Journal of Cybersecurity Education, Research and Practice

Volume 2021 | Number 2 Article 2

February 2022

The 2020 Twitter Hack – So Many Lessons to Be Learned

Paul D. Witman
California Lutheran University, witman@ieee.org

Scott Mackelprang
scottmackelprangs@gmail.com

Recommended Citation

Witman, Paul D. and Mackelprang, Scott (2022) "The 2020 Twitter Hack – So Many Lessons to Be Learned," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2021 : No. 2 , Article 2.
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss2/2

The 2020 Twitter Hack – So Many Lessons to Be Learned

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, teaching case

Cover Page Footnote

The authors appreciate the productive feedback provided by the reviewers and journal editors, as well as family members.

INTRODUCTION

This paper is written as a teaching case study for use in a cybersecurity course, either in an introductory course, or possibly a course in digital forensics. It is aimed at the student, with a separate instructor document available to provide teaching guidance. As such, it deliberately avoids answering questions and directly providing the lessons learned, but rather provides sample questions for faculty to consider using in their discussion of the case with their students. The paper also provides overview information on this particular security incident as background for the discussions. This information largely came at the time from the popular press, though much later in 2020 there was a regulatory report published by the New York Department of Financial Services (2020).

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 (Cereola and Dynowska, 2019; Jacobson and O'Rourke, 2020), 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 steal 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 cases have not been decided in court.

A large share of the impacted accounts represented public figures in the US – industry leaders, politicians, and entertainers. Some companies’ Twitter accounts were affected, including Bitcoin exchanges and technology companies. Interestingly, one account that had its Twitter direct messages downloaded belonged to a Dutch politician – one of the few non-US-based people who were impacted (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 (Krombholz, Hobel, Huber, and Weippl, 2015).

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.

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, below, 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 that 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).

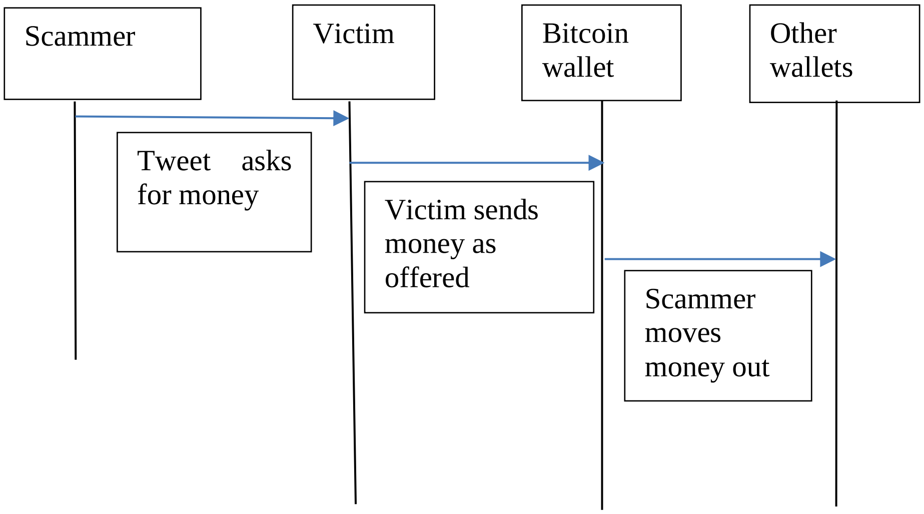


Figure 1 – Overview of scam activity

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 such messages 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 access to the administrative tool (Goodin, 2020).

Social engineering was reportedly somewhat easier due to the additional challenge of most Twitter employees working from home (Sarginson, 2020). As one example salient to this case, employees often used mobile phones in their remote workplaces, and might then receive calls from numbers other than “internal” phone extensions, including from phishing actors impersonating IT employees. This could have the effect of lowering their guard against potential phone-based phishing attacks.

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 virtual private network (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

This section addresses the activities of law enforcement, Twitter, and other parties, following detection and shutdown of the hackers' activities. Following this section are discussion and research questions intended to help students uncover the lessons that can be learned from the Twitter hack of July 2020.

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. Further reporting on the story revealed reported lags in implementing automated security monitoring and controls, the challenges of restarting operations after an administrative breach, and the pending criminal trials and other legal actions (Thompson and Barrett, 2020). Regulatory agencies have conducted analyses of the events and the recommended responses, including cybersecurity best practices and proposed regulation of social media companies (New York Department of Financial Services, 2020).

DISCUSSION QUESTIONS

Each of the following questions is intended to provoke thinking about one or more aspects of the situation. They may require research into best practices in cybersecurity to address the questions. We encourage you to think about each of these in preparation for an in-depth discussion.

Internal Controls

- Since it appears that the hack leveraged powerful customer service tools, what are some examples of the best practices Twitter could have used 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?

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?

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?

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 contract employees likely less invested in Twitter's mission than Twitter employees?
- How could the relationship with contract employees be managed to strengthen that investment?

Public Relations

- What do you think the impact of this incident 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 about security incidents – e.g., 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?

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?

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?

The Funding Scam

- Why did the hackers use multiple Bitcoin wallets?
- Why did the scam messages frequently 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?

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?

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. It has also been a lesson in some of the risks of the remote workforce, as well as sharing documentation via cloud-based services that may be insufficiently secured.

The repercussions will certainly be felt across Twitter and other companies for some time. If we are wise, we can incorporate those lessons learned into many more organizations (Krebs, 2020).

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

Cereola, S. J., & Dynowska, J. (2019). Investigating the impact of publicly announced information security breaches on corporate risk factor disclosure tendencies. *Journal of Cybersecurity Education, Research and Practice*, *2019*(2), 3.

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/

Crider, M. (2020, July 23). Twitter Says a Dutch Politician's Direct Messages Were Compromised in Hack. *ReviewGeek*. Retrieved from https://www.reviewgeek.com/48460/twitter-says-a-dutch-politicians-direct-messages-were-compromised-in-hack/

Curran, K. (2020). Cyber security and the remote workforce. *Computer Fraud & Security*, *2020*(6), 11-12.

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

Jacobson, A., & O'Rourke, M. (2020). YEAR IN RISK 2020. *Risk Management*, *67*(11), 20-25.

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/

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

New York Department of Financial Services. (2020). *Twitter Investigation Report*. Retrieved from https://www.dfs.ny.gov/Twitter_Report

NIST. (2020). Risk Management Framework. Retrieved from https://www.nist.gov/cyberframework/risk-management-framework on August 31, 2020.

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/ 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/

Robertson, J., Mehrotra, K., & Wagner, K. (2020, July 27). Twitter's Security Woes Included Broad Access to User Accounts. *Bloomberg*. Retrieved from https:/www.bloomberg.com/news/articles/2020-07-27/twitter-s-security-woes-included-broad-access-to-user-accounts

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

Sapriel, C. (2021). Managing stakeholder communication during a cyber crisis. *Cyber Security: A Peer-Reviewed Journal*, *4*(4), 380-387.

Sarginson, N. (2020). Securing your remote workforce against new phishing attacks. *Computer Fraud & Security*, *2020*(9), 9-12.

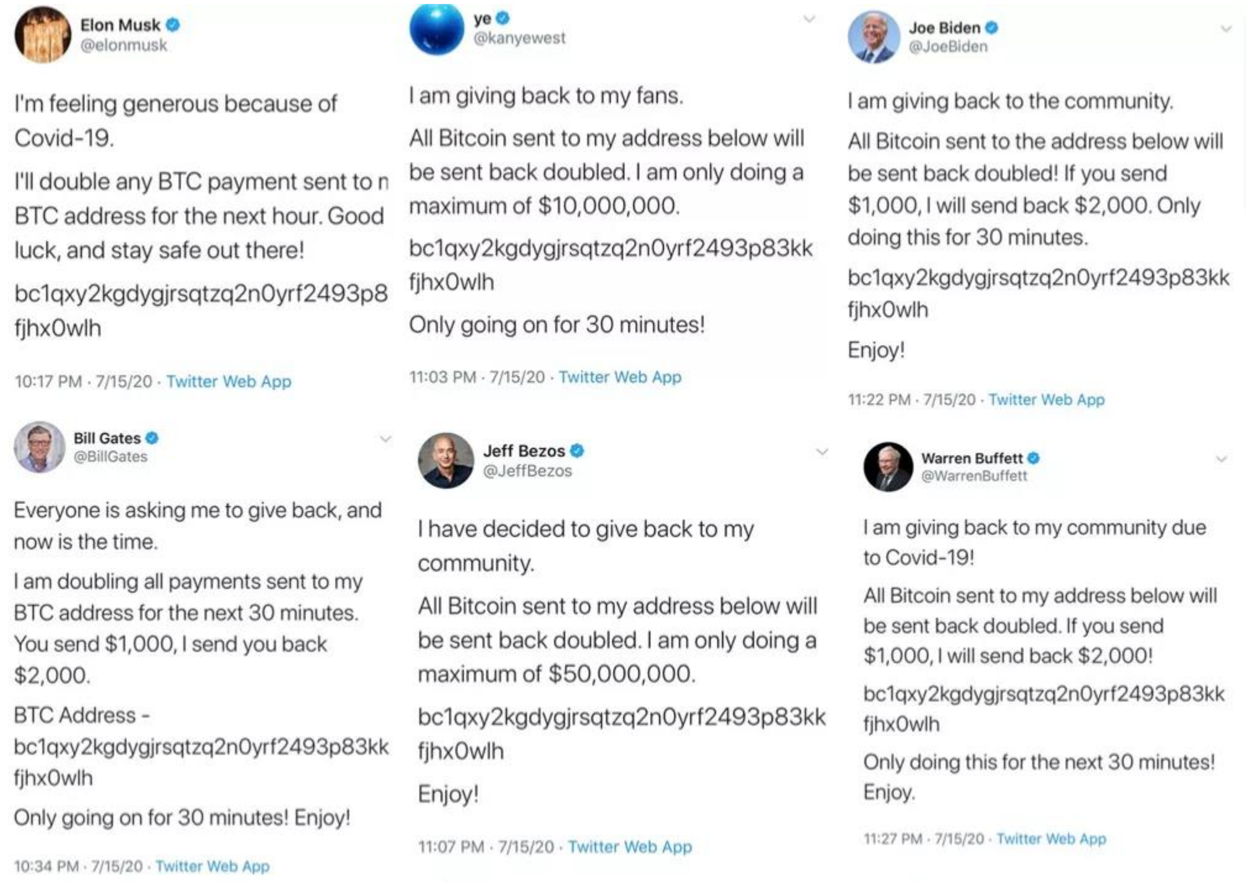
Schneier, B. (2020, July 20). On the Twitter Hack. *Schenier on Security*. Retrieved from https://www.schneier.com/blog/archives/2020/07/on_the_twitter_.html

Slack. (n.d.-a). Guide to single sign-on settings. Retrieved from https://slack.com/help/articles/220403548-Guide-to-single-sign-on-settings on August 30, 2020.

Slack. (n.d.-b). Set up two-factor authentication. Retrieved from https://slack.com/help/articles/204509068-Set-up-two-factor-authentication on August 30, 2020.

Thompson, N., & Barrett, B. (2020, September 24). How Twitter Survived Its Biggest Hack—and Plans to Stop the Next One. *WIRED*.

APPENDIX A



Elon Musk @elonmusk

I'm feeling generous because of Covid-19.

I'll double any BTC payment sent to n BTC address for the next hour. Good luck, and stay safe out there!

bc1qxy2kgdygjrsqtzq2n0yrf2493p8
fjhx0wlh

10:17 PM · 7/15/20 · Twitter Web App

ye @kanyewest

I am giving back to my fans.

All Bitcoin sent to my address below will be sent back doubled. I am only doing a maximum of $10,000,000.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk
fjhx0wlh

Only going on for 30 minutes!

11:03 PM · 7/15/20 · Twitter Web App

Joe Biden @JoeBiden

I am giving back to the community.

All Bitcoin sent to the address below will be sent back doubled! If you send $1,000, I will send back $2,000. Only doing this for 30 minutes.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk
fjhx0wlh

Enjoy!

11:22 PM · 7/15/20 · Twitter Web App

Bill Gates @BillGates

Everyone is asking me to give back, and now is the time.

I am doubling all payments sent to my BTC address for the next 30 minutes. You send $1,000, I send you back $2,000.

BTC Address -
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk
fjhx0wlh

Only going on for 30 minutes! Enjoy!

10:34 PM · 7/15/20 · Twitter Web App

Jeff Bezos @JeffBezos

I have decided to give back to my community.

All Bitcoin sent to my address below will be sent back doubled. I am only doing a maximum of $50,000,000.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk
fjhx0wlh

Enjoy!

11:07 PM · 7/15/20 · Twitter Web App

Warren Buffett @WarrenBuffett

I am giving back to my community due to Covid-19!

All Bitcoin sent to my address below will be sent back doubled. If you send $1,000, I will send back $2,000!

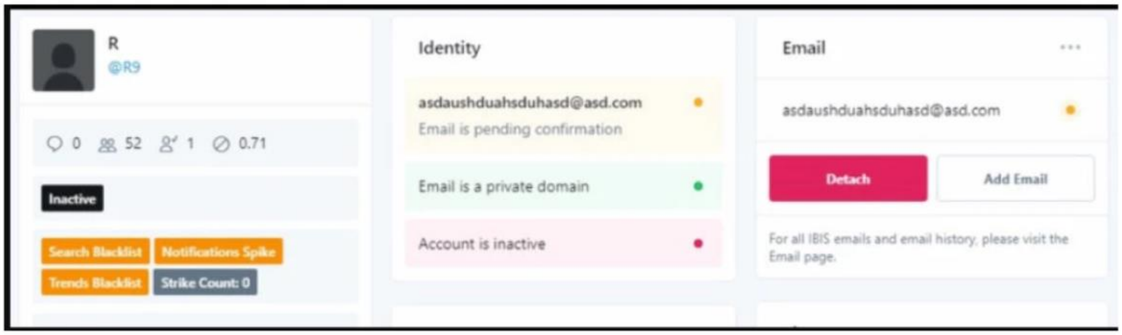
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk
fjhx0wlh

Only doing this for the next 30 minutes! Enjoy.

11:27 PM · 7/15/20 · Twitter Web App

Source: Investopedia

APPENDIX B



asdaushduahsduhasd@asd.com
Email is pending confirmation

Email is a private domain

Account is inactive

asdaushduahsduhasd@asd.com

For all IBIS emails and email history, please visit the Email page.

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