FRAUD AWARENESS

Tech Support Scams

Tech support scams often start by a user receiving a pop up window on their computer with language stating system may have detected viruses on your computer, and instructions to contact a fraudulent tech support individual via phone. If the user contacts the phone number listed, a fraudster is standing by to gain access to all information by downloading malware onto the computer. If you receive this pop up window, do not call the phone number - Microsoft and Apple companies **will not** reach out to users for tech support, this is a known attempt to commit fraud.

Red flags presented with these interactions if a call has been placed to the requested phone number:

- Fraudster may tell you that you must keep their interaction with you 100% confidential and to not talk to your family, friends, financial advisor or other trusted individuals
- They state that in addition to potential viruses held in the computer, accounts at financial institutions have been compromised, and your assets are no longer safe
- The scammer will try to convince you that your accounts are at risk and that you will need to liquidate all assets and transfer out of LPL to be safe. The scammer will provide fabricated rationale, a story they want you to tell your financial advisor or LPL when they ask you why you are making the withdrawal
- They may try to reassure you that you will get your money back at a later time, after you have liquidated and transfer to a “safe location”
- Fraudster may have a secondary individual impersonating a financial institution’s fraud department or even law enforcement. Please note: LPL’S FRAUD TEAMS are internal departments and will rarely try to speak directly with you as a client without your financial advisor

In cases where these scams are successful, and a bad actor has convinced their victim to liquidate their assets, they will often follow one or more of the steps below to steal the victim’s assets.

- Scammer will provide instructions for setting up a new account at another firm or bank, the bad actor can access this account more easily. Often Bitcoin or online cryptocurrency wallet format
- Scammer will instruct their victim how, when and where to transfer funds, and what to say to their financial advisor if they are asked about often a wire or ACH transaction
- Money is removed via a foreign or domestic wire to the account that was set up that he scammer controls
- Scammer will ask for consistent communication to ensure the transaction is complete at their instruction

How to keep yourself protected from these scams:

- If you receive a pop up on your computer that states you have been compromised, do not call the phone number listed on that pop up
- Do not provide any personal or banking information to someone you don’t know
- If you place a call for the scenario outlined above, contact your financial advisor and disconnect your internet connection. Fraudsters will no longer have access to your data without internet connection
- Call a local tech support company, or ask a family or friend for a recommendation if you feel your computer has been accessed by a fraudster
- Make sure your antivirus software is up to date

Tracking #1-05375552
Exp. 08/2025