Twitter Hack Serves as a Reminder of How Manipulative Bitcoin Scams Can Be

From the Identity Theft Resource Center , July 2020

Bitcoin scams come in many different forms. Scammers use different platforms to try and get people to pay them in bitcoin (also known as cryptocurrency or digital money). Bitcoin scams are a popular way for fraudsters to trick people into sending money. Recently, they used Twitter and some of its most notable accounts to target Twitter users.

On July 15, hackers compromised verified Twitter accounts and sent cryptocurrency scam tweets requesting bitcoin donations with the promise of doubling the investments to "give back to the community." Scammers responsible for bitcoin scams not only aim to steal people's money, but also collect their personally identifiable information (PII) and sell it to other cybercriminals.

According to Twitter , attackers are believed to have targeted certain Twitter employees through a social engineering scheme. Twitter says the attackers successfully manipulated a small number of employees and used their credentials to access Twitter's internal systems, including getting through their two-factor protections. While Twitter continues their forensic review, they believe the bad actors may have attempted to sell some of the usernames. The hackers are not believed to have viewed previous account passwords. However, they were able to view personal information, including email addresses and phone numbers.

Twitter says nearly 130 accounts were targeted, and 45 successfully hacked. The Twitter accounts hacked include high profile individuals with verified accounts such as Barak Obama, Kanye West, Elon Musk and Bill Gates. Twitter responded by preventing any blue-check marked accounts from tweeting while security teams responded to the attack. Twitter apologized for the attack; the UK's National Cyber Security Center, whom Twitter officers reached out to for support, released a statement urging people to treat requests for money or PII on social media with extreme caution.

The recent social-engineering hijack of Twitter accounts highlights a larger issue that has been on the increase since COVID-19 began: the prevalence of cryptocurrency scams . According to the Federal Trade Commission , most bitcoin scams appear as emails trying to blackmail someone, online chain-referral schemes or bogus investment/business opportunities. However, no matter how the scam is executed, a scammer wants the victim to either send money, give-up their PII or a combination of these. Once someone engages, there is usually nothing they can do to get their money back.

The Twitter hack creates a teachable moment – what should consumers do to reduce their risk of falling for a bitcoin scam? It also highlights the need for businesses to ensure their employees are educated on social engineering . This incident proves that even the most technologically-advanced companies are not immune from an employee granting access to bad actors. To avoid a bitcoin scam or other forms of social engineering, people should remember the following:

- Never share PII through social media channels and always verify the person or business asking. While these scams are designed to steal people's money, they are also designed to collect PII to sell to other cybercriminals.
- If someone sees a tweet, email, text message or other social media post that asks for payment in bitcoin, it is – most likely – a scam.
- High profile individuals will not contact anyone to give away large sums of money – especially in bitcoin – by social media message. There are other methods for informing someone if they are a recipient; if an offer seems too good to be true, it probably is.
- If a consumer receives a message telling him or her it's a guarantee to make money, it is probably a scam.
- No one should ever click a link , download a file or open an attachment if they are unsure of who sent it or what it is; they should be cautious of links that are shared on social media.
- Keep up with the latest around scams and how they work. The Twitter bitcoin scam employed a lot of common cognitive biases . Understanding how bitcoin or cryptocurrency works reduces the number of people who fall for scams about it.

If someone believes they are a victim of a bitcoin scam or has questions about other scams, they can live-chat with an Identity Theft Resource Center expert advisor. They can also call toll-free at 888.400.5530.