TechTips Newsletter

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

3 charged in massive Twitter hack, Bitcoin scam

A British man, a Florida man and a Florida teen were identified by authorities Friday as the hackers who earlier this month took over Twitter accounts of prominent politicians, celebrities and technology moguls to scam people around globe out of more than $100,000 in Bitcoin.

Graham Ivan Clark, 17, was arrested Friday in Tampa, where the Hillsborough State Attorney's Office will prosecute him as adult. He faces 30 felony charges, according to a news release.
Mason Sheppard, 19, of Bognor Regis, U.K., and Nima Fazeli, 22, of Orlando, were charged in California federal court.

In one of the most high-profile security breaches in recent years, hackers sent out bogus tweets on July 15 from the accounts of Barack Obama, Joe Biden, Mike Bloomberg and a number of tech billionaires including Amazon CEO Jeff Bezos, Microsoft co-founder Bill Gates and Tesla CEO Elon Musk. Celebrities Kanye West and his wife, Kim Kardashian West, were also hacked.

The tweets offered to send $2,000 for every $1,000 sent to an anonymous Bitcoin address.

More on next page...

August 2020

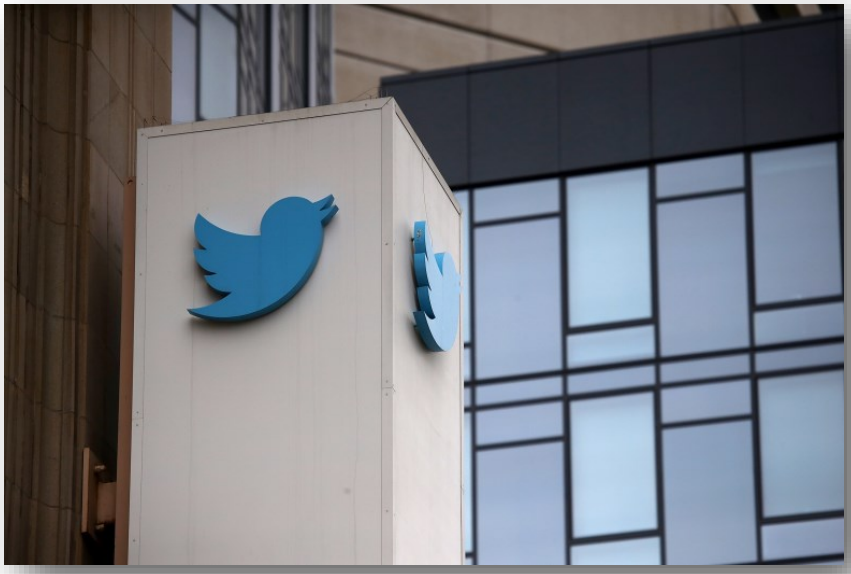
This monthly publication provided courtesy of Richard Lynn, VP of Sales and Marketing
Tech Hero

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

"There is a false belief within the criminal hacker community that attacks like the Twitter hack can be perpetrated anonymously and without consequence," U.S. Attorney David L. Anderson for the Northern District of California said in a news release. "Today's charging announcement demonstrates that the elation of nefarious hacking into a secure environment for fun or profit will be short-lived."

Although the case against the teen was also investigated by the FBI and the U.S. Department of Justice, Hillsborough State Attorney Andrew Warren explained that his office is prosecuting Clark in Florida state court because Florida law allows minors to be charged as adults in financial fraud cases such as this when appropriate. He added that Clark was the leader of the hacking scam.



"This defendant lives here in Tampa, he committed the crime here, and he'll be prosecuted here," Warren said.

Security experts were not surprised that the alleged mastermind of the hack is a 17-year-old, given the relative amateur nature both of the operation and the hackers' willingness afterward to discuss the hack with reporters online.

"I think this is a great case study showing how technology democratizes the ability to commit serious criminal acts," said Jake Williams, founder of the cybersecurity firm Rendition Infosec. "I'm not terribly surprised that at least one of the suspects is a minor. There wasn't a ton of development that went into this attack."

Williams said the hackers were "extremely sloppy" in how they moved the Bitcoin around.

He also said he was conflicted about whether Clark should be charted as an adult.

"He definitely deserves to pay (for jumping on the opportunity) but potentially serving decades in prison doesn't seem like justice in this case," William said.

Twitter previously said hackers used the phone to fool the social media company's employees into giving them access. It said hackers targeted "a small number of employees through a phone spear-phishing attack."

"This attack relied on a significant and concerted attempt to mislead certain employees and exploit human vulnerabilities to gain access to our internal systems," the company tweeted.

After stealing employee credentials and getting into Twitter's systems, the hackers were able to target other employees who had access to account support tools, the company said.

Internal Revenue Service investigators in Washington, D.C., were able to identify two of the hackers by analyzing Bitcoin transactions on the blockchain — the ledger where transactions are recorded — including ones the hackers attempted to keep anonymous, federal prosecutors said.

Spear-phishing is a more targeted version of phishing, an impersonation scam that uses email or other electronic communications to deceive recipients into handing over sensitive information.

Twitter said it would provide a more detailed report later "given the ongoing law enforcement investigation."

The company has previously said the incident was a "coordinated social engineering attack" that targeted some of its employees with access to internal systems and tools. It didn't provide any more information about how the attack was carried out, but the details released so far suggest the hackers started by using the old-fashioned method of talking their way past security.

British cybersecurity analyst Graham Cluley said his guess was that a targeted Twitter employee or contractor received a message by phone asking them to call a number.

"When the worker called the number they might have been taken to a convincing (but fake) helpdesk operator, who was then able to use social engineering techniques to trick the intended victim into handing over their credentials," Clulely wrote Friday on his blog.

It's also possible the hackers pretended to call from the company's legitimate help line by spoofing the number, he said.

Fazeli's father said Friday he hasn't been able to talk to his son since Thursday.

"I'm 100% sure my son is innocent," Mohamad Fazeli said. "He's a very good person, very honest, very smart and loyal."

"We are as shocked as everybody else," he said by phone. "I'm sure this is a mix up."

Attempts to reach relatives of the other two weren't immediately successful. Hillsborough County court records didn't list an attorney for Clark, and federal court records didn't list attorneys for Sheppard or Fazeli.

Associated Press Writers Kelvin Chan in London, Matt O'Brien in Providence, Rhode Island, and Frank Bajak in Boston contributed to this report.

FAMILY TREE MAKER GENEALOGY SOFTWARE EXPERIENCES DATA BREACH

The year 2020 has been a mind-boggling experience with regards to data protection (or lack thereof). Though it is only July, the amount of high-profile data leaks and data breaches continue to cause havoc for companies and customers. The most recent high-profile victim of data insecurity is a popular genealogy tool employed by tens of thousands. According to a blog post from Chase Williams of WizCase, Family Tree Maker (which is operated by Software MacKiev and used by Ancestry.com) has been found to be insecure.

The findings from WizCase's white-hat security team, which is led by Avishai Efrat, uncovered the following:

The misconfigured ElasticSearch server exposed information of approximately 60,000 users (including duplicates) and complaints sent to customer support and extremely vulnerable data about their physical location. As the company is based in the US, most of its users could be identified as US residents.

The data totaled around 25GB, and as the report notes, if used by cybercriminals, there could be dire consequences. The personal data in the Family Tree Maker ElasticSearch server can be used for social engineering attacks like phishing, identity theft fraud campaigns, and even business espionage. When the WizCase team discovered the misconfigured Family Tree Maker server, Software MacKiev was notified immediately. Though Williams notes in his report that the company made no confirmation regarding the disclosure, the server was, in fact, secured days later.

There is no evidence that cybercriminals gained access to the data in the ElasticSearch server. Nevertheless, anyone who uses Family Tree Maker should change their passwords and keep an eye on their personal data. Anything that the server has could have been stolen and passed around on the Dark Web, so practice defensive awareness for the time being. Make sure you only give a company, no matter what it is, the least amount of data you need to.

tech hero

Cloud Portal

Did you know about our new Cloud Portal? This new tool will allow you to open tickets directly with us here at Tech Hero at the click of a button!

To try it out, just go down to your system tray and look for the small blue IT icon. After you've double clicked on it you will need to sign in (You will only need to do this once!)

Once you are in you can click around explore the software.

If you have any questions, feel free to reach out to us at the number below!

(800) 900-8324 x2

Smart, cloud-managed IT solutions that make life simpler

cisco Meraki

Powerful technology for all

What is Cisco Meraki Cloud Managed Networking solution?

Cisco Meraki changed the way we think about network management today. Its out-of-band cloud architecture creates secure, scalable and easy-to-deploy networks that can be managed from anywhere. This can be done from almost any device using web-based Meraki Dashboard and Meraki Mobile App.

Focus on your core business and let Cisco Meraki manage your network

We understand that your family, customers and business are important to you. Spend more time looking after those who matter the most and let Cisco Meraki manage the network for you.

Call Tech Hero today to see about upgrading your network!

(800) 900-8324 x2

Client Spotlight

ALLSTATE PAVING & SITE DEVELOPMENT

We've been instrumental in helping Orlando grow for 17 years. We also perform work in Lake, Brevard, Seminole, Polk and Volusia counties. We specialize in customer satisfaction for all phases of site development and paving.

2020 ABC EXCELLENCE **IN** CONSTRUCTION AWARD

Netflix phishing attack targets users with 'legitimate' links

An effective phishing campaign that targets Netflix users has been uncovered by Armorblox researchers. In a blog post, Chetan Anand (co-founder and architect at Armorblox), describes the Netflix phishing attacks as multi-pronged. The attack begins with emails that claim to be from Netflix support.

These emails threaten users to respond in 24 hours or their account will be deleted. The reason given is related to a failure to receive payment for services rendered. Ordinarily, these sorts of emails are stopped by anti-phishing filters. However, Armorblox found that the links in the email appear legitimate. This confuses anti-phishing filters like Office 365 Exchange Protection.

The links in question are a redirect to a legitimate domain (including wyominghealthfairs[.]com) that contains a functioning CAPTCHA. Once the CAPTCHA is completed, users are redirected again to a very convincing Netflix page copy that is also hosted on a legitimate domain (axxisgeo[.]com). All of this makes the Netflix phishing attack dangerously effective.

Now, it goes without saying that any aware user would notice the URL bar not saying it belongs to Netflix. Unfortunately, many individuals are not as knowledgeable as they should be, especially if they were already fooled by the initial email and CAPTCHA link.

On the spoofed Netflix page, according to Armorblox's post, the following occurs if users have been hooked by the phishing scheme:

Continued on next page….

Once targets fill in their login details, the phishing flow continues with screens asking targets to update their billing information and credit card information respectively. These next few screens look a lot like something you'd see on legitimate streaming websites; this superficial legitimacy enables attackers to harvest their targets' billing addresses and credit card information in addition to their Netflix account details... Once the targets have filled in all their information, the phishing flow ends with a message of "success" and an automatic redirection to the real Netflix homepage.

The only lesson that can be learned from this Netflix phishing campaign is always to be aware of fraudulent emails. Do not assume your spam filter will take care of every phishing email. Double-check every address to every domain you are linked to, and of course, do not be quick to volunteer your personal data to any website.

— Derek Kortepeter for Techgenix