valencia

August 16, 2024

More Data Breaches... Do We Still Care?

Data breaches are happening more often and are getting more serious. This week, 2.7 billion data records, including sensitive information like Social Security numbers (SSNs). Although the specific origin of the breach are not entirely clear, the data allegedly comes from National Public Data, a company collecting and selling access to personal data for background checks, criminal records checks, and for private inquiries. National Public Data was also hit last April, when a threat actor known as USDoD claimed to be selling 2.9 billion records with the personal data of people in the US, UK, and Canada. At the time, USDoD claimed the breached datasets contained records for every person living in those three countries. This week, another threat actor known as Fenice leaked the most complete version of the stolen National Public Data datasets as yet for free. Researchers have confirmed that each records includes a person's name, mailing addresses, and social security numbers; none of the data is encrypted.

This is not news. In the past few years, the implications of data breaches have been steadily rising. National Public Data was known for collecting user data through data scraping, a method which is being increasingly used by a variety of different organizations. Data scraping is an automated process, where large amounts of data are extracted from websites or online sources, typically using specialized software or bots. This data is often collected without the consent of the website owner or users and can include various forms of information such as text, images, and personal details. With the rise of AI, data scraping has only increased.

Should We Care?

With privacy breaches being so common and our information being collected by so many different parties, many are asking whether we should still care. Is this our 'new normal'? We think that we should. People's indifference to data leaks come from many factors. Many are unaware of the risks, especially since the technical aspects of cyberattacks are difficult to understand, and the consequences of data leaks are often not immediate. This leads to a false sense of security, as people believe that "nothing is going to happen." The overwhelming frequency of breaches has caused "security fatigue," where constant exposure has desensitized the public. The rise of social media has normalized oversharing, making people more detached from the value of their personal information, but making them more open to data scraping and use for passive reconnaissance by threat actors.

Many believe they aren't targets because they're not famous, or they assume that their data isn't valuable. This mindset is reinforced by the idea that breaches affect millions, and attackers don't care who the individual victims are. Companies often downplay breaches to avoid bad publicity, and even when they do make announcements, they can get lost in the flood of other incidents. Currently, many also prioritize convenience over safety, where people willingly trade personal information for free services without fully considering the risks. This is compounded by the delayed consequences of data breaches, where the harm may not be felt until much later, making it hard for people to connect the breach to its effects. So, while people may know about breaches, they don't change their behavior, leading to widespread apathy that could have severe implications if not addressed through better awareness and education.

Privacy Hygiene in the Land of Breaches

In fact, limiting the information that is collected on you is simple. Privacy hygiene is simple and can easily be implemented, here's what we advise:

1. Start with the basics. Review your mobile device's security and privacy functions, they are available both on Android and iOS. Limit applications' permissions under the security settings and, for those apps that don't need it, turn off location, contact, photos, camera, BlueTooth, and microphone access. Stay on top of your application updates and enable automatic updates if possible.
2. Stay away from personalized ads. Personalized ads involve giving more permissions to applications so that they can track what you search for, where you are, and other types of personal information to send you ads that cater to your needs. While some people find these ads helpful, others find them annoying, but they are certainly a wellspring for future data breaches.
3. Protect yourself. There are many quality privacy protection plug-ins for your browser: we really like Ghostery. It tells you the information collected on you, blocks intrusive cookies. Turn off cross-site tracking and, if on an iOS, enable Private Relay. VPNs are not a silver bullet: make sure to choose reputable ones as many basic VPNs will resell the data they claim to protect.