(https://fightcybercrime.org/)

Tech Support Scams

Someone contacts you claiming there is an issue with your device and they can help fix it. Find out how to spot and recover from these types of scams.

GET STARTED

REPORT CYBERCRIME *(/REPORT)*

The Basics of Tech Support Scams

Tech support scams typically involve a scammer who tries to trick you into giving them remote access to your computer or to pay them for unnecessary services. Once you give them access, they may install malware (https://fightcybercrime.org/scams/hacked-devices-accounts/malware/) on your device in order to steal your personal information. Tech support scams are becoming increasingly common, and they can be very convincing. The scammers often use high-pressure tactics to get you to act quickly and may even threaten to delete your files or disable your computer if you don't comply.

▶ **Common Tactics Used by a Tech Support Scammer**

STEP 1:

Recognize

Red Flags of a Tech Support Scam

It's important to be aware of these scams and know how to protect yourself. Here are some common warning signs that you're communicating with a tech support scammer:

- They will contact you out of the blue, often through a pop-up message on your computer or a phone call.
- They will claim to be from a well-known tech company or support department, such as Microsoft or Apple.
- They will tell you that there is something wrong with your computer, often claiming that it has a virus or is not up to date.
- They will try to get you to give them remote access to your computer so they can "fix" the problem.
- They will then ask you for money, often demanding payment through a prepaid card or wire transfer.

STEP 2:

Immediate Actions

If you think you are the victim of a tech support scam, it is important to take action right away to protect yourself and your finances. Here are some steps to take if you think you have been scammed:

- Stop all contact with the individual(s) who contacted you.
- If you provided financial information, like your credit card number or bank account information, contact your bank or credit card company right away. They may be able to help you cancel the transaction or get your money back.
- If you sent funds via gift card or money transfer, report the scam to the issuer. They might be able to help you stop the transaction. Find their contact information by visiting their legitimate website.
- If you provided personal information, like your Social Security number, you may be at risk for identity theft (https://fightcybercrime.org/scams/identity-theft/). Keep an eye on your credit report and financial accounts for any unusual activity, and consider placing a freeze on your credit.
- If you provided any login credentials, change all passwords immediately to protect your accounts and personal information.
- If you believe they installed malware on your device, visit our malware page (https://fightcybercrime.org/scams/hacked-devices-accounts/malware/).
- Save all information and messages provided to you by the scammer. You may need to provide this information to law enforcement if you file a report.

STEP 3:

Report

Reporting any type of cybercrime, including a tech support scam, is imperative to help others avoid being scammed. As a society, the more people that report online scams and fraud, the more national reporting data that is collected, and the better chance law enforcement has to catch the criminals and decrease cybercrime.

REPORT TO FBI *(HTTPS://WWW.IC3.GOV/DEFAULT.ASPX)*

STEP 4:

Recover

Learn the Three Golden Rules to Spot a Scam

Scammers often utilize tactics to encourage you to act quickly and will use false information to persuade you to send money or personally identifiable information (PII). When faced with a questionable situation online, always follow the three golden rules to spot a scam:

Slow it down — Scammers often create a sense of urgency, hoping you'll act quickly by claiming your computer is at risk. They may be pushy or aggressive. Take your time and ask questions to avoid being rushed into a bad situation.

Spot check — Do your research to double check that the person is who they say they are. Contact the organization directly that they claim to be from. Look up the company online and call the phone number listed on their official website. Do not call the phone number or go to the website the caller directs you to, as this may not be legitimate.

Stop! Don't send — Scammers will try to steal your money by rushing you into paying with unconventional payment methods like gift cards or wire transfer. If they insist you send the money in the form of gift cards or by wire transfer, it's a scam. Additionally, never provide login credentials to any of your accounts over the phone. A reputable organization would not request this information. If they do, it's a scam.

Take 5 Steps for Better Online Security

Along with making sure you follow the three golden rules to spot a scam, it's important to strengthen your online security to help avoid all types of online scams. Take action to improve your digital posture by following these steps:

1. **Implement Multi Factor Authentication (MFA):** Passwords are generally easy for scammers to crack, and even if you use strong passphrases, there's still the possibility that a cybercriminal can obtain your passphrase in a data breach. Implementing MFA (https://fightcybercrime.org/blog/multi-factor-authentication-explained/) is a great way to maximize your security and ensure that you are the only one who can gain access to your accounts. MFA should be implemented on all accounts where it is available. Check your account's security settings to see if it is something you can set up.
2. **Update Your Privacy Settings:** Privacy settings allow you to control your personal information (name, address, phone number, date of birth, financial details, photos or videos, etc) and how that information is used. Review your privacy settings on all of your accounts including your social media accounts. Consider restricting who can see your friends list, contacts, photos and posts.
3. **Activate Automatic Updates:** Automatic updates are a set of changes to an app, software or operating system that are automatically pushed by the developer to fix or improve it.

Oftentimes, cybercriminals take advantage of security flaws to plant malicious software on your devices. By activating automatic updates, you will automatically patch security vulnerabilities to protect your data.

4. **Create Strong Passphrases:** A strong passphrase (https://fightcybercrime.org/blog/the-411-on-strong-passphrases/) is a string of unrelated words separated by hyphen, space, period, capitalized first letter or number. Use passphrases that are longer than 15 characters and include multiple words that do not have any obvious connection between them. The key to passphrases is randomness. Don't repeat your passphrases between accounts and consider using a password manager to help you remember.
5. **Learn the Elements of a Phishing Attempt:** Familiarize yourself with the elements of a phishing email (https://fightcybercrime.org/blog/dont-be-fooled-by-a-phish/). Phishing emails tend to include a sense of urgency and multiple grammar and spelling errors. If they are asking you to reveal personal information, be suspicious. If you get a strange email, try contacting the company another way to confirm they sent that email. If the email is suspicious, mark it as spam.

TESTIMONIAL

Hear from Other Victims

Without Fightcybercrime.org, I don't know if I would have been able to react as quickly to protect my personal information.

Mary - Indianapolis, IN

Latest News

The latest and greatest from our blog (/blog/).

(https://fightcybercrime.org/blog/how-microsoft-tech-support-scams-work/)

How Microsoft Tech Support Scams Work (https://fightcybercrime.org/blog/how-microsoft-tech-support-scams-work/)

Did you receive a call from someone claiming to be from Microsoft Tech Support? Learn how to recognize, report and recover from tech support scams.

READ FULL ARTICLE *(HTTPS://FIGHTCYBERCRIME.ORG/BLOG/HOW-MICROSOFT-TECH-SUPPORT-SCAMS-WORK/)*

(https://www.instagram.com/fightcybercrimecsn/)

(https://www.facebook.com/cybersupportnet/)

(https://www.linkedin.com/company/cybercrime-support-network)

(https://www.youtube.com/channel/UCe8x2nFKpdAjJ__9D2uADWg)

Scams

Financial Purchase Scams (https://fightcybercrime.org/scams/financial/)

Hacked Devices & Accounts (https://fightcybercrime.org/scams/hacked-devices-accounts/)

Imposter Scams (https://fightcybercrime.org/scams/imposter/)

Harassment (https://fightcybercrime.org/scams/harassment/)

Identity Theft (https://fightcybercrime.org/scams/identity-theft/)

Business Scams (https://fightcybercrime.org/scams/business/)

Programs

Military & Veteran Program (https://fightcybercrime.org/programs/milvet/)

Peer Support Program (https://fightcybercrime.org/programs/peer-support/)

About

About (https://fightcybercrime.org/about/)

Sponsors (https://fightcybercrime.org/about/sponsors/)

Partners (https://fightcybercrime.org/about/partners/)

Press Inquiries (https://fightcybercrime.org/about/press/)

Careers (https://fightcybercrime.org/about/careers/)

Take Action

Report a Cybercrime (https://fightcybercrime.org/report/)

Donate (https://fightcybercrime.org/about/donate/)

Feedback (https://fightcybercrime.org/about/feedback/)

ScamSpotter.org (https://scamspotter.org)

Privacy (/privacy) Terms of Use (/terms) Accessibility (/accessibility)

Gold Transparency 2022 Candid. (https://www.guidestar.org/profile/82-1013947)