America Runs on Hacked Accounts: Dunkin' Donuts Ethics Case

MSBA 6250, Spring 2019

Danny Moncada
University of Minnesota

Dunkin' Donuts (or as its current rebranding efforts refer to them, **Dunkin**') is an American multinational quick service restaurant, and one of the largest coffee and baked goods chains in the world. The company recently made news, not to debut a new flavored iced coffee or menu item, but to notify the world and customers that the company were victims of a "credential stuffing" attack by online hackers in January 2019. Credential stuffing refers to a type of cyber-attack where hackers take combinations of usernames and passwords that have been leaked from other web sites and use them to gain illegal access to an account on a new and unrelated site [3]. Hackers used customer's credentials leaked on other sites to gain entry to the Dunkin' Donuts Perks rewards accounts, which gives repeat customers that opportunity to earn points and get free beverages/discounts on DD products [2].

This is actually the *second* time in three months that Dunkin' Donuts was targeted; Dunkin' **already** reported a first credential stuffing attack at the end of November 2018 (that attack occurred at the end of October 2018). Customer's personally identifiable information (PII) like their name, email address (which was the username for the rewards program), and account information was exposed [1]. However, hackers were not actually interested in customer information; they put up the hacked account(s) for sale on "Dark Web" forums, and other "Dark Web" users gobbled up those reward points found in the accounts to receive unearned discounts on products from Dunkin' [1].

The leadership at Dunkin' did not appropriately react to the first breach that occurred at the end of 2018, and with data breaches averaging a cost of seven million dollars for U.S. companies in 2018 [7], they must do better or be prepared to take on additional costs due to negligence. As a consequence of the world becoming more digitized [8], firms feel the pressure to adopt technologies to cater to a worldwide audience without ensuring proper security measures are in place, exposing them to more risk. This situation also creates a certain level of discomfort and distrust for Dunkin' Donuts customers; an outbreak of food poisoning at a Dunkin' location might be worse press for a company that makes its living on donuts and coffee, but loyal customers had their information taken from them without any chance to protect themselves.

The firm should do a few things:

1. **Admit fault in not rectifying the situation after the first breach**
2. **Perform an in-depth analysis on the level of exposure, how many customers were affected, what it cost them in rewards and products that were stolen**
3. **Investigate the cost and feasibility of enabling two-factor authentication for their mobile and online platforms**
4. **Work with a partner or firm who specializes in anomaly detection, to better monitor customer purchasing patterns and proactively flag strange behavior** [6]

This second incident should serve as a wake-up call to Dunkin' leadership that they did not properly address the first breach (which will continue happening to other firms in other industries as more and more of the world goes online). They can immediately starting rebuilding customer confidence in their product by admitting they did not do enough to prevent it from happening again (or in the first place). Quantifying the "damage" allows Dunkin' and their leadership to properly assess the scope of the breach and whether this is part of a bigger problem.

The implementation of two-factor authentication is not a "silver bullet", however; there is plenty of evidence that it won't solve every issue [1], but it is a good starting point for providing an additional barrier for hackers trying to get into their delicious rewards. They can learn the lessons of many other firms who successfully made the change to two-factor authentication, including companies like Bank of America, Blizzard, Amazon, and Apple.

Dunkin' can be the first global coffee shop that proactively monitors user spending behavior – an argument can be made that this is just a different type of infringement (Dunkin' would have to admit to monitoring consumer behavior but plenty of firms already do this). However, Dunkin' can reassure customers that this type of data collection/monitoring is not nefarious, and provides the company with a mechanism to flag unusual behavior to identify when customers are buying products they wouldn't normally be purchasing.

Appendix

---

[1] Brandom, Russell. (2017, July 10). "Two-factor Authentication is a Mess." *The Verge*, Vox Media. Retrieved from https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess

[2] Cimpanu, Catalin. (2019, February 12). "Dunkin' Donuts accounts compromised in second credential stuffing attack in three months." *ZDNet*, CBS Interactive. Retrieved from https://www.zdnet.com/article/dunkin-donuts-accounts-compromised-in-second-credential-stuffing-attack-in-three-months

[3] Cimpanu, Catalin. (2019, November 29). "Dunkin' Donuts accounts may have been hacked in credential stuffing attack." *ZDNet*, CBS Interactive. Retrieved from https://www.zdnet.com/article/dunkin-donuts-accounts-may-have-been-hacked-in-credential-stuffing-attack/

[4] McCandless, David and Tom Evans. (2019, February 01). "World's Biggest Data Breaches & Hacks." *information is beautiful*, VizSweet. Retrieved from https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

[5] McCarthy, Niall. (2018, July 03). "The Average Cost of a Data Breach is Highest in the U.S." *Forbes*, Forbes Media LLC. Retrieved from https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#13fac482f373

[6] Murphy, Julia and Max Roser. (2019). "Internet". *Published online at OurWorldInData.org*. Retrieved from https://ourworldindata.org/internet

[7] Teich, David A. (2019, January 09). "Management AI: Anomaly Detection and Machine Learning." *Forbes*, Forbes Media LLC. Retrieved from https://www.forbes.com/sites/davidteich/2019/01/09/management-ai-anomaly-detection-and-machine-learning/#5c41ecf93223