

## Teaching Case

# The 2020 Twitter Hack – So Many Lessons to Be Learned

Paul D. Witman  
pwitman@callutheran.edu  
School of Management  
California Lutheran University  
Thousand Oaks, CA, USA

Scott Mackelprang  
Independent Consultant  
Tucson, AZ, USA

### Abstract

In mid-July 2020, the social media site Twitter had over 100 of its most prominent user accounts start to tweet requests to send Bitcoin to specified Bitcoin wallets. The requests promised that the Bitcoin senders would receive their money back doubled, as a gesture of charity amidst the COVID-19 pandemic. The attack appears to have been carried out by a small group of hackers, leveraging social engineering to get access to internal Twitter support tools. These tools allowed the hackers to gain full control of the high-profile user accounts and post messages on their behalf. The attack provides many paths for investigation into the prevention, response, and impacts of cybersecurity breaches.

**Keywords:** Hacking, social engineering, spear phishing, cybersecurity, risk management.

### 1. BACKGROUND

Twitter is a “microblogging” social media service, allowing users to post short text messages, pictures, and links to video and other content. It is used by millions of people and organizations, to broadcast news, to keep in touch, to stir public opinion, and otherwise engage with groups of “followers”. Like most young tech companies, Twitter has had its share of security incidents of one kind or another – some from inside, some from outside.

This case took place most visibly in July 2020 and appears to be an attack utilizing Twitter as a way to try to get money. The case is drawn from publicly available documentation and reflects the facts of the case as publicly reported and available at the time of writing. All claims of criminal activity are only allegations at this time, as the criminal case(s) have not gone to court.

A large share of the accounts that were impacted were public figures in the US – industry leaders, politicians, and entertainers. Some companies were affected, including Bitcoin exchanges and technology companies. Interestingly, one account that had its Twitter direct messages downloaded belonged to a Dutch politician (Sandler, 2020).

Social engineering is a hacking approach to fool victims into performing actions which would compromise confidential information or systems. Phishing and spear-phishing are two types of social engineering attacks. Phishing utilizes emails which falsely claim to be sent from legitimate, trusted sources. Phishing emails are sent broadly and rely upon careless recipients to click hostile embedded links which lead to compromise of the end user’s system or sensitive information. Like phishing, spear-phishing emails contain messages and links to compromise the

recipient’s data or system but are not distributed broadly. They are targeted at specific high-value individuals and are carefully crafted to contain detailed, believable information intended to convince the recipient to perform an action which would result in the compromise of the recipient’s data or systems. Finally, phone spear phishing uses voice calls instead of e-mail to achieve the same goals.

## 2. EVENTS OF THE CASE

### The events of July 15

The first messages related to the scam came from short-named Twitter accounts, such as @6. These had been taken over by the hackers to demonstrate their broad ability to control parts of Twitter’s systems. Then, messages appeared from Twitter accounts owned by Bitcoin trading companies, such as Coinbase. Finally, the primary scam messages appeared from many high-profile accounts.

The hack first became broadly public on July 15, when between 1 and 3 p.m. Pacific Time (PT), about 130 high-profile Twitter accounts were compromised to generate traffic for a Bitcoin scam (Bloomberg, 2020). The scam messages (tweets) offered readers the opportunity to “double their money” as an act of charity by the Twitter account owner. All the reader had to do was send Bitcoin (in any amount) to a specified Bitcoin wallet, and the Bitcoin would be doubled and returned to the reader. See examples of these tweets in Appendix A.

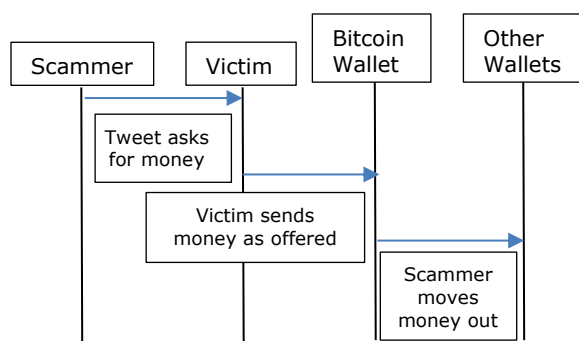


Figure 1 – Overview of scam activity

Within a very short time, reportedly over 300 deposits totaling over US\$118,000 had been deposited to one of the Bitcoin wallets (see Figure 1, above, for an overview of the information and funds flows). It is not certain whether any or all of that money came from scam victims (Twitter readers), as sometimes hackers will “seed” the target account so early victims see that others are

believing the scam as well (Roberts, 2020). In those same early minutes, about US\$61,000 was removed from the wallet through a series of transactions, likely meant to hide the hackers’ identities. Most of the added funds came from wallets with apparently Chinese ownership, though about 25% came from US-owned wallets (Isaac, Frenkel, and Conger, 2020).

Twitter soon became aware of the scam and took steps to stop the attack. They deleted the scam messages as they were discovered. Consistent wording in the scam messages made it easier to find message across the many affected accounts. The same phrase was reportedly used in over 3,000 tweets within a four-hour period. The tweets appeared to have originated from at least six countries (Bloomberg, 2020). This of course means that the compromised accounts were used to post messages repeatedly, even after Twitter started deleting the scam messages. The messages were shown on Twitter as having been posted by a user on the Twitter web page, rather than the Twitter app.

Twitter recognized that attackers had gained control of the many accounts and took steps to restrict access to them – preventing those accounts from tweeting new content and changing their password. Twitter also recognized that their administrative tools had been compromised and implemented tighter controls around access to those tools for their administrators.

Other companies also were active in mitigating the damage from the scam. For example, Coinbase, a Bitcoin trading company, blocked access to the identified Bitcoin wallets, preventing future victims from depositing their Bitcoin there. It is not known how much Twitter and Coinbase (and other Bitcoin traders) were able or willing to coordinate their efforts (Cimpanu, 2020).

By 2:45 p.m. on July 15, Twitter posted a notice that they were “aware of a security incident impacting accounts on Twitter” and that they were actively engaged in fixing it. Twitter also temporarily disabled at least some of the accounts from being able to tweet original content (they could still retweet) or reset their passwords.

### May through July

The day before the hack became public, July 14, the hackers appear to have discussed the capabilities they had acquired through their access to internal Twitter tools (Popper and Conger, 2020). The hackers claimed to have

gotten access to Twitter account support tools, used by Twitter staff to resolve problems for clients (see Appendix B), and reportedly offered to create or take control of desirable Twitter user names, for a fee of up to US\$1,500.

The actual break-in allegedly started around May 3, according to arrest records (Cimpanu, 2020). Details are sketchy, but presumably this is the start of the first part of the social engineering attack. The hackers made use of phone-based social engineering to try to get Twitter employee login credentials. They were first able to compromise login information for lower-level employees who did not have access to the administrative tools. Subsequent efforts, based on those first credentials, allowed the hackers to reach and compromise individuals who had the required tool access (Goodin, 2020). Social engineering was reportedly somewhat easier due to the shared challenge of most Twitter employees working from home.

The hackers are reported to have found access to internal Twitter documentation on the Slack collaboration tool (Popper and Conger, 2020), perhaps using the earlier sets of credentials they were able to obtain. Twitter's Slack channels appear to have contained documentation with information about remote access to Twitter's network, as well as credentials for the administration tools.

Access to these service tools reportedly was limited to about 1,500 Twitter employees, out of a total of about 4,600 employees. Access to the tool from outside a Twitter building also reportedly required VPN access plus specific authorizations on the login credentials. The service tools allowed the tool user to, among other things, reset Twitter user account e-mail addresses, which then allowed unauthorized users to change their passwords.

Given this capability, this was a hack not of a particular account or user, but rather of the entire service (Schneier, 2020). It appears that nearly any Twitter user account could have been compromised, and the hackers chose the accounts they did likely due to their ability to reach a large audience with their requests for Bitcoin.

While the phone spear phishing attack vector is now generally accepted, there was early speculation that a Twitter employee may have sold access to the tools to the hackers. This theory was fed by one of the hackers who claimed to be a Twitter employee while trying to sell

Twitter account access (Popper and Conger, 2020).

In addition to the posting of scam tweets, the hackers are reported to have downloaded the full Twitter private message archives for eight users, and "accessed" the private messages of 36 additional users. Unlike tweets, private messages are just that – private. As such, the damage from this part of the hack may be yet to come.

### **The first part of the aftermath**

The US Federal Bureau of Investigation (FBI) was engaged early in the investigation, since the scam victims were potentially in many parts of the US, as well as other countries. Three people were arrested on July 31, just a little over two weeks after the hack became public. Charges included money laundering, wire fraud, identity theft, and unauthorized computer access.

There is certainly more of the story yet to come, both in terms of criminal investigations and in terms of corporate and hacker learning.

## **3. DISCUSSION QUESTIONS**

Each of the following questions is intended to provoke thinking about one or more aspects of the situation. We encourage you to think about each of these in preparation for an in-depth discussion.

- A) Internal controls
  - Since it appears that the hack leveraged powerful customer service tools, are there things Twitter could have done to catch this problem earlier?
  - What type of tools should be in place today to help Twitter understand, alert on, and conduct after-action research on attacks such as this one?
- B) Social engineering
  - What steps can Twitter take to prevent future attacks?
  - Was this attack a result of a people issue, a technology issue, or some of both?
- C) Process documentation
  - It was reported that the hackers found some of their insights from internal Twitter documentation stored on the independent collaboration tool, Slack (slack.com). What risks do organizations take by storing sensitive corporate data

- on third-party services? What risks do they potentially avoid?
  - What authentication tools and options does Slack provide, beyond simple user ID and password?
- D) Third party contractors
- Twitter, like many large companies, uses third party contract companies to employ people to handle some customer service queries. What are the pros and cons to this type of decision?
  - Why are contractor employees likely less invested in Twitter's mission than Twitter employees?
  - How could the relationship with contract employees be managed to strengthen that investment?
- E) Public relations
- What do you think the impact has been on public confidence in the Twitter platform? In social media more broadly?
  - What challenges do you see happening in this case in managing public messaging – counts of impacted users, types of impacts, etc.? What could Twitter have done better? What did they do well?
  - Review Twitter's public communications – what are the tradeoffs (e.g., value and risk) of openness?
- F) Consequences for the company and industry
- What implications does this hack have beyond the initial financial impacts? Consider consumer confidence, politics, organizational credibility, etc.
  - What are the implications beyond Twitter? Are other social media services or technology providers impacted in any way? How?
- G) Regulatory investigations
- If you were a government regulator in a country or region of your choice, what questions would you have for Twitter's management?
  - What additional regulatory controls might be appropriate to prevent or reduce the risk of a recurrence?
  - What other industries might provide a model for this regulatory oversight? What are some pros and cons to this regulation?
- H) The funding scam
- Why did the hackers use multiple Bitcoin wallets?

- Why did the message indicate a limit to how much time or total funding was allowed for the match?
- Why did their messages relate the "offer" to the COVID-19 pandemic?

#### 4. ADDITIONAL RESEARCH IDEAS

The following provide some opportunities for deeper study of the issues.

##### Study of company culture

- Based on publicly available information, what can you infer about Twitter's company culture?
- How would you assess Twitter's prioritization of security vs. product and revenue?
- If you were Twitter's CEO, how would you go about making decisions about cybersecurity investments, especially when they compete with other investments in your products?

##### Similar hack of Reddit in August 2020

- The Reddit discussion boards suffered what on the surface appears to be a similar type of hack. Each "subreddit" (a focused discussion area) has one or more moderators who manage the conversations there. Numerous subreddit moderators had their credentials compromised in early August, with the subreddit content being defaced with political messages (Reddit, 2020).
- How does this attack compare and contrast with the Twitter hack?
- How do you assess Reddit's public response vs. Twitter's public response?
- Is there something about small companies that grow quickly that makes incidents like this possible?

#### 5. CONCLUSIONS

The 2020 Twitter hack has been a painful lesson in the need for constant vigilance by employees and security teams, and in the risks of making powerful tools broadly available within an organization. The repercussions will certainly be felt across Twitter for some time. If we are wise, we can incorporate those lessons learned into many more organizations. (Krebs, 2020)

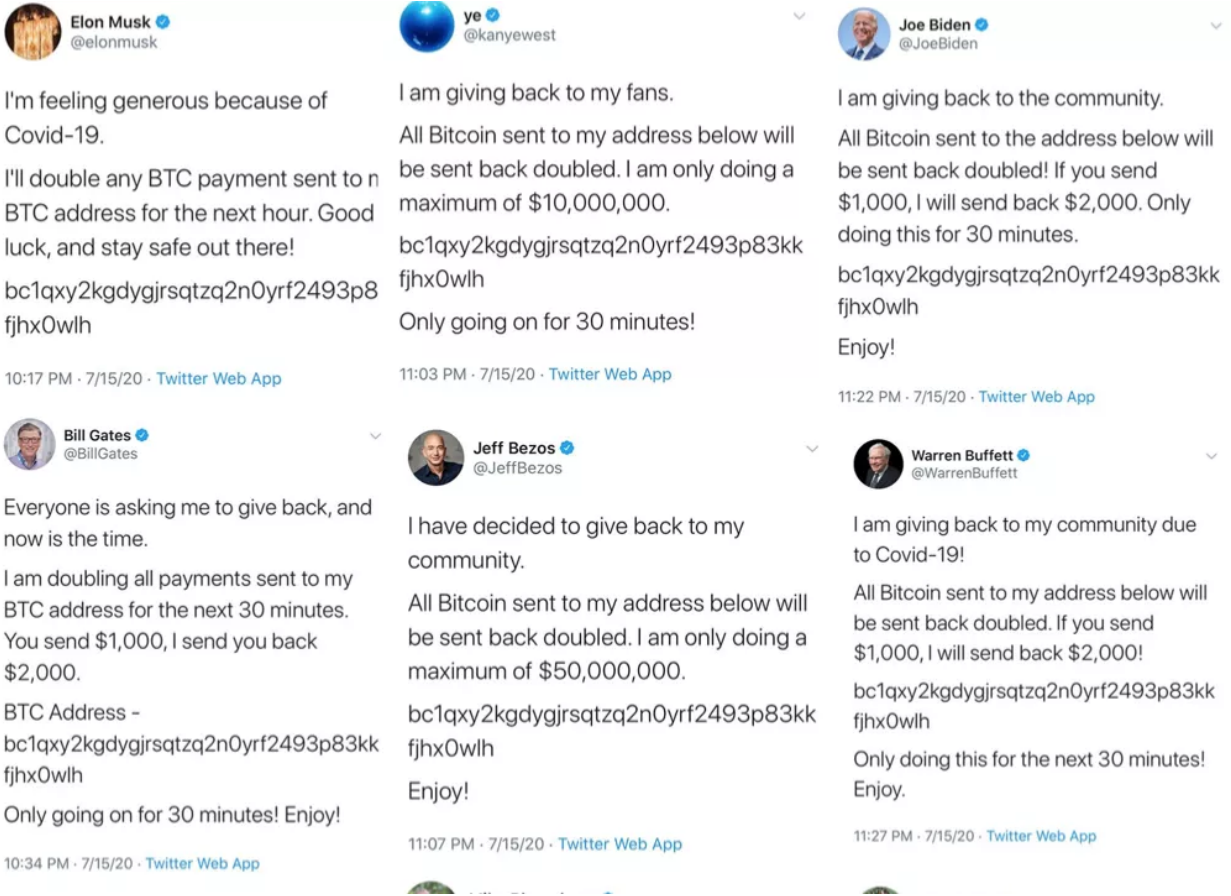
#### 6. ACKNOWLEDGEMENTS

The authors appreciate the productive feedback provided by the reviewers and conference chairs.

## 7. REFERENCES

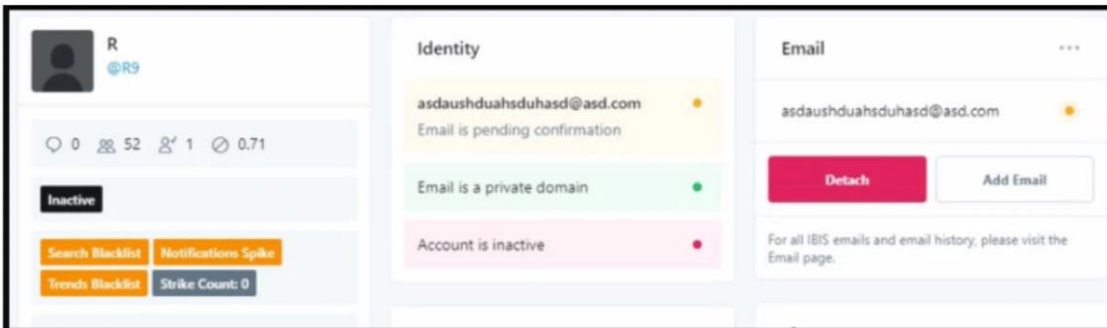
- Bloomberg. (2020, July 15). Twitter accounts of Biden, Obama and other prominent figures hacked. *Irish Times*. Retrieved from <https://www.irishtimes.com/news/world/us/twitter-accounts-of-biden-obama-and-other-prominent-figures-hacked-1.4305567>
- Cimpanu, C. (2020, August 1). How the FBI tracked down the Twitter hackers. *Zero Day*. Retrieved from <https://www.zdnet.com/article/how-the-fbi-tracked-down-the-twitter-hackers/>
- Goodin, D. (2020, July 30). Twitter hackers used “phone spear phishing” in mass account takeover. *Ars Technica*. Retrieved from <https://arstechnica.com/information-technology/2020/07/twitter-hackers-used-phone-spear-phishing-in-mass-account-takeover/>
- Isaac, M., Frenkel, S., & Conger, K. (2020, July 16). Twitter Struggles to Unpack a Hack Within Its Walls. *New York Times*. Retrieved from <https://www.nytimes.com/2020/07/16/technology/twitter-hack-investigation.html>
- Krebs, B. (2020, July 31). Three Charged in July 15 Twitter Compromise. *Krebs on Security*. Retrieved from <https://krebsonsecurity.com/2020/07/three-charged-in-july-15-twitter-compromise/>
- Popper, N., & Conger, K. (2020, July 17). Hackers Tell the Story of the Twitter Attack From the Inside. *New York Times*. Retrieved from <https://www.nytimes.com/2020/07/17/technology/twitter-hackers-interview.html>
- Reddit. (2020). Ongoing incident with compromised mod accounts. Retrieved from [https://www.reddit.com/r/ModSupport/comments/i5hhtf/ongoing\\_incident\\_with\\_compromised\\_mod\\_accounts/](https://www.reddit.com/r/ModSupport/comments/i5hhtf/ongoing_incident_with_compromised_mod_accounts/) on August 9, 2020.
- Roberts, J. J. (2020, July 15). Scammer behind massive Twitter hack has made only \$109,000—so far. *Fortune*. Retrieved from <https://fortune.com/2020/07/15/twitter-hack-accounts-hacked-elon-musk-bill-gates-joe-biden-kanye-west-bitcoin-who-is-hacker-how-much/>
- Sandler, R. (2020, July 22). Twitter Says Hackers Accessed Direct Messages From 36 Users, Including One Dutch Elected Official. *Forbes*. Retrieved from <https://www.forbes.com/sites/rachelsandler/2020/07/22/twitter-says-hackers-accessed-direct-messages-from-36-users-including-one-dutch-elected-official/#2034fcce55da>
- Schneier, B. (2020, July 20). On the Twitter Hack. *Schneier on Security*. Retrieved from [https://www.schneier.com/blog/archives/2020/07/on\\_the\\_twitter\\_.html](https://www.schneier.com/blog/archives/2020/07/on_the_twitter_.html)

## Appendix A



Source: Investopedia

## Appendix B



A screenshot, sent out by Kirk after he gave a customer access to an account, showing Twitter's back end for the @R9 account.

Source: Wikipedia