

Avoiding Scams After Losing a Loved One

The reality is that scammers **WILL** target you because of your recently widowed status. Scammers **WILL** target you, assuming you have received life insurance policy payouts, VA spouse benefits, or SSA benefits. They will parse through obituaries, searching for surviving spouses. They find you on social media and search through records online, obtaining your phone numbers and email addresses.

These scams are reportedly known to fund terrorist organizations around the world.

Be cautious of the following red flags and warning signs:

- They profess love quickly and try to build an emotional connection fast.
- They avoid meeting in person or video chatting.
- They ask for money, gift cards, or your bank information.
- Their photos look too good to be true, or they seem hesitant to share personal details about their life.

Be cautious of the following situations:

- You're contacted regarding a "can't miss opportunity," often requiring funds through cryptocurrency (bitcoin) or gift cards.
- You receive an unexpected check in the mail, asking you to deposit funds and mail or send back most of the funds.
- You receive a phone call from someone claiming they're from the bank, the IRS, or the police, demanding funds must be paid immediately to prevent legal action from being taken.
- You receive an email from Microsoft, McAfee, or another company regarding a large purchase, asking you to call them if you want a refund or to cancel. Once you call them, they convince you to let them remote into your computer to gain access to your banking information.
- You receive an email or physical mail threatening to blackmail you unless you pay them in cryptocurrency.

What to do if someone attempts to scam or exploit you:

- Stop all communication immediately. Hang up the phone, block their number, and block their email address. Cut all ties with this person. They do NOT have your best interest in mind.
- If someone is threatening you, contact the police to make a report.
- If your computer is compromised, disconnect from the internet and take your computer to a reputable tech company to have your computer scanned for viruses.
- If your social security number is compromised, you will want to contact the credit bureaus to place an alert.

Who can help?

- Contact Legacy Bank at **405-748-2535** or visit your local branch as soon as possible to discuss the situation. We want to know what happened and what personal information may be compromised.
- Forward any messages that claim to be from the IRS to **phishing@irs.gov**.
- Report any online scam to the FBI at **<https://www.ic3.gov/Home/FileComplaint>**.
- Contact the Federal Trade Commission (FTC) at **1-877-FTC-HELP (1-877-382-4357)** or visit **<https://reportfraud.ftc.gov/>** to report any scams or fraud.



MEMBER FDIC