



scam safety checklist

Got a request for your money or information? Pause to question:

- ✓ **What do they want?**
Unexpected requests to transfer money, “confirm” your information, or approve a login attempt are some of the most common signs of a scam.
- ✓ **Who’s asking?**
A familiar name doesn’t always mean the request is real. Caller ID, email addresses, websites, and even voices or videos can be faked.
- ✓ **What’s the pressure?**
Scammers often use emotion to cloud your judgment—whether it’s rushing you, scaring you, or earning your trust.
- ✓ **Can you verify?**
Check the request independently. Contact the person or company using a phone number, website, or app you found yourself and know you can trust.

Still not sure it’s a scam?

See if any of these red flags trigger your inner scam alarm.

- ⚑ **Is it promising something?**
Scams often involve quick fixes and promises that sound like dream opportunities. Reality tells us that there’s no shortcut to paying off debt or earning guaranteed returns or free money.
- ⚑ **Does it include a link, attachment, or QR code?**
Before clicking, ask yourself: “Would I normally handle this through a text or email?” If not, go directly to the company’s website, app, or customer service number instead of using the information provided in the message.
- ⚑ **Are they telling you not to tell anyone?**
A common scam tactic is convincing you not to tell anyone what’s happening. Honest businesses, government agencies, and financial institutions won’t tell you to keep it “just between us.”
- ⚑ **How is this making you feel?**
Scams are designed to make our hearts race. Fear is a common tactic, with words like “deadline,” “fine,” or “fraud alert,” but scammers also prey on loneliness, curiosity, and excitement.

Above all else: Pause and verify.

If something feels even slightly “off,” there’s nothing wrong with stepping away from the conversation until you can verify what’s really going on. If you’re an Allstate Identity Protection member, call us at (800) 789-2720 before sending money or making an unusual payment—we can help you determine whether it’s safe or a scam.