

Tech Support Scams

Home / Business Guidance / Protecting Small Businesses / Cybersecurity

[Veá esta página en español](#)

Cybersecurity for Small Business

- Cybersecurity Basics
- Understanding the NIST cybersecurity framework
- Physical Security
- Ransomware
- Phishing
- Business Email Imposters
- Tech Support Scams**
- Vendor Security
- Cyber Insurance
- Email Authentication
- Hiring a Web Host
- Secure Remote Access
- Cybersecurity Videos
- Cybersecurity Quizzes

TECH SUPPORT SCAMS

[Download/Print PDF](#) [Take the Quiz](#)

You Get a Phone Call, Pop-Up, or Email Telling You There's a Problem With Your Computer

Often, scammers are behind these calls, pop-up messages, and emails. They want to get your money, personal information, or access to your files. This can harm your network, put your data at risk, and damage your business.

How the Scam Works

The scammers may pretend to be from a well-known tech company, such as Microsoft. They use lots of technical terms to convince you that the problems with your computer are real. They may ask you to open some files or run a scan on your computer — and then tell you those files or the scan results show a problem...but there isn't one.

The scammers may then

- Ask you to give them remote access to your computer — which lets them access all information stored on it, and on any network connected to it
- Try to enroll you in a worthless computer maintenance or warranty program
- Install malware that gives them access to your computer and sensitive data, like user names and passwords
- Ask for credit card information so they can bill you for phony services or services available elsewhere for free
- Try to sell you software or repair services that are worthless or available elsewhere for free
- Direct you to websites and ask you to enter credit card, bank account, and other personal information

How To Protect Your Business

If a caller says your computer has a problem, hang up. A tech support call you don't expect is a scam —even if the number is local or looks legitimate. These scammers use fake caller ID information to look like local businesses or trusted companies.

If you get a pop-up message to call tech support, ignore it. Some pop-up messages about computer issues are legitimate, but do not call a number or click on a link that appears in a pop-up message warning you of a computer problem.

If you're worried about a virus or other threat, call your security software company directly, using the phone number on its website, the sales receipt, or the product packaging. Or consult a trusted security professional.

Never give someone your password, and don't give remote access to your computer to someone who contacts you unexpectedly.

What To Do If You're Scammed

If you shared your password with a scammer, change it on every account that uses this password. Remember to use unique passwords for each account and service. Consider using a password manager.

Get rid of malware. Update or download legitimate security software. Scan your computer, and delete anything the software says is a problem. If you need help, consult a trusted security professional.

If the affected computer is connected to your network, you or a security professional should check the entire network for intrusions.

If you bought bogus services, ask your credit card company to reverse the charges, and check your statement for any charges you didn't approve. Keep checking your credit card statements to make sure the scammer doesn't try to re-charge you every month.

Report the attack right away to the FTC at [FTC.gov/Complaint](#).

[Download/Print PDF](#) [Take the Quiz](#)

[cybersecurity_sb_techsupport-es.pdf](#) (349.61 KB)

Additional Resources

Check out these additional resources like downloadable guides to test your cybersecurity know-how.

[Guide for Employers](#)

[Start a Discussion](#)

[Cybersecurity Quizzes](#)

[Test Your Knowledge](#)

[Get the Materials](#)

[Download Materials](#)

[Order Free Publications](#)

[Cybersecurity Video Series](#)

[See All Topics](#)

[More FTC Small Business](#)

[Go to](#)
[FTC.gov/SmallBusiness](#)

[Sign up to Receive the FTC Business Blog](#)

[Sign Up](#)



<p>Enforcement</p> <ul style="list-style-type: none"> Cases and Proceedings Premerger Notification Program Merger Review Anticompetitive Practices Rulemaking Statutes Competition and Consumer Protection Guidance Documents Warning Letters Consumer Sentinel Network Criminal Liaison Unit FTC Refund Programs Notices of Penalty Offenses Competition Matters Blog 	<p>Policy</p> <ul style="list-style-type: none"> Advocacy and Research Advisory Opinions Cooperation Agreements Federal Register Notices Reports Public Comments Studies Testimony Policy Statements International Office of Technology Blog 	<p>Advice and Guidance</p> <ul style="list-style-type: none"> Consumer Advice Military Consumer Consumer.gov Business Guidance Competition Guidance Bulk Publications 	<p>News and Events</p> <ul style="list-style-type: none"> News Events Features Topics Data and Visualizations Contests Stay Connected 	<p>About the FTC</p> <ul style="list-style-type: none"> Mission History Commissioners and Staff Bureaus and Offices Budget and Strategy Office of Inspector General Careers at the FTC Contact
--	--	--	---	---