mailguard

18 Cyber-Attacks That Shook The Web

With 2019 being MailGuard's 18th birthday, we've rounded up 18 of the biggest and most noteworthy cyber-attacks that shook the web, and changed how we look at cybersecurity.

2011

Sony PlayStation 1

Famously known as an 'identity-theft bonanza', it was reported that an "illegal and unauthorised person" obtained people's confidential information, prompting the gaming company to go offline.

What
77 million users' personal information

How
Unauthorised network breach

2012

2 Linkedin (2012 - 2016)

The 2012 hack was a result of cybercriminals taking advantage of 'lightly encrypted' passwords.

What
167 million+ customers' details

How
Weak password protection

2013

(2013 and 2014) Yahoo 3

State-sponsored attackers compromised the firm's network, using web cookies to falsify login credentials. This allowed them to gain access to any account without a password.

What
3.5 billion customers' details

How
Network compromised via web cookies

MySpace 4

While it's unclear how the firm's network was exactly breached, various reports point to multiple vulnerabilities in MySpace's user security system, such as poor password encryption.

What
360 million account details

How
Poor password encryption

Target Stores 5

Target's stores suffered a security breach which gave criminals access to the data from the magnetic strips on customers' credit and debit cards.

What
110 million customers' credit card details

How
Stolen login credentials

2014

6 Home Depot

Hackers were reported using stolen credentials from one of Home Depot's vendors. Those credentials were then used to gain a foothold in the network.

What
56 million customers' credit card details

How
Stolen credentials & malware

7 eBay

Hackers got access to the login credentials of 3 eBay employees and used them to infiltrate into the company and stole highly confidential information.

What
145 million users' data

How
Compromised employee information

8 JP Morgan Chase

Hackers likely breached the bank's network via a very basic vulnerability – the bank did not use a double authentication scheme, known as two-factor authentication to protect one of its network servers.

What
76 million households & 7 million small businesses

How
Weak server protection

2015

Ubiquiti 9

The silicon valley computer company all but handed over $47 million after receiving fraudulent emails in its finance department and after falling prey to CEO Fraud.

What
$47 million

How
CEO Fraud

2016

10 Friend Finder Networks

Poor password protection & storage were once again the vulnerabilities within the company's data breach that hackers took advantage of.

What
339 million account details

How
Local file inclusion exploit

11 Facebook (2016 & 2018)

Data firm Cambridge Analytica was accused of harvesting data of Facebook users' profiles without their knowledge to help influence the 2016 American elections.

What
50 million user accounts (2016) &
90 million account credentials (2018)

How
Unauthorised harvesting & account vulnerabilityile inclusion exploit

12 Uber

According to the ride-sharing company, two people who didn't work for the company accessed the data on a third-party cloud-based service that Uber uses.

What
57 million Uber riders & drivers' details

How
Cloud data breach

2017

Equifax 13

A flaw in an internal tool designed to build web applications allowed hackers to take control of a key website.

What
148 million customers' details

How
Web tool design flaw

2018

14 Aadhaar

Hackers reportedly used a system bug to infiltrate India's largest government database that hosts confidential information of each citizen by entering the 12-digit Aadhaar number given to every Indian.

What
1.1 billion records

How
System bug

15 Marriott International Hotels

After an anomaly was detected on Marriott's Starwood guest reservation database, it was discovered that a human operator was interfering with the database and had installed malware in the hotel's network.

What
383 million guest records including 18.5 million encrypted passport numbers & 9.1 million encrypted payment card numbers

How
Remote Access Trojan (RAT)

16 Twitter

A huge security flaw that left user passwords within Twitter's systems unprotected led to passwords being saved in plain text to an internal log.

What
330 million Twitter users' passwords

How
Internal system bug

17 Under Armour

The company discovered an unauthorized party had accessed MyFitnessPal user data by exploiting its usage of a notoriously weak password protection technique.

What
150 million users' details

How
Weak password hashing

18 Google+

In 2018, a "software glitch" allowed third-party developers access to some 500,000 private profile data since 2015.

What
53 million profiles

How
Software glitch

For an in-depth look into each of these cyber-attacks and how they could have been prevented, download our entire report below.

Download Entire Report

Over our 18 years, we've learned that staying ahead of cybercrime with a multi-layered suite of leading security solutions, and keeping your users educated about cybercrime is the best way to stay protected.

Speak to a MailGuard expert about your current cybersecurity strategy and discover how we can support you more.

Phone: 1300 304 430
Email: info@mailguard.com.au