Avoiding Tech Support Scams
From Microsoft Digital Crimes Unit and AARP Fraud Watch Network

What Is a Tech Support Scam and Who Is Targeted?
If you haven't experienced a tech support scam yet, chances are you know someone who has. According to Microsoft's 2016 global survey, two out of three people have experienced a tech support scam in the previous 12 months. The "old school" method of tech support scams follows an all-too-common pattern: fraudster calls a senior citizen claiming to have a relationship with a reputable company; misrepresents the existence of computer viruses or other technical problems on a computer; and proceeds to sell the senior citizen unnecessary tech support for a fee.

While the above method still occurs today, research indicates a startling number of millennials are falling victim to tech support fraud. Fifty percent of all respondents who continued with a fraudulent interaction fell between the ages of 18 and 34. These results may, at first glance, appear surprising, challenging our preconceived notions that fraudsters target senior citizens. The research also reveals that fraudsters' tactics are evolving. By leveraging pop-up windows, unsolicited email, and scam websites as additional entry points for scams, fraudsters are reaching a broader number of people, including younger victims. The data indicates that victims older than 65 are more likely to be reached by telephone (44% were conned by an unsolicited call, 38% a popup or online ad, 33% an unsolicited email, and 26% redirected to a website). In contrast, millennials ages 18 to 34 are more likely to have been redirected to a fraudulent website (50%) or duped by a pop-up advertisement (59%) as compared to receiving an unsolicited call (26%).

Regardless of the audience or the entry method, the goal of the fraudster remains the same: use fear and deception to persuade a customer to call for support, then seek remote access to the customer's device and provide a fraudulent sales pitch. Every consumer needs to be vigilant and skeptical of any person who seeks remote access to their device. During a remote access session, fraudsters may:
• Force you to pay for phony tech support.
• Access your personal and financial information.
• Alter device settings, such as turning off your anti-virus software or regaining access to the computer long after the "support session" has ended.
• Download unwanted and potentially malicious software.

1 Source: Ipsos, Global Market Research, commissioned by Microsoft, July 2016.
2 Survey respondents could indicate if they had multiple modes of experience with scams.

Protect Yourself – Dos
If you receive a notification or call from someone offering tech support or protection from computer viruses, here are a few key tips to keep in mind:
Think. Did I seek out tech support or was this phone call, pop-up or email unsolicited? If unsolicited, disconnect. If you received a pop-up, do not call the number listed. Microsoft error and warning messages do not include a phone number.
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 and Microsoft at www.microsoft.com/reportascam
At least once a week, check for updates in your security software and run scans several times a week.

Let Microsoft Support Help You:
If you think your computer may be infected with a virus or malware, contact Microsoft Support at support.microsoft.com/contactus

Protect Yourself – Dont's
Do not purchase any software or services from an unsolicited call, email, bogus website, or online ad.
Never 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 be fooled if a phony tech support scammer knows your name, address or even some facts about how your computer operates. Cybercriminals trade information about customers and often claim to have specific information about your computer that is very generic.

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. If you have been defrauded, contact your bank or credit card company. Do NOT contact the fraudulent company or respond to a fraudster claiming to need your financial information to address overpayment or provide a refund.

Think You've Been a Tech Scam Target?
If you think you downloaded malware or allowed a cybercriminal to access your computer, take the following steps:
• Provide a report of your interaction at: www.microsoft.com/reportascam.
• Change the password on your computer, email accounts, and financial accounts. Make your passwords complicated, update them often, and don't 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.

How Is Microsoft Fighting Back
Microsoft encourages all customers to report their fraud experiences to law enforcement, and through Microsoft's "report a scam" online complaint form (www.microsoft.com/reportascam). Microsoft's Digital Crimes Unit leverages the customer reports to investigate and take action against criminals, and makes referrals to law enforcement when appropriate.

Since 2014, the Digital Crimes Unit has supported global law enforcement action against over a dozen tech support fraud enterprises and many more investigations are underway.

Microsoft continues to innovate and better protect customers from online threats. Microsoft has built-in protection in Windows 10 which includes more security features, safer authentication and ongoing updates delivered for the supported lifetime of a device. Windows Defender delivers comprehensive, real-time protection against software threats across email, cloud and web. And the SmartScreen filter, built into Windows, Microsoft Edge and Internet Explorer, helps protect against malicious websites and downloads. Windows PCs, phones and Xbox use this always up-to-date feature to protect against phishing and malware threats

Microsoft store employees are helping educate customers about how to stay safe online and avoid common scams. For more information on Microsoft store events, visit www.microsoftstore.com/workshops.

Resources:
1. Report a Microsoft Technical Support Scam: microsoft.com/reportascam
2. AARP Fraud Watch: aarp.org/money/scams-fraud/fraud-watch-network/
3. Federal Trade Commission: ftccomplaintassistant.gov
4. State Attorneys General: naag.org/current-attorneys-general
5. Better Business Bureau: bbb.org
6. Microsoft Safety & Security: microsoft.com/security

About Microsoft and AARP
Microsoft's Digital Crimes Unit investigates tech support scams and partners with law enforcement as well as the Federal Trade Commission to take legal action against known scammers. Microsoft also partners with advocacy groups such as AARP to help educate consumers on how best to protect themselves from 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: support.microsoft.com/contactus
AARP: www.aarp.org   AARP Fraud Watch Helpline: 1-877-908-3360