The New York TimesThe New York Times | https://nyti.ms/2u1Gpl3

PERSONAL TECH

How to Protect Yourself (and Your Friends) on Facebook

Leer en español

Tech Fix

By BRIAN X. CHEN MARCH 19, 2018

Revelations that a voter-profiling company that worked Donald J. Trump's presidential campaign harvested private information from 50 million Facebook profiles have many people wondering: What, if anything, can they do to protect their data connected to the social network?

Here's the harsh truth: Not much, short of ceasing to browse the web entirely or deleting your Facebook account.

Yet there are some best practices you can employ to help safeguard your data,

such as installing software to block web tracking technologies and carefully vetting the apps that you use on Facebook.

But it also helps to understand what exactly happened with those 50 million profiles in order to determine how you can better protect your data. Here's what you need to know.

So what happened?

An academic researcher at Cambridge University built an app called thisisyourdigitallife, which offered to pay Facebook users to take a personality test and agree to share that data for academic use. About 270,000 people participated in the study — enough to extract information on tens of millions of Facebooks users.

How did Cambridge Analytica get data on 50 million people when only 270,000 people had agreed to hand over their information to a third party? Facebook said people who downloaded the app gave consent for the app to collect limited information about their friends whose privacy settings were set to allow it.

That information was eventually paid for by Cambridge Analytica, the voter profiling company that worked with the Trump campaign.

O.K., so what do I do now?

There is a multipronged approach you can take to protect yourself from data-harvesting apps and programs. That includes tools you can install in your browser and settings you can tweak on Facebook. Here's a run down of what you should do:

• **Audit your Facebook apps.** If you used Facebook to sign in to a third-party website, game or app, those services may continue to access your personal data. On Facebook, go to the settings page and click on the Apps tab to see which apps are connected to your account. From there, you can take a closer look at the permissions you granted to each app to see what information you are sharing. Remove any apps that you find suspicious or no longer use. (Facebook has also made some changes to prevent the gathering of detailed information of friends of users.)

On the App Settings page there is another setting called Apps Others Use. This is where you choose which details are shared about you when your friends use apps. Make sure to uncheck all the boxes if you don't want any of your information, like your birthday or hometown, accessed by your friends' apps.

• **Audit your Facebook privacy settings.** If you are concerned about what details apps can see about you and your Facebook friends, now is a good time to check your privacy settings and minimize the information you share publicly. For example, you can make sure that only your friends can see your Facebook posts, or that only you can see your friends list.

• **Read privacy policies.** When you sign up for a new app or web tool, the company typically asks you to agree to its terms of service. Make it a habit to peruse the terms and pay particular attention to the privacy policy. If you see language that suggests your data could be shared in a way that makes you uncomfortable, don't use the program.

• **Install a tracker blocker.** There are add-ons that you can install in your browser that try to block trackers embedded on websites. But be aware that in some cases, they will make parts of websites work improperly. In our tests, Disconnect and Privacy Badger were useful tools for blocking trackers on Google's Chrome browser.

Here's a primer on how tracking works, to give you a sense of why blockers are important: When you engage with an app on Facebook, it may plant a tracker in your web browser, like a cookie, that collects information from you. Even when you close out of the app, the tracker can continue to follow your activities, like the other sites you visit or the people you interact with through status updates, according to Michael Priem, chief executive of Modern Impact, an advertising firm in Minneapolis.

"It doesn't go away after you've stopped looking at the ad," he said.

• **Install an ad blocker.** Another way to block trackers is to prevent ads from loading altogether. Ad blockers are also add-ons that you can install for your browser on your mobile device or computer. Mobile ads are fully functioning programs, and they sometimes include malware that harvest some of your data.

Even the largest websites do not have tight control over the ads that appear on their sites — and sometimes malicious code can appear inside their ad networks. A popular ad blocker among security researchers is uBlock Origin.

• **Clear your browsing data.** Periodically, you can clear your cookies and browsing history. Apple, Google and Microsoft have published instructions on how to clear data for their browsers Safari, Chrome and Internet Explorer. That will temporarily delete cookies and trackers, though they will probably reappear over time.

• **Be wary of unknown brands.** Even if you read the privacy policies, you still may have to take them with a grain of salt. In the case of the thisisyourdigitallife app, the fine print said the information would be collected for academic use, not commercial purposes. So think twice before sharing information with unfamiliar companies or organizations. (Then again, the researcher came from Cambridge University, one of the world's top schools — so who can you really trust?)

A version of this article appears in print on March 20, 2018, on Page A18 of the New York edition with the headline: Taking Practical Steps To Protect Your Data From Harvesters.