Volume 25 | Issue 17 | March 5, 2026

BCSI Investigations Inc.

The Investigator Newsletter

Phone Tech Support Scams

When “Tech Support” Calls: Protecting Yourself from Phone Scams

About Us

Since 2000, BCSI Investigations Inc. has performed thousands of successful investigations. Our integrated team of investigators and support services ensure that the investigations are conducted promptly with leading-edge techniques.

Phone tech support scams continue to target individuals and businesses across North America, costing victims millions of dollars each year. Scammers pose as representatives from well-known companies such as Microsoft, Apple, or Amazon, claiming there is a virus, security breach, or urgent problem with your device or account. Their goal is simple: to gain remote access to your computer or convince you to send money.

These scams often begin with an unsolicited phone call, voicemail, pop-up alert, or email directing you to call a "support" number. The caller may use technical language to create panic and urgency, stating that your personal information has been compromised or your device will be disabled. In some cases, they instruct victims to download remote access software, allowing the scammer to control the

With over 40 years of combined experience, BCSI Investigations Inc. is the platinum standard for private investigations.

Contact us at 604-922-6572 or visit our website at www.picanada.ca to learn more.

Visit our Website

computer and potentially install malware or steal sensitive data.

One of the most effective tactics scammers use is fear. They pressure victims to act immediately and discourage them from consulting family members, IT departments, or financial institutions. Payment is typically requested through wire transfers, cryptocurrency, gift cards, or other non-traceable methods. Once payment is made, recovering funds is extremely difficult.

To protect yourself:

- Be cautious of unsolicited calls or pop-ups claiming to be tech support.
- Legitimate companies do not proactively call customers to report viruses or security issues.
- Never provide remote access to your device unless you initiated the request through an official, verified support channel.
- Do not share passwords, verification codes, or financial information over the phone.
- If in doubt, hang up and contact the company directly using the official phone number listed on its website.

If you believe you have been targeted, disconnect your device from the internet immediately and contact a trusted IT professional. Report the incident to your local authorities or national fraud reporting center.

Awareness is your strongest defense. By recognizing the warning signs and responding calmly, you can avoid becoming a victim of phone tech support scams.

Thank you for trusting **BCSI Investigations Inc.** to keep you informed and protected.

Services | Firm Profile | Contact Us | Email

STAY CONNECTED