How to avoid falling prey to a Facebook/Cambridge Analytica-type scandal

By Ilse van den Berg

26 Mar 2018

Following revelations that British data analysis firm Cambridge Analytica exploited the personal data of millions of Facebook users, the social media platform is finding itself in a remarkably anti-social predicament.

©scyther5 via 123RF

Cambridge Analytica collected the data of roughly 50-million users on Facebook through an app. Only about 270,000 users downloaded the app but those 270,000 people gave authorisation that the Facebook app could gain data from users' friends if their Facebook privacy settings allowed.

Cambridge Analytica specialises in psychographics, meaning they take an enormous amount of data and feed it through psychological profiling tools and algorithms to try and identify how people react and behave (this could be done through a Facebook app, as mentioned above).

Aaron Thornton, operations director of Dial a Nerd explains: "They then take this data and use it to create stories, blogs, or #fakenews (if that's what their customer wants) and deliver it back into your Facebook feed to see how you behave with it. If you click, then you are engaging. When it presents something that your psychological profile indicates a 72% chance of you engaging, and you do, you increase the likelihood that you will do so again in future, and so, too, will your friends."

The Cambridge Analytica scandal, Facebook and deleting your account

Andy Walker 23 Mar 2018

This type of behavioural and psychological information is incredibly valuable to companies, governments, presidential candidates, cybercriminals, and many more. Already, such data has been used for political and financial gain, as well as to sway political influence.

How to protect yourself

So, what can users do to protect their own data, if anything? How can we guard against falling prey to these types of things where our Facebook friends end up being our worst enemies, authorising the use of our data without our knowledge or permission?

According to Thornton: "This specific data 'breach' was, in fact not, a breach at all. Rather, it was a set of rules (that these people agreed to when installing the application) to allow applications or programs access to a host of data. The only way to manage this is to increase security on Facebook to *not* allow applications to access your data, but then be aware that they may not do what you want them to."

He says new fitness trackers are a good example of this: "People want the data the tracker provides, but have not taken the time to understand who else has access to that data and whether it is transferred to other parties. Therefore, one needs to ensure that the data you share with a company or an application is for that use alone and, in terms of the 'end user license agreement', it will not be shared with others."

Be careful what you publish

Henk Olivier, MD of Ozone Information Technology Solutions says the one thing social media users need to understand is that when you publish things on the internet, you give permission for people to see it.

"There are companies that target users and harvest their information, not something that is allowed, but users should understand that there is a risk of information being harvested or leaked when it is made public on the internet," says Olivier.

"Always ensure that your privacy settings are on the highest level to limit the spread of your data to the public, and make sure it is only searchable or viewable by the friends or people you know. The problem is that most people aren't aware of these risks and leave their privacy settings open or at the lowest level. This means that every update, viewpoint and comment is then accessible by anyone.

"Also, don't publish personal information regarding where you live or real personal information which can give anyone the opportunity to get hold of you or to track you down. Ensure that you are aware of all the social networking accounts you are subscribed to, so in the event of a breach or privacy breach that you can block or close the account," concludes Olivier.

Further security advice

When it comes to security, identity theft, access control and a host of other things, Thornton advises that good password management is an easy way to start protecting your data and your identity. He says to try and change your password at least four times a year. "Set the four 'password change dates' in your calendar now so that you adhere to it. It'll be frustrating at first, but once you are used to it, you will create a methodology that you can stick to," he says.

Do you really WannaCry? A simple guide on how to get hacked

Melissa Viljoen 14 Jul 2017

Your password should always be alphanumeric, so should contain both letters and numbers and more sites and platforms these days are forcing that.

"There are simple ways to train yourself to use a system that will make sense for you in future and you can search for some of these 'life hacks' yourself and choose one that you think will work. A name followed by three digits and you add another digit every time you change is simply one example," says Thornton.

Lastly, be careful when connected to free Wi-Fi or unsecured wireless offered in most hotels, coffee shops, and similar areas as the data you are transmitting is not encrypted. This means that when you are on these connections, keep your interaction to that of email or simple browsing and do not log into your bank or other important sites where you will be inputting usernames and passwords.

"Getting back to Facebook, because of the 'tick' you gave Facebook when you signed up, and the ensuing 'ticks' you give them every time it upgrades its service to make your engagement with it that much more interesting, you sign over more responsibility to the company, more data, and more access to your life including your physical location and - perhaps the most nefarious - access to your network of friends," concludes Thornton.

It is important that internet users reconsider their online behaviour and habits. Data is the new gold, and both individuals and companies will go to great lengths to obtain your personal information for profit and influence.

ABOUT ILSE VAN DEN BERG

Ilse is a freelance journalist and editor with a passion for people & their stories (check out Passing Stories). She is also the editor of Go & Travel, a platform connecting all the stakeholders in the travel & tourism industry. You can check out her work here and here. Contact Ilse through her website here.

- #StartupStory: Aura security app to aid beleaguered Uber drivers - 13 Jul 2018
- #StartupStory: BlockMesh - 12 Jun 2018
- Taking telecoms to the next level: Who needs a long-term contract? - 4 Jun 2018
- Nokia makes a comeback in South Africa with new phones - 24 Apr 2018
- New Cape Town/Brazil subsea cable to boost SA broadband - 18 Apr 2018

View my profile and articles...

For more, visit: https://www.bizcommunity.com