

Tech support scams hitting more computer users online

December 15 2017, by Robert Channick, Chicago Tribune

For consumers who turn over control of their computers to remote technicians online, the fix may already be in.

A growing number of remote [tech support](#) scams are popping up, in which users facing "crashed" computers give online access for repairs that do nothing more than drain their wallets, according to a study released Monday by the Better Business Bureau.

"We're getting a lot more calls on these types of scams," said Steve Bernas, president and CEO of the Better Business Bureau of Chicago and Northern Illinois. "But what's really alarming is most consumers don't realize they've been scammed."

For many users, the scams begin with pop-up warnings saying their computers have been infected by viruses or malware. The computers may lock up, issue piercing alarms or even mimic the dreaded "blue screen of death" that appears when a [computer](#) has crashed completely.

Lazarus: Whatever you do, don't say yes when this chatbot asks, 'Can you hear me?' "

The pop-up messages, which often appear to come from reputable tech companies such as Microsoft, HP, Apple or Dell, offer help fixing the problem with a toll-free tech support number. In actuality, that's when the problem begins.

Consumers who call the number will be hooked up with technicians who offer to take remote control of the computers, scan for issues and repair them. The fee is generally around \$500.

In most cases, the technician will repair nothing but may spend as much as an hour nosing around the computer, looking for sensitive information and inserting malware to continue to monitor the user's activity.

"If you did pay somebody recently \$500 or so to dial in and fix your computer, it may have malware in it, so be very careful," Bernas said.

Illinois Attorney General Lisa Madigan also warned computer users to be wary.

"Do not respond to any communications claiming your computer has a problem—do not click on pop-up ads or email attachments and hang up immediately on calls; these are scams," Madigan said in a news release. "Please contact my office if you want to determine whether a call or message is a scam."

The Federal Trade Commission and the FBI received more than 41,000 remote tech scam complaints through the first nine months of 2017, resulting in more than \$21 million in losses, according to the Better Business Bureau report.

That may represent just a fraction of the actual scams taking place, with less than 10 percent of victims reporting it, according to the FTC.

Victims run the demographic gamut, with millennials more likely to continue with a fraudulent tech scam offer than any other age group.

In addition to online recruitment, victims are lured into the scams through cold calls from technicians claiming to be from Comcast,

Norton, Dell and other major companies. Scammers have also begun to use robocalls with fake caller IDs to sell the fraudulent remote computer repairs.

Beyond the initial fee, the tech support scammers may take advantage of remote computer access to view online bank accounts and other sensitive financial information to directly take money from the victims.

Inside the Indian IRS [scam](#) that cheated U.S. taxpayers out of millions "

The tech scams are becoming more common, with two out of three internet users affected in the previous 12 months, according to a 2016 Microsoft survey.

A report by Stony Brook University found that more than 85 percent of the tech scammers were based in India, where many U.S. companies outsource for legitimate information technology support. Less than 10 percent of the scammers are based in the U.S.

Consumers who believe they have been scammed should report the incident to the Better Business Bureau and the FTC, change their passwords, and take their computers to legitimate bricks-and-mortar repair shops, if necessary, the report advises.

The report recommends keeping anti-virus software up to date and thoroughly researching [tech](#) support companies before giving them online access. And for those suddenly confronted with blaring and potentially fraudulent pop-up messages warning of a computer virus, there may be a very simple fix.

In most cases, the Better Business Bureau advises, the best way to clear the warnings is simply to close the browser or reboot the computer.

©2017 Chicago Tribune

Distributed by Tribune Content Agency, LLC.

Citation: Tech support scams hitting more computer users online (2017, December 15) retrieved 24 April 2024 from <https://phys.org/news/2017-12-tech-scams-users-online.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.