How to Avoid and Recover from Remote Access Scams

Normally, most people would never let a stranger use their computer, as it would be easy for that stranger to steal your private files, your money or your identity. However, remote access scams prey on peoples' fear, greed or lack of technological understanding to impair their judgement, making them more likely to commit the grave error of giving a scammer access to their device. Learning how to recognize these scams can help you avoid them, and if you've already fallen victim to one, there are ways to fix your computer and protect your data going forward. To find out how you can mitigate the damage of remote access scams, read on.

How remote access scams work

In a remote access scam, a scammer attempts to persuade you into giving them remote control over your personal computer, which allows the scammer to con money out of you and steal your private information. Remote access scams are often related to tech support scams, (example: Dell Computer tech support) and typically starts on the phone with either a cold call from a fake tech support specialist telling you your computer is infected with malware, or a scary-looking pop-up ad that says there's a problem with your computer and gives you a phone number to call for help. Scammers may also try to convince you to give them remote access by telling you they have money to give you that they can only deliver by connecting to your computer, as seen in the recent FTC refund scam that's been making the rounds. Another very recent refund scam includes asking you to display your online bank account, and putting a fake deposit on your account statement. The scammers then lead you to believe that they made a typo on the fake refund issued and ask for a gift card as a refund to them.

Once the scammer convinces you to give them remote access, they'll ask you to install a program such as LogMeIn, TeamViewer or GoToAssist, which allows someone from another computer to operate your computer as if they were sitting right in front of it. Normally, these programs are used for legitimate tech support and worker collaboration purposes, but they can also be used by fraudsters for criminal purposes. While the scammer is connected to your computer, they will basically try to pull a high-tech confidence trick on you. As part of this trick, the scammer will make it seem like your computer has a problem and that they're fixing it, but really they're just running harmless programs that look strange to most people. Some examples include using the Command Prompt tool to generate ominous messages, or opening Temp files in Notepad and claiming that the random characters that show up are a sign of corruption. They will then offer to fix the problem for a fee of a few hundred dollars, pretend to repair your computer and take your money, possibly using any credit card or bank details you give them to make additional fraudulent charges in the future.

While a scammer has remote access to your computer, it's highly likely that they will install malware on your device, as well. This can be even worse than just conning you out of money, as undetected malware can allow hackers to steal your identity, including your passwords and financial information, over and over again, even if you get new passwords and account numbers.

How to avoid remote access scams

Steering clear of remote access scams becomes pretty simple once you realize a few key facts. First, tech support specialists from companies and government departments never cold call people, so if you receive a call purporting to be from some kind of computer tech support, it is almost definitely a scam. Even if your caller ID says the call is coming from a source you recognize, it's easy for scammers to spoof their calls to falsify their location. Second, legitimate computer companies don't put their phone numbers on security warnings and advise people to call them, preferring instead to use diagnostic and repair programs as a first line of defense. If you see a pop-up or virus warning on your computer advising you to call a number, it's a scam. Some of these pop-ups have code that make them hard to close, so if a pop-up is staying stubbornly open, you can force your Internet browser to close by hitting Ctrl + Alt + Delete and opening the Task Manager if you're using Windows, or Command + Option + Escape if you're on a Mac. Finally, and most importantly, never give remote access to anyone you don't know, as doing so lets them bypass a great deal of your cybersecurity.

What to do if you've been scammed

If you've already been victimized by a remote access scam, there are still ways you can recover from it. Contact the financial institution associated with any payment method you gave the scammer, such as your credit card issuer or bank, and tell them about the scam. While it may be difficult to recover funds taken directly from your bank account, it's often quite easy to dispute credit card charges related to fraud, and credit cards generally have better security features for customers. You should also file a complaint with the FTC, as your report will help them track down and build a case against the scammers.

Fixing any damage done to your computer can be more difficult, as digital threats are constantly evolving to escape detection. The safest approach is to wipe your hard drive and do a clean install of your operating system, but this is a drastic and time-consuming measure. If you have a Windows computer, an easier but still effective option is to use the System Restore feature to roll back your computer to a point before the scam, which can undo malware that the scammer installed. If that isn’t an option for you, at the very least you can install and run a legitimate malware cleaning program on your computer, such as Malwarebytes, and hope it can get rid of the malware. While whichever solution you chose is working, you may also want to disconnect your computer from the Internet in case the scammer left a remote access trojan to let them reconnect to your system. After your computer is clean, you should reset all of your passwords, and possibly install some kind of ad blocking software to keep from getting any more scam pop-ups.

Remote access scams can seem devastating, but if you know what to do and act fast, they aren’t so difficult to manage. To learn more about the latest scams and how to protect yourself from them, follow our scams blog.