**DAYS TO BE NOTED**

Several companies, such as [7-Eleven](https://www.theguardian.com/technology/2019/oct/25/7-eleven-fuel-app-data-breach-exposes-users-personal-details), [WhatsApp](https://www.cnn.com/2019/05/14/tech/whatsapp-attack/index.html" \t "_blank) and [Fortnite](https://www.cbsnews.com/news/fortnite-security-flaw-exposed-millions-of-users-to-being-hacked/" \t "_blank), reported security flaws in the past year that could have exposed millions of customers’ data, but the extent of the accessed data was not reported. Twitter, for example, left the passwords of its 330 million users unmasked in a log, but there was no evidence of any misuse. So, Twitter did not suffer any security breach.

**Yahoo**

**Date:** 2013-14  
**Impact:** 3 billion user accounts

* **Number of records hacked:** up to 3 billion
* **Announced:** September and December 2016

**Details:** Yahoo announced in September 2016 that in 2014 it had been the victim of what would be the [biggest data breach in history](https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html). The attackers, which the company believed we “state-sponsored actors,” compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users. Yahoo claimed that most of the compromised passwords were hashed.

Then in December 2016, Yahoo disclosed another breach from 2013 by a different attacker that compromised the names, dates of birth, email addresses and passwords, and security questions and answers of 1 billion user accounts. Yahoo revised that estimate in October 2017 to include all of its [3 billion user accounts](https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1).

The timing of the original breach announcement was bad, as Yahoo was in the process of being acquired by Verizon, which eventually paid $4.48 billion for Yahoo’s core internet business. The breaches knocked an estimated $350 million off the value of the company.

**Sina Weibo**

**Date:** March 2020  
**Impact:** 538 million accounts  
**Details:** With over 500 million users, Sina Weibo is China’s answer to Twitter. However, in March 2020 it was reported that the real names, site usernames, gender, location, and -- for 172 million users -- phone numbers had been posted for sale on dark web markets. Passwords were not included, which may indicate why the data was available for just ¥1,799 ($250).

Weibo acknowledged the data for sale was from the company, but claimed the data was obtained by matching contacts against its address book API. It also said that since doesn't store passwords in plaintext, users should have nothing to worry about. This, however, doesn’t tally as some of the information being offered such as location data, isn’t available via the API. The social media giant said it had notified authorities about the incident and China’s Cyber Security Administration of the Ministry of Industry and Information Technology said it is investigating.

**3. Veeam**

* **Number of records hacked:** 445 million
* **Announced:** September 2018

It’s not good when a data management firm makes news for mishandling customer data. But that’s exactly what happened to Switzerland-based Veeam. The [company said in a statement](https://www.veeam.com/executive-blog/veeam-data-incident-resolved.html) that one of its “marketing databases was mistakenly left visible to unauthorized third parties.”

Due to “human error,” about 445 million records containing names, emails and IP addresses in the database were visible for about 10 days. But [Veeam said](https://www.veeam.com/executive-blog/veeam-data-incident-resolved.html" \t "_blank) many of those records were duplicates and only about 4.5 million unique email addresses ended up exposed.

**Marriott International**

**Date:** 2014-18  
**Impact:** 500 million customers

* **Number of records hacked:**383 million
* **Announced:** November 2018

**Details:** Marriott International announced in November 2018 that [attackers had stolen data](https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html) on approximately 500 million customers. The breach initially occurred on systems supporting Starwood hotel brands starting in 2014. The attackers remained in the system after Marriott acquired Starwood in 2016 and were not discovered until September 2018.

The attackers were able to take some combination of contact information, passport number, Starwood Preferred Guest numbers, travel information, and other personal information. The credit card numbers and expiration dates of more than 100 million customers were believed to be stolen, but Marriott is uncertain whether the attackers were able to decrypt the credit card numbers. The breach was eventually attributed to a Chinese intelligence group seeking to gather data on US citizens, according to a [New York Times article](https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html).

**MySpace**

**Date:** 2013  
**Impact:** 360 million user accounts  
**Details:** Though it had long stopped being the powerhouse that it once was, social media site MySpace hit the headlines in 2016 after 360 million user accounts were leaked onto both LeakedSource (a searchable databased of stolen accounts) and put up for sale on [dark web](https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html) market The Real Deal with an asking price of 6 bitcoin (around $3,000 at the time).

According to [the company](https://myspace.com/pages/blog), lost data included email addresses, passwords and usernames for “a portion of accounts that were created prior to June 11, 2013, on the old Myspace platform.” According to Troy Hunt of HaveIBeenPwned, the passwords were stored as SHA-1 hashes of the first 10 characters of the password converted to lowercase.

**5. Exactis**

* **Number of records hacked:**340 million
* **Announced:** June 2018

Most Americans had not heard of the marketing and data aggregation firm Exactis before June 2018, but the company had quietly built a database consisting of personal information on hundreds of millions of Americans and businesses.

But that database was built on an unsecure server, a flaw [security researcher Vinny Troia discovered](https://www.wired.com/story/exactis-database-leak-340-million-records/) in early June 2018. Exactis exposed about two terabytes worth of data that included email addresses, home addresses, phone numbers and other personal information such as hobbies and information on any children in the household.

**NetEase**

**Date:**  October 2015  
**Impact:** 235 million user accounts  
**Details:** NetEase is a provider of mailbox services through the likes of 163.com and 126.com. It was reported in that email addresses and plaintext passwords of some 235 million accounts from NetEase customers were being sold by a dark web marketplace vendor known as DoubleFlag. The same vendor was also selling information taken from other Chinese giants such as Tencent’s QQ.com, Sina Corporation and Sohu, Inc. NetEase has reportedly denied any breach. HaveIBeenPwned [lists](https://haveibeenpwned.com/PwnedWebsites#NetEase) this breach as “unverified.”

**Zynga**

**Date:**  September 2019  
**Impact:** 218 million user accounts

* **Number of records hacked:** 218 million
* **Announced:**September 2019

Mobile game producer [Zynga announced in October](https://investor.zynga.com/news-releases/news-release-details/player-security-announcement" \t "_blank) that a hacker had accessed account log-in information on Sept. 12 for customers who play the popular “Draw Something” and “Words with Friends” games.

In addition to the log-in credentials, the hacker accessed usernames, email addresses, log-in IDs, some Facebook IDs, some phone numbers and Zynga account IDs of about 218 million customers who installed iOS and Android versions of the games before Sept. 2, 2019.

In September 2019, a Pakistani hacker who goes by the name Gnosticplayers claimed to have hacked into Zynga's database of Draw Something and Words with Friends players and gained access to the 218 million accounts registered there. Zynga later [confirmed](https://investor.zynga.com/news-releases/news-release-details/player-security-announcement) that email addresses, salted SHA-1 hashed passwords, phone numbers, and user IDs for Facebook and Zynga accounts were stolen.

**7. Republican National Committee (Deep Root Analytics)**

* **Number of records hacked:**198 million
* **Announced:**June 2017

Independent cyber experts found [voter information for 198 million Americans](https://fortune.com/2017/06/19/deep-root-analytics-voter-data-exposed/) on a publicly accessible server in June 2017. It turned out that the Republican National Committee had hired conservative marketing firm Deep Root Analytics, which failed to keep voter information secure.

Deep Root’s cloud server was [publicly accessible](https://www.upguard.com/breaches/the-rnc-files) for about 12 days and contained personal information on voters, including home addresses, birthdays, phone numbers and opinions on political issues.

**LinkedIn**

**Date:**  2012 (and 2016)  
**Impact:** 165 million user accounts  
**Details:** As the major social network for business professionals, LinkedIn has become an attractive proposition for attackers looking to conduct [social engineering](https://www.csoonline.com/article/2124681/what-is-social-engineering.html) attacks. However, it has also fallen victim to leaking user data in the past.

In 2012 the company announced that 6.5 million unassociated passwords (unsalted SHA-1 hashes) were stolen by attackers and posted onto a Russian hacker forum. However, it wasn’t until 2016 that the full extent of the incident was revealed. The same hacker selling MySpace’s data was found to be offering the email addresses and passwords of around 165 million LinkedIn users for just 5 bitcoins (around $2,000 at the time). LinkedIn [acknowledged](https://blog.linkedin.com/2016/05/18/protecting-our-members) that it had been made aware of the breach, and said it had reset the passwords of affected accounts.

**8. Dubsmash**

* **Number of records hacked:**161.5 million
* **Announced:**February 2019

In February, video messaging app [Dubsmash announced](https://www.securedata.com/blog/dubsmash-accounts-hacked" \t "_blank) that hackers nabbed nearly 162 million users’ account holder names, email addresses and hashed passwords.

The breach actually occurred in December 2018, but cyber thieves posted that the data was for sale on the dark web in February. It was part of a data dump that included over 600 million accounts from 16 hacked websites.

**Adobe**

**Date:** October 2013  
**Impact:** 153 million user records  
**Details:**[As reported](https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/) in early October of 2013 by security blogger Brian Krebs, Adobe originally reported that [hackers had stolen](https://www.csoonline.com/article/3268035/adobe-s-cso-talks-security-the-2013-breach-and-how-he-sets-priorities.html) nearly 3 million encrypted customer credit card records, plus login data for an undetermined number of user accounts.

Later that month, Adobe raised that estimate to include IDs and encrypted passwords for 38 million “active users.” Krebs reported that a file posted just days earlier “appears to include more than 150 million username and hashed password pairs taken from Adobe.” Weeks of research showed that the hackers had also exposed customer names, IDs, passwords and debit and credit card information.

An agreement in August 2015 called for Adobe to pay a $1.1 million in legal fees and an undisclosed amount to users to settle claims of violating the Customer Records Act and unfair business practices. In November 2016, the amount paid to customers was reported at $1 million.

**My Fitness Pal**

**Date:**  February 2018  
**Impact:** 150 million user accounts

* **Number of records hacked:**143.6 million
* **Announced:** March 2018

**Details:** As well as Dubsmash, UnderArmor-owned fitness app MyFitnessPal was among the massive information dump of 16 compromised sites that saw some 617 million customers accounts leaked and offered for sale on Dream Market.

In February 2018 the usernames, email addresses, IP addresses, SHA-1 and bcrypt-hashed passwords of around 150 million customers were stolen and then put up for sale a year later at the same time as Dubsmash et al. MyFitnessPal [acknowledged](https://content.myfitnesspal.com/security-information/FAQ.html) the breach and required customers to change their passwords, but didn’t share how many accounts were affected or how the attackers gained access to the data.

**eBay**

**Date:** May 2014  
**Impact:** 145 million users  
**Details:** eBay reported that an attack [exposed its entire account list](https://www.csoonline.com/article/2157782/security-awareness-raising-awareness-quickly-the-ebay-database-compromise.html) of 145 million users in May 2014, including names, addresses, dates of birth and encrypted passwords. The online auction giant said hackers used the credentials of three corporate employees to access its network and had complete access for 229 days—more than enough time to compromise the user database.

The company asked customers to change their passwords. Financial information, such as credit card numbers, was stored separately and was not compromised. The company was criticized at the time for a lack of communication with its users and poor implementation of the password-renewal process.

**Canva**

**Date:**  May 2019  
**Impact:** 137 million user accounts  
**Details:** In May 2019 Australian graphic design tool website Canva suffered an attack that exposed email addresses, usernames, names, cities of residence, and salted and hashed with bcrypt passwords (for users not using social logins — around 61 million) of 137 million users. Canva says the hackers managed to view, but not steal, files with partial credit card and payment data.

The suspected culprit(s) — known as Gnosticplayers — contacted ZDNet to boast about the incident, saying that Canva had detected their attack and closed their data breach server. The attacker also claimed to have gained [OAuth](https://www.csoonline.com/article/3216404/what-is-oauth-how-the-open-authorization-framework-works.html" \t "_blank) login tokens for users who signed in via Google.

The company confirmed the incident and subsequently notified users, prompted them to change passwords, and reset OAuth tokens. However, according to a later [post by Canva](https://support.canva.com/contact/customer-support/may-24-security-incident-faqs/), a list of approximately 4 million Canva accounts containing stolen user passwords was later decrypted and shared online, leading the company to invalidate unchanged passwords and notify users with unencrypted passwords in the list.

**Heartland Payment Systems**

**Date:** March 2008  
**Impact:** 134 million credit cards exposed  
**Details:** At the time of the breach, Heartland was processing 100 million payment card transactions per month for 175,000 merchants — mostly small- to mid-sized retailers. The [breach was discovered](https://www.csoonline.com/article/2935814/lessons-from-the-heartland-payment-systems-data-breach-redux.html) in January 2009 when Visa and MasterCard notified Heartland of suspicious transactions from accounts it had processed. The attackers exploited a known vulnerability to perform a [SQL injection](https://www.csoonline.com/article/3257429/what-is-sql-injection-how-sqli-attacks-work-and-how-to-prevent-them.html) attack. Security analysts had warned retailers about the vulnerability for several years, and it made SQL injection the most common form of attack against websites at the time.

Because of the breach, the Payment Card Industry (PCI) deemed Heartland out of compliance with its [Data Security Standard (DSS)](https://www.csoonline.com/article/3529475/8-pci-dss-questions-every-ciso-should-be-able-to-answer.html) and did not allow it to process payments of major credit card providers until May 2009. The company also paid an estimated $145 million in compensation for fraudulent payments.

The Heartland breach was a rare example where authorities caught the attacker. A federal grand jury indicted Albert Gonzalez and two unnamed Russian accomplices in 2009. Gonzalez, a Cuban American, was alleged to have masterminded the international operation that stole the credit and debit cards. He was sentenced in March 2010 to 20 years in federal prison.