Devolutions

How to Check Whether You're Part of the Massive Facebook Data Breach

"USER TRUST" IS CERTAINLY NOT ON THE LIST OF BREAKABLES

Facebook's motto is "move fast and break things." And although "user trust" is certainly not on the list of breakables, that may be the case in the wake of a massive data breach at the social media giant.

About the Breach

On April 3, 2021, security researcher Alon Gal revealed that the personal details of 533 million Facebook users had been leaked on the Dark Web. The details included:

- Phone number
- Facebook ID
- Full Name
- Current Location
- Past Location
- Birthdate
- Account Creation Date
- Relationship Status
- Bio

In some cases, email addresses were also stolen. It is expected that bad actors will use the information to carry out social engineering, scamming, and other illicit activities. As reported by theconversation.com, the breach is believed to relate to a vulnerability that Facebook claimed it fixed in August 2019. While the precise source of the data cannot be confirmed, some cybersecurity experts believe that it was acquired through the misuse of legitimate functions within the Facebook systems.

The Impact

While all breaches are worrisome, what makes this one particularly alarming is that it includes phone numbers. Commented Troy Hunt, the creator of Have I Been Pwned? database:

For a targeted attack where you know someone's name and country, it's great for mobile phone lookup. Much harder to do en masse as there's no reliable key; I couldn't take a big list of emails and resolve them to phone numbers as email is rare in the data. But for spam based on using phone numbers alone, it's gold. Not just SMS, there are heaps of services that just require a phone number these days and now there's hundreds of millions of them conveniently categorized by country with nice mail merge fields like name and gender.

What to Do About It

If you're one of 2.6 billion Facebook users — and there's a very good chance you are — then the first thing you need to do is see if you've been caught up in the breach. There are a couple of sites that can help you:

- Have I Been Pwned? You can also see if you have been part of any other known breaches.
- The News Each Day. To protect privacy, this site generates random phone numbers that start with the same 5 digits as your number, and then sends 99 fake and 1 real number to the server — which ultimately means the server doesn't know which number is real, and neither will hackers who may be snooping.

Additional Advice

Hopefully, you are not part of the 533 million users who are affected by this breach. Regardless, however, we urge all users to adopt the following password management best practices:

- Use 2FA on all of your accounts. There are many good 2FA tools out there, including our own (and free) Devolutions Authenticator.
- Use a robust password manager. Yet again, there are many good password managers out there, including our own (and yes, free) tool Password Hub Personal.
- Never use the same password more than once, and never re-use an old password.
- Before choosing a password, check to see whether it has been compromised in the past. You can do this by going to the above-noted site Have I Been Pwned? As you may be aware, Remote Desktop Manager's built-in password check feature is integrated with the Have I Been Pwned? database. For a video overview and to find out how to set up the Pwned password check, please click here.
- Be very careful about what you share on social media! Even seemingly harmless activities like posting a photo of an airline boarding pass can lead to an identity theft nightmare.

We will keep our eye on Facebook breach, and publish updates as they become available. Until then, stay safe out there in the cyber jungle!