BIZCOMMUNITY

Twitter hack exposes broader threat to democracy and society

By Laura DeNardis

21 Jul 2020

In case 2020 wasn't dystopian enough, hackers on July 15 hijacked the Twitter accounts of former President Barack Obama, presidential hopeful Joe Biden, Elon Musk, Jeff Bezos, Kim Kardashian and Apple, among others. Each hijacked account posted a similar fake message. The high-profile individual or company wanted to philanthropically give back to the community during Covid-19 and would double any donations made to a bitcoin wallet, identical messages said. The donations followed.

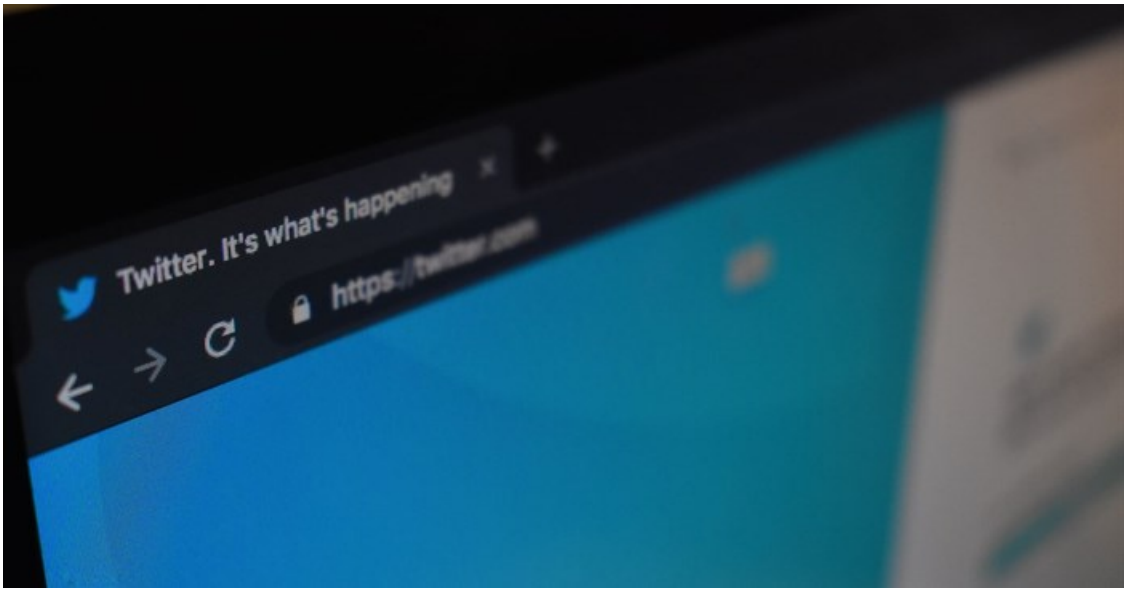


Photo by Kon Karampelas on Unsplash.

The hack on the surface may appear to be a run-of-the-mill financial scam. But the breach has chilling implications for democracy.

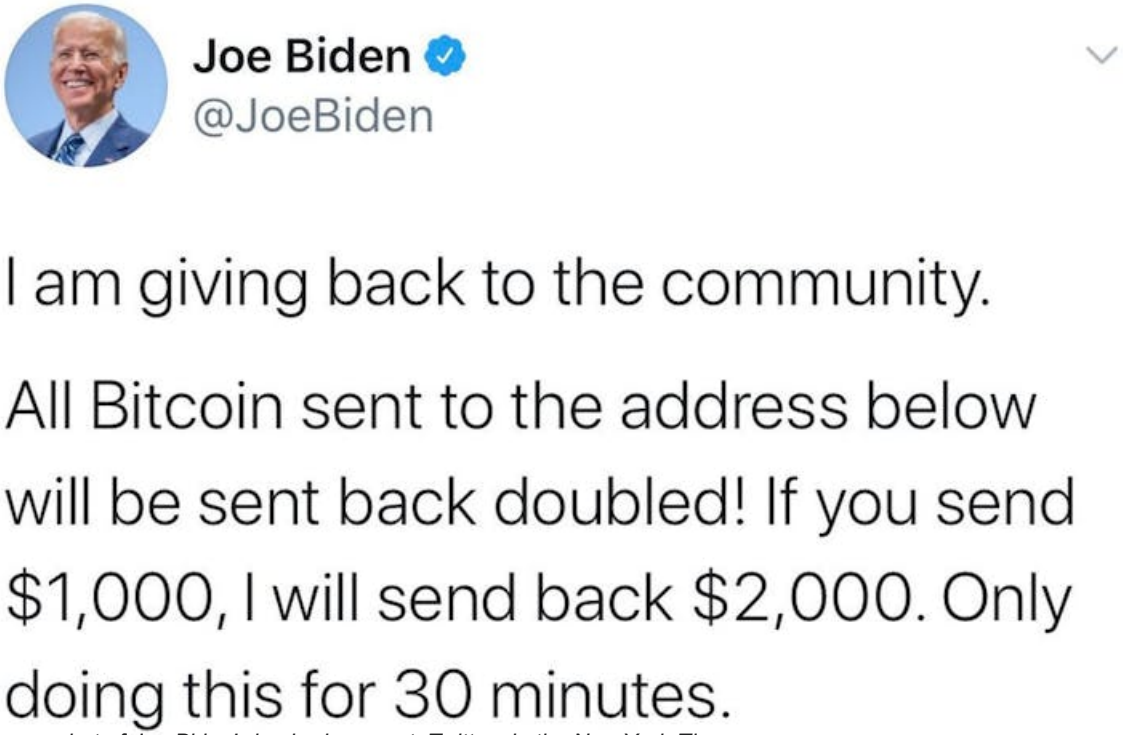
Serious political implications

As a scholar of internet governance and infrastructure, I see the underlying cybercrimes of this incident, such as hacking accounts and financial fraud, as far less concerning than the society-wide political implications. Social media – and Twitter in particular – is now the public sphere. Using a hijacked account, it would be simple to wreak economic damage, start a national security crisis or create a social panic.

Consider some of the potential threats to society posed by the takeover of technology infrastructure

- Market stability. Coordinated rogue tweets from the accounts of Apple, Facebook, Google, Netflix and Microsoft could easily crash the stock market, at least temporarily, eroding confidence in markets.
- Societal panic. A false warning about an impending terrorist attack from a major media company account could create a dangerous public panic.
- National security. Twitter is the platform of choice for President Donald Trump. A foreign adversary hijacking his account and announcing a nuclear strike on North Korea could be catastrophic.
- Democracy. Hijacked accounts could sow well-timed political disinformation that sways or seeks to delegitimize the 2020 presidential election.

As such, what happened is not about financial crime. It is a serious threat to us all.



Screen shot of Joe Biden's hacked account. Twitter via the New York Times

Politicians are rightly calling for hearings and investigations. The House Committee on Oversight and Reform ranking member, Kentucky Republican James Comer, issued a letter demanding answers from Twitter CEO Jack Dorsey about what happened. New York Governor Andrew Cuomo ordered a full investigation of the hack, warning that "Foreign interference remains a grave threat to our democracy."

The FBI is investigating the incident.

Social engineering

On the day of the attack, Dorsey tweeted, "Tough day for us at Twitter. We all feel terrible this happened." But what did happen?

Twitter disclosed that approximately 130 accounts were affected and that "attackers were able to gain control of the accounts and then send Tweets from those accounts." The affected accounts seemed to be "verified accounts" with the blue check mark meant to authenticate the identities of high-profile public figures.

Because these accounts are potential hacking targets, Twitter recommends additional security such as having a second log-in verification check, and requiring personal information such as a phone number to reset a password.

How were the accounts taken over? There are two general possibilities: Either hackers gained the login credentials, including passwords, or gained access to systems from inside the company. Twitter has, as of this writing, described the attack as having "successfully targeted some of our employees with access to internal systems and tools." In other words, it may have originated inside Twitter's secure system.

But this explanation raises more questions. Are Twitter employees (or hackers) with unauthorized access to "internal systems" actually able to tweet from the account of someone like Joe Biden? Another major question is whether the hackers also were able to read the private direct messages in each of these accounts.

To begin to regain trust, Twitter will have to clarify what happened and explain what the company will do to mitigate such an attack in the future.

Outsiders were apparently able to take over Twitter accounts of high-profile individuals by 'social engineering,' which allowed them to convince Twitter employees to provide access to its systems. Maskot via Getty Images

In terms of the tactics used, Twitter described the incident as having used social engineering, a term that refers to a cyberattack exploiting some human action. Examples include phishing attacks that prompt someone to click on a malicious link in an email or divulge a password or personal information. These techniques date back decades, such as the infamous I Love You attack of 2000, when emails with the subject line "I Love You" prompted people to download a virus-infected file, creating massive economic damage to companies. It can be a range of activities aimed at deceiving people into providing information useful to another party, such as a hacker trying to penetrate a company's network.

The essential feature of a social engineering attack is that a human being is prompted to make an error in judgment. If anyone ever thought an individual has no agency in cybersecurity, simply recall the Democratic National Committee email data breach in advance of the 2016 U.S. presidential election. That incident in part originated via a phishing attack that tricked someone into disclosing email credentials. Cybersecurity is a problem of human psychology and cyberliteracy as well as a complex technical area. Not only do Twitter employees appear to be victims of social engineering, according to the initial explanation, but so too were those people who were tricked into giving bitcoin donations.

Not just a tech company problem

Cybersecurity is the great human rights issue of our time simply because the security of everything in our society – from elections to health care to the economy – is dependent upon the security of the digital world. Private companies now mediate the public sphere and so they bear great responsibility for this security. From the Facebook Cambridge Analytica scandal to the Yahoo! data breach, tech companies have had trust problems. At the same time, the Covid-19 pandemic lays bare how much we need the digital world and must get cybersecurity right.

The disclosure that the Twitter hack originated via a social engineering technique is a reminder that cybersecurity is an individual human responsibility as much as a technical or institutional one. We are all responsible. Twitter was originally not designed to be something so politically relevant. Now we all know it is. That's why this latest attack is so serious.

Laura DeNardis, Professor and Interim Dean, *American University School of Communication*

ABOUT THE AUTHOR

Professor and Interim Dean, American University School of Communication