



2018's Worst Cyber Scandals

Looking back on 2018, it's evident that, even after the introduction of GDPR, corporate security just isn't keeping up with hackers and cybercrime groups who are becoming more and more sophisticated. A number of data breaches made headlines - perhaps most notably the British Airways and Facebook hacks - but that's just the tip of the iceberg.

It's estimated that there were [3,676 data breaches](#) in the first nine months of the year alone, leaving billions of personal records compromised. With that being said, 2018 is on

track to be the worst ever for data breaches, so it seems only right that we recount the worst cyber scandals.

Facebook Hack

While, for the most part, cybersecurity and tech news tend to float under the mainstream media's radar, Facebook made headlines around the world when a security breach exposed the accounts of 50 million users. Of course, the attack came at a bad time for Facebook. They were already facing scrutiny for how they handled user information and for the spread of disinformation which affected the 2016 US Presidential election.

Hackers gained access to Facebook's systems through three software flaws, two of which were actually introduced by an online tool meant to improve the privacy of users. Attackers were able to access any app that allowed users to log in through Facebook, including Spotify, Instagram and hundreds of others.

Under Armour Hack

In late February, hackers breached Under Armour's MyFitnessPal app, giving them access to the usernames, e-mail addresses, and passwords of the app's 150+ million users. Fortunately, hackers weren't able to get their hands on more valuable information like credit card numbers, locations, and birthdates.

While Under Armour was somewhat diligent in their security, having hashed some users passwords using bcrypt, most user passwords were encrypted using a weaker hashing scheme called SHA-1.

British Airways Hack

Between August 21 and September 5, the personal and financial details of BA customers who made or changed flight details either on the airline's website or through the app were compromised. Unlike the Under Armour hack, valuable information was stolen, including all the information (card numbers, expiration dates, and three digit CVC numbers) needed to authorise a transaction.

It's estimated that 380,000 transactions were affected.

Marriott Hack

After an unauthorised party gained access to Marriott's Starwood guest authorisation database, information relating to 500 million guests was seized. Of that 500 million, nearly 350 million had a combination of name, address, passport number, and check-in/check-out information stolen.

The breach began in 2014, and Marriott has advised that any guest staying on or before September 8 of this year could have been affected.

Aadharr Hack

As mentioned in the previous article, in early January, reporters with the Tribune News Service in India learned of an ominous service being offered via WhatsApp that gave anyone with login details access to the personal information of over 1.1 billion Indian citizens. The reporters paid just 500 rupees (just over £5.60) to receive their login credentials and, after entering any Aadhaar number (the 12-digit unique identifier assigned to every Indian citizen), you could retrieve the queries citizen's name, address, photo, phone number, and e-mail address.

For just 300 rupees more, you could access software that would allow you to print an ID card for any Aadhaar number.