

What are Remote Access Scams?

Remote access scams involve fraudsters gaining control of a victim's computer through remote desktop software. These scams typically start with a call, email, or pop-up message claiming to be from a trusted organization, such as a tech support company, bank, or government agency. The scammer convinces the victim that their computer is infected, their bank account is compromised, or that they need urgent help with a technical issue.

Once the victim is persuaded, the scammer instructs them to download and install a legitimate remote desktop access tool like TeamViewer, AnyDesk, or UltraViewer. These applications are designed for secure remote access and are widely used for legitimate purposes. However, in the hands of scammers, they can be misused to control the victim's computer, giving them access to sensitive information, financial accounts, and personal files.



Tactics Used by Scammers

- **Social Engineering:** Scammers often use fear tactics or a sense of urgency to convince victims that immediate action is necessary. They may claim that the victim's data or finances are at immediate risk.
- **Spoofing Trusted Entities:** Scammers frequently impersonate well-known companies, banks, or even government agencies to appear legitimate.
- **Technical Jargon:** To confuse and intimidate victims, scammers often use technical terms or claim that they are fixing complex issues, making the victim more likely to comply without questioning.
- **Request for Payment:** Once the scammer has control, they might demand payment for their "services" or attempt to transfer funds from the victim's bank account, sometimes even instructing the victim to log in to their online banking while the scammer is still in control.

Security Risks

- **Unauthorized Access:** Once scammers gain remote access, they can steal personal information, install malware, and even lock users out of their own devices.
- **Data Theft:** Scammers can view, copy, or delete files on the victim's computer, including sensitive documents, passwords, and financial information.
- **Financial Loss:** With access to online banking, scammers can transfer funds, make purchases, or manipulate financial accounts to steal money.
- **Compromised Security:** Scammers might disable security software, install backdoors, or leave remote access tools active for future exploitation.

How To Avoid Remote Access Scams

- **Ask Scamio Pro:** Use [Bitdefender Scamio Pro](#) to check if a message is genuine. Our AI-powered scam detector analyzes potential frauds and lets you know if someone tries to scam you. Simply describe the situation or upload any images/links/text received, and Bitdefender will guide you further.
- **Be Skeptical of Unsolicited Contact:** If you receive an unexpected call, email, or pop-up message claiming your computer has issues, don't engage. Legitimate companies will not contact you out of the blue to offer help.
- **Don't Grant Remote Access:** Only allow remote access to your computer when you're certain you're dealing with a legitimate support service that you have contacted directly.
- **Verify the Source:** Before taking any action, verify the identity of the person or organization contacting you. Use official websites or trusted contact methods to confirm legitimacy.
- **Hang Up on High-Pressure Tactics:** Scammers often use urgency or scare tactics to pressure you. If you feel rushed or threatened, hang up or close the communication immediately.

What To Do If You've Been Scammed

If you think you have provided your account details to a scammer or if you have already paid for fake services, contact your bank immediately and open a chargeback.

You may wish to file a complaint with the appropriate authorities or your regional fraud reporting center:

- in the **US**: file a report with the [FBI](#) | [FTC](#)
- in **Canada**: contact [Canadian Anti-Fraud Centre](#)
- in the **UK**: file a report with the [National Fraud & Cyber Crime Reporting Centre](#) | [Report a cold call](#)
- in **Australia**: contact the [ACCC](#)
- **other countries**: report international scams at [ECONSUMER.GOV](#)