Tackling Data Theft – Read, Check, Review

Delving a few months back in time, USA was witness to an outright, well schemed and open robbery in pure daylight. No, we're not talking about any bank robbery. Neither are we referring to an economic scam or a political scandal that seems to have gained a fair share of popularity. The crooks in this crime were armed with the most modern form of weaponry in the digital age today – Ability to access information!

People in the US had their personal details palmed off by an e-mail subscription service to Uber. Most of them were consumers of Lyft, a competitor of Uber. And the name of this offending e-mail service was Unroll.me.

Uber did not stop here. It was widely reported in the American press that the company had fingerprinted its users. This meant that even after a user deleted the Uber app from his/her mobile phone, Uber would still be able to track the user's mobile usage.

This crime found an identical twin in the security breaches of 17 million accounts with Zomato and 3 billion accounts with Yahoo.

Scary, isn't it? One moment you entrust your personal information in the hands of the world's top global service providers and in the next, some Russian hacker is memorizing your password in the comforts of his room.

However, you can still ensure the safety of your digital identity by following certain steps:-

1. **Read the fine print** - Runa Sandvick, Director of Information Security at The New York Times strongly recommends that users read the privacy policies of all the apps that they intend to use. To be fair to Unroll.me, the Company had declared its intention to share users' data to third parties. Unfortunately, many subscribers of the e-mail service ignored the fine print.

   The point is, you must read all terms and conditions of the privacy statement of the app before signing up for its services. It may seem a daunting task, but as the saying goes, "better safe than sorry".

2. **Check the business model** - It is likely that the app that you are going to sign up for is free to use and doesn't have any advertisements running either. Now, doesn't it sound funny to you? How would this app monetize itself?

   Some apps that are free and do not serve ads share users' data like age, genders, income, etc. with third parties. So, whilst your name and e-mail id may not be stolen, your other indicators may go to an anonymous business. All this information is incredibly valuable to many marketing companies.

   However, there are some non-profits like the Electronic Frontier Foundation which provide data protection by offering Privacy Badger, which is basically an ad blocker.

   It is strongly suggested that you should check the business model of the app that you are interested in. A little bit of research in the present can save you the troubles of many problems in the future.

3. **Review and delete unwanted apps -** Experts suggest that we should periodically audit our apps. Now what does that mean?

   It means that once in a while, you must scan your electronic devices and delete the apps that have been idle for a long time. Chances are, you have used your Twitter, Facebook or Google accounts to access these apps. Over a period, you tend to forget you ever downloaded them but they are present on your devices, leeching off information. Ms. Sandvick suggests that once a year, prune down those apps that you don't recognize and get them off your device. All it takes is to visit the settings page of your social media accounts.

In the world of today, data theft is an extremely hideous crime of serious nature that must be dealt with an equally serious attitude. The first step to protecting yourself is believing the fact that you need protection. And in this case, all you need to do is Read, Check and Review.