MONSTER.COM DATA BREACHES

CARLOS R. OCASIO

CSCI 301-61

PROF O'NEILL

DATA BREACH

- Data Breach – “Security incident in which information is accessed without authorization” (Norton, 2020).
- Data Breaches can be costly
  - Data Breaches cost the healthcare industry $6.2B (Higgins, 2016).
  - The out-of-pocket cost of victims in 2016 was estimated to be $56.B (Meisner, 2017).

WHAT IS MONSTER.COM ?

Monster.com is a global employment website that:

- Allows employers to post job requirements for a position to be filled.
- Allows potential candidates to apply for job postings.
- Provides career advice to users.
- Allows users to compare salaries by career fields.

DATA BREACH INCIDENTS

Monster.com is to blame for multiple data breaches and security incidents.

A timeline of the known security incidents at Monster.com:

MONSTER.COM 2007 DATA BREACH

In August 2007, a criminal ring was able to obtain the login information of various employer accounts of the website by using a trojan horse.

- The criminals gained access to records that included personal information of prospective employees (Menn, 2007).
- The stolen information was used to send emails with fake job offerings, which included the stolen information as a form of validation (Menn, 2007).
- The emails contained an executable file that installed a keylogger and ransomware (Menn, 2007).

MONSTER.COM 2007 DATA BREACH

- It took the company five days to notify the users of the data breach (Finkle, 2007).
- The company later admitted that the incident had been going on for a longer period than what was previously thought (QuinStreet Enterprise, 2007).
    - Involved more customers than originally announced (QuinStreet Enterprise, 2007).
    - The company pledged to improve security protocols.
- Two months later, a group of hackers managed to inject an Iframe to the website (InformationWeek, 2009).
- The original breach could have been prevented if the data had been encrypted (Menn, 2007).

MONSTER.COM 2009 DATA BREACH

In January 2009 it was reported that cybercriminals had infiltrated the database and stolen the contact information of users (InformationWeek, 2009).

- Monster refused to cite the numbers of people that were affected (UBM, 2009).
- The estimated number of people affected by this breach is estimated to be in the millions (InformationWeek, 2009).
- Much like before, phishing emails were being used to infect Monster.com users.

MONSTER.COM 2009 DATA BREACH

- After the attack, the company refused to contact affected customers and opted for a public message (InformationWeek, 2009).

- The company also refused to provide details about the attack
  - Spokeswoman Nikki Richardson mentioned “I cannot disclose specific details of the situation because we need to protect the integrity of our security systems and our ongoing inquiry into this situation” (Fraunheim, 2009)

MONSTER.COM 2019 DATA BREACH

- In September 2019, an exposed webserver of Monster.com was found storing the resumes of job applicants (Whittaker, 2019).
- The resumes contained documents that were dated all the way from 2014 to 2017 (Ikeda, 2019).
- The information included in the documents include:
  - Names
  - Phone Numbers
  - Personal Emails
  - Addresses
  - Past Work Experience

MONSTER.COM 2019 DATA BREACH

- The company claims the server exposed is owned by an unnamed third-party (Ikeda, 2019).
- Monster.com did not warn any of its customers.
- Monster.com is no longer working with the unnamed third-party company (Whittaker, 2019).
- The company does not consider itself responsible as the unnamed third-party company “owns the data” (Ikeda, 2019).

MONSTER.COM 2019 DATA BREACH

- The companies' denial of responsibility is legally acceptable under US federal laws.
- The company is not duty bound to disclose the exposure of regulators.

- The company may be held responsible due to the European Union's General Data Protection Regulation.
- The company may have some responsibilities in the matter under California's new “GDPR Lite” law (Ikeda, 2019).

TAKEAWAYS FROM THE MONSTER.COM DATA BREACHES

- Be mindful of the permissions you extend to third-party companies.
- Create an Incident Response Plan.
- In the event of a data breach, notify your customers as soon as possible.
- Encrypt and back-up your data.
- Only store data that you **absolutely** need to run your business.

TAKEAWAYS FOR EVERY-DAY USERS

- Be mindful of the permissions you extend to companies.
- Be mindful of the information you share.
- Do not include personal information on resumes that is not **absolutely** necessary.
- Do not download files from unverified sources.
- Reputable companies will never ask for your personal information over emails.
- Keep track of the companies you have shared personal information with.
- If you no longer need an account with a company, request that the company delete your information from the database.
- Ask companies if you can opt out of your information being sold off to third-parties.
- Back up your data and if possible, keep it away from the network.

Do you trust Monster.com?

“Hackers don’t cause breaches, people do.”
-Frank Abagnale

REFERENCES

- Don't search for jobs, Find the right fit instead. (2020). *Monster*. Retrieved from https://www.monster.com/
- Frauenheim, E. (2009). Latest Breach of Monster's Data Fuels Disclosure Debate. *Workforce*. Retrieved from https://www.workforce.com/news/latest-breach-of-monsters-data-fuels-disclosure-debate
- Higgins, K. (2016). Healthcare Suffers Estimated $6.2 Billion In Data Breaches. *Dark Reading*. Retrieved from https://www.darkreading.com/threat-intelligence/healthcare-suffers-estimated-$62-billion-in-data-breaches/d/d-id/1325482
- Joseph Menn. (2007, August 23). The Nation; Online job hunters become the prey; Thieves cull data from Monster.com, then aim for users' bank accounts: HOME EDITION. *The Los Angeles Times*. https://search-proquest-com.mendel.csuniv.edu/docview/422217585?rfr_id=info%3Axri%2Fsid%3Aprimo

REFERENCES (CONTINUED)

- Quin Street, Monster.com Admits It's Been Hit Before. (2007). *eWeek*. https://link.gale.com/apps/doc/A168198625/AONE?u=chazsu_main&sid=AONE&xid=5582b100
- Quin Street, Monster.com Took Five Days to Disclose Data Theft. (2007). *CioInsight*. https://link.gale.com/apps/doc/A168006913/ITOF?u=chazsu_main&sid=ITOF&xid=29731dee
- Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting, 6*(3), 1-8. http://dx.doi.org/10.12775/CJFA.2017.017
- Monster.com. (2020). *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Monster.com

REFERENCES (CONTINUED)

- Read, C., & Scott Ikeda (2020). How Much Responsibility Should Monster.com Take for Third Party Data Breach? Retrieved October 04, 2020, from https://www.cpomagazine.com/cyber-security/how-much-responsibility-should-monster-com-take-for-third-party-data-breach/
- UBM, "Monster.com Hit With Possible Monster-Sized Data Breach; The company declined to cite the number of affected accounts, raising the possibility that every Monster user could be affected." *InformationWeek*, 26 Jan. 2009. *Gale Academic OneFile*, https://link.gale.com/apps/doc/A192609057/AONE?u=chazsu_main&sid=AONE&xid=217a1934. Accessed 4 Oct. 2020.
- What is a data breach?. (2020). *Norton Online*. Retrieved from https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html
- Whittaker, Z. (2019). Monster.com says a third party exposed user data but didn't tell anyone. Retrieved from https://techcrunch.com/2019/09/05/monster-exposed-user-data-years/