By curtesy of Microsoft

Avoid technical support phone scams

Cybercriminals don't just send fraudulent email messages and set up fake websites. They might also call you on the telephone and claim to be from Microsoft. 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.
- 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.

Neither Microsoft nor our partners make unsolicited phone calls (also known as cold calls) to charge you for computer security or software fixes.

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 website to install software that will let them access your computer to fix it. Once you do this, your computer and your personal information is vulnerable.

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

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)

How to protect yourself from telephone tech support scams

If someone claiming to be from Microsoft tech support calls 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 caller'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 phone 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 the Microsoft Safety Scanner to find out if you have malware installed on your computer.
- Install Microsoft Security Essentials. (Microsoft Security Essentials is a free program. If someone calls you to install this product and then charge you for it, this is also a scam.)

Will Microsoft ever call me?

There are some cases where Microsoft will work with your Internet service provider and call you to fix a malware-infected computer—such as during the recent cleanup effort begun in our botnet takedown actions. These calls will be made by someone with whom you can verify you already are a customer. You will never receive a legitimate call from Microsoft or our partners to charge you for computer fixes.

More information

For more information about how to recognize a phishing scam, see Avoid scams that use the Microsoft name fraudulently.

If you need help with a virus or other security problem, visit the Microsoft Virus and Security Solution Center.

To help protect against viruses and other malicious software, download Microsoft Security Essentials.

Posted 26th September 2014