

Top Ten Scams

Community Protection Division
Boulder County District Attorney's Office



1. Imposter Call Cons

Scammers posing as the IRS, Sheriff, Social Security, Medicare call and tell you that your benefits are suspended or cancelled, you owe taxes, penalties, missed jury duty, etc.

- **HANG UP! These are SCAMS**

2. Tech Support Tricks

The scammer calls or emails, or a popup appears on your screen. They say they are “tech support” with a well-known company such as Microsoft or Apple. They’ve detected a computer virus or a “cloud breach,” and try to trick you into paying for bogus repairs, or giving them remote access.

- **HANG UP! Never give control of your computer to someone who calls you**
- **Buy virus protection software from a reputable retailer, and keep it up to date**

3. Romance & Companion Scams

Scammers create fake profiles on dating or caregiver websites to take advantage of those looking for love or companionship. You might converse with them online for a long time, then they ask you for money; it might be for a plane ticket, a family member’s medical needs, a new business opportunity, or an emergency.

- **Never send money or gifts to someone you haven’t met in person**
- **Tell a friend or family member about a new online friend when you begin the relationship**

5. Buys and sellers online, Beware:

Scammers will mimic well-known retailers, will design realistic popups, and even offer fake deals online.

- **Never pay by putting money on a gift card and transmit the gift card number – That’s a SCAM!**
- **Check website addresses and descriptions**

4. Prizes, Sweepstakes and Lotteries

Scammers will send you a letter that comes with a check that says it’s from the Publisher’s Clearinghouse, or another prize company. Or maybe you receive a check in the mail as “bonus” saying you can make money by taking a survey.

- **Publisher’s Clearinghouse will NEVER call, email or write in advance to say you are going to be a big winner. They will NEVER ask you to pay taxes or any money in advance to collect their prize. And they’ll NEVER send you a big check in the mail**
- **Don’t fall for prize scams and don’t cash that check!**

5. Contractor/Home Repair Scams

A contractor offering a quick inspection or a repair on the cheap. They ask for payment up front, or say you must act right away, but they don’t give you a contract.

- **Hire a reputable contractor. Check up on contractors with the BBB, the CO Secretary of State, the Community Protection Division, and online reviews**
- **Obtain written quotes and a written contract**

6. Don’t go “Phishing”

An email or popup looks as if it comes from your bank, credit card company, Netflix, Microsoft, Apple, etc.

- **Never provide payment or personal or financial information in response**
- **Never reply, never click a link, never open an attachment**
- **Take a closer look. While some phishing emails look completely legit, bad grammar and spelling can tip you off to phishing**



Michael Dougherty, District Attorney

BOULDER OFFICE: JUSTICE CENTER · 1777 6TH STREET · BOULDER, COLORADO 80302 · 303.441.3700
LONGMONT OFFICE: 1035 KIMBARK · LONGMONT, COLORADO 80501 · 303.441.3700
WWW.BOULDERCOUNTY.ORG/DISTRICT-ATTORNEY · TDD/V: 303.441.4774

9. Gift Card Grabs

A caller will tell you to go buy a gift card. Once you buy it the caller asks for the gift card number and PIN on the back. Those numbers let them get the money you loaded onto the card.

- **Anyone who demands payments by gift card is always a scammer. Every time**
- **Gift cards are for gifts, not for payments**
- **Never pay a bill or for a service with a gift card**

10. Gift Card Grabs

A caller will tell you to go buy a popular gift card. Once you buy it, the caller asks for the gift card number and PIN on the back. Those numbers let them get the money you loaded onto the card.

- **Anyone who demands payment by gift card is always a scammer. Every time**
- **Gift cards are for gifts, NOT payments**
- **Never pay a bill or for a service with a gift card**

Thieves find store gift card racks and scan the card numbers. When a buyer loads money onto the card, the thieves go on an online shopping spree.

- **Get a gift card from behind the service counter, or from a retailer's website.**

8. Charity Cheats

Bogus charities call asking for donations; you might think they're authentic, because charities are exempt from "do not call" rules. But before giving:

- **Verify a charity's legitimacy through the CO Secretary of State's charity database, or at www.ColoradoGives.org (you can make a donation there, too!)**
- **Unless you initiate the call, never provide payment over the phone**

Prevent Identity Theft

- Keep your personal identifying information (PII) safe at home and keep an eye on it everywhere
- Always monitor your bank and credit card statements
- Opt out of telemarketing mail and calls to reduce the circulation of your information
- Use different passwords for different accounts

Reporting Scams

Report phone scams to the Federal Trade Commission at:

www.ftc.gov/complaint

Report computer scams to the Internet Crime Complaint Center (IC3) at:

www.ic3.gov

For questions about fraud, identity theft, or scams, call the Community Protection Division at 303-441-3700

**Call the DA's Community Protection Division
with Questions
303-441-3700**