CYBER SCAMS

Cyber scammers often pose as legitimate enterprises. Don't be fooled. LADA urges wildfire victims and donors to exercise caution when asked for personal or financial information over text, email, websites, or social media.

It is important to thoroughly vet individuals and organizations offering services or soliciting donations. Watch out for fake:

- Contractors
- Debris clearance companies
- Towing companies
- Insurers
- Public adjusters
- Charities
- Fundraising campaigns for victims
- Government representatives

Don't Answer the Door for Cyber Scammers

Treat unsolicited messages the same way you would if a complete stranger knocked on your door and asked for your financial information. Instead of closing the door, delete the messages.

Pay attention to details. Look closely at emails, texts, website pop-ups, and social media solicitations for misspellings, grammatical errors, and odd URL addresses.

Do not click on any links until you have verified the organization.

Do not donate to a fundraising campaign for fire victims unless you have verified the page with the creator.

Know the Facts:

No legitimate enterprise will ask for payment with gift cards, wire transfers, or crypto currency.

Insurance companies will NOT reach out to you first.

Legitimate businesses will not pressure you into signing contracts, ask you to sign a blank contract, require you to sign over your insurance check, suggest you borrow money from a lender they know, or offer to help you qualify for FEMA relief for a fee.

Additional Resources:

Los Angeles County Department of Consumer and Business Affairs	dcba.lacounty.gov
California Department of Insurance	insurance.ca.gov
Federal Trade Commission	consumer.ftc.gov

If you or someone you know has been a victim of a scam, please contact your local law enforcement. To learn how to protect yourself from other scams, visit da.lacounty.gov/fraud-alerts.