Avoiding Technical Support Scams

Cybercriminals don't just send fraudulent email messages. They might call you on the telephone and claim to be from Microsoft. They might also setup websites with persistent pop-ups displaying fake warning messages and a phone number to call and get the “issue” fixed. They might offer to help solve your computer problems or sell you a software license. Once they have access to your computer, they can do the following:

- Trick you into installing malicious software that could capture sensitive data, such as online banking user names and passwords. They might also then charge you to remove this software.
- Convince you to visit legitimate websites (like www.ammyy.com) to download software that will allow them to take control of your computer remotely and adjust settings to leave your computer vulnerable.
- Request credit card information so they can bill you for phony services.
- Direct you to fraudulent websites and ask you to enter credit card and other personal or financial information there.

“Remember, Microsoft will never proactively reach out to you to provide unsolicited PC or technical support. Any communication Microsoft will have with you must be initiated by you.”

Telephone Tech Support Scams: What you need to know

Cybercriminals often use publicly available phone directories, so they might know your name and other personal information when they call you. They might even guess what operating system you're using.

Once they've gained your trust, they might ask for your user name and password or ask you to go to a legitimate website (such as www.ammyy.com) to install software that will let them access your computer to fix it. Once you do this, your computer and your personal information are vulnerable.

Do not trust unsolicited calls. Do not provide any personal information.

Scam Pop-Ups: What You Need to Know

Another well-known trick is the website pop-up, that little browser window that sometimes appears while you’re searching the Web. Cybercriminals set up websites with scam pop-ups with messages and phone numbers. These pop-ups usually are not easy to close.

While some pop-ups are useful and important, others are traps that attempt to mislead you into revealing sensitive personal or financial information, paying for fake anti-virus software, or even installing malware and viruses onto your device.

Do not call the number in the pop-up. Microsoft’s error and warning messages never include a phone number.

Here are some of the organizations that cybercriminals claim to be from:

- Windows Helpdesk
- Windows Service Center
- Microsoft Tech Support
- Microsoft Support
- Windows Technical Department Support Group
- Microsoft Research and Development Team (Microsoft R & D Team)

Whenever you receive a phone call or see a pop-up window on your PC and feel uncertain whether it is from someone at Microsoft, don’t take the risk. Reach out to Tech Plus and we will assist you in this endevour.

How to protect yourself from tech support scams

If someone claiming to be from Microsoft tech support contacts you:

- Do not purchase any software or services.
- Ask if there is a fee or subscription associated with the "service." If there is, hang up.
- 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.
- Take the person's information down and immediately report it to your local authorities.
- Never provide your credit card or financial information to someone claiming to be from Microsoft tech support.

What to do if you already gave information to a tech support person

If you think that you might have downloaded malware from a tech support scam website or allowed a cybercriminal to access your computer, take these steps:

- Change your computer's password, change the password on your main email account, and change the password for any financial accounts, especially your bank and credit card.
- Scan your computer with Anti-Malware program (Malwarebytes is recommended) to find out if you have malware installed on your computer.

Microsoft does not make unsolicited phone calls to help you fix your computer.

In this scam cybercriminals call you and claim to be from Microsoft Tech Support. They offer to help solve your computer problems. Once the crooks have gained your trust, they attempt to steal from you and damage your computer with malicious software including viruses and spyware.

Although law enforcement can trace phone numbers, perpetrators often use pay phones, disposable cellular phones, or stolen cellular phone numbers. It's better to avoid being conned rather than try to repair the damage afterwards.

Treat all unsolicited phone calls with skepticism. Do not provide any personal information.

If you receive an unsolicited call from someone claiming to be from Microsoft Tech Support, hang up. Microsoft does not make these kinds of calls.