BIZCOMMUNITY

YouTube comments become new tool for scammers

Cybersecurity company Kaspersky says it has witnessed an unusual scam where attackers promote fake crypto services on YouTube. "They are trying to reach those interested in cheap cryptocurrency by leaving comments on popular videos - but of course, the currency won't be received," a statement from the company reads.

Source: Unsplash

Kaspersky explains that scammers leave comments under videos that are trending on YouTube to promote a fake 'breach' in the crypto market. To make their message more visible, they falsify statistics in comments and place bot replies to amplify the initial comment.

The comment encourages viewers to visit the author's own YouTube channel and watch a video that provides instructions on how to benefit from a supposed exchange rate bug. Users may not notice that this video is the only one published on the channel.

The video is definitely fabricated: the edits in the exchange rate rows are visible to the naked eye, and the comments are packed with overjoyed feedback, Kaspersky warns. The link under the video leads to a fraudulent exchanger.

Crypto crash: market volatility is testing investor will but crypto-enthusiasts still see a future for the asset class

Andrew Urquhart and Brian Lucey 29 Jun 2022

Once a user arrives on the webpage linked in the description, the victim sees a facility to exchange bitcoin – but if they use it, they will never see this money again, as the service is fake.

"Cryptocurrency is coping with difficult times because of a constant drop in exchange rates. Those who want to buy currency at the best price are frequently being targeted by fraudsters. Our recent investigation shows that today attackers resort to new, and more mainstream ways to reach their victims – even considering their YouTube preferences. We

strongly recommend users carefully check the crypto resources they turn to and do not rely on random comments on YouTube," comments Mikhail Sytnik, a security expert at Kaspersky.

Tips to avoid scams:

- Check any link before clicking. Hover over it to preview the URL and look for misspellings or other irregularities. It's also good practice to only enter a username and password over a secure connection. Look for the HTTPS prefix before the site URL, indicating the connection to the site is secure.
- Sometimes fake emails and websites look just like real ones. It depends on how well the criminals did their homework. In particular, the hyperlinks will, most likely, be incorrect — with spelling mistakes. However, the links can also be disguised to look like valid links and redirect you to a different page, impersonating the legitimate site.
- To protect your data and finances, it is good practice to make sure the online checkout and payment page is secure. You'll know it is if the web page's URL begins with HTTPS instead of the usual HTTP; an icon of a lock will also typically appear beside the URL and the address bar in some browsers will be green. If you don't see these features, do not proceed.
- Use a trusted security solution that can help you check the security of the URL that you're visiting and also provides the ability to open any site in a protected container to prevent theft of sensitive data, including financial details.