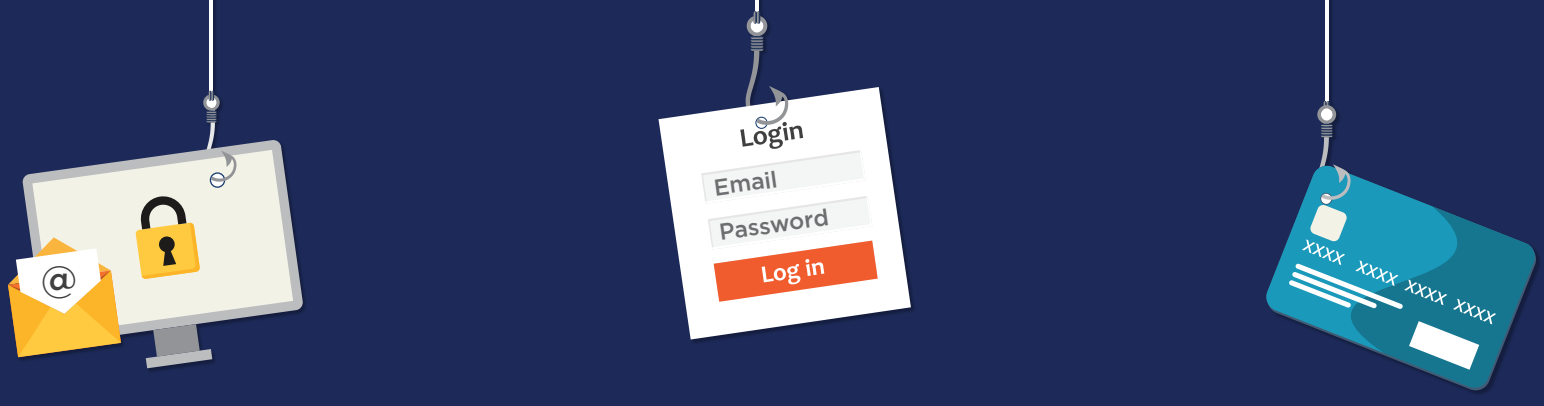

TECH SUPPORT SCAMS

Criminals could target you, saying there's something wrong with your device, or claim that your financial accounts have been hacked — or are at risk of being hacked — and indicate they can fix it.

It's all a scam to access your devices, personal information – and ultimately – your money.

$1.3 billion

lost by consumers in 2023 to tech support and government impersonation scams.*

Over 17,000

cases of tech support scams reported to the FBI by older adults in 2023.*

People 60+

lost more money to these scams than all other age groups combined.*

**FBI's 2023 IC3 Elder Fraud Report*

HERE'S HOW IT WORKS

The scam usually begins with an unsolicited call, email, text or pop-up message.

Scammers impersonate tech support companies, and often bring in other impostors to pose as bank representatives or government officials.

Bad actors may also attempt to persuade you to withdraw cash, invest your money in a bogus crypto platform, or buy gold or other precious metals to send to them.

Then they will send couriers to retrieve your assets, under the guise of safeguarding them. If you comply, they will steal your money.

They will tell you that you need to protect your device, and encourage you to sign up for a bogus subscription and install software to protect yourself.

If you follow through, however, you will be installing malicious software (malware) used by criminals.

PROTECT YOURSELF

Remember, the safest place to keep your money secure is in a federally-insured bank.

Never disclose your address or agree to meet with strangers to deliver cash or precious metals.

Don't click on unsolicited pop-ups, text message links, or email links and attachments.

Don't call unknown telephone numbers from pop-ups, texts or emails.

Don't download any software at the request of unknown people who contact you.

Don't allow unknown people access to any of your devices.

Spot the Scam? Report It!

1. **Tell your bank.**
2. **Contact law enforcement.**
3. **File a report with the FBI at IC3.gov.**

When Reporting, Include:

- How and where you encountered the criminals.
- Your communications with the criminals.
- The criminals' names, email addresses and phone numbers.
- Cryptocurrency exchanges you were instructed to use.
- The timeline of the scam.
- Domain names, websites or apps that the criminals instructed you to use.

ABA FOUNDATION