Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2018-0012

Safeguarding Personally Identifiable Information on Social Networking Sites

Original Issue Date: March 22, 2018

Description

According to Facebook Inc, the personal data of Facebook users has been obtained without knowledge of both the users and Facebook for unauthorized activities. In 2013, an app was developed by a third party that offered a personality test which allowed people to log in to the application using their Facebook credentials. The app also tracked personal information of users along with details of the users' friends. Facebook admitted there has been a data breach as the personal data tracked was used by various external parties for unauthorized activities. In the wake of this development, users are advised to take diligent measures to safeguard their personal data.

Security Best Practices to Social Media Users

In order to keep the social media accounts safe and secure, the user's are requested to follow the below mentioned best practices:

- Do not post private information and do not disclose your location. Facebook being part of a public network could allow easy access to information which should not be disclosed. It is advised that Facebook and all other social media users should not share their Personally Identifiable Information (PII) or Personal Information (PI) on these sites or Apps.
- Users should not share official data or personal secrets on social media messaging platforms. Social media users should never share details like there vote preferences, PIN, Passwords, Credit Card details, Banking details, Passport Details, Aadhaar Card details and all those details which are meant to be kept secret for personal safety & security.
- Do not allow unknown / untrusted applications to access your Facebook account. Be diligent in giving permission to third party apps that can access public profile, which includes name, profile pictures, username, user ID (account number), networks including your friends list, gender, age range and locale.
- Do not open messages/images received from untrusted sources or received unexpectedly from trusted sources.
- Use Strong Account-Specific Passwords Create a strong password which includes symbols, capital Letters, and lower-case letters. Use a mix of different types of characters to make the password harder to crack. You should also create an equally strong and unique password for the email

address associated with your social media account. Keep your password in a safe place. Consider using password management software to store all of your login information securely.

- Exercise caution while visiting websites or web links that ask users to add browser extensions or downloads plugin files.
- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
- Close accounts which are not being used. They could be compromised without the user's knowledge
- Assess the applications being used in your mobile devices or browsers. Most of the applications either use Facebook or Google to Sign In.
- Keep all mobile apps updated. Update security settings on social networks regularly.
- New login Email alerts. Enable alerts for new log in or change of credentials.
- In case of any abuse or data breach, users are advised to immediately contact Abuse/Helpdesk of concerned social media portal as well as, lodge a complaint with the local cyber police station.

References

CERT-In Advisory on Safeguarding Online Identity (CIAD-2017-0011)
https://www.facebook.com/zuck/posts/10104712037900071
https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas
https://www.thrillist.com/news/nation/how-to-protect-your-facebook-data-breach-settings
http://www.bbc.com/news/world-us-canada-43494337

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India