Hello **Everyone**,

I found this interesting **Threat, or the Data Breach** happened with the Facebook, it has often been criticized for the way it handles user information and for the security measures it takes to protect user data. Once, again, much to the users' horror, Facebook profile data of over 267 million users was stolen and was being sold on the dark web.

Now-a-days the social media platforms like Facebook, Instagram, TikTok, etc. are always on the receiving end of outrage when it comes to handling user data, which makes out the question on the data-sharing practices and lax security measures which acts as an open invitation for threat actors. A “threat actor” was found dropping an online bomb by dropping the identities of 237 Million Facebook users and the prices for the data drove for just $540.

A company named **Comparitech**, collaborated with security researcher **Bob Diachen**ko, came across the cache of Facebook accounts data stored on the Elasticsearch server. Researchers at **Cyble** also purchased the data off the dark web to verify and found that cache data didn’t contained the password, or any information used for authentication except the sensitive user information including email, phone number, Facebook ID, last connection, status and age.

Sadly, this is not the first time that Facebook user data has made its way on to hacker forums or deep web sites. Just last month, a similar dataset of Facebook profiles, mostly from the United States, was made available in an open database on Elasticsearch, containing details including users’ full name, their phone number, and a unique Facebook ID.

Even though no passwords were breached here, users are well advised to change their passwords and to ensure that they have not reused a password on Facebook that they use elsewhere. With email addresses in hand, attackers can match those addresses against breaches which do include passwords and then try various sites. Password reuse is the single biggest enabler of account hijacks. Facebook users—as with other sites—are also well advised to enable two-factor authentication. This ensures that any username and password breach will not enable an attacker to access your account, the use of such protection will prevent more than 99% of successful attacks on your accounts. The option is available under Settings—Security and Login.

Meanwhile, users can check whether their email addresses have been found in dark web data breaches on Cyble’s site here: <https://amibreached.com/>

**References:**

<https://www.forbes.com/sites/zakdoffman/2020/04/20/facebook-users-beware-hackers-just-sold-267-million-of-your-profiles-for-540/?sh=2d74a2ed7c85>

<https://www.techradar.com/news/millions-of-facebook-profiles-for-sale-on-the-dark-web>

<https://securityboulevard.com/2020/06/your-hacked-facebook-account-goes-for-75-on-the-dark-web/>

<https://gadgets.ndtv.com/internet/news/facebook-account-data-267-million-sold-dark-web-542-security-breach-2215560>

Facebook is desperate to repair the reputational damage that started with the Cambridge Analytica scandal and lurched through various data protection, privacy and ad tracker scandals. This data is likely from a past breach and does not suggest current weaknesses with Facebook’s systems—the company was approached for any comments on this latest story or further detail on the user data involved.

Even though no passwords were breached here, users are well advised to change their passwords and to ensure that they have not reused a password on Facebook that they use elsewhere. With email addresses in hand, attackers can match those addresses against breaches which do include passwords and then try various sites. Password reuse is the single biggest enabler of account hijacks.

Facebook users—as with other sites—are also well advised to enable two-factor authentication. This ensures that any username and password breach will not enable an attacker to access your account, the use of such protection will prevent more than 99% of successful attacks on your accounts. The option is available under Settings—Security and Login.

Meanwhile, users can check whether their email addresses have been found in dark web data breaches on [Cyble’s site](https://amibreached.com/" \o "https://amibreached.com" \t "_blank) here.