About Microsoft and the AARP Fraud Watch Network

Microsoft is proactively investigating online fraudsters who prey on consumers with new and evolving scams. To help protect seniors from tech support scams and other fraud, Microsoft partners with law enforcement, the Federal Trade Commission and advocacy groups, such as AARP, to take legal action against known scammers and to educate consumers on how best to help protect themselves against fraudsters.

The AARP Fraud Watch Network gives you access to information about how to protect yourself and your family. Non-members and members alike can get Watchdog Alerts, stay up on con artists' latest tricks, and find out what to do if you've been victimized. It's free for everyone because AARP is committed to safeguarding Americans' financial futures.

Contact Us

Microsoft Answer Desk:
www.support.microsoft.com/en-us/answerdesk

Microsoft Customer Service:
1-800-642-7676

AARP Fraud Watch Network:
www.aarp.org/fraudwatchnetwork
AARP Fraud Watch Helpline:
1-877-908-3360

Microsoft | FRAUD WATCH NETWORK AARP Real Possibilities

Avoiding Tech Support Scams

From Microsoft and the AARP Fraud Watch Network

Microsoft | FRAUD WATCH NETWORK AARP Real Possibilities

What is a Tech Support Scam?

Tech support scams are not a new phenomenon.

Scammers have been peddling useless security software and services for years, tricking people into spending millions of dollars on non-existent computer problems via phone calls, unsolicited emails, or bogus websites, ads or pop-up windows. In fact, this year alone, an estimated 3.3 million people in the United States will be affected, suffering losses of more than $1.5 billion. Today's scam artists have added a new twist — using a so-called "technician" to help gain access to a person's computer.

Cybercriminals often pose as Microsoft tech support employees or Microsoft Certified Partners. They may claim your PC is infected with a virus or malware, your software isn't working properly, or that you've made some changes to your Microsoft account and need to confirm your identity. These cybercriminals also try to gain remote access to your PC in order to:

- Force you to pay for phony tech support
- Install malicious software that captures sensitive information and often times charge you to remove this software
- Adjust settings which leave your computer vulnerable
- Access your personal, financial, or credit card information

Lowell's Story:
How It Happened To Me

I was at home watching television when the phone rang.

The woman on the other end introduced herself as a Microsoft technician and said my computer was at risk. She claimed to be from Redmond, though the area code was not even a Washington State number.

To investigate the problem, she transferred the call to a colleague, who asked for remote control access of my computer to show me what needed to be fixed. The mouse flitted across my screen, pointing to "corrupt files" he said needed repairing or I would soon lose access to my machine.

He then passed me to a third person who claimed to have a Microsoft ID. She was polite, yet at the same time, pushy. Showing me several news articles, she explained the dangers of this issue and said I needed to purchase a service to clean my computer immediately.

The situation was very suspicious and my wife and I decided to investigate further before buying anything. I later learned from my daughter this was a tech support scam.

- Lowell, Washington State

Reminder:

If you receive an unsolicited email or phone call from someone claiming to be from Microsoft, take down their information, and report your experience to authorities. Scammers may also try to contact you through pop-up windows claiming your computer is infected or via bogus websites or online advertisings. You will never receive an unsolicited call or email from Microsoft asking for your personal or financial information to fix your computer.

Protect Yourself – Dos

- Collect as much information as possible without putting yourself or your PC at risk.
- Ask if there is a fee or subscription associated with the "service." If there is, hang up.
- Report the caller's information to local authorities or Microsoft.
- At least once a week, check for updates in your security software and run scans several times a week.
- Let the Microsoft Answer Desk help: If you get a phone call, email or pop-up window on your PC and you're not sure it's from Microsoft, contact a tech support expert at the Microsoft Answer Desk to confirm. If you think your PC may be infected with a virus or malware, let one of our Answer Desk Technicians check it to be sure: www.support.microsoft.com/en-un/answerdeskcom/en-us/answerdesk

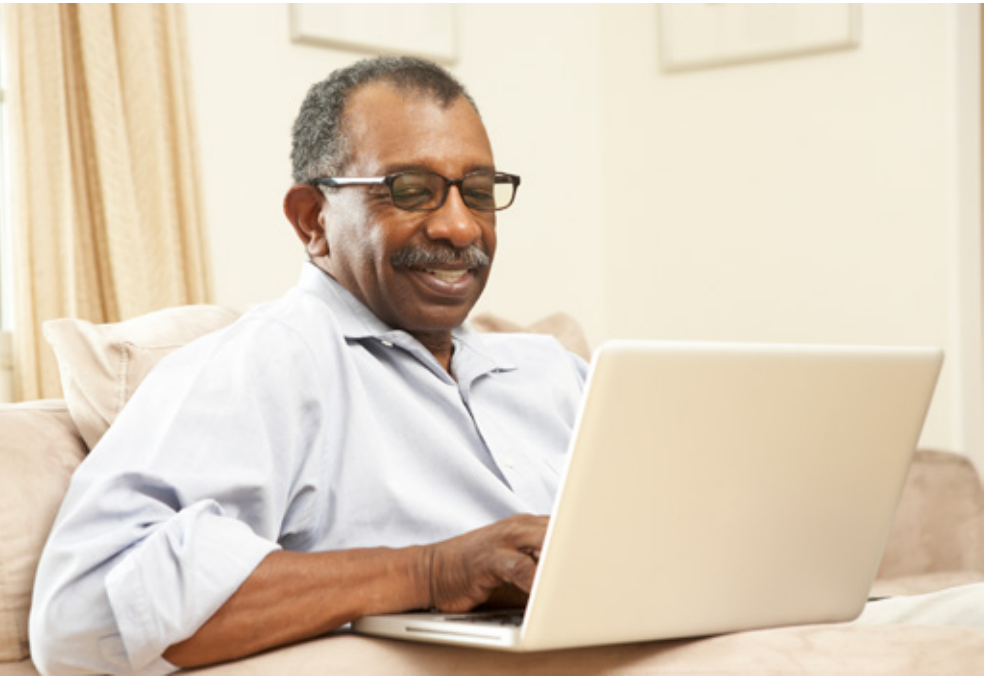
Protect Yourself – Don'ts

- Do not purchase any software or services from an unsolicited call or email or from a bogus website or online advertisement.
- Do not give control of your computer to a third party unless you can confirm that it is a legitimate representative of a computer support team with whom you are already a customer.
- Do not provide your credit card or financial information to someone claiming to be from Microsoft tech support.
- Do not be fooled if a phony tech support scammer knows your name, address or even the operating system you're using. Cybercriminals glean their targets through public phone directories and often "guess" your operating system by citing more popular ones.
- Do not rely solely on monthly statements from your bank or credit card companies; check account activity online or by phone at least weekly for quick indicators of fraud.

Think You've Been a Tech Scam Target?

If you think you downloaded malware or allowed a cybercriminal to access your PC, take these steps:

- Provide a report of your interaction at: www.support.microsoft.com/reportascam
- Change the password on your computer, email accounts, and financial accounts. Make your passwords complicated, update them often, and do not share them with anyone.
- Scan your computer with Microsoft Safety Scanner to determine if there's any malware installed. Download this free program at www.microsoft.com/security/scanner.
- Install Microsoft Security Essentials (it's free!) if you're running Windows 7 or Vista. Windows Defender replaces Microsoft Security Essentials in Windows 8 and Windows 10 and is already built-in.
- Keep your PC up-to-date by allowing automatic updates.



Resources

Report a Microsoft Tech Support Scam
www.support.microsoft.com/reportascam

Microsoft Safety & Security
www.microsoft.com/security
or
www.microsoft.com/security/online-privacy/avoid-phone-scams.aspx

AARP Fraud Watch Network
www.aarp.org/fraudwatchnetwork

Federal Trade Commission
www.ftccomplaintassistant.gov

State's Attorneys General
www.naag.org/current-attorneys-general

Better Business Bureau
www.bbb.org

Canada, the Royal Canadian Mounted Police
www.rcmp-grc.gc.ca/scams-fraudes

United Kingdom
www.actionfraud.police.uk