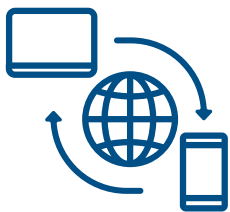# Tech Support Scams

A technical support scam, or tech support scam, is a type of fraud in which a scammer claims to offer a legitimate technical support service. Victims contact scammers in a variety of ways, often through fake pop-ups resembling error messages or via fake "help lines" advertised on websites owned by the scammers. Technical support scammers use social engineering and a variety of confidence tricks to persuade their victim of the presence of problems on their computer or mobile device, such as a malware infection, when there are no issues with the victim's device. The scammer will then persuade the victim to pay to fix the fictitious "problems" that they claim to have found. Payment is made to the scammer through ways which are hard to trace, such as gift cards, and have fewer consumer protections in place which could allow the victim to claim their money back.

It could start with a pop-up in your internet browser that looks like a

blue screen error

or

anti-virus software
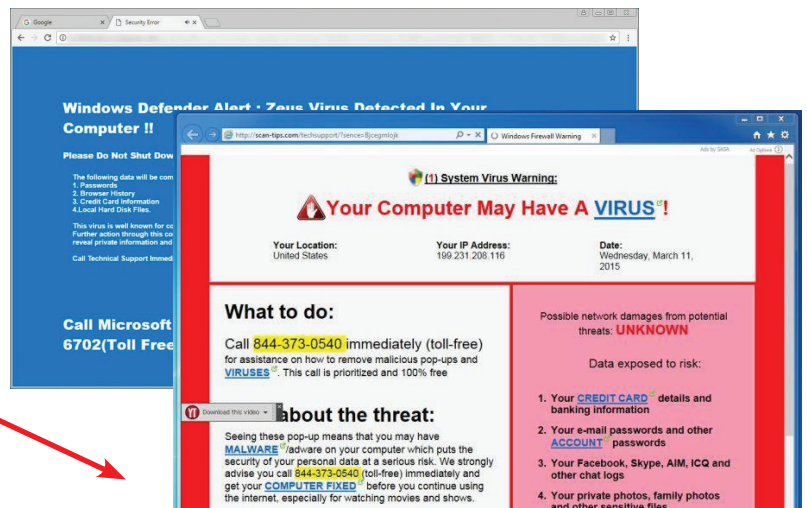
and will likely urge you to call a toll-free number IMMEDIATELY and may make threats that you could lose your personal data if you don't call right away.

If the scammer is lucky enough to get a call from you, they will likely:

request that you grant them remote access,

act like they are running diagnostic testing,

pretend they have found a virus or other security breach,

and attempt to sell you repair service or a new security subscription.

Cyber-Savvy Seniors

Tech Support Scams

You'll be asked to pay a fee, but the "services" you'll get are at best worthless, and at worst, malicious.

things you can get elsewhere for free

things you already have

"fixing" a problem that doesn't exist

subscriptions that don't do anything

installing malware

What Can Be Done?

If you get a pop-up, call, spam email or any other urgent message about a virus on your computer, stop.

- Don't click on any links or call a phone number.
- Don't send any money.
- Don't give anyone control of your computer.

Microsoft does not display pop-up warnings and ask you to call a toll-free number about viruses or security problems.

Report it at ftc.gov/complaint. Include the phone number that you were told to call.

Keep your security software up to date. Know what it looks like so you can spot a fake.

Tell someone about this scam. You might help them spot it and avoid a costly call.