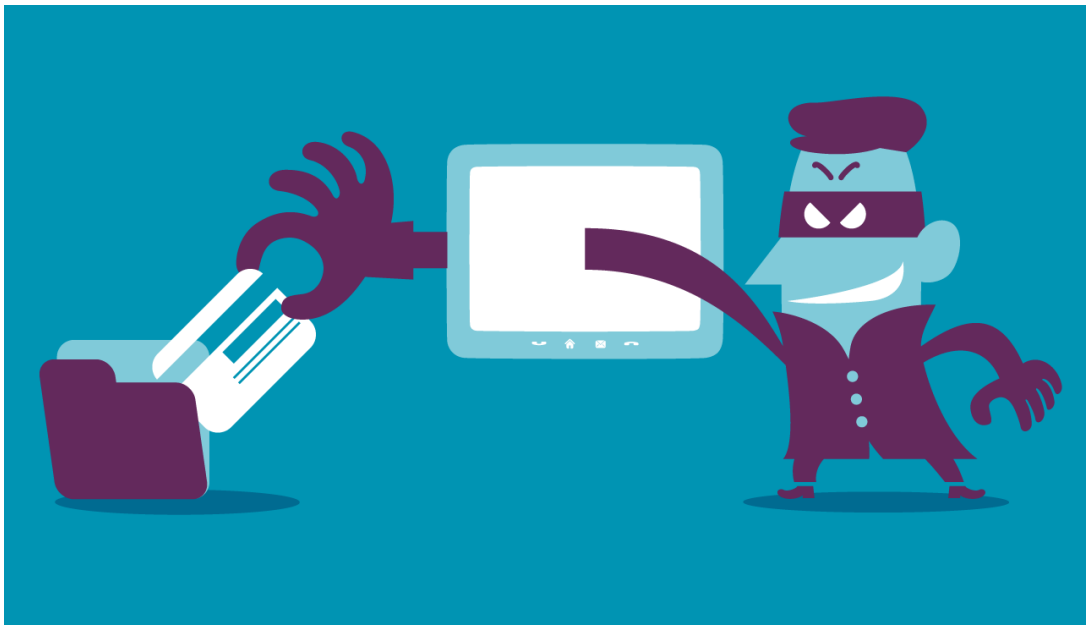
5 devastating data breaches and what you can learn from them…

Running a business is hard, and with technology growing and becoming all the more sophisticated, you are having to constantly adapt and grow with this technology. Unfortunately, we have some bad news for you; as you are adapting to new forms of technology and doing your best at keeping up to date, so too are hackers. Worms, malware, bots, spyware, and many other forms of cyber-crime can easily affect your business, therefore it's crucial business owners and managers have the knowledge they need to prevent these attacks and keep sensitive information secure.

Here we discuss 5 different data breaches and cyber-attacks. Hopefully after reading this you will have learnt some new tips to protect yourself against and be more knowledgeable about how to deal with threats in the future.



The 2008 Heartland payment systems Inc. card number breach…

The first cyber-attack that will be covered is the 2008 security breach: affecting Heartland payment systems Inc. This attack exposed around 130 million card numbers that customers had inputted into the Heartland systems, with the company known to process card information and store it- and the hacker responsible; Albert Gonzalez.

Gonzalez used a common hacking technique named SQL injection; he was able to enter malicious code in SQL statements through web page input. This allowed him to install sniffer software, which monitors and records data of any traffic that enters their website. Consequently, any card numbers, contact details, or other sensitive information that is entered onto the site could possibly be compromised and hacked into.

In order to prevent this hacking from occurring to you and possible affecting your business, encrypt the information stored by using a third-party encryption tools and using two factor authentication (2FA). This may seem like obvious advice, but it's great practice when it comes to keeping your data secure; as CSO mentioned in an article surrounding data breaches: 'while endeavouring to detect and respond to sophisticated attacks from advanced persistent threats, don't forget the fundamentals of security'.

Living Social 2013 customer information hack…

The Living Social online marketplace website was hacked in April 2013, with the impact being disastrous, 15 million customers' names, dates of birth, emails, and passwords being leaked. This means the hackers has access to the customers' personal information, which likely caused a lot of damage as well as decreasing the company's reputation, as less customers trust the site with inputting their data.

However, the breach could have been a lot worse and (ironically) due to Living Social's security they prevented at least the customers' card information from being stolen as well as other sensitive information. This is because the card information was fortunately stored in different systems, not affected by the breach, which may teach Living Social to learn from themselves in the future and secure their systems one step more by taking action's such as these further. Other companies can also learn from both their mistakes and lead to them storing information on separate systems in order to avoid financial chaos among customers if hacked.

Adobe 2013 customer information hack…

Tech giant Adobe is no exception to the rule that any company, big or small, can be hacked: as they were in 2013- with a hacker gaining access to customer information such as credit card information as well as the source code of Adobe products. This breach impacted 38 million users, giving the hacker access to extremely sensitive information and, as before, causing Adobe's reputation to weaken in trust from their customer's.

In this case, a great prevention technique to stop the hacker's would have been if their user's passwords had been hashed. This means that if they were encrypted using a process that cannot be reversed to show the original text, the passwords would be much more secure and would be an example of how zero-knowledge networks from companies can help prevent hacking. Therefore, if you're a business who doesn't want to get hacked, you should always be encrypting and storing data in safe locations, as opposed to keeping all of the information in the same place.

However, Adobe suffered another breach in 2019 and had clearly learnt their lesson at least partially from the first attack, as the exposed data didn't include any passwords or financial detail. However, they didn't learn enough, it seems, as the breach did involve email addresses. This could have easily been avoided by Adobe not leaving data exposed and always password-protecting their systems more securely, such as using multi factor authentication. They also should have been careful as to which online database they used, as relying upon a database that has been hacked before such as Elasticsearch likely wasn't their smartest move…

If you're a company looking to back up your data in a secure location in order to avoid a possible data breach/ you act quickly if it happens, consider using a system such as Amazon Web Service (AWS) as they are reliable and cost effective, therefore great for smaller business!

Marriott hotel chain customer records hack…

The Marriott hotel chain in London is currently facing a lawsuit over a vast data breach that occurred in mid-January 2020. The breached data included guests' names, home and email addresses, telephone numbers, as well as passport and credit card details, with a massive 5.2 million records being breached. Other sensitive information such as the customers' Marriott loyalty account information, other personal details such as employers, their age and gender, birthday's, their company partnerships, and language preferences. This additional information may not seem very important but it can be extremely useful to hackers when guessing passwords and hacking other accounts relating to the individual customers. This also damaged trust in the company's brand which may affect them in the long run. Personal data such as this can also be sold on the dark web allowing criminals to impersonate those involved and ultimately get id and loans in their names.

Attackers breached the Marriott by gaining access to their application, being operated and franchised through the Marriott brand in order to provide more services to guests at hotels. The hackers gained access to this and therefore access to customers by compromising 2 members of staff at one of the hotels and using their login's. this may have been caused by traditional hacking, but may also have been caused by social engineering, in which the hacker physically visits the location they want to hack into, or make contact through calling or emailing the victim; all while disguising as someone trustworthy. In this case it may have been a cleaner or another employee to gain access to information such as the information stored on the application.

Overall, this is a example of what training your staff well can achieve in terms of preventing data breaches such as this one. Software updates and patching may also be a factor, as having the most secure systems they can be can give businesses a huge advantage when helping to prevent data breaches such as this one.

British Airways stolen card information hack…

With airlines such as British Airways (BA) needing so much information about their customers in their databases, it was only a matter of time before a colossal hack such as this occurred. Customer's names, where they intended to fly to, their addresses, email addresses and even card

information were all breached, including the most valued information on the card: the card verification value (CVV) found on the back of the card.

Hackers achieved this by directing the customers to a site they perceived as a BA website, then entering their details and those details being hacked.
However, BA paid for this breach in more ways than one. With a diminishing reputation for data security being inevitable, but also through fines of approximately £183 million (paid to the government in order to support government funds), as severe damage was done here to many of their customers. The Information Commissioner's Office (ICO) has also stated that BA will receive a Data Protection Act penalty notice. Finally, GDPR states that (as BA did not succeed in protecting their customer's information) they could be looking at fines up to £488 million, equating to 4% of BA's annual income in 2017.

Situations such as these show just how vital IT security is right now, with large companies facing such severe data breaches. And if hackers can target these companies and hack into their databases to collect information, what makes you think they couldn't hack into yours?
A hack like this can be prevented by adding an extra layer of security such as two factor authentication, as well as continuously updating your systems to stay up to date with the latest security software.

Update: as of October 2020, British Airways now only have to pay a fine of £20 million, after investigators of the card information hack took into consideration the airline's financial dilemma and the circumstances of the cyber-attack.