Data Breach Case Study

Team 1

Hung-Wei Lin

CASE STUDY

MY FITNESS PAL

myfitnesspal

MyFitnessPal is a web-based exercise and fitness social media applications available.

Keep track of user's daily intake of

- food
- Beverage

Calculating all user's

- nutrients
- calories
- vitamins

breach checklist

- What types of data were affected?
- What happened?
- Who was responsible?
- Were any escalation(s) stopped - how?
- Was the Business Continuity Plan instigated?
- Was the ICO notified?
- Were affected individuals notified?
- What were the social, legal and ethical implications of the decisions made?

What types of data were affected?

Affected

- email addresses
- IP addresses
- login credentials
  - usernames
  - passwords

Not affected

- birthdays
- location information
- credit card numbers

What happened?

Date: February 2018
Impact: 150 million user accounts

Around 150 million unique email addresses, IP addresses and login credentials such as usernames and passwords stored as SHA-1 and bcrypt hashes.

The following year, the data appeared for sale on the dark web and more broadly. The company acknowledged the breach and said it took action to notify users of the incident. “Once we became aware, we quickly took steps to determine the nature and scope of the issue. We are working with leading data security firms to assist in our investigation. We have also notified and are coordinating with law enforcement authorities,” it stated.

Who was responsible? Part 1

MyFitnessPal data breach was caused by Under Armour's failure to safeguard the data they held for users.

Under Armour admitted that some proportion of the exposed passwords were only hashed using a notoriously weak function called SHA-1, which has had known flaws for a decade

Who was responsible? Part 2

MyFitnessPal data breach

Hashing function	SHA-1	bcrypt
Used	minority	majority
Affected in breach	Yes	No

Were any escalation(s) stopped - how?

- Work with leading data security firms to assist in our investigation.
- Notify and have coordinated with law enforcement authorities.

Was the Business Continuity Plan instigated?

- Notifying MyFitnessPal users to provide information on how they can protect their data.
- Requiring MyFitnessPal users to change their passwords and urge users to do so immediately.
- Continue to monitor for suspicious activity and to coordinate with law enforcement authorities.
- Continue to make enhancements to our systems to detect and prevent unauthorized access to user information.

Was the ICO notified?

The ICO is the UK's independent body set up to uphold information rights. Find out more about our organisation and structure.

MyFitnessPal belonged to Under Armour, an US based company.

I could not find information about if ICO is notified regarding this breach.

Were affected individuals notified?

MyFitnessPal has notified MyFitnessPal users by the email regarding the issue.

What were the social, legal and ethical implications of the decisions made?

- Shares of Under Armour dropped 3.8 percent
- Negative impact to reputation of the company and application
- The incident raises the awareness of the data security

Reference

Michael, H. & Dan, S. (2021). The 15 biggest data breaches of the 21st century | CSO Online. Available from: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

MyFitnessPal. (2018). Security Information FAQ. Available from: https://content.myfitnesspal.com/security-information/FAQ.html

Lawyers Limited. (n.d.). MyFitnessPal data breach triggers Under Armour lawsuit - Data Leaks, Breaches & Hacks. Retrieved May 8, 2022, Available from: https://www.dataleaklawyers.co.uk/blog/myfitnesspal-data-breach-triggers-under-armour-lawsuit

Newman, L. (2018). The Under Armour Hack Was Even Worse Than It Had To Be | WIRED. Available from: https://www.wired.com/story/under-armour-myfitnesspal-hack-password-hashing/