BEWARE OF TECH SUPPORT PHONE SCAMS

Cybercriminals don't just send fraudulent email messages and set up fake websites, they will also call you on the telephone and claim to be from Microsoft. They might offer to help solve your computer problems or claim that malware has been detected on your PC. Once they have access to your computer, they can trick you into installing malicious software or visiting fraudulent websites that could capture sensitive data, such as online banking user names and passwords. They might also then charge you to remove this software and request credit card information so they can bill you for phony services. If you allow them to take control of your computer remotely they can adjust settings to leave your computer vulnerable.

If you think that you might have downloaded malware from a phone tech support scam website or allowed a cybercriminal to access your computer, 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. Then scan your computer for malware.

The bottom line is that Microsoft will never cold call you. Do not trust unsolicited calls and do not provide any personal information. If someone claiming to be from Microsoft tech support calls you, take the caller's information down and immediately report it to your local authorities.