. It's really necessary to take preventive action and keep a watch on the information you provide to companies.

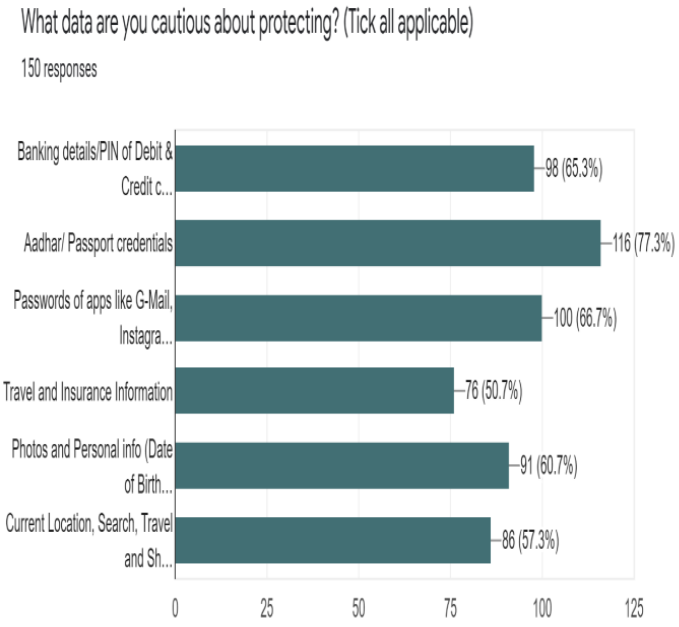
73.3% of our survey participants are concerned about the information they provide to social media

sites, travel sites etc.



40.7% of participants have been victim of online fraud, scam or hack.

People were mostly concerned about their Aadhar and passport details with 77.3% votes as these include biometrics like retina and fingerprint. This was followed by concern for their online account information and passwords with 66.7% votes. Banking details, as well as Credit/Debit card details, were concerns of 65.3% of the participants. Participants were least concerned about their travel details and insurance information, which could lead to identity theft or monetary loss.

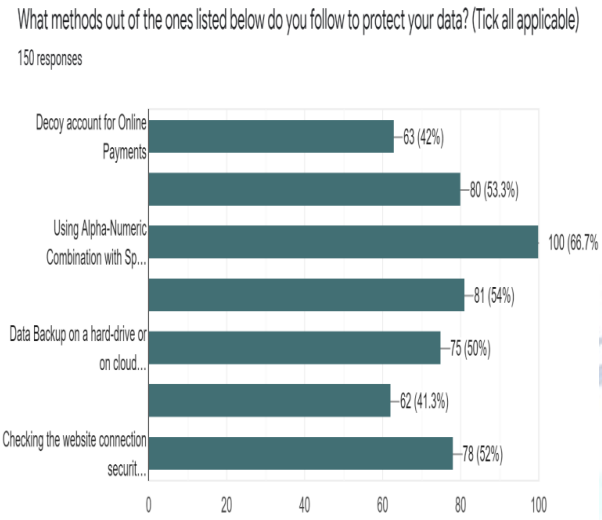


66.7% of the participants know that using 8 characters long combination of alpha--numeric combination of password including special characters like #,$,*,@ is a better choice. Not only they are aware of this but they also follow this practice while choosing their password.

If software or app get out--dated, they might have some vulnerabilities or backdoor which an attacker can easily exploit to get hold of your data. So, it is advised to update your software or apps periodically to keep your data safe and secure. In May 2017, Attackers were able to get hold of 230,000 computers across 150 countries and ask for ransom. This cyber--attack was known as “WannaCry ransomware attack”. The attackers were able to exploit a backdoor in out of date windows system. 54% of the survey participants are aware of the risk imposed by out--dated software/apps and thus they update them at regular intervals.

Using the same password for every online account can be very dangerous. If someone or an attacker gets access to one of your account’s passwords he might access all of them. So, it's advised to use different passwords for different accounts. 53.3% of participants in the survey follow and practice this to keep their information safe online.

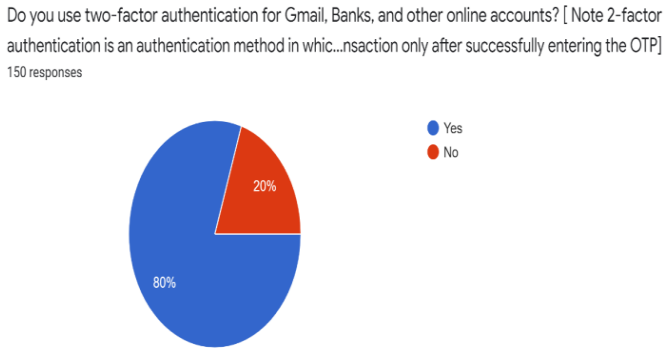
Before entering sensitive information like passwords, atm pin, or other banking/personal information on the website, it is advised to first check whether the site is connection is secure or not. This can be done by simply checking whether the HTTPS (HyperText Transfer Protocol Secure) symbol is present at the beginning of the URL or not. 52% of survey participants have a habit of checking site security before entering sensitive information.



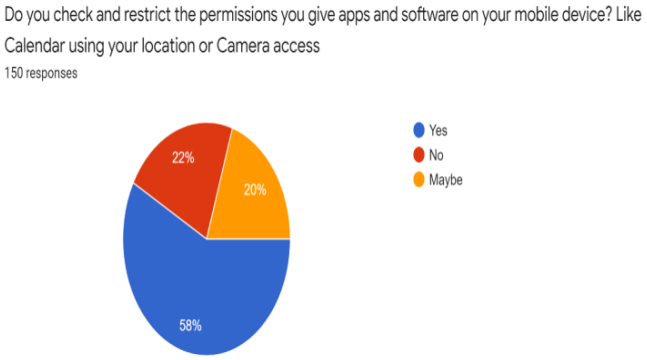
50% of the participants in the survey make a backup of their computer or mobile data into physical storage or cloud. It is a healthy practice that might help you to recover some important data in case your original device is compromised.

Setting up decoy accounts for online payments and using some security software are some of the other practices which might help to stay safe online. Decoy accounts for online payments might help you in safeguarding yourself against monetary loss, whichmight occur in case your account or credit/debit card details are exposed.

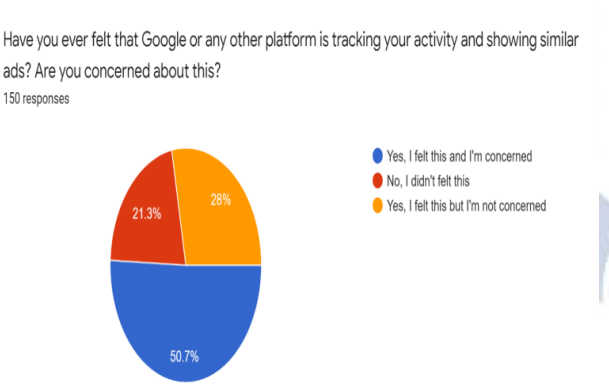
80% of the survey participants use 2--factor authentication for accessing their accounts.



Checking the access or permission granted to apps/software while installing. Sometimes, people end up installing spyware disguised as software and apps. So, it's a healthy practice to ensure that an app/software is only granted with permission related to its use. 58% of our survey participants check the permissions they grant to apps/software.



Most of us have once in a while encountered seeing ads similar to something we searched or bought online. 78.7% of the survey participants felt that their search, travel and shopping habits is being monitored by Google but only 50.7% of them were concerned about this. If you are among those people who are concerned about this, it is advised to use incognotio mode for surfing web to refrain from revealing your search and shopping habits.



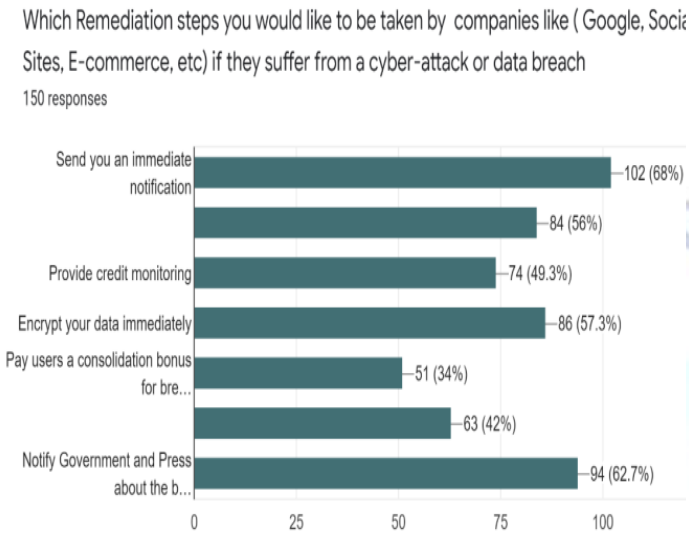
V. HANDLING EXPOSED DATA

Many times companies don't notify its users about the breach or cyberattack immediately. Examples of such incidents are Yahoo and Myspace where both these companies disclosed publicly about data breach two and three years after the incident.

This not only jeopardized the user's data once but for two three years until they were made aware of the situation. The data was posted on a public database which was easily accessible by anyone with a stable internet connection.

To prevent user data from being exposed for a longer duration in case of a data breach, companies should adopt some userfriendly remediation steps.

We asked the participants of our survey to choose all the remediation steps they would like companies to follow in case of a data breach.



42% of the participants were comfortable only with the company fixing the issue and securing their data. But 34% of participants were in favor of getting a consolidation bonus from the company for breaking their trust and lack in their security services.

Our report gives an insight into user expectations as well as concerns.

However, before drawing a line in the sand for best methods of securely handling exposed/breached data, it is also crucial to consider the views of Government, cybersecurity experts, and researchers.

VI. CONCLUSION

Data breaches are likely here to stay, and the best defense against them is a good offense. At this juncture, it is highly important that we educate ourselves continuously about healthy practices. The presence of laws, policies, and procedures that are in place to protect our information should not stop us from being alert while we enjoy the convenience that the internet world gives us.

This report investigated and presented details about different data breach incidents in the recent past, especially related to famous companies/firms that are generally believed to attach utmost importance to user data privacy. This again only proves that nobody is immune to such cyberattacks. This report gave a detailed study of the data breach incidents by collecting data from credible sources like news articles and reports, company official statements, etc. that are available on the internet. A major focus was done to collect details like who was breached, was there a security lapse, was there an immediate threat to the user/users' data, were the users informed, etc.

We have inferred that even though data breaches have become a common sight to the general public, rarely do companies acknowledge the claim, and the lost data is often exposed. This brings forth the idea of safe online practices that a user can follow to stay safe online. Some of these are also shared in the report and user awareness about the same is analyzed through the survey. The survey in the report, that was answered by 150 participants, has helped to draw various useful conclusions regarding the understanding of data privacy and practices adopted by users who hail from the different socio educational background.

REFERENCES

[1] Norton. (n.d.). What is a data breach? https://us.norton.com/internetsecurity privacy data breaches what you need to know.html

[2] Karunakaran, S., Thomas, K., Bursztein , E., &Comanescu, O. (2018, August 12 14). Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data [Paper Presentation]. SOUPS 2018, Baltimore, Maryland, USA. https://www.usenix.org/conference/soups2018/presentation/karunakaran

[3] Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., &Koutbi, M. E. (2019). Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time. Procedia Computer Science, 151, 1004 1009. https://doi.org/10.1016/j.procs.2019.04.141

[4] Cio, E. T. (2019, November 30). Global cybersecurity firm Palo Alto Networks suffers data breach. ETCIO.Com. https://cio.economictimes.indiatimes.com

[5] Swinhoe, D. (2020, April 17). The 15 biggest data breaches of the 21st century. CSO Online. https://www.csoonline.com/article/2130877/the biggest data breaches of the 21st century.html

[6] UpGuard. (2020, June 1). The 36 Biggest Data Breaches [Updated for 2020]. https://www.upguard.com/blog/biggest data breaches

[7] Major data breaches leak millions of user records. (2013, December). Computer Fraud & Security, 3 20. https://doi.org/10.1016/s1361 3723(13)70108 8

[8] Hassanzadeh, Z. (2019, August). USER UNDERSTANDING OF INTERNET DATA BREACHES (Thesis). Carleton University. https://doi.org/10.22215/etd/2019 13871

[9] Fowler, K. (2016). Data Breach Preparation and Response: Breaches are Certain, Impact is Not (1st ed.). Syngress. https://doi.org/10.1016/c2014 0 04209 8

[10] Data Breach Preparation. (2015, March). https://doi.org/10.2172/1172869