@SENENGROUP

SENENGROUP.COM

SWIPE FOR MORE

12 Months of Data Breaches *2023 Recap*

SENEN

01

JANUARY 2023

Twitter & T-Mobile

A criminal hacker put over 200 million Twitter users' email information on the dark web for sale as a result of this data breach. This was one PR scandal of many for Twitter this year.

T-Mobile USA suffered another data breach that resulted in around 37 million postpaid and prepaid customer data being affected. Information ranged from highly sensitive data such as social security numbers to surnames, and this was T-Mobile's 9th data breach since 2018.

SENEN

FEBRUARY 2023

Activision & Reddit

02

The video game publisher (known for the popular game “Call of Duty”) gave official confirmation of a major data breach in December 2022. Thanks to a SMS phishing attack, hackers gained access of sensitive employee data such as emails, phone numbers, salaries & more, while also gaining access to the company’s 2023 game release schedule. Activision delayed warning employees under the false understanding of the size of the attack.

In a statement regarding the attack on Reddit, the social media company assures that the attacker did not breach their primary system, but they did gain limited access to some employee information and internal dashboards.

SENEN

MARCH 2023

ChatGPT & AT&T

03

A bug discovered in ChatGPT's open-source library caused the AI chatbot to leak customer personal data. This included information such as names, chats initiated, and some limited credit card information, but the company asserts that full credit card information was not exposed.

AT&T notified 9 million customers of the data breach that exposed information including people's names, wireless account numbers, phone #s and email addresses. Although they assert no sensitive information was breached, a small % of cases involved financial information that was several years old.

SENEN

APRIL 2023

04

Yum! Brands & Shields Health Care Group

Yum! Brands (owner of Pizza Hut, KFC, and Taco Bell), reported a data breach from a January ransomware attack. Personal data, including names and IDs, was compromised. An investigation is still underway to assess potential fraudulent use.

The largest data breach of April happened at Shields Health Care Group, a Massachusetts-based medical service provider, affecting 2.3 million individuals. The breach involved sensitive data, including Social Security numbers, DOB, addresses, healthcare history, financial details & more. This information was exposed for two weeks.

SENEN

MAY 2023

05

US Department of Transport & PharMerica

Personal details of 237,000 government employees were exposed in a Department of Transport breach. In a report to Congress, the breached system, typically handling "TRANServe transit benefits," (employee transport expense claims) was mainly isolated to administrative functions, with no impact on transportation safety systems.

PharMerica, a US pharmacy network, notified 5.8 million patients in May of a data breach from March. An unauthorized party compromised systems, exposing personal details, including names, addresses, DOB, SSN, and medical data. Data of deceased individuals was also affected.

SENEN

JUNE 2023

MOVEit

06

MOVEit, a widely-used file transfer tool, was hacked and impacted more than 200 organizations and up to 17.5 million individuals. Multiple federal agencies were affected, including the Department of Energy, Department of Agriculture, and Department of Health, as well as the sensitive data of international firms like Zellis, British Airways, BBC, Shell, Siemens Energy, Schneider Electric, First Merchants Bank, City National Bank, and many more. The Russian ransomware group Clop claimed responsibility for the attack.

As a result, Genworth Financial was among the organizations affected, exposing at least 2.5 million records. US states of Oregon and Louisiana reported compromises in their motor vehicle departments, with the theft of at least 6 million records, including driver's license information.

SENEN

JULY 2023

07

Indonesian Immigration Directorate General

More than 34 million Indonesians had their passport data leaked as a hacker gained unauthorized access to the Immigration Directorate General at the Ministry of Law and Human Rights, with cybersecurity researcher Taguh Aprianto attributing the attack to a hacktivist named Bjorka. The incident, which involved the sale of personal data on the dark web for $10,000, includes residents' full names, genders, passport numbers, issue and expiry dates, and dates of birth. Despite initial speculation about hacktivism, law enforcement is treating the incident more like a traditional cyber attack than a politically motivated one.

SENEN

AUGUST 2023

UK Electoral Commission

08

The UK Electoral Commission disclosed a cyber-attack where hackers accessed the electoral registers containing personal data of around 40 million people. The incident, detected in October 2022, involved compromised servers with emails, control systems, and reference copies of electoral registers from 2014 to 2022, affecting voters' names, addresses, and voting age information. A whistleblower revealed the Commission failed a Cyber Essentials audit around the time of the attack, suggesting inadequate security measures. The Commission, known to run an unpatched version of Microsoft Exchange Server, still hasn't passed the audit.

SENEN

SEPTEMBER 2023

09

MGM Grand & MOVEit

MGM Resorts International faced a significant cyberattack in early September 2023, attributed to the Scattered Spider group and ransomware by ALPHV (BlackCat), resulting in an estimated $80 million revenue loss over five days.

The MOVEit breach continued, notable victims including Better Outcomes Registry & Network had compromised personal health information of around 3.4 million individuals. Another affected organization include the Ontario Birth Registry Data Breach, with over 3.4 million individuals who sought pregnancy care in the past decade had their information accessed, as well as the healthcare data for over 2 million babies.

SENEN

OCTOBER 2023

23andMe & ICMR

10

California-based consumer genetics and research company, experienced a data breach through a credential-stuffing attack. The breach initially revealed 1 million data packs of Ashkenazi Jews on a hacking forum. An additional 4.1 million genetic data profiles of UK and German residents were compromised. The hacker, claiming possession of 20 million 23andMe data records, suggests the likelihood of further data leaks. This breach exposed sensitive data and information regarding users' genetic ancestry and history.

The Indian Council of Medical Research (ICMR) faced a data breach impacting 815 million Indian citizens. Allegedly extracted from the ICMR's Covid-testing database, it surfaced on the dark web recently, containing sensitive information and Aadhaar numbers (a 12-digit government identification number), as reported by Resecurity.

SENEN

NOVEMBER 2023

11

Kid Security & Idaho National Labratory

The widely used parental control app, Kid Security, inadvertently exposed user activity logs on the Internet for over a month due to misconfigured Elasticsearch and Logstash instances. The breach impacted more than 300 million data records, including phone #s, email addresses, and some exposed payment card data.

Idaho National Laboratory (INL), a crucial part of the U.S. Department of Energy, faced a data breach orchestrated by the SiegedSec hacking group. The breach compromised “hundreds of thousands of user, employee, and citizen data," including sensitive information like SSN, bank and health records. The attack impacted current, former, and retired employees.

.

DECEMBER 2023

12

Xfinity (so far)

A security breach at Comcast-owned Xfinity has exposed the personal data of nearly all of its 35.8 million customers, including usernames, passwords, and security question answers. The intrusion, attributed to a vulnerability in Citrix software, occurred in October. While Citrix patched the vulnerability in October, unauthorized users gained access to Xfinity's internal systems, compromising customer data. Xfinity is urging all customers to reset their usernames and passwords, use two-factor authentication, and change passwords for other accounts with similar credentials.

SENEN

SENENGROUP.COM

SENEN GROUP
@SENENGroup

Follow SENEN for more data insights.