CYBER SECURITY AND DATA PRACTICES

[1]Aftab Mirza,[2]Shoheb Kazi,[3]Ahtesham Syed,[4]Shadab Khan
[1,2,3,4]Student
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Anjuman-I-Islam's Abdur Razzak Kalsekar Polytechnic, New Panvel, India

Abstract*—It is not uncommon nowadays to hear about data breaches and user information leaks. Something even more worrying, the users themselves are aware of these developments to a certain degree, but only to the benefit of nothing. Hence, the motive of this paper is to shed light on what actually constitutes Cyber Security and how to enforce them in the real world along with analysing the alleged negligence of the big companies when it comes to data protection.

***Index Terms*—Data Security, Data Breach, Cyber Attack, Online Phishing, Data Theft**

I. INTRODUCTION

When a service is free, we are the product. This can be experienced when seemingly millions and millions worth of data is violated in a data breach, only to be consoled later as "lack of security" or "unforeseen attack arsenal." A data breach occurs when the attacker(s) gain access to digital, sensitive pieces of information with which the identity of the owner is compromised and becomes free to manipulate. These sensitive piece(s) of information generally include the victim's name, email, passwords, address, telephone number, account number, personal identification number, etcetera.

II. CYBER SECURITY

To understand Cyber Security, we need to understand what 'Cyber' exactly refers to. Cyber means simply a computer, or anything which is related to it. Cyber Security is referred to the preventive measures taken to secure and protect online data, applying preventive measures against the theft and abuse of that very data. It is of immense importance for any IT company, dealing with sensitive information i.e. of consumers and alike, to have a firm grasp on the security of the database and personal information. Likewise, it is also the responsibility of the particular regional government to ensure that periodic International Standards Benchmark audits are carried out and defaulters are fined or banned if necessary.

Cyber companies store millions and millions worth of data and, consequently, offer a plethora of mouth-watering assets to attack. It doesn't matter how big or small a company might be, but it is incumbent upon them to remain vigilant and prioritize the information of customers than to become lazy regarding their responsibility. We will talk about the data practices of a few well known companies with huge consumer bases and how they mishandled the privacy of billions.

i. Google

The Multinational American company is already infamous regarding its privacy policies. The most recent slip up comes from a string revelations detailing how Google stores a snapshot of where a person is when the user merely opens it Maps app[1]. If that is insufficient, Google Maps stores data even when specifically asked not to. Not only does this build up enormous privacy risks for the user, but also endangers the life of the user if the data falls into malicious hands. Google has been alleged with a lawsuit for deceiving users into believing that they are not being tracked[2].

Another recent blunder was when hordes of Indians began noticing a strange helpline number saved in their mobile contact lists[3]. After investigation, it turned out to be the number of Unique Identification Authority of India [UIDAI]. The users were concerned why a number was inserted into their Android phones without their permissions. A situation where this intrusion could be abused is no longer a hyperbole.

ii. Facebook

A new study has revealed that Facebook is one of the favourite playgrounds for cyber attackers with around 600,000 attacks in a single day[4]. Moreover, the company itself is also splurged in a host of data breach accusations. Another study revealed in 2011 that Facebook tracks its user's activity even after they sign off from their respective accounts[5].

The icing on the cake is unarguably reserved for the Cambridge Analytica scandal, where the data mining firm abused Facebook data, spent $1 million harvesting millions of Facebook profiles in order to manipulate the US Presidential election results in 2016[6]. Facebook has all the information on its 2.6 billion users. This makes it a free nest to make a social weapon. In an honest reveal, a former employee of the data mining firm disclosed how they collected 50-60 million Facebook profile, analysed their preferences and their reactions to different types of news and accordingly personalised their election propaganda for the users to see, manipulating their election choices.

iii.Yahoo

Yahoo holds the record for suffering the biggest data breach in history, when more than 1 billion accounts were compromised[7]. The hackers used 'forged cookies', which are snippets of code that stay in a user's browser cache so that the user can be identified and given access without a password, to access the accounts without a password. Yahoo said that the compromised user account information may have included names, email addresses, contact numbers, birth dates, hashed passwords and also encrypted or unencrypted security questions and answers.

Another mistake was confirmed when Britain's Intelligence Agency reportedly captured still web-cam images of millions of Yahoo users which include a large quantity of inappropriate and explicit images[8]. Yahoo itself was unaware of this development and said that if the news is true then this would be a new level breach violating their data protection policies.

iv. Microsoft

The ever popular multi-billion technology company which gave rise to the world's richest man in terms of wealth last in 1999, has received a scathing warning from the French Government as Stop collecting excessive data and tracking browsing by users without their consent[9]. The reason behind the admonishment becomes clear when one goes through the settings in the Windows 10 Privacy menu, and browses through data collection options set to on be default. An average user is negligent of the hideous and complex 'Setting' options.

Moreover, from among the things that Microsoft collects to "improve its services" is the collection of keystrokes received from the user, also known as keylogging[10]. A keylogger can be a hardware device, or as in this case, a software program which has the ability of collecting the keystrokes pressed by the user on their keyboard. This raises enormous privacy risk of users regarding their sensitive information like passwords, addresses, phone numbers, and so forth.

III. PREVENTIVE MEASURES

After going through the mishaps of the above mentioned companies, one might think as to how he can protect himself from the online poachers. Here lies a responsibility of not only the government and the company, but also of the consumer. When a consumer doesn't take active steps to secure his or her account, they are in actuality risking their assets to be victim of cyber attacks. And attackers are also notorious for often attacking those users who don't seem to take their online security seriously enough. But where there's darkness, there is also light, and the internet cyber heroes, like Mozilla, have been trying their best to spread awareness about the importance of user security by campaigns, lectures, blogs and almost everything else they can possibly do. Accordingly, we'll be following their approach to cyber security and lay down versatile ways through which, a common cyber user, can improve his online security.

i. Password Creation

It is no secret that passwords are the among the biggest assets of a user; they're practically the gate to all information, since the username or email ID is generally publicly available. According to a study, about 90% of passwords of users are estimated to be prone to hacking due to poor strength or lack of vigilance[11]. If the password is user generated, then the problem that arises is that the users typically choose easy-to-remember passwords, which are easy-to-crack for the hackers. On the other hand, if the password is computer generated, then this gives rise to problems like passwords which are very complex to remember. This dilemma can be solved by using a reputed password manager like 1Password[12] which promises a centralized and secure location to store all passwords and offers features like unique password generator and a master password with which you can get access to your other passwords, much like a safe vault.

ii. Virtual Private Network

Also more popularly known as simply a VPN, is a mechanism to encrypt all your network traffic so that it becomes untraceable for outside forces to track you; you become able to communicate on a public network as of it were a private network! There are a number of free options available but it is best for ultimate security to invest in premium VPN services like SaferVPN[13].

iii. Trusted Software

It goes without saying that a user should use only verified softwares from trusted companies that have a long record of good consumer data protection and short update intervals. Each software has its own strengths and weaknesses, so it is necessary for the user to choose his options wisely. One can check Sucuri[14] for any suspicious websites and then proceed to download from them if the are free from malware.

iv. OS Updates

Microsoft and similar vendors regularly releases updates and patches to fortify user security and vulnerabilities. A user shouldn't delay important updates. Nowadays, vendors have incorporated 'push' update methodology i.e. as soon as the user is connected to a stable internet connection, install the updates while letting the user use his computer. This is in contrast to the traditional methodology of 'pull' updates, where the user is simply notified of an update and the user can conveniently install them when he feels like doing it. But this gives rise to risks because the volume and velocity of today's cyber attacks require tougher guidelines. Hence, 'push' updates allow vendors to ensure that their devices are updated since it is true that there are many users who don't bother to 'pull' update their devices.

v. Backing Up Data

If the data of a user unfortunately becomes entangled in an attack, a reliable back up that he made at a point in time will atleast enable him to roll back his important data and get on with his life. Datasets speak for themselves[15] of the poor performance of commercial data back ups when they were needed the most. Hence, it is the responsibility of the user to use dependable back up services. For Windows users, the built-in Windows Recovery can be considered as a go-to option.

IV. CONCLUSION

A regular human in his desire to ease his way of life, digitalizes himself on the internet, but the cyberspace is not all friendly. It is astonishing, to say the least, how big data companies collect our data, many times without giving the user much choice, and do not fulfil the due responsibility attached with it. We wouldn't let a stranger follow us to our door, so why are we so sloppy with our online information? Unarguably, with data we're basically uploading ourselves on the internet and therefore the common user needs to create awareness in himself regarding information protection, for when a datum is compromised, it is the user himself who is impeded.

ACKNOWLEDGMENT

The authors would like to thank Mr. Ubaid Saudagar for handing us this wonderful opportunity to prepare our debut research paper and made sure to scrutinize mistakes to fix them. Special thanks also goes for Ms. Tahseen Shaikh who was a decisive motivator for the completion of the paper. The respective families of the authors sponsored us with financial help and for that we all express our due gratitude.

REFERENCES

[1] www.ETCIO.com, “No privacy here: Google will track your movements, even if you tell it not to - ET CIO,” ETCIO.com. [Online]. Available:https://cio.economictimes.indiatimes.com/news/digital-security/no-privacy-here-google-will-track-your-movements-even-if-you-tell-it-not-to/65385833

[2] “Google sued for secretly tracking people’s phones,” The Independent, 21-Aug-2018. [Online]. Available:https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-location-history-tracking-iphone-android-lawsuit-a8500681.html

[3] “Google acknowledges adding UIDAI helpline number to Android phones in 2014- Technology News, Firstpost,” Tech2, 04-Aug-2018. [Online]. Available:https://www.firstpost.com/tech/news-analysis/google-acknowledges-adding-uidai-helpline-number-to-android-phones-in-2014-4890071.html

[4] E. Barnett, “Hackers go after Facebook sites 600,000 times every day,” 29-Oct-2011

[5] “Is nothing private? Facebook tracks which sites 800m users visit... even AFTER they sign off,” Mail Online, 19-Nov-2011. [Online]. Available:http://www.dailymail.co.uk/news/article-2063709/Facebook-watches-800million-users-AFTER-sign-off.html

[6] The Guardian, Cambridge Analytica whistleblower: “We spent $1m harvesting millions of Facebook profiles.” 2018.

[7] S. Thielman, “Yahoo hack: 1bn accounts compromised by biggest data breach in history,” The Guardian, 15-Dec-2016.

[8] ARIRANG NEWS, UK spies captured millions of webcam images of Yahoo users. 2014.

[9] “France issues formal notice to Microsoft about Windows 10: ‘stop collecting excessive data and tracking browsing by users without their consent.,’” Private Internet Access Blog, 21-Jul-2016. [Online]. Available:https://www.privateinternetaccess.com/blog/2016/07/france-issues-formal-notice-microsoft-windows-10-stop-collecting-excessive-data-tracking-browsing-users-without-consent/

[10] “Windows 10’s ‘built-in keylogger’? Ha ha, says Microsoft – no, it just monitors your typing.” [Online]. Available: https://www.theregister.co.uk/2014/10/07/windows_10_data_collection/

[11] T. Telegraph, “90 Percent Of Passwords ‘Vulnerable To Hacking,’” Business Insider. [Online]. Available: https://www.businessinsider.com/90-percent-of-passwords-vulnerable-to-hacking-2013-1.

[12] G. Ballard, “1Password Password Manager Review— Is It Worth It?,” Security Baron, 13-Nov-2017.

[13] “Next Gen Small Business VPN,” Perimeter 81. [Online]. Available: https://www.perimeter81.com/.

[14] sucuri.net, “Sucuri Security,” Sucuri Security. [Online]. Available: https://sucuri.net.

[15] B. Gammons, “4 Surprising Backup Failure Statistics that Justify Additional Protection.” [Online]. Available: https://blog.barkly.com/backup-failure-statistics.