Scams of the Holidays

Community Protection Division
Boulder County District Attorney's Office
Updated 11/2/2022

General Safety Tips for the Holidays

- **STOP** – Or hang-up the phone so you don't share Personal Identifying Information (name, address, Social Security Number, bank account info, etc.)
- **Hang up on scammers**, no reason to be nice since they are trying to scam you out of your money
- **Don't immediately provide payment** or personal information to calls who solicit you first
- **Talk to someone you trust** to discuss the situation

1. **Imposter Scams** – Scammers posing as local, state, or federal organizations or agencies stating that your account was "froze" or pretending to be a lawyer requesting payment for medical bills for a loved one. Add Yourself to Do Not Call registries
   - **National Do Not Call List** www.DoNotCall.gov (1-888-382-1222)
   - **Colorado Do Not Call Registry** www.ColoradoNoCall.com (1-800-309-7041)
2. **Charity Scams** – Phone calls from fake charities or pop-up ads asking for donations. Most times these donations never make it to the communities you think they are going to. **Donate to credible charities. Below are some places to check for charities:**
   - Colorado Gives at www.ColoradoGives.org
   - Charity Navigator www.CharityNavigator.org
   - Charity Watch at www.CharityWatch.org
   - BBB Wise Giving Alliance at www.Give.org
3. **Online Shopping Scams** – Online website pop-ups or online ads for bogus sites offering bargain basement prices, fake freebies.
   - If the offer is **too good to be true**, it just might be a scam
   - **Shop from trusted online places and sellers** and compare prices before buying
   - **Do your research** before making a purchase to compare prices, quality, and reviews
   - **Don't click on unfamiliar links, popups, or open attachments from unfamiliar sources** on websites, emails or text messages on your smart phone. Instead, go to the secure website online to check for information on your accounts
4. **Social Media Scams** – Be skeptical of any claims made by social media sites that appear to offer miracle cures, holiday promotions, or contests.
   - **Do you due diligence if you come across a social media ad and research the information**
5. **Seasonal Jobs Scams** – Online postings of fake jobs at real employers. If the job is "too good to be true", it more than likely is a scam.
   - **Don't accept money from an unknown individual who is reaching out to you**
   - **Be wary of reshipping jobs as these could be scams**
6. **Package Theft Scams** – Individuals and groups stealing orders off your front porch when they are delivered.
   - **Avoid package theft** by requiring a signature, enlist a neighbor to help, or look into alternative delivery options

Michael Dougherty, District Attorney

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

7. **Romance or Companionship Scams** – Creating a romantic relationship with you and eventually asking you to give money so they can come visit (like airfare), medical costs, or other expense. Beware these costs are not real
   - **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**

8. **Tech Support or Tech Takeover Scams** – Pop-ups warning you that your computer has been taken over or that you need to contact tech support. Or emails from a tech support company saying that your account has been charged for services you did not agree to.
   - **DO NOT CALL THE NUMBER PROVIDED!**
   - **Never download a program or app that an anonymous person sends you**
   - **Never give control of your computer** to someone who calls you
   - **Use your malware and anti-virus software that is already on your computer** or purchase virus protection software from a reputable retailer and keep it updated

9. **Prize, Sweepstakes or Giveaway Scams** – Letters or emails stating that you won a sweepstakes or prize, but beware if they ask you to pay for the prize first (taxes, postage, handling, etc.) as this might be the telltale signs of a scam
   - **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

10. **Quizzes & Survey's** – Text messages or emails asking you to respond to quizzes, surveys, or tell you that you can receive an item for sharing your thoughts.
    - **Do not share your bank or credit card information with these anonymous links**
    - **Most times scammers are looking to gain more of your info to conduct identity theft.**

11. **Phishing Scams** – Emails from organizations or businesses stating that you need to take action on your account. These emails will take you to false websites to collect your personal or bank information
    - **Never provide payment or personal or financial information in response**
    - **Never reply, never click a link, never open an attachment**
    - **Never add an application or program that an unknown persons asks you to download**
    - **Take a closer look.** While some phishing emails look completely legit, bad grammar and spelling can tip you off to phishing

12. **Identity Theft** – Scammers will often collect your personal identifying information and bank information to open illegal accounts which could affect your credit, public benefits, or other personal matters.
    - **Always monitor bills and credit card activity** and pull your credit report at least one time a year to make sure there are no unusual accounts.
    - **Consider a credit report freeze** to prevent anyone from opening new credit in your name at www.AnnualCreditReport.com or call 1-877-322-8228
    - **Consider using multi-factor authentication** or an authenticator app to protect your online accounts

Report Scams to the Federal Trade Commission at https://reportfraud.ftc.gov/#/ or 1-877-382-4357

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