State Privacy Office
October Privacy Tip

How To Spot, Avoid, and Report Tech Support Scams

Tech support scammers want you to believe you have a serious problem with your computer, like a virus. They want you to pay for tech support services you don't need, to fix a problem that doesn't exist. They often ask you to pay by wiring money, putting money on a gift card, prepaid card, or cash reload card, or using cryptocurrency or a money transfer app because they know those types of payments can be hard to reverse.

The FTC will never threaten you, say you must transfer your money to "protect it," or tell you to withdraw cash or buy gold and give it to someone. That's a scam. ***Report it at ReportFraud.ftc.gov.***

Spotting and Avoiding Tech Support Scams

Tech support scammers use many different tactics to trick people. Spotting these tactics will help you avoid falling for the scam.

Phone calls

Tech support scammers often call and pretend to be a computer technician from a well-known company. They say they've found a problem with your computer. They typically ask you to give them remote access to your computer and then pretend to run a diagnostic test. Then they try to make you pay to fix a problem that doesn't exist. Listen to an FTC undercover call with a tech support scammer. If you get a phone call you didn't expect from someone who says there's a problem with your computer, hang up.

Pop-up warnings

Tech support scammers may try to trick you with a pop-up window that appears on your computer screen. It might look like an error message from your operating system or antivirus software, and it might use logos from trusted companies or websites. The message in the window warns you about a security issue on your computer and tells you to call a phone number to get help. If you get this kind of pop-up window on your computer, don't call the number. Real security warnings and messages will never ask you to call a phone number.

Online ads and listings in search results pages

Tech support scammers try to get their websites to show up in online search results for tech support. Or they might run their own ads online. The scammers are hoping you'll call the phone number to get help. If you're looking for tech support, go to a company you know and trust.

Two Things To Know To Avoid a Tech Support Scam
1. Legitimate tech companies won't contact you by phone, email, or text message to tell you there's a problem with your computer.

2. Security pop-up warnings from real tech companies will never ask you to call a phone number or click on a link.

What To Do if You Think There's a Problem With Your Computer

If you think there may be a problem with your computer, update your computer's security software and run a scan. If you need help fixing a problem, go to someone you know and trust. Many software companies offer support online or by phone. Stores that sell computer equipment also offer technical support in person.

What To Do if You Were Scammed

If you paid a tech support scammer with a credit or debit card, you may be able to stop the transaction. Contact your credit card company or bank right away. Tell them what happened and ask if they can reverse the charges. If you paid a tech support scammer with a gift card, contact the company that issued the card right away. Tell them you paid a scammer with the gift card and ask if they can refund your money.

If you gave a scammer remote access to your computer, update your computer's security software. Then run a scan and delete anything it identifies as a problem. If you gave your username and password to a tech support scammer, change your password right away. If you use the same password for other accounts or sites, change it there, too. Create a new password that is strong.

Avoid Tech Support Refund Scams

If someone calls to offer you a refund for tech support services you paid for, it's likely a fake refund scam. How does the scam work? The caller will ask if you were happy with the services you got. If you say, "No," they'll offer you a refund. In another variation, the caller says the company is giving out refunds because it's going out of business. No matter their story, they're not giving refunds. They're trying to steal more of your money. Don't give them your bank account, credit card, or other payment information.

Reporting Tech Support Scams

If a tech support scammer contacts you, report it to the FTC at ReportFraud.ftc.gov.

When you report a scam, the FTC uses the information to build cases against scammers.

Note: *Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.*