SMALL BUSINESS

TECH SUPPORT SCAMS

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 les. This can harm your network, put your data at risk, and damage your business.

: A I F : 6 E 4 2 ? I A D = E

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 les or run a scan on your computer — and then tell you those les 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

Install malware that gives them access to your computer and sensitive data, like user names and passwords

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

F a to enroll you in a worthless computer maintenance or warranty program

2 b Y h ^ d c ^ _ M h f W c V M P a P M a Q ^ a U W S c P M a Q S ^ a _ b R a e W P R b ^ a b R a e W P R b M R Z b R f V R a R S ^ a S a R R

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

FEDERAL TRADE COMMISSION

36DE64GD;FK ZAD

SMALL BUSINESS

HOW TO AVOID TECH SUPPORT SCAMS

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

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

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

...ever give someone your password, and don't give remote access to your computer to someone ...ho contacts you unexpectedly.

WHAT TO DO IF YOU'VE BEEN 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.