The Biggest Data Breaches and Leaks of the First Half of 2019

NordVPN Reviews the Most Significant Data Breaches and Leaks of the First Six Months of 2019

August 2, 2019. The first six months of 2019 have been enough for data breaches to affect at least a few billion people. The leaked data includes influencers' phone numbers, security audit logs, student records, banking data, medical records, and much more.

"Assume that if you are online, your data has already been leaked. Criminals can use that data to lure you into a sophisticated phishing attack or influence your votes with personalized ads," says Daniel Markuson, a digital privacy expert at NordVPN.

According to NordVPN's digital privacy expert, the US remains the most popular target country for data breaches and hacks, but they've been happening all over the world.

Here are the five largest data breaches and leaks of the first six months of the year 2019:

1. Collections #1-5 (approx. 3 billion accounts)

Collections #1-5 was a megaleak containing around 3 billion users' records. Cybersecurity researcher Troy Hunt discovered links to all these databases being shared on a hacking forum. This is the biggest selection of compromised data ever, collected over time from several other breaches.

- Collection #1 appeared on the dark web in January. It is said to contain addresses and passwords from over 2000 previous data breaches, which includes the emails and passwords of 770 million people. It appeared on the cloud service MEGA and was available for download via torrent magnet links. Collection #1 contained over 12,000 files and "weighs" more than 87 gigabytes.
- A few weeks later, a megaleak titled Collections #2-5 containing approximately 25 billion unique records and roughly 2.2 billion unique usernames and passwords became available on the internet. It was distributed through hacker forums and torrent sites. Collections #2-5 amount to 845 gigabytes of stolen data. As with Collection #1, most of the stolen data come from earlier thefts, like the breaches of Yahoo, LinkedIn, and Dropbox. Same as with the first batch of data, most of it came from years-old leaks.

2. Cloud service leak (2.3 billion files)

At the end of May, researchers from the Photon Research Team at Digital Shadows discovered that 2.3 billion files were accessible online due to configuration errors. The data was public across data-sharing and cloud services, online storage services, and companies' servers. These files included medical scans, credit card details, payroll files, intellectual

property patents, and at least 11 million photographs, many of which were considered private images. They went public on a Japanese photo-sharing platform called Theta360. Fortunately, the company reacted quickly and sealed the leak over the next 24 hours.

3. Facebook, WhatsApp, and Instagram (2.1 billion users)

This list would not be complete without Facebook and its companies. They are responsible for a whopping 2.1 billion users' data getting breached or leaked.

- In April, a cybersecurity firm called UpGuard found and reported that two third-party Facebook app developers – Mexico-based Cultura Colectiva and an app called At The Pool – stored a total of about 540 million Facebook user data entries on unsecured Amazon Web Services (AWS) servers. This included "comments, likes, reactions, account names, FB IDs, and more" from millions of Facebook users.
- In May, Facebook-owned WhatsApp was breached. Hackers found and exploited a security flaw that left its users vulnerable to spyware. The exact number of victims is unknown, but the app has 1.5 billion users, all of which could have been affected. An Israeli government surveillance agency called the NSO Group designed the spyware. It could turn on a device's microphone and camera, gain access to emails and messages, and collect location data.
- In the second half of May, the contact details of nearly 50 million Instagram users became accessible on a massive unsecured online database. The breached data contains the personal information, such as emails and phone numbers, of high-profile influencers, celebrities, and brand accounts. The database itself was on an Amazon server and was not password-protected. It was traced to a Mumbai-based marketing company called Chtrbox.

4. Internet of Things: Orvibo (2 billion records)

The most recent breach on the list happened at the beginning of July. Noam Rotem and Ran Locar, researchers from vpnMentor, discovered that a user database belonging to a Chinese company called Orvibo, was left openly accessible online. Orbivo runs an Internet of Things management platform. Its database contained over 2 billion logs, including, among other things, users' passwords, email addresses, geolocation details, and, most disturbingly, reset codes. They could be used to reset passwords and email addresses – leaving the users locked out of their accounts forever.

5. Breaches & collections by Gnosticplayers (over 1 billion accounts)

A hacker called Gnosticplayers has been putting batches of hacked data on a darknet website called Dream Market since mid-February. He stole 1.071 billion credentials from 45 companies by the end of May, a goal he was aiming for.

The hacker requested varying sums of bitcoin in exchange for the stolen info and promoted the data in the mass media. He claimed that his two main goals are money and the "downfall of American pigs.".

Gnosticplayers released the stolen information in six rounds, which varied in size and price. It contained data from various apps and companies and included users' full names, email addresses, passwords, location data, social media pages, etc. Some of the affected companies paid fees so that their information would not be released.

One of the largest Australian tech companies, Canva, was affected the most. The company did spot the hacker and managed to close their database server, but not before he stole 139 million users' data – login information, real names, addresses, etc. 61 million of the passwords were hashed with the bcrypt algorithm, one of the most secure algorithms today. The remaining 78 million accounts used Google tokens, which let users sign up for the service without a password.

Why did he do it? According to the hacker himself, sometimes he put the data for sale just because the companies didn't encrypt their users' passwords. "I just felt upset at this particular moment, because seeing this lack of security in 2019 is making me angry," the hacker told *ZDNet*.

Dishonorable mention: medical and financial institutions

It was a difficult half-year for medical and financial institutions as well. A lot of security incidents were relatively small, but the overall number raises concerns. Only few to mention:

- In June, nearly 12 million patients were exposed in a Quest Diagnostics data breach.
- The next day, LabCorp disclosed that the same hack also impacted 7.7 million of their customers.
- American Medical Collection Agency's security breach was by far the worst. It exposed personal and financial information of over 20 million people.

Unfortunately, a lot of financial institutions also suffered from similar attacks. Just a few examples:

- In June, data on 2.7 million individuals and 173,000 businesses was stolen by an employee of Canada's largest credit union, Desjardins. Names, social insurance numbers, age, addresses, emails, and phone numbers were compromised.
- Hackers infiltrated Chile's ATM interbank network, Redbanc, after tricking an employee into downloading a malicious program.
- In February UK-based Metro Bank became the first major bank to suffer from a new type of cyber intrusion that intercepts text messages with two-factor authentication codes.

What it means to digital privacy

These breaches and leaks are more dangerous than they might seem at first. The frequent cyber-attacks could be numbing the public to the privacy risks they represent.

"Due to frequent cyber-attacks and data leaks, people are becoming less attuned to privacy risks," explains NordVPN's digital privacy expert Daniel Markuson. "This may lead to a careless attitude towards their own personal safety, and that would mean more severe damage for all internet users."

Billions of people were affected only this year. It's evident that internet users can't trust companies and even government agencies to keep their data safe. Therefore, they must take cybersecurity into their own hands.

ABOUT NORDVPN

NordVPN is the world's most advanced VPN service provider that is more security oriented than most VPN services. It aims to become the world's easiest-to-use VPN with a strong focus on user experience. NordVPN offers double VPN encryption, malware blocking and Onion Over VPN. It apps provide a unique algorithm, allowing to automatically connect to the fastest server. The product is very user friendly, offers one of the best prices on the market, has over 5,000 servers worldwide and is P2P friendly. For more information: nordvpn.com.