CAUTION
Fraud Alert

PLEASE READ FOR YOUR SAFETY

FRAUD IS BECOMING MORE & MORE COMMON

It is always evolving - keep up to date to keep yourself and those close to you safe!

Provided by Red Hawk Realty

#WeKnowTheBackcountry

Trust But Verify

~ Ronald Reagan

Tips To Avoid Fraud:

STOP. SLOW DOWN. VERIFY.

- If you have an "app" for your bank - and there is an option to use fingerprint ID to sign in - use it.
- Never save credit card information online on any website or on your computer - it's convenient but not safe!
- Don’t let your computer remember passwords to financial information or anything that you want to keep secure.
- Never apply for a job online without verifying. We don't recommend ever sending your social security number or any secure information online. Pick up a phone to call or visit in person and drop off an application.
- When ordering online, if you can order the same thing through a well known provider (i.e. AMAZON), do it. Avoid giving your card and information to more vendors - even if it will save you a few bucks.
- Be wary of any sense of "URGENCY" to do anything. Be cautious of urgency via phone call, text, social media message or email
- GIFT CARDS are a very common source of fraud - always proceed with caution!
- After experiencing any fraud - always change your credit card number! It’s better to be safe! This also ensures that your card isn't saved to any websites. It's easy to forget!
- Spoofing - or impersonating someone, can be done via phone (voice impersonation), text or email! When receiving a message, be sure to call the person back and verify their identity. Have a conversation. Make sure the person is responsive and holding a normal conversation with you.
- Have your bank send texts of transactions so you are able to see where your money is going in real time.
- Attention iPhone owners - if someone has his/her email hacked and texts or calls you - your iPhone will try to "guess" who is texting you. If they have a phone hooked to the hacked email your phone may say "found contact - the persons name". ALWAYS verify that phone number with the person's actual phone number.
- Credit card companies only count fraud as purchases made without your knowledge. They can only help if you report that your card was stolen and that you don't know where the charges came from. Be sure to understand how you are protected before you call.

Provided by Red Hawk Realty

#WeKnowTheBackcountry

Common Scams

Proceed With Caution:

- GIFT CARDS: That is a common thing for someone stealing your credit card information to buy. NEVER share the codes off of the back of gift cards with someone that you do not know. If you do fall victim to a scam, immediately contact the company directly and ask them to freeze those cards. You may be able to beat the scammers to the funds if you act IMMEDIATELY.
- JOB APPLICATIONS: Never apply for a job online without verifying the company and the job. We don't recommend ever sending your social security number or any secure information online. Pick up a phone and call or visit in person and drop off an application. Often times people are feeling desperate or rushed and want to fill out many job applications online to increase their chances. This is especially common with young people. Scammers know this and exploit this in order to gain private information.
- FAKE WEBSITES: Always read reviews to ensure that people aren't upset with this website or service provider. Ensure it is an "HTTPS" address.
- SPOOFING: Always notice the email address or phone number that is contacting you and make sure it is really that person's true information. Don't fall for emails that are simply close to the person's information.
- RUNNING ERRANDS: Asking someone to run an errand that involves you fronting money or using a company card that is out of the ordinary.
- SDGE: Calling and demanding payment and threatening that if payment isn't immediately received the power will be shut off.

BE CAUTIOUS: You never think it will happen to you - every day people are targeted via email, phone calls, text messages & social media. KEEP IT IN THE FRONT OF YOUR MIND!

See Attached For These Common Scams:

- Telephone Scams
- Charity Scams
- IRS Imposter Scams
- Banking Scams
- Ticket Scams
- Lottery & Sweepstakes Scams
- Pyramid Schemes
- Tax ID Theft
- Census Related Fraud
- Ponzi Schemes
- Government Grant Schemes

Provided by Red Hawk Realty

#WeKnowTheBackcountry

3 STEPS

If something seems out of the ordinary or urgent, take these three steps:

1. **VERIFY** - Contact the person via an already known form of contact.

2. **RUN IT BY SOMEONE** - Always run unusual circumstances past someone close to you.

3. **SAFETY CHECK** - If you are going somewhere physically or exchanging money, are you certain that you are SAFE?

Provided by Red Hawk Realty

#WeKnowTheBackcountry

Telephone Scams

Telephone scammers try to trick you out of money or get access to your personal information. Scams may come through phone calls from real people, robocalls, or text messages. The callers often make false promises, such as opportunities to buy products, invest your money, or receive free product trials. They may also offer you money through free grants and lotteries. Some scammers may call with threats of jail time or lawsuits if you don't pay them.

Report Telephone Scams

- To the Federal Trade Commission online or by phone at 1-877-382-4357. This is the primary government agency that collects scam complaints.
- Report robocalls and unwanted telemarketing calls to the Do Not Call Registry.
- Report caller ID spoofing to the Federal Communications Commission either online or by phone at 1-888-225-5322.

How to Protect Yourself

Do

- Be careful of claims that you've won a prize or vacation package.
- Hang up on suspicious phone calls.
- Be cautious of caller ID. Scammers can change the phone number that shows up on your caller ID screen. This is called "spoofing".
- Research separately, apart from the information the caller has provided.

Don't

- Don't give in to pressure to take immediate action.
- Don't say anything if a caller starts the call asking, "Can you hear me?" This is a common tactic for scammers to record you saying "yes." Scammers record your "yes" response to use as proof that you agreed to a purchase or credit card charge.
- Don't provide your credit card number, bank account information, or other personal information to a caller.
- Don't send money if the caller tells you to wire money or pay with a prepaid debit card.

Charity Scams

Some scammers set up fake organizations to take advantage of the public's generosity. They especially take advantage of tragedies and disasters.

Report Charity Scams

- Your state consumer protection office can accept and investigate consumer complaints.
- File a complaint with the Federal Trade Commission (FTC). The FTC does not resolve individual matters, but it does track charity fraud claims and sues companies on the behalf of consumers.
- Contact the National Center for Disaster Fraud if the suspected fraud is because of a natural disaster.

The Do Not Call Registry doesn't apply to charities, but you can ask an organization not to contact you again.

How to Protect Yourself

Do

- Check out the charity with your state consumer protection office or the Better Business Bureau before you donate.
- Verify the name. Fake charities often choose names that are close to well established charities.

Don't

- Don't give in to high pressure tactics such as urging you to donate immediately.
- Don't assume that you can get a tax deduction for donating to an organization. Use the IRS's database of 501(c)3 organizations to find out if it has this status.
- Don't send cash. Pay with a check or credit card.

IRS Imposter Scams

IRS imposter scams occur when someone contacts you pretending to work for the IRS. The imposter may contact you by phone, email, postal mail, or even a text message. There are two common types of scams: **Tax collection** - You receive a phone call or letter, claiming that you owe taxes. They will demand that you pay the amount immediately, often with a prepaid debit card or wire transfer. They may even threaten to arrest you if you don't comply. **Verification** - You receive an email or text message that requires you to verify your personal information; it often includes a hyperlink phrase "click here" or a button to a fraudulent form or website.

Report IRS Imposter Scams

Contact the Treasury Inspector General for Tax Administration (TIGTA) if you believe that an IRS imposter has contacted you. Report IRS imposter scams online or by calling TIGTA at 1-800-366-4484. Forward email messages that claim to be from the IRS to phishing@irs.gov.

Do:

- Beware if someone calls claiming to be from the IRS. The IRS will always contact you by mail before calling you about unpaid taxes.
- Ask a caller to provide his/ her name and badge number and callback number. Then call TIGTA at 1-800-366-4484 to determine if the caller is an IRS employee with a legitimate need to contact you. If the person legitimately is from the IRS, call them back. Otherwise report it to the IRS.
- Become familiar with what fraudulent IRS email messages look like. Review a sample IRS phishing email.
- Verify the number of the letter, form, or notice on the IRS website. Be suspicious of threats. The IRS won't threaten to have police arrest you for not paying a bill.

Don't:

- Don't give in to demands to pay money immediately. Be especially suspicious of demands to wire money or pay with a prepaid debit card.
- Don't trust the name or phone number on a caller ID display that shows "IRS." Scammers often change the name that shows on caller ID.
- Don't click on any links in email or text messages to verify your information.

Banking Scams

Banking scams involve attempts to access your bank account. Some popular banking scams include: Overpayment scams - A scam artist sends you a counterfeit check. They tell you to deposit it into your bank account, and wire a portion of the money back to them. Since the check was fake, you'll have to pay your bank the amount of the check, plus you'll lose any money you wired. Unsolicited check fraud - A scammer sends you a check for no reason. If you cash it, you may be authorizing the purchase of items or signing up for a loan you didn't ask for. Automatic withdrawals - A company sets up an automatic debit from your bank account as part of a free trial or to collect lottery winnings. Phishing - You receive an email message that asks you to verify your bank account or debit card number.

Report Banking Scams

- Report fake checks you receive by mail to the US Postal Inspection Service.
- Report counterfeit checks to the Federal Trade Commission, either online or by phone at 1-877-382-4357.
- Contact your bank to report and stop unauthorized automatic withdrawals from your account.
- Forward phishing emails to the Federal Trade Commission at spam@uce.gov.

How to Protect Yourself

Do

- Be suspicious if you are told to wire a portion of funds from a check back to a company.
- Be wary of lotteries or free trials that ask for your bank account number.
- Verify the authenticity of a cashier's check with the bank that it is drawn on before depositing a check.
- When verifying a check or the issuer, use contact information on a bank's website.

Don't

- Don't be fooled by the realistic appearance of checks or money orders. Scammers make them look legitimate and official.
- Don't deposit checks or money orders from strangers or companies with which you don't have a relationship with.
- Don't wire money to people or companies you don't know.
- Don't give your bank account number to someone who calls you, even for verification purposes.
- Don't click on links in an email to verify your bank account.
- Don't accept a check that includes an overpayment.

Ticket Scams

Ticket selling scams happen when a scammer uses tickets as bait to steal your money. The scammer usually sells fake tickets or you pay for a ticket, but never receive it. They are common when tickets for popular concerts, plays, and sporting events sell out. Scammers, including individuals and fake resale companies, take advantage of the situation by:

- Charging prices much higher than the face value of a ticket.
- Creating counterfeit tickets with forged barcodes and logos of real ticket companies.
- Selling duplicates of a legitimate ticket and emailing it to several buyers.
- Pretending to sell tickets online to steal your credit card information.

Report ticket scams

- Contact your state consumer protection office.
- Contact the Federal Trade Commission (FTC) using the Online Complaint Assistant.
- File a local police report, especially if you met the scammer in person or have a picture of him or her to give the police.
- File a complaint about a ticket company using the Better Business Bureau's Scam Tracker.
- If you paid by credit card, report the problem to the card company. You may be able to dispute the charge.

Do

- Buy tickets at the venue box office.
- Buy tickets from authorized brokers and third-party sellers, with verified contact information. Stub Hub, for example, allows third party sellers on their website.
- Verify that the seller has a real physical address and phone number. Scammers often post fake addresses, PO Boxes, or no address on their websites.
- Check the actual web address of the resale ticket seller. Some scammers create phony websites that closely resemble authentic ticket company websites.
- Search for negative reviews about the seller. Use the seller's name, email address, and phone number, along with the words "fraud", "scams", and "fake tickets" for your online search.
- Look at the tickets before you buy and verify the date and the time printed on them.
- Make sure the section and seat numbers on the tickets actually exist at the venue.
- Have the seller meet you in person in a public place for the ticket exchange.
- Ask the seller for proof that they bought the tickets, if you are buying from an individual.
- Use a credit card to pay third party sellers. Your credit card offers protections if you need to dispute a charge.
- Check for complaints against a ticket seller with your state's consumer protection agency.

Don't

- Don't wire transfer money to pay for tickets.
- Don't trust sellers who want you to pay with a prepaid money card.
- Don't pay before seeing the tickets.
- Don't meet an individual ticket seller alone or in a low-traffic area.Don't automatically trust online search results for ticket sellers. Search results can include paid ads, sellers that charge high fees, and scams.

Pyramid Schemes

Pyramid schemes are scams that require a constant flow of new participants to keep them going. They are marketed as multi-level marketing programs or other types of legitimate businesses. They use new recruits' required payments to provide "profits" to those participating longer. Pyramid schemes collapse when they run short of new recruits needed to pay earlier investors. These scams always fail—it's mathematically guaranteed.

Report Pyramid Schemes

- Your state consumer protection office or your state attorney general.

Do

- Be wary of "business opportunities" that require you to recruit more participants to increase your profit, or recoup your initial investment.
- Be wary if the company sells non-tangible products or technical services, rather than physical items.
- Independently verify the legitimacy of any business with the Better Business Bureau, your state attorney general, etc.
- Ask to see documents, such as financial statements audited by a certified public accountant (CPA), showing that the company generates revenue from selling its products or services to people outside the program.
- Be skeptical of success stories and testimonials of fantastic earnings.

Don't

- Don't invest until you've verified that the business is legitimate.
- Don't get involved in businesses that require you to recruit new participants.
- Don't buy into franchises that guarantee big profits quickly.
- Don't invest in any "opportunity" bearing warning signs of a pyramid scheme.

Lottery and Sweepstakes Scams

Prize scammers try to get your money or personal information through fake lotteries, sweepstakes, or other contests. Many claim that you've won a prize but must pay a fee to collect it. Others require you to provide personal information to enter a "contest." These scams may reach you by postal mail, email, phone call, robocall, or text message. State and local laws govern legitimate lotteries and sweepstakes. 43 states in the United States, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands sponsor lotteries to raise money for the state's programs. States that sponsor lotteries publish the results of their lotteries online, or broadcast them on television.

Report Lottery and Sweepstakes Scams

- Contact the Federal Trade Commission online or by phone at 1-877-382-4357.
- Contact a postal inspector if the scam uses U.S. mail to further its scheme. It doesn't matter if the scam notice arrived by phone or email.
- Report robocalls and unwanted telemarketing calls to the Do Not Call Registry.

Do

- Check the postage on a mailed prize notice. If it was sent bulk rate, it's probably a scam.
- Try to remember if you entered a particular contest. If you don't remember entering it, you probably didn't.
- Contact the actual company to verify a prize notice from an organization known to run a real sweepstakes.
- Register your phone number with the National Do Not Call Registry. You may register online or by calling 1-888-382-1222. If you receive telemarketing calls after registering, there's a good chance that the calls are scams.
- Report spam text messages to your mobile carrier, then delete them.
- Hang up on suspicious calls.

Don't

- Don't pay a fee, taxes, or shipping charges to receive a prize.
- Don't wire money to, or deposit a check from any organization claiming to run a sweepstakes or lottery.
- Don't provide your credit card number, bank account information, or other personal information.
- Don't believe anyone who says they're from the government or an official-sounding organization.
- Don't reply to, or click on any links in a spam text message.
- Don't attend a sales meeting to be eligible to win a prize.
- Don't give in to pressure to take immediate action.
- Don't believe anyone claiming to be from a foreign lottery or sweepstakes. It's illegal to enter foreign contests like these.

Tax ID Theft

Tax-related identity theft occurs when someone uses your Social Security number to get a tax refund or a job. You may not be aware of the problem until you E-file your tax return and find out that another return has already been filed using your Social Security number. If the IRS suspects tax ID theft, they will send a 5071C letter to the address on the federal tax return. Keep in mind, the IRS will never initiate contact with you by sending an email, text, or social media message that asks for personal or financial information. Watch out for IRS imposter scams, when someone contacts you saying he/she works for the IRS.

Report Tax ID Theft

- File a report with the Federal Trade Commission (FTC) at IdentityTheft.gov. You can also call the FTC Identity Theft Hotline at 1-877-438-4338 or TTY 1-866-653-4261.
- Contact one of the three major credit bureaus to place a fraud alert on your credit records:
  - Equifax: 1-888-766-0008
  - Experian: 1-888-397-3742
  - TransUnion: 1-800-680-7289
- Contact your financial institutions and close any accounts opened without your permission or that show unusual activity.
- Respond immediately to any IRS notice; call the number provided. If instructed, go to the IRS Identity Verification Service.
- Complete IRS Form 14039, Identity Theft Affidavit (PDF, Download Adobe Reader), print, then mail or fax.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.

Do

File your income taxes early in the season, before a thief can file taxes in your name. Also keep an eye out for any IRS letter or notice that states:

- More than one tax return was filed using your Social Security number.
- You owe additional taxes, you have had a tax refund offset, or you have had collection actions taken against you for a year you did not file a tax return.
- IRS records indicate you received wages from an employer unknown to you.

Don't

- Don't reply to or click on any links in suspicious email, texts, and social media messages. Make sure to report anything suspicious to the IRS.

Investment Scams

Investment scams prey on your hope to earn high returns on a regular basis, without financial risk.

Report Investment Scams

- File a complaint about an investment or an investment account with the Securities and Exchange Commission (SEC).
- Report pyramid or Ponzi schemes to the Federal Trade Commission (FTC).
- Report investment scams by companies that are licensed in your state to your state's securities administrator.

The SEC may forward your complaint to the investment company and request that the company reply. The FTC will not research your individual case of investment fraud.

Do

- Research investment opportunities and investment professionals with your state securities regulator and the Financial Industry Regulatory Authority.
- Learn where the investment and the investment professional are registered, whether in your state or with other regulators.
- Get all the details of an investment in writing, but still do your own research.
- Ask questions about costs, timing, risks, and other issues.

Don't

- Don't be pressured to invest immediately.
- Don't be influenced by promises that seem too good to be true, such as "guaranteed earnings" or "risk-free" investments
- Don't be swayed to invest in something because the investment professional is likable, seems trustworthy, or has credentials and professional titles.
- Don't feel pressured to invest because you were told that many other people with similar financial circumstances have invested.
- Don't feel obligated to invest because the professional gave you a free gift, lunch, or reduced commission fees.

Census Related Fraud

The U.S. Census Bureau collects data about the people and economy of the United States. It collects personal and demographic information from people and businesses. Some scam artists may pretend to work for the Census Bureau. They'll try to collect your personal information to use for fraud or to steal your identity. These scam artists may send you letters that seem to come from the U.S. Census Bureau. Others may come to your home to collect information about you.

Report Census Related Fraud

If you suspect fraud, report it to the Census Bureau's regional office for your state. Forward scam emails to the Census Bureau at ois.fraud.reporting@census.gov. =

Do

- Verify that the study is legitimate. Check the survey name on the Census Bureau's list of surveys .
- If someone comes to your home and claims to be a census worker, verify that they work for the Census Bureau.
- Look up the employee's name in the Census staff directory.
- Ask to see their badge. A Census Bureau badge has a picture of the field agent, a Department of Commerce watermark, and an expiration date.
- Follow these tips to help you spot census scams so you don't become a victim.

Don't

- Don't share your full Social Security number, bank or credit card account numbers, or your mother's maiden name. The Census Bureau won't ask for this type of information.
- Don't trust emails from anyone claiming to be from the Census Bureau. This agency sends letters to invite individuals to take part in its surveys. If you get an email from the Census Bureau, it's probably a scam.
- Don't trust caller ID. Call the Census Bureau's National Processing Center to verify a telephone survey.

Ponzi Schemes

A Ponzi scheme is a type of investment fraud that relies on money from new investors to pay "returns" to current investors. To keep the scam going, the scheme organizers must continually attract new investors and discourage current investors from cashing out. When they can't, the scheme collapses.

Report Ponzi Schemes

- The Securities and Exchange Commission (SEC).
- The Financial Industry Regulatory Authority.
- Your state's securities administrator.

Do

- Be wary of any investment that regularly pays positive returns regardless of what the overall market is doing.
- Avoid investments if you don't understand them or can't get complete information about them.
- Be alert to account statement errors, which may be a sign of investment fraud.
- Be suspicious if you don't receive a payment or have difficulty cashing out.

Don't

- Don't put your money in investments that promise big returns with little to no risk.
- Don't contribute to any investment that isn't registered with the SEC or with state regulators.
- Don't get financially involved with any unlicensed investment professional or unregistered firm.

Government Grant Scams

Government grant scammers try to get your money by guaranteeing a free grant to help you pay for college, home repairs, or other expenses. They ask for your checking account information so they can "deposit the grant money into your account" or withdraw a "one-time processing fee." In reality, the government rarely grants money to individuals. It's generally awarded to state and local governments, universities, and other organizations to pay for research and projects that benefit the public.

Report Grant Scams

If you think you've been a victim of a government grant scam, report it to the Federal Trade Commission. You can file a complaint with the FTC online, or call toll-free 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters fraud-related complaints into a database available to law enforcement agencies in the U.S. and abroad.
If you've paid a fee to learn about or apply for a government grant, you can report it to your state consumer protection office. The government does not charge for information or applications for federal grants.

Do

- Be wary of advertisements and calls about free government grants. These are usually scams.
- Register your phone number with the National Do Not Call Registry to reduce the number of telemarketing calls you receive. Register online at donotcall.gov or by calling 1-888-382-1222(TTY: 1-866-290-4236) from the phone number you wish to register.

Don't

- Don't give your bank account information to anyone you don't know.
- Don't pay any money for a government grant. You can get information about government grants for free at public libraries and online at Grants.gov. Government agencies don't charge processing fees for grants they've awarded.
- Don't believe callers who claim they're from an official-sounding government agency with news about a grant. Check out the name of the agency online or in the phone book—it may be fake.
- Don't assume a phone call is originating from the area code displayed on your caller ID. Some scam artists use technology to disguise their location and make it appear as if they're calling from Washington, DC.