A Deep Dive into the 2020 Twitter Hack

Student Name: Cameron Kim

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Diwakar Yalpi

Date: 21 April 2026

Overview

On July 15, 2020, Twitter's internal systems and high profile accounts were compromised to carry out a Bitcoin scam that brought in over $120,000 in just a few hours (Franceschi-Bicchierai). Some high profile accounts that were targeted were tied to big figures like Obama, Elon Musk, and Apple. The breach itself required no complicated malware. Attackers used voice based phishing (vishing) to impersonate Twitter staff and make employees give up their credentials. This incident shows that the most dangerous cybersecurity vulnerabilities are often human, making it a critical subject for social science analysis.

Analysis

The attackers got access by calling Twitter employees and impersonating members of the IT team hoping to build trust and get their credentials. Afterwards, they bypassed the two-factor authentication and took control of these verified accounts. The breach demonstrated that technical systems don't matter if employees are manipulated into granting access (Aggarwal et al. 49).

Solutions

Addressing social engineering requires integrating safeguards with social science based human intervention. Organizations should implement security training grounded in social psychology. Employees need education on influence tactics and manipulative strategies so they can recognize and resist them. Simulated vishing exercises can provide experimental learning that modules can not (Hadnagy 201).

Reflection

This analysis confirms that cybersecurity can't be reduced to a technical skill. The 2020 Twitter Hack makes it clear that human psychology is just as exploitable as software

vulnerabilities. Cybersecurity is fundamentally a human problem; how they respond to pressure determines whether the technical defenses can hold. Integrating social sciences in training produces a more complete picture of real life risk. This approach is not supplementary, it is essential.

Conclusion

The 2020 Twitter breach demonstrates that effective cybersecurity includes a social science approach. Attackers succeeded by manipulating human behavior instead of exploiting code or encryption. Addressing this requires solutions that are equally human centered. Behavioral training can help employees mitigate breaches that they technically cause. Future cybersecurity frameworks should institutionalize this collaboration, treating social science as a core component of security rather than an optional supplement. In the end, securing systems means securing the people within them.

Works Cited

Hadnagy, Christopher. *Social Engineering: The Science of Human Hacking.* 2nd ed., Wiley, 2018. Accessed 21 April 2026. https://digtvbg.com/files/books-for-hacking/Social%20Engineering%20-%20The%20Science%20of%20Human%20Hacking%20by%20Christopher%20Hadnagy.pdf

Aggarwal, Poonam, et al. "Cybersecurity and Human Factors: Behavioral Approaches to Organizational Resilience." Journal of Information Security, vol. 13, no. 2, 2022, pp. 45–62.