Hackers use Anydesk to log into computers and steal everything remotely: Ftcyber.com alerts users

Once the victim has downloaded and installed AnyDesk, the hacker then has full control of their computer and can see everything they are doing.

FT Cyber

BERLIN, GERMANY, September 8, 2022 /EINPresswire.com/ -- AnyDesk is a free remote desktop application that allows users to log into computers from anywhere in the world. And while it's an excellent tool for legitimate users, it's also a great tool for hackers.

> Once the victim has downloaded and installed AnyDesk, the hacker then has full control of their computer and can see everything they are doing."
>
> *Peter Thompson*

That's because AnyDesk can be used to remotely access a computer without the user's knowledge or permission. FTCyber.com, a cyber intelligence firm helping online scam victims and fund recovery companies work with authorities to recover stolen funds, witnessed that once a hacker has access to a computer, they steal sensitive information, install malicious software, or even steal identification documents.

AnyDesk Scam: How hackers log into computers and steal everything

A new wave of "AnyDesk" scams are sweeping the internet, with hackers using remote desktop software to log into people's computers and steal everything.

Recently, a woman in her mid-30s lost her entire inheritance in an AnyDesk fraud. The scam, which has been doing the rounds on social media and email, starts with the hackers cozying up to victims. They then introduce a third-party trading company that proposes to "help" victims purchase bitcoin and other cryptocurrencies. To "assist," they send a link to AnyDesk - a legitimate remote desktop software - to their victim to log in and make illegal transfers to their account.

In another such incident, the victim from the United Kingdom in her late 50s received a call from

a scammer claiming to be from the fraud department of HSBC bank.
The scammer asked the woman if she had received a payment for £60,000 on a particular date and time. When the victim denied she received it, the scammer asked her to download the AnyDesk app to help her approve the transaction. In no time, the fraudster stole money from the victim's bank account in a background window. This was done with the victim's assistance, who had to provide two-step authentication for the transaction.

"Once the victim has downloaded and installed AnyDesk, the hacker has full control of their computer and can see everything they are doing. They can also access any files or documents stored on the computer and install viruses through the back door. In some cases, the hackers have even been able to follow their victims through their webcams and see everything they are doing in real-time." says Timothy Benson of FTCyber.com's investigative team.

How do hackers use AnyDesk to scam people?

AnyDesk allows users to access another computer from a remote location. This can be done using either the AnyDesk address or generating a session code.

Hackers often use the latter method in AnyDesk scams. They will send victims an email or message with a seemingly innocent request, such as asking for help with a technical issue. Once they click on the link and enter the session code, the scammer will have full access to the victims' computers as if they were sitting in front of it.

They can then steal their personal information, passwords, and financial details. Sometimes, they install malware on the computer, giving them ongoing access even if the victim changes the AnyDesk password.

How to be safe from AnyDesk scams?

Recently, another victim, a senior citizen out of Reno, Nevada, lost $50,000 to an AnyDesk scam in January 2022. With the rise in popularity of remote working, scammers are increasingly targeting users with fraudulent schemes through remote desktop applications.

In suggesting ways to protect oneself from AnyDesk scams, Timothy Benson of FTCyber.com says -

-Never accept unsolicited AnyDesk requests
-Do not download AnyDesk from unofficial sources
-Do not click on links from unknown senders
-Always be skeptical of anyone connecting to your computer. Ideally, check the ID and confirm with the company they work at with the company.
-if you have downloaded Anydesk or another remote desktop application, keep the AnyDesk software up-to-date.

-Install reputable security software on the computer and do your best to turn it off if not in use to avoid hackers.
-FTcyner recommends uninstalling such applications to stay on the safe side if you must use them.

What should be done in case anyone is scammed via AnyDesk?

If one is scammed via AnyDesk, the best thing to do is take immediate action to protect computer and personal information. Here are a few steps everyone can take:

-Run a malware scan on a computer using an antivirus program like McAfee or Norton
-Run a scan to check drivers and consider allowing a professional to check; sometimes, backdoors are hard to spot.
-Be sure to monitor accounts for any suspicious activity and change passwords to sensitive websites such as email, bank accounts and government websites such as social security.
-Last but not least, if money or anything has been stolen, report the scam to the police so they can take appropriate action and help prevent others from being scammed in the future.

How to report an AnyDesk scam?

To do so:
Visit the AnyDesk website and click on the "Support" tab.
Click the "Contact Us" link and fill out the form.
Include as much detailed information as possible, such as the scammer's name, address, phone number, method of communication, emails, chats, wallet addresses, banking information, and any other relevant information.

AnyDesk scams: Tips for avoiding

AnyDesk scams are rising as hackers take advantage of distance learning and working-from-home trends. There are a few things everyone can do to avoid becoming a victim of an AnyDesk scam:

- Avoid clicking on links or downloading files from unknown or untrusted sources. If anyone receives an AnyDesk request from someone they don't know, verify their identity before accepting.

- Be cautious of any unexpected AnyDesk requests, even if they come from a trusted source. If anyone's not expecting a request, it's best to err on the side of caution and decline it.

- Keep AnyDesk software up to date with the latest security patches. This will help close any potential security gaps that hackers could exploit.

- Make sure to have strong antivirus and anti-malware software installed on the computer. This will help protect the system from any malicious files used in an AnyDesk scam.

How Does a Fund Recovery Service Such As Ftcyber.com Help Scam Victims?

Ftcyber.com conducts a thorough interview with the victim and prepares necessary documents that aid in the facilitation, investigation, and a cyber forensic audit of the trajectory and location of stolen funds. This is often done with the assistance of investigators, lawyers and authorities. FTCyber.com may run various honeypot methods to catch the scammers with the authorities' permission. They also assist the Client in filing a complaint with the local police or appropriate regulators. Finally, they also engage with a law firm on behalf of the Client to liaise with authorities, Courts, or the perpetrators themselves to allow for the retrieval and recovery of their stolen defrauded funds.

Peter Thompson
FTCyber.com
+1 917-463-3216
email us here
