

Trader Defense Advisory Warns: Don't Let Scammers Gain Control of Your Computer or Device

Some of these fraudulent parties go beyond encouraging people to part with their money, They will find ways to get into your computer and your bitcoin wallet

SCHAUMBURG, ILLINOIS, UNITED STATES, March 22, 2021 /EINPresswire.com/ -- [Trader Defense Advisory](#) Warns: Don't Let Scammers Gain Control of Your Computer or Device

The warnings of trading and [cryptocurrency scams](#) are becoming more persistent. The COVID-19 crisis has led directly to increased internet activity, and with it, an upsurge in fraudulent activities. One example that expresses the scale of the crisis is one man [who recently lost \\$563,000 to a scammer](#) impersonating Elon Musk on Twitter.

Internet scam artists are finding innovative ways of cheating unsuspecting consumers. Some lure would-be traders with promises of incredibly high returns or suggest bitcoin for dollars for a once-in-a-lifetime investment opportunity. Some of these fraudulent parties go beyond simply encouraging people to part with their money, but may find ways to get into their computer and devices to access personal financial information or bitcoin wallet.

Trader Defense Advisory warn that fraudulent brokers and bitcoin scammers are increasingly engaging tactics that require installing software - such as RemotePC, AnyDesk and TeamViewer - that allow scammers remote access of the victim's computers. The criminals represent fake cryptocurrency companies and urge clients who may not be tech savvy or familiar with bitcoin to let them help them access their virtual coins.

1. TDA sees a new trend
2. Many clients want to join the bitcoin party but don't understand the technical process to buy.
3. Scammers are taking advantage of this demand, and pretend to 'help' clients remotely.
- 4) At the advice of the criminals, victims install remote desktop software, giving the scammers access to their crypto and bank accounts.
- 5) The scammers advise the victims to identify themselves to the regulated exchange, legitimizing the entire process.
- 6) They then proceed to wire money to the exchange, where the funds are laundered through dozens of accounts.

While pretending to work on behalf of the client, these scammers will create an account on a regular exchange such as Coinbase or Kraken. They will ask the clients for personal information so they can verify the account. Once the account is verified, the cybercriminals can then authorize transactions as the client and deposit up to millions of dollars into their own holding wallets. They will then launder the funds to dozens of accounts around the globe.

Without the assistance of a legitimate fund recovery company and authorities, getting funds back from this kind of cryptocurrency scam is nearly impossible. That is why Trader Defense Advisory provides a valuable service to those who have fallen victim to bitcoin fraud. TDA professionals consult with clients and assist them in making claims that will aid in fund recovery.

Steps to Avoid Remote Desktop Fraud

Trader Defense Advisory suggests several steps to avoid being the target of fraud using AnyDesk or similar software. First of all, no broker should ask for access to a computer or device, ever. And no one should ever gain access to your online banking or bitcoin wallet.

Even if a client is having difficulty with a trading platform, there is no need for any customer service representative or broker to ask clients to request remote access. These are all tell-tale signs of fraud.

Also, if a broker or a cryptocurrency service alleges that there is a problem with your computer or device and suggests having a technician help, be suspicious of this offer. Usually, the process of computer repair is initiated by the owner of the device rather than vice versa. If someone provides unsolicited technical assistance and requests remote access to devices, do not answer their requests.

Have You Been the Target of a Remote Desktop Trading Scam? Contact Trader Defense Advisory

If you have allowed computer access to a third party you suspect has scammed you, contact Trader Defense Advisory immediately. TDA has the tools and expertise to deal with many types of fraud. Our experts guide clients in their path to making a claim against fraud and help clients take their first steps toward fund recovery.

Contacts:

Dan Arnheim, Media Relations Director

Trader Defense Advisory

news@traderdefenseadvisory.com

1900 E Golf Rd Suite 950 Schaumburg, IL 60173

Daniel Arnheim

TDAI Group, LLC

+1 917-920-6749

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/537317504>

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.

© 1995-2021 IPD Group, Inc. All Right Reserved.