America Runs on Hacked Accounts

Dunkin' Donuts Ethics Case by Danny Moncada

Agenda

- Who is Dunkin' Donuts
- Why did they make the news
- What could they have done differently
- Solving the world's mysteries, one step at a time (if time at the end)

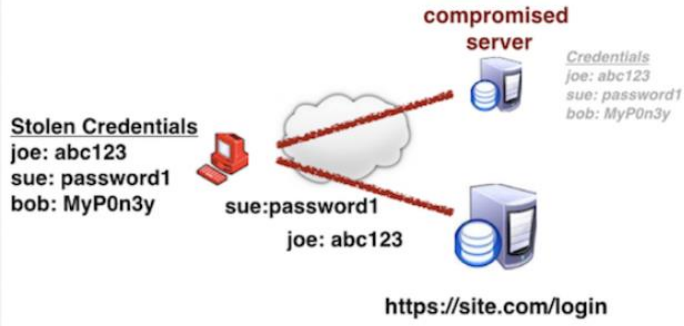
Dunkin' Donuts… err, Dunkin'

- American multinational quick service restaurant founded in 1950
- One of the largest coffee and baked goods chains in world
- Going through rebranding effort simply known as Dunkin'

DUNKIN'

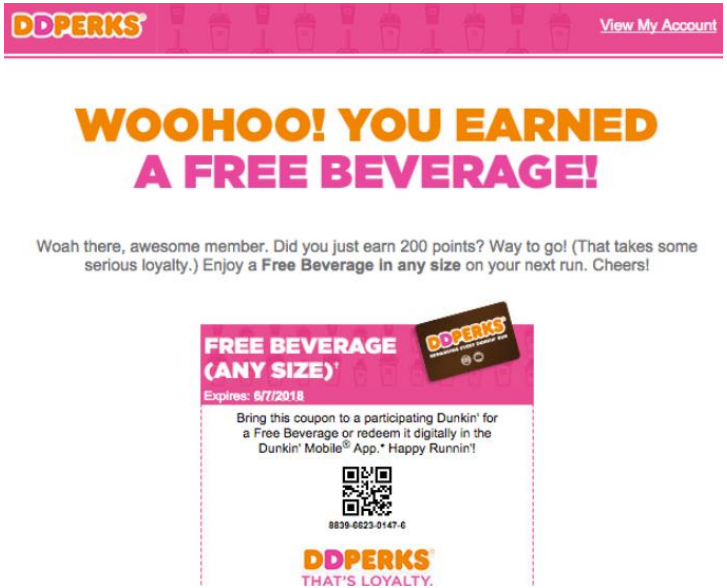
Dunkin' makes the news… for all the wrong reasons

- Not debuting a new flavored iced coffee (yum) or menu item
- Firm became victim of "credential stuffing" attack
  - Hackers used usernames and passwords leaked from other sites to gain access to DD Perks rewards accounts
- **Second** time in three months' Dunkin' was successfully targeted



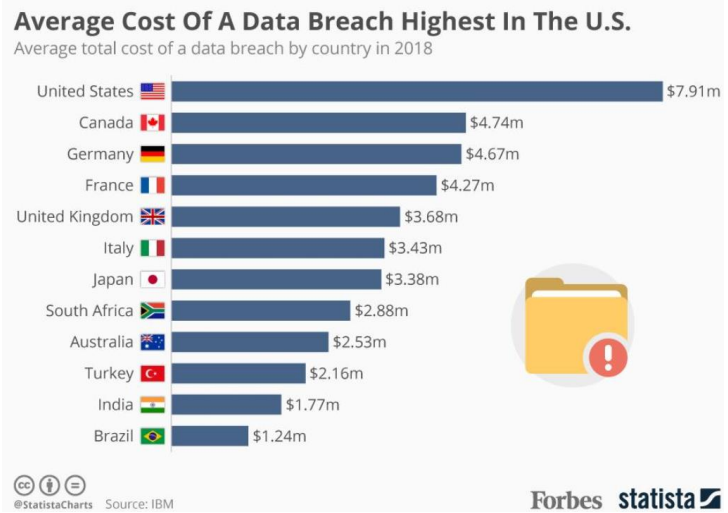
Hackers not interested in customers, but rewards

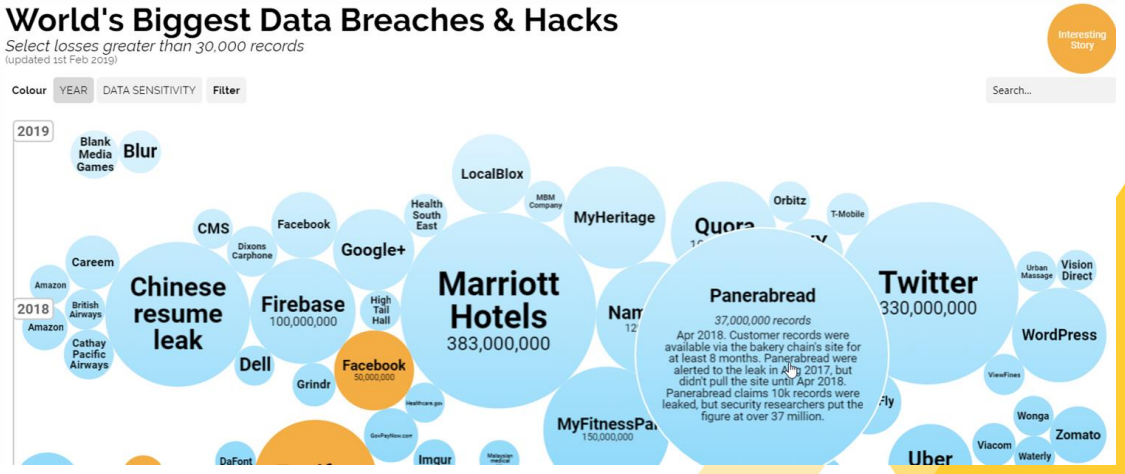
- Customer personally identifiable information (PII) readily available, but not the target
- DD Rewards program accounts were sold on the "Dark Web"
- Other users received unearned discounts on products



Why is this bad?

- Data breaches cost U.S. companies an average of $7M in 2018
- More and more of the world is getting digitized; these situations will continue happening
- Loyal customers had information exposed



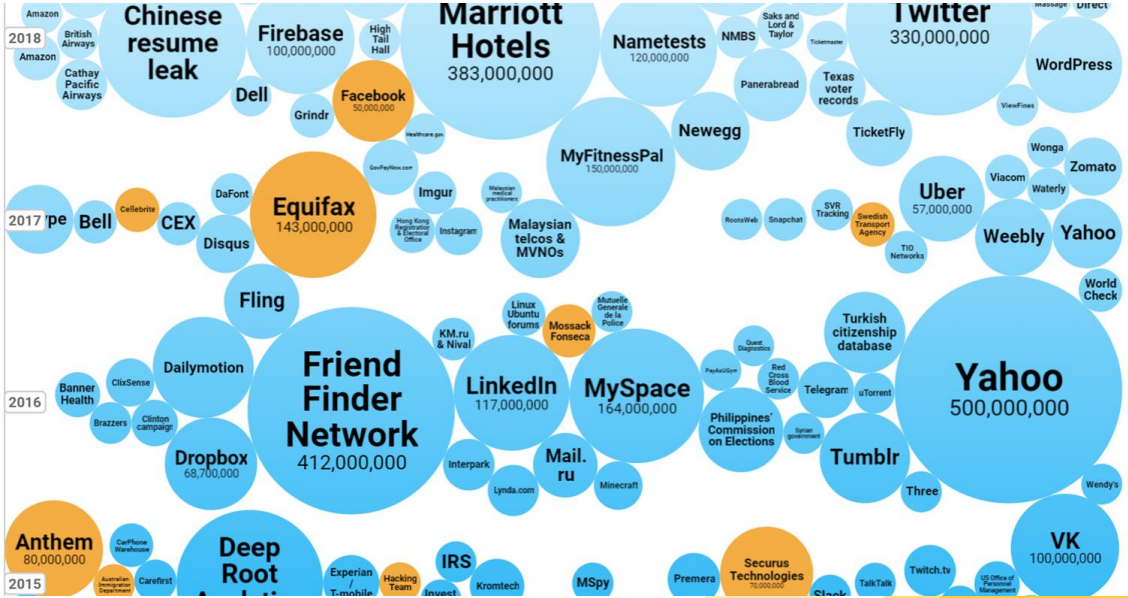


What can Dunkin' DO?

1. Admit fault in not rectifying situation after first breach
2. Perform in-depth analysis on level of exposure (how many accounts affected, what the cost to customers was)
3. Investigate cost and feasibility of enabling two-factor authentication
4. Work with partner or firm specializing in anomaly detection, and better monitor purchasing patterns

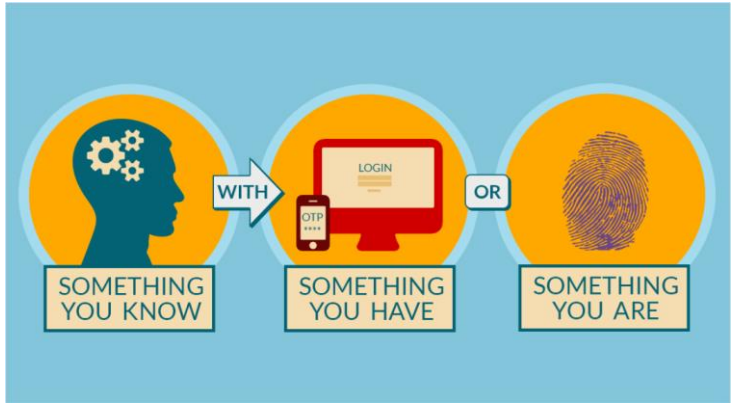
What can Dunkin' DO, Cont.

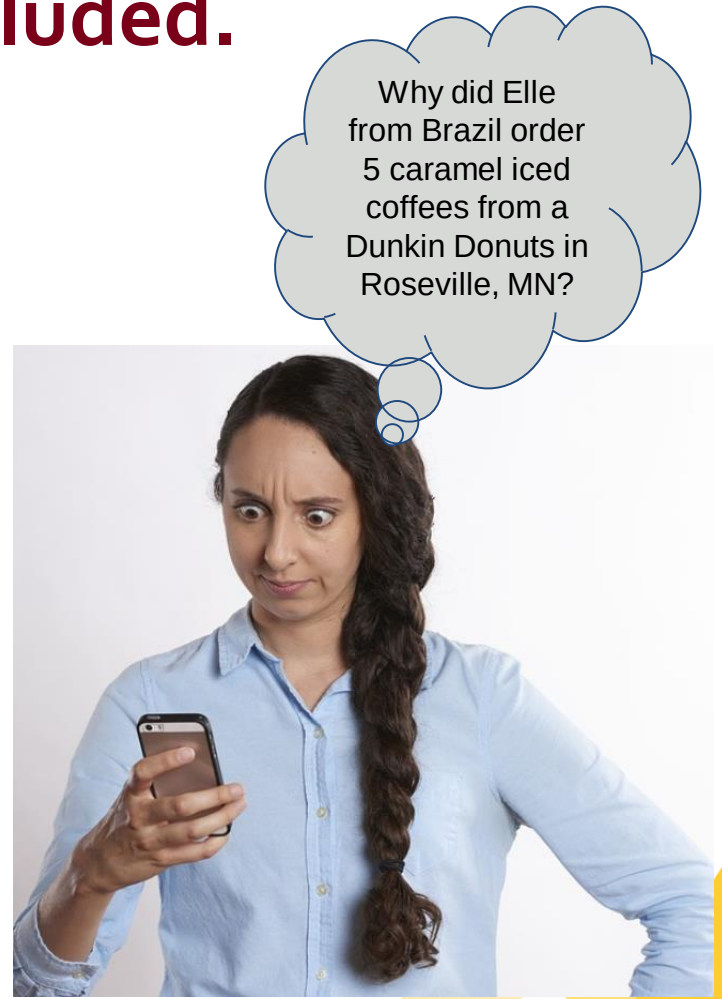
- Second incident is a wake up call to Dunkin' leadership; immediately rebuild customer confidence in product
- Quantify the "damage" allows Dunkin' leadership to properly assess scope of breach



What can Dunkin' DO, Concluded.

- Learn lessons from other firms who successfully implemented two-factor authentication systems
- Proactive monitoring user spending habits behavior provides mechanism to flag unusual behavior





Drawbacks to Proposals

- Two-factor authentication = / = “silver bullet”; plenty of evidence to suggest it doesn’t solve every issue
- Proactively monitoring consumer behavior is just a different type of infringement