First County Bank™
It's where you belong.

CustomerFirst
CONTACT CENTER
Weekdays 203.462.4400
Touch Tone 203.462.4300

Avoid “Tech Support” Telephone Phishing Scams

Cybercriminals don’t just send fraudulent email messages and set up fake websites. They might also call you on the telephone and claim to be from a trusted company. They might offer to help solve your computer problems or sell you a software license. Once they have access to your computer, they can do the following:

- Trick you into installing malicious software that could capture sensitive data, such as online banking user names and passwords. They might also then charge you to remove this software.
- Take control of your computer remotely and adjust settings to leave your computer vulnerable.
- Request personal information such as a debit/credit card and even possibly your social security number so they can bill you for phony services.
- Direct you to fraudulent websites and ask you to enter debit/credit card and other personal or financial information there.

Telephone Tech Support Scams: What You Need To Know

Cybercriminals often use publicly available phone directories so they might know your name and other personal information when they call you. They might even guess what operating system you’re using.

Once they’ve gained your trust, they might ask for your user name and password or ask you to go to a website to install software that will let them access your computer to fix it. Once you do this, your computer and your personal information is vulnerable.

Do Not Trust Unsolicited Calls. Do Not Provide Any Personal Information.

Here are some of the organizations that cybercriminals claim to be from:

- A popular technology company’s help desk
- A popular retailer’s service center or tech support area
- A popular technology company’s research and development team

Report Phone Scams

Learn about how to report phone fraud in the United States at the Federal Trade Commission’s website (http://www.consumer.ftc.gov/articles/0076-phone-scams). Outside of the US, contact your local authorities.

How To Protect Yourself From Telephone Tech Support Scams

If someone claiming to be from tech support calls you:

- Do not purchase any software or service.
- Ask if there is a fee or subscription with the “Service.” If there is, hang up.
- Never give control of your computer to a third party unless you can confirm that is it a legitimate representative of a computer support team with whom you are already a customer.
- Take the caller’s information down and immediately report it to your local authorities.
- Never provide your debit/credit card or financial information to someone claiming to be from tech support.

What To Do If You Already Gave Information To A Tech Support Person

If you think that you might have downloaded malware from a phone tech support scam website or allowed a cybercriminal to access your computer, take these steps:

- Change your computer’s password, change the password on your main email account
- Contact your bank to inform them that your accounts may have been compromised.
- Scan your computer with a safety scanner to find out if you have malware installed on your computer.