

The Linus Tech Tips YouTube hack is the latest in a line of crypto scam breaches

Popular YouTube channel Linus Tech Tips has been hacked this morning, with the channel's 15.3 million subscribers seeing videos for crypto scams instead of tech hardware reviews. It's the latest breach in a series of high-profile YouTube accounts being hacked, with scammers regularly gaining access to prominent accounts to rename them and livestream crypto scam videos.

The main Linus Tech Tips channel was breached earlier this morning, with several live videos broadcast before the hacker started making old private videos public. The account was eventually suspended, presumably as YouTube employees work to restore it. Other Linus Media Group YouTube channels, including Techquickie and TechLinked, have also been breached and given new names focused on Tesla.

It's not immediately clear how the channels have been breached, but owner Linus Sebastian tweeted that he was aware of the situation. Later, in a statement posted to Floatplane (a streaming service spun out of Linus Media Group), he said that the company is working on it with Google, and is "getting to the bottom of the attack vector with the (hopeful) goal of hardening their security around YouTube accounts and preventing this sort of thing from happening to anyone in the future." He also promised to discuss additional details on the company's podcast, though warned they might not come this week as it's "still a developing situation."

This is just the latest in a series of breaches that have

occurred over the past year, generally designed to promote livestreams that push viewers to amateur-looking crypto sites through links or QR codes. The British army's YouTube channel was hacked to promote crypto scams last year, just months before tens of thousands of "viewers" watched a fake Apple crypto scam on YouTube. Popular Vevo channels on YouTube for artists like Lil Nas X, Drake, Taylor Swift, and more were also affected by a breach last year that saw videos uploaded from an "unauthorized source."

We've reached out to Google to comment on this latest YouTube incident and to provide information on exactly what the company is doing to protect creators here. While today's breaches could be from a combination of passwords and two-factor authentication being compromised, it feels like YouTube could do more to prevent the damaging effects of this.

These scams have been going on for months, and one YouTuber claims they work through fake sponsors reaching out to creators. The YouTubers are then convinced to download a file related to the sponsorship, which is just malware designed to steal cookies, remotely control PCs, and ultimately hijack YouTube accounts.

I would personally like to see YouTube implement a lockdown mode for high-profile accounts where if you sign in from an unknown browser or location (based on IP and other factors), then you can't perform a channel rename or access livestreaming options or video deletion for a period of time. Combined with alerts for when a new location has signed in, this could help channel owners recover their YouTube accounts before any real damage is done.

YouTube could also implement a guardian system where you'd need second approval from another account to rename a channel or delete videos or even additional two-factor prompts for channel actions. This could also help slow down the impact of a YouTuber's own machine being breached. Hopefully, YouTube

has some even better ideas and can get this under control because I'm sick of waking up to a phone full of notifications about junk crypto videos from YouTube.

Update March 23rd, 10:05AM ET: Article updated with more information on how the scam works.

Update March 23rd, 2:39PM ET: Added an additional statement from Linus about the hack.

<https://www.theverge.com/2023/3/23/23653115/linus-tech-tips-youtube-hack-crypto-scam>