Massive <u>New</u> Facebook Breach: Personal Data from Millions of Users Available on Open Web

BY **PHIL BAKER COMMENTS**

While Mark Zuckerberg prepares to testify before the Senate, 100 cardboard cutouts of the Facebook founder and CEO stand outside the U.S. Capitol in Washington. (Kevin Wolf/AP images for AVAAZ)

Facebook Android app caught seeking 'superuser' clearance (theregister.co.uk)
by roznak to **technology** (**+32**|**-0**)

comments

We've all heard by now about the massive leak of the personal data of three million Facebook users and friends when a personality app, myPersonality, was used to extract personal information. The data was then used by Cambridge Analytica as part of their election targeting efforts.

Mark Zuckerberg testified before Congress, apologized for the breach, and blamed it on the app company that shared the data.

His solution was to more carefully screen the thousands of other apps; Facebook recently banned 200 of them.

But, like many times before, this was just the tip of the iceberg. We've just learned that intimate details about these three million users were freely available on the web for anyone to access for years, according to a New Scientist investigation.

According to New Scientist, "Academics at the University of Cambridge distributed the data from the personality quiz app myPersonality to hundreds of researchers via a website with insufficient security provisions, which led to it being left vulnerable to access for four years. Gaining access illicitly was relatively easy."

Facebook Can Hear You at Home, Whistleblower Says

According to the report, the intent was to make all of the data available to those who registered as a collaborator on the project. More than 280 people from nearly 150 institutions registered, including researchers at universities and employees from Facebook, Google, Microsoft, and Yahoo.

That makes Zuckerberg's approach to protecting data by punishing the app companies both naive and totally ineffective.

For those who didn't qualify for access, there was another easy way to access it: a publicly available name and password have been freely available on the web for anyone to use for the past four years!

According to New Scientist, "The publicly available username and password were sitting on the code-sharing website GitHub. They had been passed from a university lecturer to some students for a course project on creating a tool for processing Facebook data.

Uploading code to GitHub is very common in computer science as it allows others to reuse parts of your work, but the students included the working login credentials too."

"This type of data is very powerful and there is real potential for misuse," says Chris Sumner at the Online Privacy Foundation.

What's the lesson here? Never participate in online games or tests in which you provide data that helps others target information back to you unless it's totally innocuous data. As we all know, you can hardly move anywhere on the web without being asked to fill out a questionnaire or survey. Every one of them should be met with suspicion.

More importantly, this shows that no company is able to protect your personal data and you just have to assume it will end up in the hands of others, often cybercriminals. Facebook was hugely irresponsible, and some think criminal, in thinking they could just request that the data not be shared and take the word of a company that was motivated not to comply. With the thirst for personal data by most everyone these days, the only way to prevent its dissemination is to never provide it. These games and surveys may seem to be fun, but they are often just as nefarious as an anonymous caller asking for your bank account number.

Yahoo and AOL Just Gave Themselves the Right to Read Emails, Access Bank Records