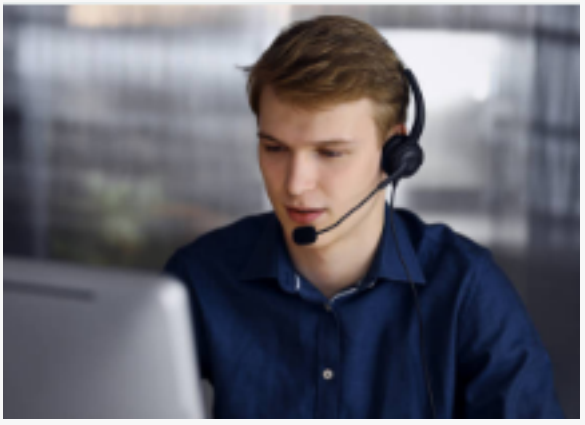
Watch Out For Rogue Anti-Virus Software: Cyber-Forensics Briefs On How To Avoid Fake Software

Fake Anti-Virus Software is created by fraudsters to access the user's computer, steal personal details, or ask for money by showing them false data.

Cyber-Forensics.net



Cyber Forensic Specialist

SOFIA, BULGARIA, August 31, 2022 / EINPresswire.com/ -- We all know that the internet is filled with scammers and hackers looking for a target and trying to steal their personal information and money with the help of their toolkits like viruses, trojans, crypto miners, etc. The first step to protect oneself from such fraudsters is installing anti-virus software in their system. But now it seems there are fake anti-virus softwares created by criminals that, if installed, will transfer an individual's details to the scammer.

Research has shown that over 2,000 people fall victim to such scams and pay anywhere from $50 to $100 for the fake anti-virus software.
A woman became the victim of a fake anti-virus scam. When asked about the incident, she said a pop-up alert appeared on her computer screen while working, saying, "Your computer is infected. Download the anti-virus software to remove the virus." She followed the instruction believing it was a legitimate alert but lost almost all the data on her system.

Cyber-Forensics, a stolen cryptocurrency recovery service provider, notices; "A common way people get scammed into installing fake anti-virus software is through pop-up window appearing on their browser alarming the user that they have detected a virus on their computer that can cause a lot of damage if not cure ASAP. They need immediate action in convincing the user to install the fake anti-virus software. This can also happen on your mobile phone. If you see these popups, try pressing back and not clicking the button."

What Is A Fake Or Rogue Anti-virus Software?

A rogue anti-virus software refers to malicious software that claims to have found an infection in the victim's computer. The scammer manipulates the victim to install the fake anti-virus and

> An individual should ensure the source is legit before believing in something they saw online. Installing anti-virus software without knowing where it came from can harm the user and their system."
>
> *Timothy Benson*

then tries to extract payments or personal information from the victim.

Such Rogue anti-virus software will be of two types: one built from scratch by a company that no one has heard about and one that is a modified version of legitimate anti-virus software.

To avoid an anti-virus scam, one should never prefer a pirated anti-virus. An individual should buy legit anti-virus software produced by a legitimate company.

How To Identify A Fake Anti-Virus Software?

 Fake notifications: Scammers try to exaggerate things. They will claim threats that may not exist on the victim's computer. They try to create a sense of panic and urgency.

 Infections in every scan: Fake anti-virus software contains mysterious technology that helps them detect many infections with every scan.

 Pay per clean: Fake anti-virus software is created to siphon money from the users. These types of fake software pretend to scan the computer for infections; after checking, they will charge money to clean the system. Legitimate anti-virus software will never ask for charges to inspect and clean the system.

 Unnecessary alerts and notifications: A fake anti-virus software has this annoying way of getting users' attention. They will keep pushing fake pop-ups and warnings. A genuine anti-virus software never tries to bother the user unless it is a matter of great urgency.

 Bad Google reviews: If an individual finds terrible reviews and comments on google regarding the anti-virus, it is better not to install it. Before installing anti-virus software, one should verify if they have a legitimate website or source or not.

How To Avoid Getting A Fake Anti-virus Software?

Timothy Benson, a bitcoin fraud recovery specialist at Cyber-Forensics.Net, says, "An individual should ensure the source is legit before believing in something they saw online. Installing anti-virus software without knowing where it came from can harm the user and their system." Let us see some important points to stay protected from such fake anti-virus software:

Research: Before installing any program or software, it is essential to research the reputation of the company selling the software and review previous users' reviews and comments. Just

because the company is trustworthy does not mean it can be trusted blindly. Clicking on random banner ads or links can lead to malicious websites.

 Use security settings: After conducting sound research, when an individual installs a trustworthy anti-virus, they should take advantage of the security settings offered.

 Look out for signs: No matter how reliable an anti-virus software looks, individuals should ensure they are doing their part to keep themselves safe. The easiest way to do this is by familiarizing oneself with the anti-virus software. One should know what alerts and messages look like to recognize fake watches and notifications.

How Can Fund Recovery Company Be Helpful In Such Situations?

A fund recovery company is equipped with the best technology that helps the victims get the right services they need. They execute the proper investigation and work with authorities to trace funds, especially digital currency transactions. Legitimate fund recovery companies will also assist victims with appropriate advice to ensure they do not fall into another fraud.

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
