Connecting Generations
Cyber-Seniors™

How to Spot Tech Support Scams

Tech support scams are a common form of cyber fraud where criminals pose as legitimate technical support representatives from well-known companies such as Microsoft, Apple, or Geek Squad. Their goal is to trick individuals into believing that their devices have issues that require immediate attention, leading them to pay for unnecessary services or give up personal information.

How Do Tech Support Scams Happen?

In order to stay safe from Tech Support Scams it's crucial to understand how they happen.

Step One: Initial Contact
Scammers reach out via email, text messages, phone calls, or fake websites, pretending to be from trusted companies. For example, you may receive an email that appears to be from Best Buy's Geek Squad.

Step Two: Fake Warnings
They claim your device has been compromised, that you owe money for services, or that you need to verify your identity by providing personal information such as credit card details, Social Security Number (SSN), or Social Insurance Number (SIN).

Step Three: Gaining Access
Scammers may persuade victims to download malware or grant remote access to their computers under the guise of security updates or diagnostics.

Step Four: Exploitation
Once they gain access, scammers may steal sensitive data, empty bank accounts, or demand further payments for their so-called "services."

Common Tech Support Scam Tactics

Scammers use a variety of methods to deceive victims, including:

- **Direct Contact Scams** – Scammers initiate contact through cold calls, phishing emails, pop-up messages, or fake websites, often pretending to be from reputable tech companies.
- **Malware and Remote Access** – Victims may be tricked into downloading harmful software or allowing remote access, enabling scammers to manipulate systems and steal data.
- **Fake Warnings and Error Reports** – Fraudulent security alerts or system messages claim there are issues with a device, prompting victims to seek assistance from scammers.
- **Fake Refund and Payment Scams** – Fraudsters offer fake refunds or claim victims owe money, persuading them to share banking details or make payments.
- **Impersonation and Social Engineering** – Scammers use logos, branding, and psychological manipulation to create urgency and gain trust.

Signs of Common Tech Support Scams

- **Auto-Renewal Scams** – Receiving emails about fake subscription renewals, often from companies like Geek Squad.
- **Fake Antivirus Scams** – Messages falsely claiming your device has a virus and prompting you to download software.
- **Fake Browser Pop-Ups** – Warning messages that falsely indicate a virus threat, urging you to call a number for support.
- **Bogus Protection Plans** – Fake security service offers from scammers pretending to provide digital protection.

Protecting Yourself from Tech Support Scams

- **Ignore Unsolicited Messages** – Do not respond to unexpected calls, texts, or emails claiming to be from tech support.
- **Use Legitimate Security Software** – Install reputable antivirus programs and keep them updated.
- **Avoid Clicking Suspicious Links** – Hover over links in emails to check their authenticity before clicking.
- **Never Share Personal Information** – Do not give out passwords, 2FA codes, or financial details.
- **Verify Phone Numbers** – Only contact companies using numbers found on their official websites.
- **Sign Up for Credit Monitoring** – Services can help detect fraud and unauthorized access to financial accounts.

Need More Help?

For more information, contact Cyber-Seniors at **844-217-3057** or visit **www.cyberseniors.org**.

*This lesson guide was made possible by a **CIRA Net Good Grant**. Learn more at **cira.ca**.*