

Secure future or crypto scam? Cyber-Forensics.net alerts about crypto scammers posting fake ads on Facebook

Criminals in Australia are posting fake advertisements to lure investors. They are using pictures of well-known Australian personalities to target victims.

SOFIA, BULGARIA, April 1, 2022 /EINPresswire.com/ -- Social media has become an integral part of everyday lives. However, despite the uncountable benefits, sites like Facebook, Twitter, Instagram are full of scammers looking to take advantage of the victims.

In a new type of online crypto fraud, Australian citizens are reporting being targeted by fake crypto investors mainly using Facebook to target them.

The latest figures from leading newspapers indicate that higher authorities in Australia received more than 18300 reports in February, with financial losses accounting for more than \$38,000,000.

Cyber-Forensics.net, a cyber forensics service for online scam victims, informs: "scammers succeeded in duping hundreds of Australians causing them to lose over \$38 million in March 2022 only. All these victims fell victim to a range of fraudulent schemes launched through fake ads on Facebook."

“

scammers succeeded in duping hundreds of Australians causing them to lose over \$38 million in March 2022 only.”

Timothy Benson

The investigations resulted in unprecedented legal actions taken by the Australian Competition and Consumer Commission. The parent company of Facebook Meta faced critical allegations as the Australian government found that the platform failed to prevent scammers from using fake advertisements to endorse misleading crypto schemes.

How Did the Fake Advertisements Mislead Australian



Cyber-Forensics.net



Cyber Forensic Specialist

Consumers?

The specific advertisements for cryptocurrencies and other investment schemes started appearing in 2019. These advertisements contained links to fake media articles directing consumers to another website that mirrored well-known Australian celebrities endorsing the crypto schemes.

Some of these advertisements featured images of multi-millionaire celebrities like Andrew Forrest, Dick Smith, David Koch. Interestingly, all of these individuals had no prior knowledge or had any connection to these advertisements. Additionally, other celebrities from overseas also found their names associated with these fake crypto schemes.

Rod Sims, chair of the Australian Competition and Consumer Commission (ACCC), informed “the fake ads may have led to more than A\$ 650,000 in financial losses for one consumer.

He adds: “Those who visited landing pages from ads generated substantial revenue for the platform.”

Why are fake advertisements most prominent amongst scammers?

For crypto scammers, there’s a lot to like about social media. It’s the least cost-requiring way to reach billions of people within a small time frame. It’s easy to manipulate one’s identity and can be operated from anywhere. And it’s easier to skip separating scams from genuine schemes because victims think they are receiving requests from their relatives, friends, or people they admire.

Timothy Benson, who helps victims [recover stolen funds](#), thinks: “Social media’s algorithms and business models are designed to reach a mass audience. It is a key to enabling scammers to target users and most likely get them to click malicious links in the ad or visit fraudulent landing pages using Facebook algorithms.

How to avoid clicking fake advertisements on facebook?

□ Think about the display of the ads: The way the ads are presented can reveal if it's coming from a genuine advertiser or fake organization.

Invest in fraud detection software: Automated scam detection systems that use machine learning to break down the complex algorithms may be beneficial in detecting and filtering invalid clicks before the users can even click them.

□ Study Facebook ads properly: Even though people have been using Facebook for years, many don't know how Facebook Ads work. However, the social media giant attempts to make it as humanly possible to learn their ad system.

□ Look for spelling mistakes: To identify a crypto scam or any online scam, read the information

being displayed in the banner. Check for spelling mistakes and also see if the images look professional.

What to do if one clicked a fake advertisement on Facebook?

If someone clicks the fake advertisement on Facebook, here is what they can do:

- Close the tab immediately: Once the user spots a fake advertisement, immediately close the tab from the browser.
- Switch off the device from all networks: The next logical step is to disconnect the device from all networks and switch off the device's power.
- Report the matter: When someone comes across fake advertisements on Facebook or any social media platform, it is advised to report the issue or submit a ticket to the platform company itself.

If someone has witnessed a potential crypto scam online that might be dangerous, it is recommended to reach out to local authorities first to put them on alert.

The next step is to spread the news to keep others from falling victim to the scam.

How to report the fake advertisements on Facebook?

Cyber-Forensics.net, a firm that also provides counseling on how to [recover stolen crypto](#), says if scammers have been targeted by someone on Facebook into clicking fake advertisements, they should immediately report the matter to the social media platform.

- To report the scam running on Facebook: Open the ad library, search the ads box, enter the related keyword, and select "report ad."
- To report the scam to authorities: Visit online websites or physically submit the information. Users can also choose to send emails to the concerned authorities.
- To report the scam to fund recovery services: If someone has lost a portion of their valuable investments, it is highly recommended to hire fund recovery services.

How Can Fund Recovery Services Help Crypto Scam victims?

There is no shortage of online resources to search for how one can get help related to [bitcoin recovery service](#). But when it comes to practicality, there are only several limited resources. And the most important one among these is hiring a credible fund recovery company.

These services are equipped with specialized teams of experts who know about cryptocurrency, blockchain technology, business models on which social media platforms work. This allows victims to gain all the information under one roof and secure their finances as quickly as possible.

About Cyber-Forensics.net

Cyber-Forensics.net is committed to providing the most accurate tracing service for victims of online scams. Cyber-Forensics.net empowers and simplifies the process of tracking down the cyber-criminals and assists in recovering the funds and creating an atmosphere for a negotiated settlement. For more information, please visit <https://cyber-forensics.net/>.

Peter Thompson
Cyber-Forensics.net
+1 917-920-6613

[email us here](#)

Visit us on social media:

[Twitter](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/567227534>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 Newsmatics Inc. All Right Reserved.