Report Fraud

Tech Support Scams

Business Guidance Protecting Small Businesses Home Cybersecurity Vea 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

Secure Remote Access

Hiring a Web Host

Cybersecurity Videos

Cybersecurity Quizzes

TECH SUPPORT SCAMS

Download/Print PDF

Take the Quiz

Problem With Your Computer Often, scammers are behind these calls, pop-up messages, and emails. They want to get your

You Get a Phone Call, Pop-Up, or Email Telling You There's a

money, personal information, or access to your files. This can harm your network, put your data at risk, and damage your business.

The scammers may pretend to be from a well-known tech company, such as Microsoft. They

may ask you to open some files or run a scan on your computer — and then tell you those files

use lots of technical terms to convince you that the problems with your computer are real. They

or the scan results show a problem...but there isn't one.

How the Scam Works

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

names and passwords

available elsewhere for free



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



Try to sell you software or repair services that are worthless or available elsewhere

Ask for credit card information so they can bill you for phony services or services



for free

personal information

Direct you to websites and ask you to enter credit card, bank account, and other

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

pop-up message warning you of a computer problem.

someone who contacts you unexpectedly.

How To Protect Your Business

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

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.

computer issues are legitimate, but do not call a number or click on a link that appears in a

What To Do If You're Scammed

Never give someone your password, and don't give remote access to your computer to



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,

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.

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

If the affected computer is connected to your network, you or a security professional

Download/Print PDF Take the Quiz

consult a trusted security professional.

Consider using a password manager.

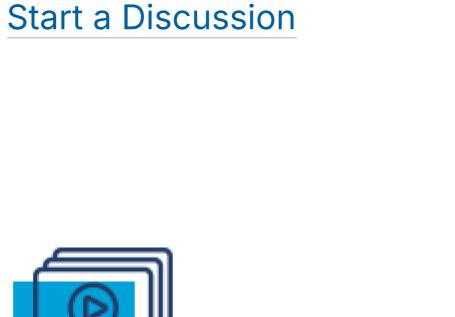
credit card statements to make sure the scammer doesn't try to re-charge you every month. Report the attack right away to the FTC at FTC.gov/Complaint.

to test your cybersecurity know-how.

Additional Resources

cybersecurity_sb_techsupport-es.pdf (349.61 KB)

Check out these additional resources like downloadable guides



Guide for Employers

Cybersecurity Video

Series

See All Topics

FEDERAL TRADE

Test Your Knowledge

Cybersecurity

Quizzes

Business Go to

FTC.gov/SmallBusiness

More FTC Small

Order Free Publications

Get the Materials

Download Materials

Blog Sign Up

Sign up to Receive

the FTC Business

COMMISSION National Institute of Standards and Technology U.S. Department of Commerce

Advice and Guidance

Report Fraud



U.S. Small Business

Administration

SBŅ

About the FTC

Submit Public Comments

Homeland

Security

Premerger Notification Advisory Opinions Cooperation Agreements Federal Register

Competition and Consumer Protection Guidance Documents

Criminal Liaison Unit FTC Refund Programs Notices of Penalty Offenses

Network

Studies Testimony Policy Statements International

Office of Technology

Consumer Advice Military Consumer Consumer.gov

Business Guidance Topics **Data and Visualizations** Contests

Get Consumer Alerts

Events Features

> **Bureaus and Offices Budget and Strategy**

Staff

Mission

History

Careers at the FTC

Statutes

Enforcement

Program

Cases and Proceedings

Competition Matters

Public Comments

Reports

Policy

Advocacy and

Research

Competition Guidance Bulk Publications

Stay Connected

News and Events

News

Office of Inspector General

Commissioners and

Privacy

Policy and Notices

FEDERAL TRADE COMMISSION PROTECTING AMERICA'S CONSUMERS

Merger Review Anticompetitive **Practices Notices** Rulemaking

Warning Letters Consumer Sentinel

Contact

Policy

Blog

Accessibility

Blog

Office of Inspector

General

No FEAR

Act

FOIA

USA.gov



