



## Lincoln Investment Wants You to Be Wary of Tech Support Scams: Don't Fall for the Scare Tactics

The FBI is warning the public of a nationwide uptick in technical support scams targeting older adults, where scammers can get remote access to devices, or even convince victims to pay the scammers using cash payments via couriers, ACH or through gift cards or cryptocurrency.

### How Tech Scams Are Perpetrated

Tech support scammers usually initiate contact with a victim through a phone call, text, email or pop-up window purporting to be technical support from a legitimate company. Sometimes they will spoof caller ID so that it appears the call is coming from a legitimate business like Microsoft, Apple or a bank. Scammers might also initiate contact by displaying fake error messages on websites you visit or displaying support numbers on your device and enticing you to call. These fake error messages aim to scare you into calling their "technical support hotline."

The scammer will use fear to convince you of problems with your device, software, bank accounts or that there are illegal files found on your device. Sometimes they convince the victim to download a software program that gives the scammer remote access to the victim's computer and once a connection is established, the victim is convinced to log on to their bank accounts. Other times, they may advise that the "problem" can be fixed through making direct payments to the scammer. It is important to note that scammers will use a wide range of stories to convince you there is a problem that they can fix.

### Tips to Protect Yourself

- » Never download software at the request of an unknown individual who contacted you.

- » Never allow an unknown individual who contacts you out of the blue to have control of your computer.
- » Do not click on unsolicited pop-ups, links sent via text messages, email links or attachments. Do not contact the telephone number provided in a pop-up, text or email.
- » Never send cash via mail, shipping companies or payment in the form of gift cards.
- » If you get an unsolicited call, email or text telling you that there is a problem with your computer, ignore it. Legitimate tech support staffers will never contact you out of the blue.

### If You are a Victim, Report It

If you are a victim, contact your bank right away to mitigate any losses. Contact your financial professional to ensure that Lincoln Investment is notified and can help assist in the protection of your Lincoln assets.

The FBI requests victims report tech scams to the FBI Internet Crime Complaint Center at [ic3.gov](https://ic3.gov). You can also make reports to the FTC at [reportfraud.ftc.gov](https://reportfraud.ftc.gov), and/or to local law enforcement.

If you think you have given your personal information to a scammer, go to [IdentityTheft.gov](https://IdentityTheft.gov) for steps you can take to protect your identity.

Finally, tell your friends and family. Help them avoid getting scammed.

Sources: [Internet Crime Complaint Center \(IC3\) | Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash through Shipping Companies](#)