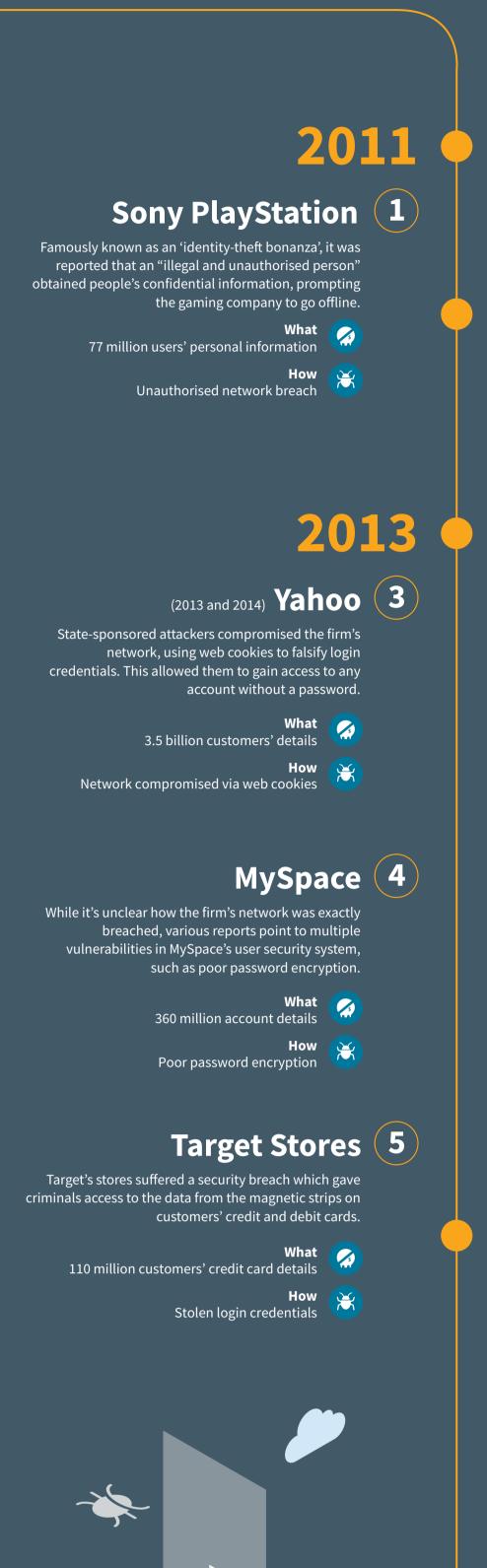




18 Cyber-Attacks That Shook The Web

and most noteworthy cyber-attacks that shook the web, and changed how we look at cybersecurity.

With 2019 being MailGuard's 18th birthday, we've rounded up 18 of the biggest



What \$47 million

How
CEO Fraud

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.





148 million customers' details

Web tool design flaw



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

What

2012

What
167 million+ customers' details

How
Weak password protection

Linkedin (2012 - 2016)



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

What
56 million customers

Home Depot

Hackers were reported using stolen

56 million customers' credit card details

How

Stolen credentials & malware

eBayHackers 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

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 busin

76 million households & 7 million small businesses

How

Weak server protection

2016 10 Friend Finder Networks

breach that hackers took advantage of.

What

339 million account details

Local file inclusion exploit

Facebook (2016 & 2018)

Poor password protection & storage were

once again the vulnerabilities within the company's data

their knowledge to help influence the 2016 American elections.

What

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

Unauthorised harvesting & account vulnerabilityile inclusion exploit

Data firm Cambridge Analytica was accused of

UberAccording 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.

largest government database that hosts confidential information of each citizen by entering the 12-digit

Aadhaar number given to every Indian.

1.1 billion records

What
57 million Uber riders & drivers' details

How
Cloud data breach

Aadhaar

Hackers reportedly used a system bug to infiltrate India's

How System bug

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.

payment card numbers

saved in plain text to an internal log.

What

technique.

Google+

Remote Access Trojan (RAT)

Marriott International Hotels

383 million guest records including 18.5 million encrypted passport numbers & 9.1 million encrypted

TwitterA huge security flaw that left user passwords within

Twitter's systems unprotected led to passwords being

330 million Twitter users' passwords

How
Internal system bug

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

HowWeak password hashing

150 million users' details

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

53 million profiles

How Software glitch

been prevented, download our entire report below.

Download Entire Report

Over our 18 years, we've learned that staying ahead of cybercrime with a

educated about cybercrime is the best way to stay protected.

Email: info@mailguard.com.au

For an in-depth look into each of these cyber-attacks and how they could have

multi-layered suite of leading security solutions, and keeping your users

Speak to a MailGuard expert about your current cybersecurity strategy and

discover how we can support you more.

Phone: 1300 304 430

