Don’t Fall Victim to Tech Support Scams

Phony calls, pop-up messages, the “blue screen of death.” Americans have lost over $1.5 billion to tech support scams.

How it Works:

Tech support scams can take various forms:

- A scammer posing as an employee of a well-known tech company calls to say the victim’s computer is sending messages that it has a virus.
- A victim sees a pop-up message on his screen claiming viruses are attacking the device. The message includes a phone number to call for assistance.
- A victim’s screen freezes (known as the Blue Screen of Death) with a phone number and instructions to call a tech support company.

What You Should Know:

The scammer’s goal is to gain remote access to your device. Once this happens, he claims to find multiple viruses or “malware” that he can fix for a fee. The scammer then asks for a form of payment, usually a credit card or a wire transfer.

What You Should Do:

- Avoid clicking on pop-up notices that say you have a problem with your computer.
- If you get a tech support call out of the blue, hang up.
- Never give control of your computer to someone who calls you.
- Don’t give out your credit card number to someone who claims to be from tech support.
- Don’t give a caller your password; legitimate companies will never ask for it.
- Report scams like this to www.ftc.gov/complaint and let others know about it on our scam-tracking map.