**11/29/2023**

**(IS 401/501-01 MERGED) (FA23) CYBERSECURITY PRINCIPLES**

**Final Project - Twitter Hack 2020**

**Amogh Patel**



**Table of Contents:**

[**1. Introduction**](#_1g992um3am2x)

[**2. What Happened?**](#_o7rrk5ymu5oq)

[**3. Company Affected**](#_xgizzhll9ll)

[**4. Weaknesses and Vulnerabilities**](#_aa84lofk1750)

[**5. Impact on the Organization**](#_iujgsj8j4z4z)

[**6. Threat Actors and Motivations**](#_f6ekyxd3x4lt)

[**7. Recommendations to prevent this happening to us**](#_mod5ny1mxjzk)

[**8. Conclusion**](#_eup13135pjlg)

[**9. References**](#_9s98hxqegxwp)

# 

# Introduction:

Typically, when we hear about cybersecurity breaches, we imagine a very skilled technical group or individual performing the attack. However, this is not the case here. The Twitter hack did not involve any of the high-tech or sophisticated techniques often used in cyberattacks—no malware, no exploits, and no backdoors. Instead, they used techniques akin to more traditional scam artists.

The hackers utilized social engineering, posing as IT staff in phone calls to Twitter employees. They exploited common VPN issues arising from remote work during the pandemic. Through phishing, employees unknowingly provided login credentials, enabling the hackers to access internal tools. No advanced cyber techniques like malware or exploits were employed.

# What happened?

The Twitter Hack of July 15, 2020, stands out as a stark reminder of the vulnerabilities inherent in even the most prominent social media platforms. Executed by a 17-year-old hacker and accomplices, the breach exposed critical weaknesses in Twitter's cybersecurity infrastructure, allowing the perpetrators to seize control of high-profile accounts belonging to political figures, celebrities, and business magnates.

The initial breach involved social engineering tactics, with hackers posing as Twitter IT personnel to deceive employees into divulging crucial information. Exploiting this access, the attackers then set their sights on the coveted "original gangster" Twitter usernames, a prelude to the more audacious phase three. This final stage saw the compromise of verified accounts, including those of prominent cryptocurrency companies, leading to the dissemination of a bitcoin scam that netted the hackers over $118,000.

Beyond the immediate financial implications, the Twitter Hack laid bare the potential for widespread manipulation and interference through social media platforms, raising concerns about the integrity of elections, financial markets, and national security. As social media continues to play a central role in shaping public discourse and disseminating news, the incident underscores the urgent need for robust cybersecurity measures to safeguard these influential communication channels.

# Company Affected:

The Twitter Hack, occurring on July 15, 2020, targeted Twitter, a publicly traded technology company valued at the time at $37 billion. The hackers compromised 130 Twitter accounts, including those of high-profile individuals, politicians, celebrities, business personals and cryptocurrency companies.

# Weaknesses and Vulnerabilities:

**1. Lack of Chief Information Security Officer (CISO):** Twitter did not have a Chief Information Security Officer since December 2019, seven months before the hack. The absence of a strong leader in cybersecurity can contribute to vulnerabilities.

**2. Weak Leadership and Senior-level Engagement:** The lack of strong leadership and senior-level engagement in cybersecurity was noted as a common source of weaknesses. Effective leadership is crucial in addressing and preventing cybersecurity threats.

**3. Transition to Remote Working:** The COVID-19 pandemic prompted Twitter, like many other organizations, to transition to remote working. This shift put a strain on Twitter's technology infrastructure, and employees experienced problems with VPN connections. The hackers exploited this vulnerability by pretending to be from Twitter's IT department, taking advantage of the VPN issues to trick employees into entering their credentials on a fake website.

**4. Social Engineering (Vishing):** The hackers used social engineering techniques, specifically "vishing" (voice phishing) over the phone. They posed as IT personnel and called employees about VPN issues, convincing them to provide their credentials. Social engineering relies on deception to manipulate individuals into divulging confidential information.

**5. Lack of Compensating Controls:** Twitter failed to identify and assess new security risks created by the pandemic; Twitter did not implement significant compensating controls after March 2020. The lack of adequate measures to mitigate the heightened risk to the remote workforce provided an opportunity for the hackers.

**6. Insufficient Employee Training:** The hackers conducted research to gather basic information about Twitter and its employees, enabling them to impersonate the IT department more convincingly. This suggests that employees may not have received sufficient training on cybersecurity awareness, making them more susceptible to social engineering attacks.

**7. Delayed Implementation of Security Controls:** Twitter, in response to the hack, is reported to be implementing additional security controls such as improved Multi-Factor Authentication (MFA) and cybersecurity awareness training. However, the passage emphasizes the importance of implementing robust controls before experiencing a cyber incident, rather than after.

# Impact on the Organization:

The impact on the affected organization, Twitter, was significant in terms of both reputation and operational disruption. The hack exposed vulnerabilities in Twitter's internal systems and raised concerns about the platform's security, especially considering the potential for more malicious activities, such as spreading misinformation or even influencing political events. Some aspects of the impact are:

**1. Reputation Damage:** The hack eroded trust in Twitter's security measures, both among its users and the public. High-profile accounts being compromised, including those of prominent figures like Elon Musk and Bill Gates, drew widespread attention and raised questions about the platform's ability to protect user data.

**2. Operational Disruption:** The company had to take immediate and drastic measures to contain the hack, including blocking verified accounts from tweeting. This decision disrupted the normal flow of communication on the platform, affecting various users, including businesses, news organizations, and individuals who rely on Twitter for updates.

**3. Financial Costs:** While the direct financial cost is not explicitly made public, responding to such a security incident involves significant resources. Twitter likely incurred expenses related to investigating the hack, implementing security measures, and potentially compensating affected users.

**4. Data Breach Consequences:** The attackers accessed the direct messages of 36 accounts and downloaded Twitter data of eight victims. This breach of sensitive information could have long-term consequences for the affected individuals, both in terms of privacy concerns and potential misuse of their data.

**5. Response and Recovery Efforts:** Twitter had to invest time and resources in investigating the incident, implementing immediate security measures, and planning long-term changes to prevent similar incidents in the future. This included mandatory password changes, enhanced employee training, and the rollout of physical two-factor authentication.

Beyond monetary losses, the incident exposed Twitter's cybersecurity vulnerability, raising concerns about the potential weaponization of major social media platforms. The compromise of high-profile accounts also posed risks to national security, elections, and financial markets. Twitter's reputation suffered, and the incident disrupted verified accounts, affecting communication and public safety updates.

# Threat Actors and Motivations:



In terms of the individuals behind the attack, the investigation revealed that it involved a group of young individuals, including a 17-year-old from Florida, who was later arrested. The attackers exploited social engineering techniques to gain access to Twitter's internal systems and compromise the targeted accounts.

Fortunately, the perpetrators did not realize the extent of access and power they held in their hands. They used their administrative access to sell OG Twitter usernames and commit cryptocurrency scams. They could have employed this power to manipulate stock prices of top companies or even trigger political incidents.

The motivations behind the attack appear to have been primarily financial. Once the attackers gained admin access to Twitter, they aimed to trick Twitter users into sending them Bitcoin, leading to monetary gains.

# Recommendations to prevent this happening to us:

**1. Employee Training and Awareness:** Educate employees about the importance of strong, unique passwords. Train them to recognize and report phishing attempts and social engineering attacks. Implement regular security awareness programs to keep employees informed about the latest threats.

**2. Access Controls:** Implement ***Principle of least privilege***. Limit access to sensitive systems and information only to those who need it. Regularly review and update access permissions based on employees' roles and responsibilities.

**3. Security Audits and Assessments:** Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in systems. Stay informed about the latest security threats and vulnerabilities.

**4. Incident Response Plan:** Develop and regularly update an incident response plan outlining the steps to take in the event of a security incident. Test the plan through simulated exercises to ensure its effectiveness.

**5. Monitoring and Logging:** Implement robust monitoring and logging systems to detect unusual or suspicious activities. Regularly review logs for signs of unauthorized access or other security incidents.

**6. Communication Protocols:** Establish secure communication protocols within the organization. Verify the authenticity of requests for sensitive information, especially those involving financial transactions or changes in account details.

**7. Backup and Recovery:** Regularly back up critical data and ensure that backups are stored securely. Test data restoration procedures to ensure quick recovery.

**8. Collaborate with Security Experts:** Consider engaging with cybersecurity experts or consulting services to assess and improve your organization's security posture.

# Conclusion:

This hack is the perfect example to show that the weakest link in the security chain is the users. This hack demonstrates that even with strict password policies, Multi-Factor Authentication would not have stopped the attack, as the perpetrators had access to a Slack channel containing all the access information for Twitter's internal systems.

We live in a world where everyone is interconnected through technology. With the right skills, anyone's devices, accounts, and data can be breached. Parents usually teach their children from a young age not to interact with strangers and not to accept anything from strangers. Since we live in an interconnected world, we as a society need to adapt and, from a young age, be aware of these social engineering techniques so that we can recognize them.

Twitter Hack serves as a wake-up call for the cybersecurity risks associated with major social media platforms. Beyond financial losses, the incident highlights the potential for significant harm to public trust, elections, and global stability. This report calls for urgent action, proposing specific measures to enhance the cybersecurity resilience of large social media companies and protect the public interest.

# References:

1. Department of Financial Services, New York. (2020, October 14). Twitter Investigation Report.

<https://www.dfs.ny.gov/Twitter_Report>

2. Witman, P. D, Mackelprang, S. (2020, February). Journal of Cybersecurity Education, Research and Practice. The 2020 Twitter Hack - So Many Lessons to be learned. <https://files.eric.ed.gov/fulltext/EJ1332789.pdf>

3.Frenkel, S. Popper, N. Conger, K. Sanger, D. E. (2021, May 5). The New York Times. A Brazen Online Attack Targets V.I.P Twitter Users in a Bitcoin Scam.

<https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html>

4. X. (2020, July 30). Twitter Blog. An Update on our security incident. <https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident>

5. Thompson, N. Barret, B. (2020, September 2020). Wired. How Twitter Survived Its Biggest Hack-and Plans to Stop the Next One. <https://www.wired.com/story/inside-twitter-hack-election-plan/>

6. ChatGPT - Grammar check