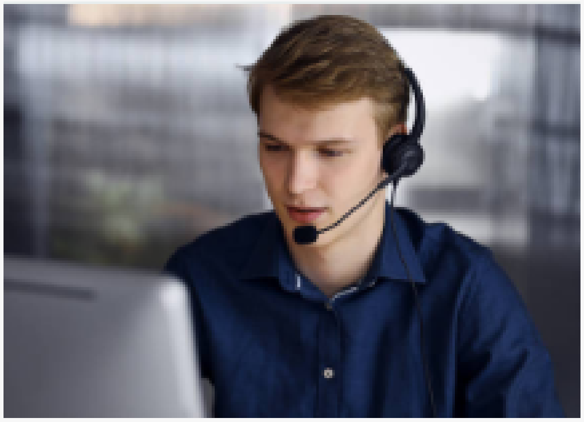
EINPRESSWIRE

Cyber-Forensics.Net Issues Warning: Protect Yourself Against From Social Engineering and Cryptocurrency Scams

Cyber-Forensics.Net warns victims about the use of remote desktops in scams and tips on how to avoid fraudulent companies.



Cyber Forensic Specialist

SOFIA, BULGARIA, January 5, 2023 /EINPresswire.com/ -- Cyber-Forensics.Net, a leading fraud recovery specialist and fund recovery service, is warning victims of remote desktop scams to be vigilant against social engineering tactics used by cryptocurrency scammers.

According to Timothy Benson, Chief Intel Officer at Cyber-Forensics.Net, "Remote desktop scams are becoming increasingly sophisticated, and it's important for victims to understand that these scammers use various social engineering tactics to manipulate and deceive their targets. They may pretend to be a legitimate representative of a company or government agency, or use fake notifications or alerts to trick victims into revealing sensitive information or transferring funds."

> Remote desktop scams are...increasingly sophisticated...[I]t's important for victims to understand that these scammers use various social engineering tactics to manipulate and deceive their targets.”
>
> *Timothy Benson*

How do you spot a remote desktop scam?
To spot a remote desktop scam, be on the lookout for unsolicited phone calls or emails, especially if they appear to be from a legitimate company or government agency. Scammers may trick you into revealing personal or financial information, such as passwords or account numbers, or request that you transfer money through a new or unfamiliar payment method, so look out for this. Be cautious of any suspicious links or attachments, and be wary of high-pressure tactics that try to get you to act quickly.

Tips to Avoid Remote Desktop Scams:

Cyber-Forensics.net

1. Do not trust unsolicited phone calls or emails, even if they appear to be from a legitimate company or government agency.
2. Do not give out personal or financial information, such as passwords or account numbers, in response to unsolicited requests.
3. Be cautious of any requests to transfer money, especially through a new or unfamiliar payment method.
4. Do not click on links or download attachments from unknown or suspicious sources.
5. Check sender emails! A government agency or a legitimate company will not send from a Gmail account.
6, Check the exact URL of the sender and ensure that it is not replacing letters such as the number 1 for the lowercase letter L and other similar tricks that scammers use to spoof the actual sender's email address.
7. Regularly update your security software and use strong passwords to protect your devices and accounts.
8. As a general rule, always be very cautious about whom you give remote access to your computer. It must be someone you know, and you should check with them that it is really them by phone or another verification method.

If you suspect that you may be a victim of a remote desktop scam, it is important to contact law enforcement and a reputable fraud recovery specialist as soon as possible. They can help you to trace the funds and work towards recovering them.

Benson advises victims to seek the assistance of a bitcoin recovery expert, such as those at Cyber-Forensics.Net, who can help trace the funds and work towards recovering them. However, he also warns victims to be cautious when speaking to fund recovery companies, as not all are alike.

When it comes to recovery companies, Benson recommends looking out for the following warning signs:
1. No guarantees - Any company that offers a guarantee is likely a fraud.
2. They discourage working with police and authorities - Legitimate companies will not be afraid of law enforcement and will encourage victims to report
3. scams to the authorities.
4. They claim to get the money from an exchange or insurer - This is unrealistic and a tactic used by fraudulent companies.
5. They accept money in cryptocurrency - Legitimate companies will not accept payment in cryptocurrency.
6. High-pressure techniques - High-pressure sales tactics are a red flag and should be avoided.
7. Confusing concepts or avoiding questions - A legitimate company will not try to confuse or evade questions.

Benson urges victims to contact Cyber-Forensics.Net as soon as possible to increase the chances of a successful recovery. "Our team of experienced professionals has the knowledge and resources to track down these cybercriminals and assist in the recovery process," he said.

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 cyber criminals and assists in crypto recovery services, and creating an atmosphere for a negotiated settlement. For more information, please visit https://cyber-forensics.net.

Monika Miltchova
New Safe Services
+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/609663530