EINPRESSWIRE

Scammers Using Remote Desktops To Extort Money: Cyber-Forensics.net suggests preventive ways

The remote desktop scam involves convincing users to install apps like Anydesk to gain control of your computer and get hold of bank details.

Cyber-Forensics.net

SOFIA, BULGARIA, November 16, 2021 /EINPresswire.com/ -- With significant aspects of our lives digitized today, work from home proved to be a boon for many. However, the latest reports indicate that remote desktop protocol attacks increased by 768% between Q1 and Q4 in 2020, leading organizations to issue warnings against online scam activities.

Cyber-Forensics.net, an industry leader in providing cyber-forensics services for victims of online scams, uncovered the dangers of the increased adoption of remote desktops. Cyber-Forensics.net reported hackers posing as IT professionals could gain control over your personal computers by convincing you to connect with your computer through platforms like Anydesk, LogMeIn, TeamViewer, and GoToAssist.

The new remote desktop scam involves fraudsters tricking you into installing one of many apps like Anydesk and cleverly taking control of your bank details.

Since it is difficult to find the suspect's whereabouts in the middle of the scam, there are a few things Cyber-Forensics.net suggests that can allow you to keep at arms away from such harm.

Never Share your OTP
For any fraudster to run a successful scam includes getting a unique id code of your computer. The scammers usually call these computer IDs One Time Password confirmation codes to confuse users. To avoid this fraud technique, never share any OTP, PIN, or password with anyone you do not know.

Keep Password Strength Strong
Entering a password is the first line of defense against any unprotected or unauthorized access to your personal information. Meaning, the stronger the password strength is, the harder it is for scammers to penetrate through your details. A good way to keep essential details protected is to

keep changing passwords frequently and keeping a regular check on financial transactions.

Gather knowledge about steps to follow
A usual reaction of any individual after learning they have been scammed is to go into full panic mode. However, maintaining calm in the situation helps you think through better and take thoughtful steps. The first step is to report the fraud to the police. You can further take other actions like closing accounts, and reaching consumer protection agencies or cyber forensics.

Federal Trade Commission Consumer Information states that
“Contact your bank and tell them it was an unauthorized debit or withdrawal. Ask them to reverse the transaction and give you your money back.”

What to do if you have been scammed?
The most crucial step is first to check all the transactions made by you in the past 24 hours. In case there is any suspicious withdrawal, visit your nearest bank immediately and lock down all transactions.

At the same time, uninstall the remote control application and put your desktop on full factory reset. This will erase any malicious data on your computer. Additionally, it is suggested to change the passwords of your bank accounts and other financial accounts immediately.

How to stay safe from such tricks?
Ever since the rise of digital payments caught pace, it has been easy to lose your money. But that does not mean that you cannot get your money back. Often fund recovery is a multi-level process, but with expert consultation, you can get your hard-earned money back.

Refrain from installing any third-party payment applications suggested by anyone you met online:
Most hackers persuade you to install unprotected apps that enable an untraceable gateway to a user's device. Thus, avoid installing any such app.

Turn computer run device on safety mode:
Every smart device contains a built-in safety protocol that allows users to get notifications before any third-party app or suspicious app tries to gain access to your computer or phone.

Recent investigations by Toronto Police revealed that impersonators contact people to tell them about issues like bank security, issues with computer software, investment opportunity, or fund recovery.

The Toronto Police said that since people often have their user profile information stored inside their web browsers, the scammer quickly gets unfettered access to such details using certain websites.

The pattern of cheating people is common. A report by UK Finance revealed that "Impersonation fraud shot up by 84% in the first half of 2020, with almost 15,000 reports and £58m lost. At a more granular level, Action Fraud says that it has received 14,893 'computer software service fraud' reports between October 2019 and September 2020, with reported losses reaching around £16.5 million over that period."

The use of remote access is an integral part of modern-day users- but a few safety precautions and hope for better security breakthroughs promise a stop to increasing scams.

Venn, the industry's first Virtual Desktop Alternative (VDA) , launched its breakthrough LocalZone Technology. The VDA offers solutions to modern-day security challenges of remote and hybrid work environments.

"LocalZone Technology marks a powerful new approach for MSPs and IT leaders who have seen legacy virtual desktop infrastructure tools fall further and further out of step with the modern mode of work."
— David Matalon, CEO and Co-Founder of Venn

Venn claims that LocalZone will be able to address the growing challenges in the market related to security parameters. The solution ensures employee privacy while working with sensitive information at remote desktops.

Experts believe that powerful desktop infrastructures can be a game-changer in the future ensuring productivity, protection, and privacy. Users will be able to have more control of data privacy resulting in profound compatibility with technology.

About Cyber-Forensics.net

Founded in 2021 and headquartered in Sofia, Bulgaria, 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/or 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

This press release can be viewed online at: https://www.einpresswire.com/article/556089528

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 IPD Group, Inc. All Right Reserved.