OUCH! January 2026

OUCH!

Workforce Security and Risk Training

The Monthly Security Awareness Newsletter for You

Fake, Tech Support: The Only Thing They're Fixing Is Your Bank Account

How a "Helpful" Call Turned Costly

Aisha was working from home when a browser pop-up suddenly appeared on her laptop: ***"Your Windows operating system is no longer supported and appears to be infected! Your personal information, banking details, and other sensitive data are most likely compromised. For your security, please contact Windows Technical Support immediately. Call now: 1-8XX-XXX-XXXX"***

Worried she might lose her finances and files, Aisha called the number. After a brief hold, a professional-sounding "technician" answered and assured her they could fix the problem remotely. They guided her to download "security software" that allowed them to scan her system. She watched as dozens of fake "viruses" appeared on her screen. The technician explained that her computer was "heavily infected" but for a one-time fee of $375, they could clean and secure it. Relieved, Aisha paid with her credit card.

Later that week, her credit card company alerted her to multiple unauthorized charges. That's when Aisha realized the friendly "tech support" team were actually scammers, and now they not only had access to her credit card but also her computer!

Unfortunately, Aisha's story is all too common—and it's exactly how many **tech support scams** work.

What Are Tech Support Scams?

Tech support scams occur when criminals convince people that something is wrong with their computer, phone, or online account—and that they need immediate help from "technical support." Scammers impersonate legitimate companies such as Microsoft, Apple, or your bank. Their goal? **To trick you into giving them money, sensitive information, or remote access to your devices or accounts.**

These scams often start with fake browser or operating system update pop-up alerts, phone calls, or text messages claiming your computer is infected or your account has been compromised. No matter how they start, their goal is to create panic and make you believe you must act **immediately**.

What Are They After?

Tech support scammers are after three main things:

1. **Your Money:** They may charge to "fix" non-existent problems, often demanding payment via gift cards, wire transfers, or cryptocurrency—methods that are hard to trace.

2. **Your Information:** They request your name, address, passwords, or banking details under the pretext of verifying your identity or processing a refund.
3. **Access to Your Device or Accounts:** By convincing you to install remote access software, scammers can spy on your activity, steal files, or install real malware for future attacks.

How These Scams Work

Tech support scams rely heavily on **social engineering**—manipulating emotions to create fear and urgency. Here's a typical pattern:

1. **They Hook You Using Fear:** You see a pop-up or receive a text message or phone-call claiming your system or account is compromised. The message uses alarming language such as "Your data will be lost!" or "Your account will be suspended!"
2. **The Trust:** The scammer poses as a professional from a well-known company, even using official logos or spoofed phone numbers.
3. **The Control and Payment:** They ask you to install software or click a link, giving them access to your device. They then charge a fee for "repairs" or "protection services." Even if you realize it's a scam and disconnect, they may still have access or data from your device.

How to Protect Yourself

1. **Stay Calm and Think:** Real companies **do not** display pop-up warnings with phone numbers or call you out of the blue. If something seems urgent or frightening, pause and verify independently.
2. **Never Call Numbers from Pop-ups:** If you see a warning message in a pop-up, close your browser. Don't engage with the number or link displayed.
3. **Do Not Grant Remote Access:** Never allow anyone you don't know remote access to your devices or accounts. If they contacted you and are pressuring you to give them access, it's a scam.
4. **Monitor and Secure Your Accounts:** If you suspect you engaged with a scammer, immediately change your passwords and monitor your financial accounts for unusual activity.

Final Thoughts

Tech support scams prey on fear, urgency, and trust—And they can happen to anyone, regardless of technical experience. Remember: **legitimate companies will never call, email, or display pop-ups asking for remote access or payment to fix an issue.** Staying calm and skeptical is your best defense.

Guest Editor

Jennifer Cox is a Solutions Consulting Director at Tines, an intelligent automation company transforming cybersecurity operations. A multi-award-winning cybersecurity leader, she is passionate about mentoring future industry professionals and driving innovation, excellence, and inclusion across technical teams within the global cybersecurity and automation ecosystem. https://www.linkedin.com/in/jennifermcox/

Resources

The Power of Updating: https://www.sans.org/newsletters/ouch/power-updating/
How Cybercriminals Exploit Your Emotions: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
The Power of Passphrases: https://www.sans.org/newsletters/ouch/power-passphrase/

You can find more Ouch! On the following link: https://www.sans.org/newsletters/ouch