TDA Encourages Best Practices to Stay Safe from Vishing and Remote Access Scams

Cybercriminals urge employees of major companies to download apps that will give them access to their devices containing malware which robs the victim of data.

SCHAUMBURG, ILLINOIS, UNITED STATES, July 8, 2021 /EINPresswire.com/ -- The FBI has issued a warning about vishing and remote access attacks after employees at major companies were called by scammers pretending to be from IP Helpdesk.

Cybercriminals urge these employees to download an app that will give them access to their devices. This app often contains malware which robs the victim of data.

The results of these scams have been staggering and have affected individuals, small companies, and large corporations. The high-profile celebrity imposter scam that affected Twitter in 2020 had its source in a spear phishing attack and a vishing attack when the scammer uses voice technology to sound like a trusted source.

Trader Defense Advisory assists companies and individuals who have been affected by identity theft and cybercrime. TDA experts have confirmed an uptick in client complaints about vishing and remote access scams, partly in response to the trend of working from home as the result of COVID-19.

As more people are working remotely, warns TDA, vishing and remote access scams are likely to increase to take advantage of the varying degrees of tech savvy among remote workers and awareness of these scams. Anyone who uses the internet, but particularly those who work remotely, should use best practices outlined by TDA to stay safe from having individual and company information compromised.

The Twitter Vishing Case
A total of 130 high-profile client accounts were hacked as the result of vishing and remote access scams targeting Twitter employees. These accounts were ultimately vehicles of a bitcoin scam that used fake celebrity endorsements to encourage Twitter users to make quick bitcoin trades. This crypto scam robbed traders of millions.

Scammers contacted Twitter employees through vishing methods or voice calls that created a false sense of security. They convinced the employees that they were from Twitter's IT

department and asked for access to information. The scam worked through shared credentials from many employees, so if some would dismiss the request, thinking it was suspicious, others would grant it and pass along information.

The result was a crypto scam that accessed the accounts of Elon Musk and Barack Obama. Those who were convinced, correctly, that these were real and not knock-off accounts were more likely to part with their money and lose their bitcoin.

Remote Access Scams

Often used in tandem with vishing and spear-phishing scams, remote access scammers request access to a computer or a device. They will pretend to be from IT within a company and request the employee download a fake app so they can gain control of the computer and have access to files.

This doesn't just happen in a corporate context, but can also be a tactic as part of a forex trading scam. A fake broker may offer to assist the client with a trading platform and say that the only way they can help them is to gain access to their computer.

This is usually not necessary, but if the user is not tech-savvy and can feel easily frustrated with technology, they may be willing to put their suspicions aside and allow access. According to TDA, it is always a good idea to be suspicious of any request to gain direct access to a computer or device.

How to Avoid Vishing and Remote Access Scams

Be suspicious of any case when someone, even if they are reportedly from your company, asking for direct access to your computer. It is almost never necessary

If you notice something suspicious, ask for a number and call the person back to verify it is them

Ask for a video call in addition to just an audio call and ask to see documents or other forms of identification

Do not be concerned that it is rude to hang up on a suspicious call if it is in your company. You will most likely not get in trouble if you can demonstrate that you were worried it was a case of vishing

Ask for multiple types of verification before making money transfers or giving over data

Remember that most IT departments can give instructions that do not require direct access to computers or devices

If you have been the target of vishing or remote access scams, it is important to take steps immediately to track down the source of the scam and for fund recovery. Trader Defense Advisory has the resources to assist clients and combat various types of fraud.

About Trader Defense Advisory

Trader Defense Advisory offers all clients a free consultation to assess their cases and design a roadmap for pursuing their claims. The TDA team works tirelessly to advocate for clients and will fight back against Crypto and broker scams.

Contacts:
Dan Arnheim, Media Relations Director
Trader Defense Advisory
Telephone: +1-917-920-6749
news@traderdefenseadvisory.com
1900 E Golf Rd Suite 950 Schaumburg, IL 60173
Twitter
FaceBook

Daniel A
TDAI Group, LLC
+1 9179206749
email us here
Visit us on social media:
Facebook
Twitter
