NEWS BRIEF

Data From 87 Million Facebook Accounts Exposed

Facebook recently announced that political consulting firm Cambridge Analytica obtained information from up to 87 million accounts without their users' consent. Experts believe that collected data could include locations, interests, photos, status updates and more.

Facebook applications and third-party services can normally request access to an account's information in order to add functionality or advertise products. However, experts allege that Cambridge Analytica violated Facebook's terms of service by using the data to direct political campaigns and influence voters.

These allegations have highlighted concerns about data security, social media privacy and Facebook's data protection practices. In order to keep your personal information safe, it's important for you to be aware of how it can be exposed and what steps you can take to ensure you control access to your data.

Timeline of Events

In 2014, University of Cambridge researcher Aleksandr Kogan created a Facebook personality quiz that gave him data on approximately 270,000 Facebook users. At the time, Facebook's terms of service also allowed Kogan to access data on these users' friends—a total of 87 million accounts.

Although Kogan told users that their information would only be used for research, he later worked with Cambridge Analytica to market the data to political groups. While many experts speculate that Cambridge Analytica's clients used this data to direct political messages and influence voters, investigators have yet to confirm if or how the data was used.

Facebook learned that Cambridge Analytica possessed the data in 2015 and requested that all copies be deleted. However, in March 2018, a number of news sources reported that the consulting firm kept and continued to use at least a portion of the data for its business practices. As a result, Facebook's data protection practices are now under investigation by regulators.

Protecting Your Data

Many social media users assume that their personal information is safe, but this scandal has shown the importance of re-evaluating online security. Hackers can use data posted on social media to engage in identity fraud, social engineering schemes and more. Here are some tips you can use to secure your data on social media platforms:

- Check Facebook's webpage about the exposed data to see if Cambridge Analytica obtained any of your personal information.
- Go through all of the privacy settings on each of your social media accounts to see if the security features or terms of service have changed.
- Always assume that any information you post online can be shared with the public.
- Enable two-factor authentication on all devices and services that offer it.
- Create strong passwords and update them regularly.

Call us at 920-921-5921 for more help staying safe online.

hierl