The Twitter hack targeted the rich and famous. But we all lose if trusted accounts can be hijacked

July 16 2020, by Kobi Leins

The list of US figures whose Twitter accounts were hijacked by scammers on Wednesday US time reads like a Who's Who of the tech and celebrity worlds: Tesla boss Elon Musk, Amazon chief Jeff Bezos, Microsoft founder Bill Gates, former president Barack Obama, current Democratic nominee Joe Biden, celebrities Kanye West and Kim Kardashian, billionaires Warren Buffett and Mike Bloomberg, the corporate accounts of Apple and Uber, and more besides.

The point of the hack? To lure followers into sending US$1,000 in Bitcoin, with the classic scammer's false promise of sending back twice as as much.

After a preliminary investigation, Twitter said it believed the incident was "a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools".

The details are still far from clear, but it seems likely someone with administrative rights may have granted the hackers access, perhaps inadvertently, despite the presence of two-factor authentication on the accounts—widely considered the gold standard of online security. It appears insiders may have been involved, although the story is still unfolding.

The use of the niche currency Bitcoin limited the number of potential victims, but also makes the hackers' loot impossible to trace. Ironically enough, Bitcoin is a currency designed for a post-trust world, and the anonymity of its transactions makes the hackers even harder to track down.

Whom do we trust?

This is not the first time we have seen the complex and profound impact social media can have. In 2013, hackers gained access to @AP, the official Twitter account of the respected Associated Press news agency, and tweeted: "Breaking: Two Explosions in the White House and Barack Obama is Injured."

The stock market dived by US$136.5 billion almost immediately but bounced back within six minutes, illustrating the interconnected systems that move so quickly a human cannot intervene—algorithms read the headlines and the stock market collapsed, albeit fleetingly.

By shorting stocks, whoever hacked AP's Twitter account stood to make enormous profits from the temporary stock market tank. We do not know what the financial benefits, if any, to the hackers in 2013 were.

This week's Twitter hack definitely had financial motives. The Bitcoin scammers in this recent hack netted more than US$50,000.

More sinister still, however, are the implications for democracy if a similar hack were carried out with political motives.

What if a reliable source, such as a national newspaper's official account, tweets that a presidential candidate has committed a crime, or is seriously ill, on the eve of an election? What if false information about international armed attacks is shared from a supposedly reliable source such as a government defence department? The impacts of such events would be profound, and go far beyond financial loss.

This is the inherent danger of our growing reliance on social media platforms as authoritative sources of information. As media institutions decline in size, funding and impact, the public increasingly relies on social media platforms for news.

The Bitcoin scam is a reminder that any social media platform can be hacked, tampered with, or used to spread false information. Even gold-standard technical systems can be outwitted, perhaps by exploiting human vulnerabilities. A disgruntled employee, a careless password selection, or even a device used in a public space can pose grave risks.

Who's in charge?

The question of who polices the vast power accrued by social media platforms is a crucial one. Twitter's reaction to the hack—temporarily shutting down all accounts verified with the "blue tick" that connotes public interest—raised the ire of high-profile users (and prompted mirth among those not bestowed with Twitter's mark of legitimacy). But the underlying question is: who decides what is censored or shut down, and under what circumstances? And should companies do this themselves, or do they need a regulatory framework to ensure fairness and transparency ?

Broader questions have already been raised about when Twitter, Facebook or other social media platforms should or should not censor content. Facebook was heavily criticised for not removing oppressive posts about Rohingya Muslims in Myanmar, and what the United Nations referred to as a genocide ensued. Twitter much later suspended some accounts that had been inciting violence, with some criticism.

What is the responsibility of such platforms, and who should govern them, as we become more heavily reliant on social media for our news? As the platforms' power and influence continue to grow, we need rigorous frameworks to hold them accountable.

Last month, the Australian government pledged a A$1.3 billion funding increase and an extra 500 staff for the Australian Signals Directorate, to boost its ability to defend Australia from attacks. Australia's forthcoming 2020 Cyber Security Strategy will hopefully also include strategies to proactively improve cyber security and digital literacy.

In an idea world, social media giants would regulate themselves. But here in the real world, the stakes are too high to let the platforms police themselves.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: The Twitter hack targeted the rich and famous. But we all lose if trusted accounts can be hijacked (2020, July 16) retrieved 19 April 2024 from https://techxplore.com/news/2020-07-twitter-hack-rich-famous-accounts.html