TECH HIVE ADVISORY

SECURITY ADVISORY SERIES

Cybersecurity, News, Events and Threat Advisories.

Volume 1. Issue 4.

THREAT ADVISORY

9 Million Nigerians' Personal Data Exposed in Facebook Data Breach

TLDR: Facebook experienced a data breach in which 533 million users from over 100 countries were found on the dark web and free to download. This breach was discovered by a security researcher, Alon Gal. The personal data include the names, phone numbers, email addresses, workplace, location, dates of birth and account creation dates of 9 million Nigerians.

See detailed information here.

SEVERITY **HIGH**

What is the issue?

In 2019, threat actors explored a vulnerability that let them access phone numbers of Facebook users. Facebook claimed that the personal data exposed were not just scraped off Facebook. It claimed that they were part of those breached in 2019 but were just being exposed by the threat actors. It further claimed that it had fixed the vulnerability since 2019. It is still unclear if this is the case. However, the exposure of the personal data shows that the possible risks were not adequately mitigated.

The leaked data represent more than 30% of Facebook users in Nigeria. If you use Facebook in Nigeria, there is a high chance that your personal data is part of the leaked information.

Possible Risks

Identity Theft: Criminals can use your personal data to impersonate you to steal more of your data or trick your friends or family into parting with some money while they think it is you.

Phishing: Threat actors may send fake emails to your leaked email address posing as genuine organisations asking you to take urgent actions by clicking on a malicious link which may lead you to a lookalike page of the genuine organisation. Here, you may be asked to enter or provide sensitive information that can be stolen and used to steal from you.

Smishing: This is similar to phishing but is perpetrated through text messages.

Vishing: You may receive calls from perpetrators who pose as your bank, public authorities, or service providers asking for sensitive information.

What should you do ?

- Visit "Have I Been Pwned" website to confirm if your phone number is among the leaked data.
- Change your password if you are impacted. Use unique and strong passwords. It can be created using a trusted password manager.
- Look out for suspicious calls, text messages, and email addresses. Confirm any such requests from the appropriate quarters.
- You are advised to reduce the amount of information revealed online because perpetrators look out for your digital footprints to put together and give meaning to information about you.

Curated by Tojola Yusuf
@tojolabilqis Tojola Yusuf

contact@techhiveadvisory.org.ng
www.techhiveadvisory.org.ng
@Hiveadvisory