

Theft by hacking is becoming a nightmare for crypto coin holders: Cyber-Forensics.net alerts cryptocurrency investors

Hacking involves breaking into a computer system or network without permission and stealing financial assets like crypto. Experts suggest ways to stay protected

SOFIA, BULGARIA, August 21, 2022 /

EINPresswire.com/ -- Statistically speaking, theft by hacking has grown drastically. According to suggested figures by scam surveys, the cybercrime environment has expanded since 2021. It will cost countries trillions in financial losses by 2025.

And as users continue to spend more and more time online, hacking has become a more significant issue. Cyber-Forensics.net, a cyber forensics service for online scam victims, has been receiving several complaints explaining what theft by hacking looks like:

How does theft by hacking work?

All computer networks are required to provide a safe passage for internet browsing. For example, in online purchases, internet users are supposed to visit official websites that undergo multiple checks to ensure that a website protects consumer data and stores wallet information safely.

“

Anytime an individual trespasses the information on someone's computer without permission, it is a crime.”

Timothy Benson

But according to experts, in reality, nothing is perfectly secure. As per the latest investigations, hackers have repeatedly discovered new ways to break into computer networks, such as exchanges created by various mining companies that make digital wallets where people can store their cryptos.



Cyber-Forensics.net



Cyber Forensic Specialist

Like a trespasser, hackers penetrate computer networks. At first, they may bypass a secured network to look for information. However, they soon access the folders where digital wallets may be, sensitive corporate data may be and steal it when they can.

Is Hacking Illegal?

Timothy Benson, who guides crypto scam victims on [how to recover scammed bitcoin](#) and other financial assets, opines: Anytime an individual trespasses the information on someone's computer without permission, it is a crime. Hacking is illegal even if the hacker has not caused any system damage. Criminals can be prosecuted as per state or federal law.

How do you stay protected from theft by hacking crimes?

Since cyber security is critical, here are a few steps to take to stay protected from theft by hacking crimes:

Don't put blind trust in anyone online: Approach every contact online with extreme caution.
Set up firewalls on your devices: Firewalls prevent unauthorized access and alert users via email or text message in case someone attempts to.

□ Install antivirus software. Antivirus programs like Avast, Bitdefender, and Malwarebytes can protect unauthorized codes from being added as an extension to the operating system.

□ Consider safe browsing: The first thing to do is to secure computers and mobile devices. Check virtual private networks and if a website has an SSL (Secure Socket Layer) certificate.

□ When using public wifi, never allow computers to save passwords entered to access digital wallets.

□ Keep operating systems, apps, and browsers up-to-date.

□ Choose Strong Passwords: Make sure to encrypt the files containing all the financial assets by using strong passwords. Easy-to-remember passwords are an open invitation for hackers to conduct organized crimes.

□ Switch off autocomplete.

□ Clear caches and delete browsing history regularly. Browsing history may have cookies and cached files to give hackers plenty of information.

□ Beware of other financial crimes prevalent around you: Scams like phishing, vishing, investment-related, crypto-related, and others receive close attention from the media. Thus, anything that's affecting many people is sure to make the headlines.

How do you get back at scammers involved in theft by hacking?

□ Report the matter: When someone has been a target of such scams, it is a logical approach to file a report with the local police officers. Approaching local investigators tends to provide a preliminary screening of how the fraud happened.

□ Keep scammers at bay by joining forces with authorities. Connect with specialists such as Cyber-Forensics.net, who have years of experience collaborating with lawyers, cyber experts, and ethical computer hacking experts, and team up to scam the scammers. Getting proper help will ensure victims know what happened.

□ Hire fund recovery services: A logical approach is to seek expert advice. One can do it by hiring the [best bitcoin recovery expert to recover scammed bitcoin](#) or getting connected with legal help providers. The former ensures increased chances of recouping lost funds.

How do fund recovery services help victims secure financial assets after theft by hacking?

A few situations in online scams are worse and cannot be handled by the customers. It can be proven a crime if one can show how hackers penetrated their computer devices, accounts, or digital wallets without their permission. Once confirmed, the funds can be reported as stolen. And this can ensure victims' eligibility to get the total amount back.

Hiring fund recovery agencies and [bitcoin recovery services](#) when cryptocurrency is involved acts as an advocate like individuals would hire a lawyer for a personal or financial issue. There are different types of services a fund recovery company can offer. Thus, it is recommended to identify which kind of service victims need.

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. Cyber-Forensics.net commonly deals with Bitcoin scams and Forex withdrawal problems. 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/571219533>

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.