

ATTORNEY GENERAL RAÚL LABRADOR'S CONSUMER WATCH

Scam Alerts, Fraud Trends, and Consumer Tips for Idahoans



SCAM ALERTS



FRAUD TRENDS



PROTECT YOURSELF



RESOURCES



CONSUMER TIPS



COMMUNITY PARTNERS



Welcome to the Fall edition of *Idaho Consumer Watch*. Every day, my office works to protect Idaho families and small businesses from fraud, scams, and unfair business practices, taking action against bad actors, and educating the public before they become a victim. This newsletter gives insight to scams and fraud trends that are currently hitting Idaho, plus consumer tips and resources that protect and inform families while navigating the marketplace.

Want scam alerts and updates from our office more often than once a season? [Follow us](#) on Facebook for daily consumer alerts and updates on what we're doing across the state, or sign up for our [weekly newsletter](#), the **Labrador Letter**, to get it straight to your inbox. Together, we can put scammers out of business!

In this Issue:

- Avoiding Utility Scams
- Medicare Open Enrollment Scams
- Charity Scams: How to Give Safely
- Anatomy of a Scam: The Missed Jury Duty Call



Pull the Plug on Utility Scams

Attorney General Raúl Labrador is warning Idahoans about the increasing number of utility scams involving Idaho Power Company and electrical services across the state. Currently, Idaho Power has almost 400 customer accounts that have experienced fraudulent activity, including unauthorized service requests, fraudulent payment processing, customer impersonation, and unauthorized changes to customer account information.

"My office is working with Idaho Power's investigators to identify the source of these scams," Attorney General Labrador said. "We suspect they originate overseas with scammers using spoofed phone numbers and websites registered in foreign countries. Consumers must be vigilant and never give private information to unknown callers or suspicious websites. Prevention and awareness are always the best ways to beat scammers."

- **Recognize Red Flags:** Idaho Power will never demand immediate or same-day payment over the phone or in person under threat of instant service disconnection.
- **Reject suspicious payment methods:** Never pay using prepaid gift cards, cryptocurrency, money transfer apps, or QR codes. Official payments are not accepted through these methods.
- **Refuse fees for "defective meters":** Idaho Power does not require customers to pay out-of-pocket fees or immediate deposits for meter repair or replacement.
- **Beware of door-to-door solar sales:** Idaho Power employees do not sell solar panels door-to-door or partner with third-party contractors for door-to-door sales.
- **Verify in-person employees:** Legitimate field employees will always arrive in a branded company vehicle, wear company clothing, and display an official corporate ID badge. Always ask to see their physical ID badge before granting access or discussing account details.
- **Hang up and call back directly:** If caller ID displays "Idaho Power" or "IPCO," but the interaction feels suspicious, hang up immediately. Scammers often spoof caller ID numbers and area codes.

Is this a Utility Scam? A quick checklist for Idaho Consumers:

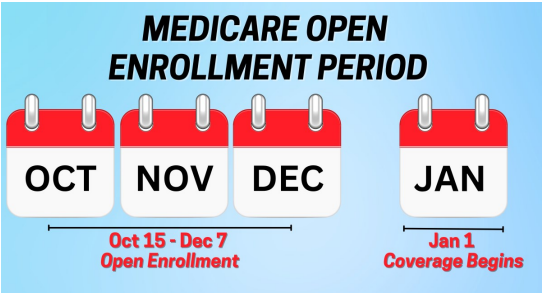
- ☐ Is the caller demanding immediate payment, threatening disconnection, or legal action?
- ☐ Is the caller insisting you pay with gift cards, cryptocurrency, or an unknown third-party payment app or link?
- ☐ Is the caller asking you for personal information, like account numbers, passwords, or social security numbers?
- ☐ Is the caller asking you to pay through a text or email link that looks or feels suspicious?

Trust your instincts—if something feels suspicious, take time to verify before

If you think you are the victim of utility scams, visit ReportScamsIdaho.com to file a consumer complaint with the Idaho Attorney General's Consumer Protection Division.

ALERT: Medicare Open Enrollment - Protect Your Private Data

October 15th starts Open Enrollment for Medicare. It's a prime time for scammers who have stolen billions of taxpayer dollars. Victims will get calls from criminals pretending to be from Medicare. They will ask for Medicare account numbers, banking information, or social security numbers, saying that coverage and benefits are about to be cancelled, or offer free services in exchange for information. An account number is all they need to file fraudulent benefit claims for visits, services, and procedures. The following tips can help prevent this kind of fraud before it ever gets started:



Ignore unsolicited contact. Do not respond to unexpected calls, texts, emails, ads, or door-to-door visits claiming to be from Medicare or offering to “help” with your plan.

Use official sources only. For plan comparisons or changes, visit **Medicare.gov**, **Healthcare.gov**, or your state’s Health Insurance Assistance Program (SHIP).

Verify before you act. If you suspect a call or message is legitimate, hang up and call Medicare directly at **1-800-MEDICARE (1-800-633-4227)**.

Guard your information. Never give your Medicare number, Social Security number, or financial details to anyone you do not know and who has not initiated contact through official channels.

Beware of “free” offers. Medicare will never ask for your Medicare ID in exchange for gifts or screenings.

Check your statements. Review your Medicare and insurance bills regularly for unauthorized charges. If you were billed for services, visits, tests, or medical equipment that you didn’t receive—report it immediately at: **ReportScamsIdaho.com**



Giving Safely: How to Spot Charity Scams at the Holidays

The upcoming holidays are a perfect time to support your favorite charities with your time, money, and giving spirit. Many charities depend on your donations at this time of year. Often, we are bombarded with char-

itable requests at the holidays. But scammers will take your money AND hurt your favorite charity too. Here are some tips to make sure your donations get to the right place.

First, pay attention to the charity name. Scammers will often create a very similar name to a popular and well-known charity—and then raise money off that other charity’s reputation. These scams hurt the real charities that are doing the hard work. (For example, don’t write any checks to the Salvation Navy.)

Second, if you are approached by call, email, text, or even door-to-door for a donation, it’s perfectly ok to wait to donate until you have taken time to research or verify for yourself. Take their information and donate when YOU are confident it’s legitimate.

Third, every scam operates on time. Scammers create a ticking clock and a sense of urgency to separate people from their hard-earned money. Charity scams are no different, so no matter what the crisis is, take the time to research. Don’t be pushed into a donation by aggressive tactics.

Fourth, any “charity” that asks you to donate via a prepaid gift card or cryptocurrency is almost guaranteed to be a scam. Even asking for cash-only donations is concerning. Those payments are untraceable and unrecoverable. Also, never click on payment links, especially in unsolicited texts or emails. Go directly to the charity’s website yourself.

Fifth, use watchdog tools like **CharityWatch** or the **IRS** itself to research a charity’s non-profit status. Legitimate charities are always registered and take the time to protect their donors. Overseas criminal scammer networks rarely go to such effort.

Approached by a fake charity? File a consumer complaint with the Idaho Attorney General’s Office at **ReportScamsIdaho.com**.

ANATOMY OF A SCAM

#2: MISSED JURY DUTY



LIFECYCLE OF A JURY DUTY IMPERSONATION SCAM: FROM FIRST CONTACT TO PAYMENT DEMAND



Scams come in all shapes and sizes. We often see the above "Jury Duty" scam come through our phones as an unsolicited call, and every courthouse and sheriff's office in Idaho are aware of them. Scammers are getting more sophisticated every day, but most scams have common elements that savvy consumers can spot immediately.

- **Scams pretend to be a person, government agency, or company you TRUST.** They will use logos, phone numbers, names, emails and websites that look official. Appearing official can lower a victim's defenses and hesitation to ask critical questions.
- **Scams will create a time crisis.** You have to pay now, a warrant is being issued for your arrest....unless you pay right NOW. A time crisis works to override a victim's good judgment by pressuring for immediate action or risk a penalty.
- **Scams often ask you to pay in unconventional ways.** Gift cards, money orders, via a cryptocurrency ATM, or through "convenient" links THEY provide in texts or emails are typical in scams. The only thing those methods have in common is once you pay...the money is gone and untraceable.
- **Scammers make people think they've broken the law.** People who are normally law-abiding will overlook warning signs and ignore their instincts, and scammers know that. But city, county, state, or federal governments don't demand payment via texts, and they certainly don't ask for payment with gift cards or cryptocurrency.

Go to **ReportScamsIdaho.com** for more resources and partners for scam prevention, or to file a consumer complaint with the Idaho Attorney General's Consumer Protection Division.