



PROTECT THE
GOOD LIFE

Newly Updated

Recognize and Report Scams

Nebraska Attorney General's Office

Nebraska Attorney General's Office

Consumer Affairs Response Team

1445 K Street, Room 2115

PO Box 98920

Lincoln, NE 68508

(402) 471-2682

ProtectTheGoodLife.Nebraska.gov



Dear Fellow Nebraskans,

Nebraska is a state built on strong roots, caring communities, and a spirit of generosity. Sadly, scammers often try to take advantage of these very qualities, preying on the trust and kindness of our citizens. No age group is spared, and each year, our office hears from hundreds of Nebraskans who have been targeted by scams.

The best defense for preventing scams is education. By taking a moment to read this guide, you become part of a network of informed citizens taking action to prevent fraud.

If you have a question or concern, please call our Consumer Affairs Response Team at (402) 471-2682 and let us help. Our team is available to help Nebraska consumers identify the warning signs of a scam.

In the meantime, trust your instincts. If something seems too good to be true, it probably is.

Sincerely,

A handwritten signature in black ink that reads "Mike Hilgers".

Mike Hilgers
Nebraska Attorney General





Table of Contents

| | |
|--|----|
| Scams in Nebraska | 1 |
| Imposter Scams: An Overview | 2 |
| Romance Scams | 4 |
| Tech Support Scams | 5 |
| Government Imposter Scams | 6 |
| Family Emergency Scams | 8 |
| Business Imposter Scams | 9 |
| Social Media Scams..... | 10 |
| Identity Theft | 11 |
| Veterans Scams: Jeff's Story | 13 |
| Home Repair Scams | 14 |
| Cryptocurrency Scams..... | 15 |
| Online Shopping Scams | 17 |
| Best Practices for Charity Donations | 18 |
| Stopping Unwanted Calls..... | 19 |
| Tips for Buying a Car..... | 21 |
| If It Happens to You | 22 |
| Important Numbers and Websites | 23 |

Scams in Nebraska

According to the Federal Trade Commission, Nebraska ranks among the ten safest states in the country for identity theft and scams.

However, a large percentage of consumers under the age of 30 are losing money to scams, and scammers disproportionately target Nebraskans over the age of 60.

The following pages identify some of the more frequently reported scam complaints and, importantly, what you can do to prevent it from happening to you.



Imposter Scams: An Overview

What Are Imposter Scams?

Imposter scams are one of the largest categories of scams facing Nebraskans today. These scams have many different forms, but the methods used are often the same regardless of which imposter scam it is.

Imposter scams rely on your trust. It could be your trust in a tech support worker, a government official, or even a family member. The imposter scammer knows you are much more likely to make a payment or share personal information with someone you trust.

Imposter scams are evolving and becoming more sophisticated. With new technology, scammers can spoof caller ID, search social media for information about you, or even mimic the voice of a family member on the phone using artificial intelligence.

These scams may seem challenging to combat but can be avoided with common-sense tactics. The following pages explore types of imposter scams and how to avoid them.

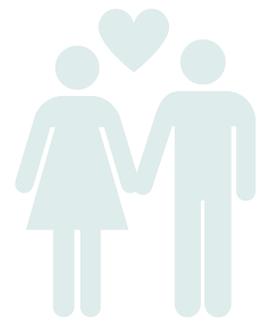


Protect Yourself from Imposter Scams:

- Ask a family member or friend for help if you are concerned about a scam.
- Trust your gut if a website, email, text, or phone call seems suspicious.
- Resist the urge to act quickly when someone requests money from you, even if they say it is an emergency.
- Never pay via gift cards, cryptocurrency, wire transfer, or by mailing cash to someone who reaches out unsolicited.
- Read reviews online of companies or individuals before sending money.
- Make sure your bank is set up to alert you of unusual activity.



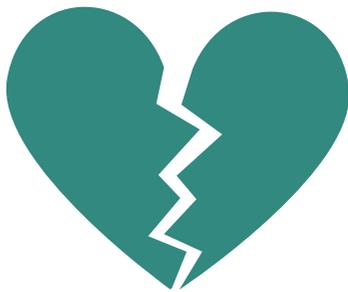
Avoid Romance Scams



What Is a Romance Scam?

Romance scams occur when a scammer, posing as an online or long-distance love interest, builds a false relationship to use their emotional influence to ask for money. The scammer is not only lying about their intentions, but they are typically using fake photos from someone else's account as well. The scammer usually disappears after money is sent or only hangs around in the hopes of scamming the same person again.

A Romance Scam Can Look Like:



- An online profile that looks too good to be true.
- A relationship that develops extremely fast compared to other relationships online.
- A love interest who only wants to communicate via text or a dating website, never video calls or in-person visits.
- Dire stories of emergencies or travel issues that prevent them from visiting you. They ask for money to address these emergencies with no intention of ever meeting.

How to Avoid a Romance Scam:

Ask to Video Chat

If you become invested in an online profile, ask to video chat early on, but be cautious.

Scammers can use hired actors to fake live chats.

Don't Send Money

Don't send gift cards, cryptocurrency, wire transfers, or mail cash to someone you have not met in person, even if they claim it is an emergency.

Do an Image Search

Take the photos from the dating profile and search them online to see if they are stock photos or photos taken from other profiles.

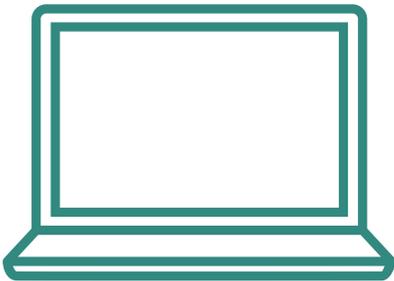
Stop Tech Support Scams



What Is a Tech Support Scam?

Tech support scammers may reach out through pop-up messages or phone calls. They pretend to be technicians from a trusted company who can fix a non-existent problem on your device. They might ask for remote access to your device, pretend to run a diagnostic test, and require payment to fix the "problem." What starts as a tech support scam can quickly escalate. The scammer may claim there are illegal files or activity on your device and ask for large sums of money to "protect you" from legal trouble.

Common Tactics of a Tech Support Scam:



- **Unsolicited Phone Calls:** Scammers call pretending to be from Microsoft, Apple, or another company, claiming your device has a serious problem.
- **Scary Pop-Up Messages:** A pop-up window appears urging you to call a number to fix an infected computer.
- **Urgency:** Scammers may tell you that your data or account is at risk to convince you to give them control of your devices or make payments.

What You Can Do:

- Regularly update your computer. If you need help, contact a local company.
- Ignore unsolicited calls, emails, or pop-ups claiming to be tech support.
- Reboot your device and disconnect from Wi-Fi if a suspicious pop-up appears.
- Contact companies directly through websites and numbers you know are accurate.
- Never allow remote access to your device unless you've verified the source.
- Don't send gift cards, cryptocurrency, wire transfers, or cash to pay anyone claiming you need urgent tech support.

Government Imposter Scams Checklist

What Are Government Imposter Scams?

These imposter scams rely on implicit trust in government authorities. The scammers, posing as government officials, will use fear and urgency to pressure you into making a payment or giving personal information. They may threaten you with a loss of benefits, a fine, or even jail time.



Do be wary of any unsolicited calls from government agencies. Distrust any message not delivered to you initially by U.S. Mail.



Don't trust Caller ID – it can be faked to look like a real agency.



Do verify claims by calling the government agency directly using an official number.



Don't share your Social Security number or Medicare ID with unexpected callers.



Do be wary if you're told to stay on the phone and not tell anyone.



Don't give payment information to anyone claiming to be from a government agency like the IRS, Social Security Administration, Medicare, or local law enforcement.



Do make sure your bank is set up to notify you of unusual activity.



Don't pay with gift cards, cryptocurrency, digital payments, wire transfers, or by mailing cash. Scammers prefer untraceable, hard-to-reverse methods.



Prevent Family Emergency Scams

What Is a Family Emergency Scam?

This scam, sometimes referred to as "the grandparent's scam," occurs when a scammer, posing as a family member or authority figure, calls with an urgent request for money.

How They Hook You:

The scammers may pretend to be an authority figure (i.e., a lawyer, police officer, or doctor) with an urgent financial need regarding a family member. They play with your emotions and claim you are the only one who can help. The scammer may also impersonate a family member. The scammer could say, "Grandma, it's me. Don't you recognize my voice?" They then wait for you to guess and volunteer a name.

Lines the Scammer May Use:

"I'm in trouble, and I need money fast – but please don't tell Mom or Dad."

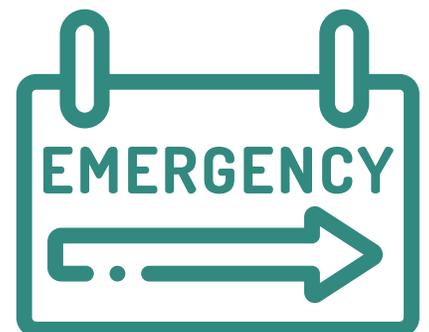
"I was in an accident/arrested and need bail money right away."

"My phone is almost dead. Just send the money now, and I'll explain later."

"The lawyer/police will explain everything. Please just talk to them."

What You Can Do:

- Resist the urge to act quickly.
- Hang up and contact the family member directly.
- Ask the caller questions a scammer isn't likely to know, such as "What did I give you for Christmas this year?" or "When is your birthday?"
- Talk to another family member. Don't keep it a secret.



Stop Business Imposter Scams

What Are Business Imposter Scams?

These imposter scams involve someone posing as an employee of a well-known business. They contact you first and rely on your trust in the company to gain access to your finances and personal information.

-  **Do** be wary of any unsolicited calls from a business. Most large businesses will not be reaching out to you unless you contact them first.
-  **Don't** accept a refund for an "overpayment" that you made. This is a scam.
-  **Do** contact the business directly using contact information from their official website to ensure you're speaking with the real company, not a scammer. This is especially important if you're told there's a problem with your order, a refund, or another urgent issue.
-  **Don't** pay for services with gift cards, wire transfers, cryptocurrency, or by mailing cash. Scammers request forms of payment that are hard to reverse.

What It Sounds Like:



"This is Amazon security. We've noticed a suspicious \$299 charge on your account. If you didn't authorize this purchase, press 1 now or stay on the line to speak with a representative about having this charge reversed."

Social Media Scams

What Is a Social Media Scam?

Scammers often use platforms like Facebook, Instagram, TikTok, X, and LinkedIn to trick users into providing personal information, sending money, or clicking on malicious links. Think twice before sharing information or responding to unsolicited messages online.

Common Examples:

- **Phishing Messages** – Scammers pose as friends, celebrities, or government officials, often using familiar accounts to trick you into trusting and believing their stories.
- **Fake Giveaways and Contests** – Scammers create fake promotions claiming users have won prizes and ask for personal or payment info to claim the reward.
- **Fake Job Offers** – Scammers post fraudulent job listings offering attractive positions and high salaries that require upfront payments or personal information.



Protect Yourself:

- Be wary of unsolicited messages. Verify the sender's identity before responding.
- Check the company's official website before participating in online giveaways.
- Don't share sensitive data like your Social Security number, bank information, or passwords on social media.
- Use a strong, unique password on your account and set up two-factor authentication.

Identity Theft: An Overview

What Is Identity Theft?

Identity theft occurs when someone fraudulently uses your personal identifying information to take out a loan, open accounts, obtain credit cards, get a tax refund, or do other things that involve impersonating you. Identity theft is a serious crime that can cause severe damage to someone's financial well-being and personal reputation if not taken care of promptly.

What Type of Information Is Used?

- Full name
- Address
- Email address
- Social Security number
- Driver's license number
- Credit/debit card numbers
- Bank account number
- Insurance information
- Birthday
- Passport number
- IP address
- Location information

How Often Does It Happen?

At times, the Federal Trade Commission receives over one million identity theft reports in a single year. The FTC estimates as many as 1 in 3 Americans could face identity theft in their lifetime.

Protect Yourself Against Identity Theft

Steps You Can Take:

- Create and place **complex passwords** on your bank, credit card, and phone accounts.
- Set up **two-factor authentication** on your accounts.
- **Secure your Social Security card**, and don't give out the number unless absolutely necessary.
- **Check your mail** every day to protect against mail theft.
- **Pay attention to billing cycles** and make sure your bills and financial statements arrive regularly.
- **Review** your credit card and bank account statements frequently to catch unauthorized transactions.
- **Don't give out personal information** to anyone over the phone, internet, or mail unless you initiated the first contact.
- Be aware of phishing schemes, and **don't click on links from pop-ups** or suspicious-looking emails.
- **Check your credit report regularly.** Review your reports for unfamiliar activity, especially recent inquiries that signal someone is using your credit.

Did You Know?

The Nebraska Attorney General's Office has a free consumer guide regarding identity theft available at ProtectTheGoodLife.Nebraska.gov.



Veterans Scams:

Jeff's Story



Jeff received a call from someone who claimed to work for the Department of Veterans Affairs. The caller stated they'd detected fraudulent activity on his account and suspended his monthly disability compensation until they could verify his information to determine eligibility. The caller asked Jeff for basic information like his name and address, as well as his Social Security number, monthly pay amount, and direct deposit information.

Jeff had an uneasy feeling after the call. He contacted the VA, who told him they had not originated the call. They confirmed everything was fine with his benefits.

Jeff realized he'd been talking to a scammer. He contacted his bank to redirect his monthly direct deposit to a new account. He placed credit freezes on his accounts with the three national credit reporting agencies to protect himself from identity theft. He also began routinely monitoring his account statements.



Protect Yourself from Home Repair Scams

What Are Home Repair Scams?

These scams occur when contractors accept payment but do not start or complete work as promised. Choose the right contractor to protect your home and wallet.

- Verify a contractor's credentials** with the Nebraska Department of Labor on their website at DOL.Nebraska.gov or by calling 402-471-2239.
- Don't sign contracts or make payments before verifying their license.**
- Get multiple estimates** from competing contractors before you decide. Be wary of suspiciously high or low bids.
- Make sure your estimate includes a deadline.** Keep a copy of the contract and your receipts.
- Negotiate a reasonable down payment.** Pay in full upon completion.
- Verify all claims made about insurance** coverage with your insurance company.



Did You Know?

You can cancel a contract within 3 business days if signed at home (and the seller initiated contact) or somewhere other than the seller's usual place of business.



Cryptocurrency Scams:

What you need to know

Cryptocurrency investment scams happen in Nebraska and can lead to substantial financial loss for consumers. These fake investment opportunities often appear legitimate, use convincing websites and testimonials, and promise high returns. Many times, consumers believe their investment is rapidly growing. As a result, they give additional funds to the scammer to chase even higher returns.

Sometimes, the scammer might initially build a romantic relationship with a consumer online to build trust before convincing them to invest. They exploit the excitement and confusion around cryptocurrency to pressure victims to act quickly, then disappear with the money.

Always remember, do not invest in what you do not understand. If you feel confused by cryptocurrency, consider other investments that you are more familiar with. If you are interested in investing, meet with a local financial expert in person.

If an investment feels too good to be true, trust your instincts – it's likely a scam.

Cryptocurrency Scams

The Warning Signs:

- **Unsolicited contact** – Someone you don't know reaches out first to offer a crypto investment opportunity. Legitimate investments are rarely initiated by strangers.
- **Confusing** – If the investment details feel confusing, step back. Scammers know that when you are confused, you are easier to manipulate.
- **Encrypted Apps** – Scammers may ask you to use encrypted apps like WhatsApp or Telegram to avoid being traced. Real financial experts don't do this.
- **Guaranteed Profits** – Scammers promise quick, high returns with little risk. All real investments carry some risk and grow gradually over time.
- **Romance + Crypto = Red Flag** – A romantic partner you've only met online asking you to invest in crypto is a huge warning sign. Trustworthy partners won't ask for money, especially early in the relationship.
- **No Access to Funds** – If you can't withdraw your funds or are asked to pay more to "unlock" them, this is a scam.

What to Do If You've Been Scammed:

- Stop all communications with the suspected scammer and block them.
- Don't send additional money, even to "unlock" funds.
- Document everything, including messages, screenshots, email addresses, crypto wallet addresses, and transaction records.
- Change passwords, enable two-factor authentication, and monitor financial accounts for unusual activity.

Report:

File a complaint with IC3.gov (FBI Internet Crime Complaint Center), the Federal Trade Commission (ReportFraud.ftc.gov), or the Securities and Exchange Commission (SEC).

If you shared financial information or transferred funds, contact your bank immediately.

Avoid Online Shopping Scams

Shopping online can be convenient, cost-effective, and gives you a wider variety of options. You can avoid most online shopping scams with a few common-sense tools.



There are three major ways to avoid online shopping scams:

Be Wary of Social Media

Many online shopping scams use social media. Do research before buying products advertised to you online.

Use Trusted Payment Types

Avoid paying with wire transfers or payment apps that are hard to reverse. Credit cards offer more protection.

Read Reviews

Read reviews both on and off their website. Search the company's name with the words "scam" or "fraud."

Additional Tips:

- Be suspicious of websites that appear unprofessional, have misspelled words, or look similar to other well-known companies.
- Be wary of unusually low prices. Check out similar products to find out a reasonable price range.
- Not all reviews are legitimate. If a product or company has only positive reviews, it could be a sign of fake reviews or that negative reviews have been deleted.
- Be careful sharing sensitive information. Legitimate online businesses won't ask for your bank account number. Make sure your bank notifies you of unusual activity.
- Double-check that ads posted on social media are legitimate. If a deal seems too good to be true or the seller is unfamiliar, research the company before purchasing.



Best Practices for Charity Donations

- Don't donate to a charity that doesn't have a professional-looking website or won't send you a brochure.
- Scammers ask for donations to organizations that sound like well-known charities. Contact the charity directly to verify.
- Ask what percentage of your donation goes directly to the cause. Legitimate charities give full details on how your donation will be used.
- Verify a charity through trusted watchdog sites like Give.org, CharityNavigator.org, or GuideStar.org.
- Ask the charity for their address, phone number, and a copy of their IRS tax-exempt status (IRS Determination Letter).
- Don't give money to a charity that claims you owe money you never promised.
- Don't donate to a charity to claim a prize.
- Don't assume all crowdfunding efforts on sites like GoFundMe are legitimate. Watch out for copycat fundraisers that may be illegitimate.

Stopping Unwanted Calls on a Cell Phone



Built-in Features

Cell phones come with the ability to block calls from specific numbers and unknown callers. See the following page for details.



Carrier-Provided Features

Carriers offer services to identify and block unwanted calls. Some services are free, others for a small fee. Check with your carrier for info.



Call-Blocking Apps

Free call-blocking apps are available. They may require access to your contacts or call history. Read the terms of service and privacy policy before installing.

Report It:

If you're still receiving unwanted calls, report them to these agencies:

Federal Trade Commission

1-877-FTC-HELP

(1-877-382-4357)

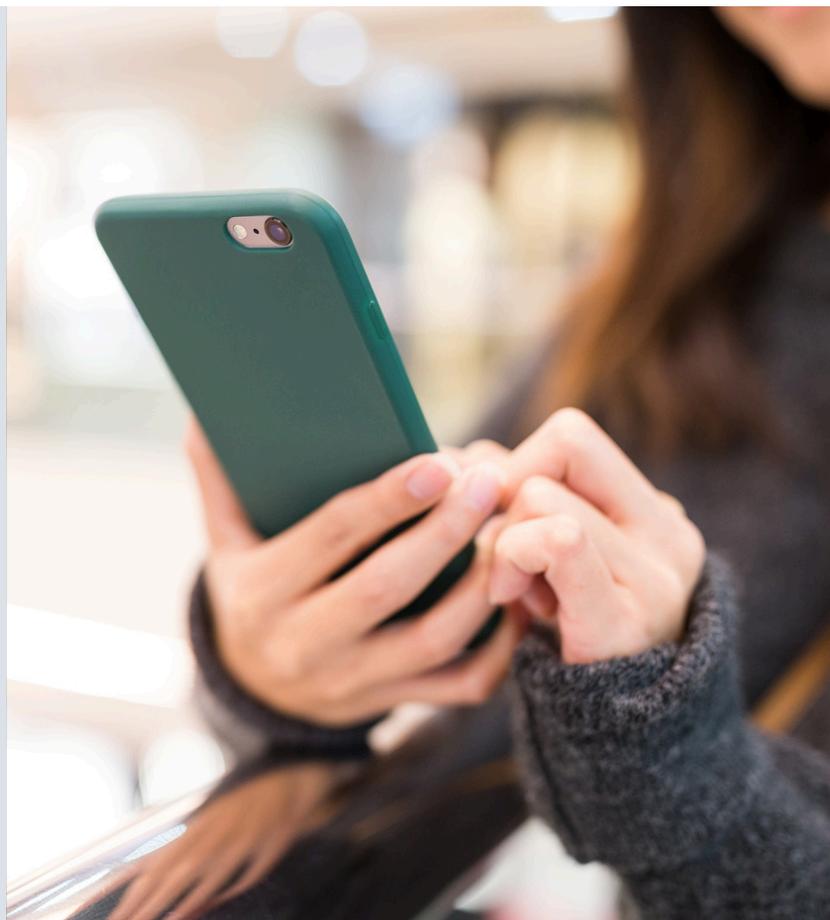
[ReportFraud.FTC.gov](https://www.reportfraud.ftc.gov) and [DoNotCall.gov](https://www.donotcall.gov)

Federal Communications Commission

1-888-CALL-FCC

(1-888-225-5322)

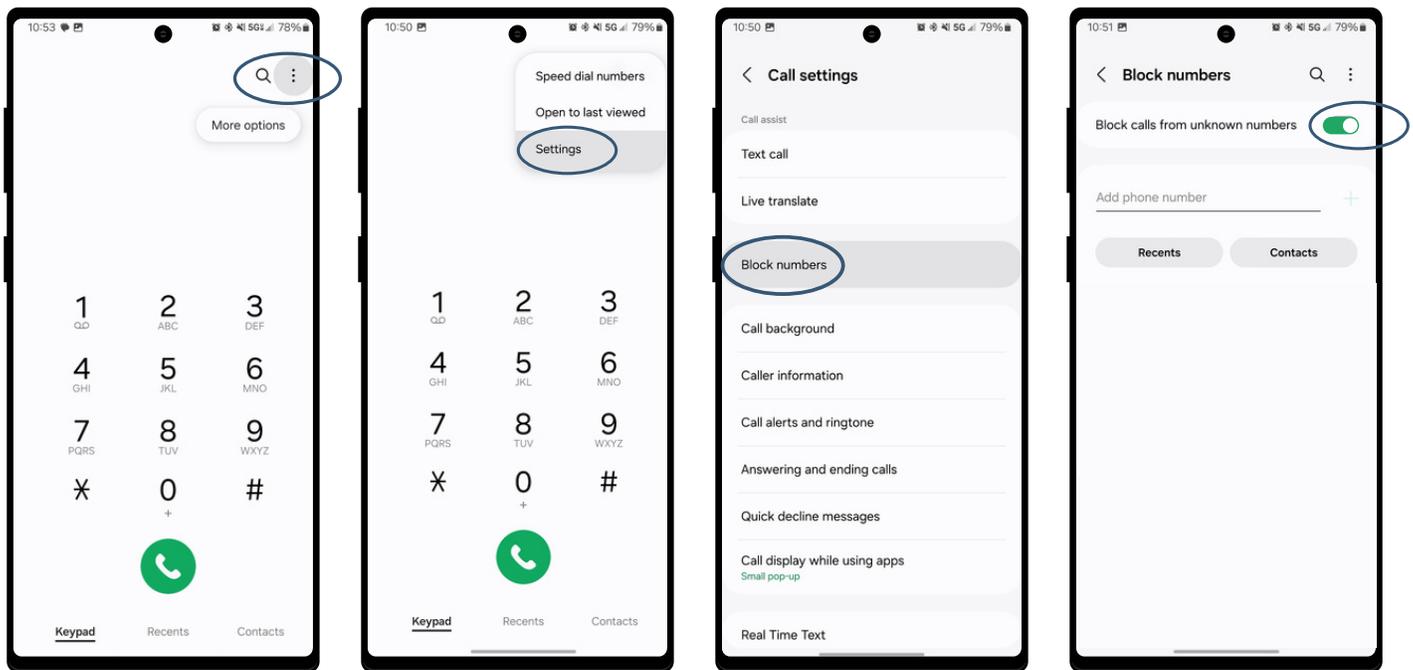
[ConsumerComplaints.FCC.gov](https://www.consumercomplaints.fcc.gov)



On iPhone iOS 18 and Newer



On Android



If you need assistance blocking unwanted calls on a landline or an older version of the iOS software on an iPhone, visit ProtectTheGoodLife.Nebraska.gov.

Tips for Buying a Car



- Buy from a reputable dealer or seller.** Read reviews online and ask for recommendations from family and friends.
- Look for the vehicle's buyer's guide.** It should be displayed prominently on or in the sale vehicle. It tells you some of the major problems consumers should look out for and whether the vehicle is being sold "as is" or with a warranty.
- Remember, "as is" used cars are exactly that:** if something breaks down in the future, it will be your financial responsibility.
- Get an inspection** from a trusted mechanic before purchasing a used car.
- Get a vehicle history report** on a used car to find out if the car has been in any accidents and has a clean title.
- Dealers should provide titles within 30 days and private sellers at the time of sale.** Verify the status and condition of the title before finalizing a sale.
- Ask detailed questions about financing and fees** before signing a loan.
- Look for the Truth-in-Lending disclosure** in your loan contract. Lenders are required to inform you what the cost of your loan will be, including all the following information: amount financed, Annual Percentage Rate (APR), finance charges, and total number of payments.
- Research Nebraska's Lemon Law and what qualifies.** Vehicles must be purchased new in the state, under warranty, and less than one year old when notice is sent to the manufacturer. The same problem must occur four or more times or have left you without use of the vehicle for 40 or more days.



If It Happens to You:

There is no shame in falling victim to a scammer. They are professionals and practiced in their craft. But don't suffer in silence. **Let someone know what has happened.**

If you've lost money, possessions, or other personal and valuable information, contact local law enforcement. If not, visit the Federal Trade Commission's website to report the scam at [ReportFraud.FTC.gov](https://www.reportfraud.ftc.gov).

You have a friend in the Nebraska Attorney General's Office. Submit the Scam Report attached in this guide by mail, online at [ProtectTheGoodLife.Nebraska.gov](https://www.ProtectTheGoodLife.Nebraska.gov), or call our Consumer Affairs Response Team during business hours at (402) 471-2682.

By reporting a scam, you could help identify fraud and protect yourself and others in the future. We want to hear from you!



Nebraska Attorney General's Office Scam Report Form

Return To:
Consumer Affairs Response Team
 PO BOX 98920
 Lincoln, NE 68509



Mike Hilgers
 Attorney General

Phone: (402) 471-2682 | Fax: (402) 461-0006 | Website: ProtectTheGoodLife.Nebraska.gov

| | | | |
|--|---------------------------------|----------------|---------|
| Reported By: | | | |
| Your Name: | | | |
| Your Address: | | | |
| City: | State: | ZIP Code: | County: |
| Phone Number: | | Email Address: | |
| Age: <input type="checkbox"/> 19 and under <input type="checkbox"/> 20-29 <input type="checkbox"/> 30-39 <input type="checkbox"/> 40-49 <input type="checkbox"/> 50-59 <input type="checkbox"/> 60-69 <input type="checkbox"/> 70+ | | | |
| Reported Against: | | | |
| Name of Business or Person: | | | |
| Business Address: | | | |
| City: | State: | ZIP Code: | |
| Phone Number: | Business Website/Email Address: | | |
| Name of Individual with whom you dealt: | | | |
| How were you contacted? | | | |
| Type of scam: | | Amount lost: | |
| Describe the Scam You Experienced: | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

The information given above is true to the best of my knowledge and belief. I authorize the Nebraska Attorney General's Office to send this report form to the federal reporting agencies. I understand that this report is a public record, but that it may be kept confidential by the Attorney General's Office under Neb. Rev. Stat. § 84-712.05(5) of the Nebraska Public Records Statutes, Neb. Rev. Stat. §§ 84-712 to 84-712.09. I also understand that the Attorney General's Office is not my private attorney.

 Signature _____
 Date

**Please enclose photocopies of any documents that may relate to your report.
 DO NOT SEND ORIGINALS.**

Important Phone Numbers



| | |
|---|---------------------|
| Nebraska Attorney General's Consumer Affairs Response Team | 402-471-2682 |
| State Unit on Aging | 402-471-2307 |
| State Health Insurance Information Assistance Program (SHIP) | 800-234-7119 |
| Senior Medicare Patrol (SMP) | 877-808-2468 |
| Adult Protective Services | 800-652-1999 |
| Better Business Bureau | 800-649-6814 |
| Contractor Registration Certificates | 402-471-2239 |
| National Do Not Call Registry | 888-382-1222 |
| Federal Trade Commission | 877-382-4357 |
| Federal Communications Commission | 888-225-5322 |
| U.S. Postal Inspection Service | 877-876-2455 |
| Free Credit Report | 877-322-8228 |
| Opt Out (Opt out of credit and insurance offers) | 888-567-8688 |



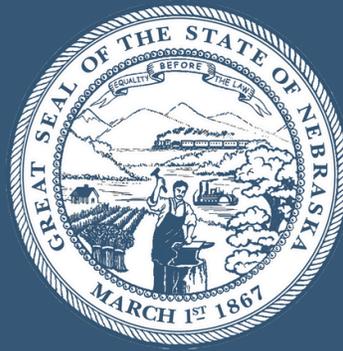
Important Online Resources



| | |
|--|--|
| Nebraska Attorney General's Main Website | AGO.Nebraska.gov |
| Nebraska Attorney General's Consumer Website | ProtectTheGoodLife.Nebraska.gov |
| State Unit on Aging | DHHS.NE.gov/pages/aging |
| National Do Not Call Registry | DoNotCall.gov |
| Better Business Bureau's Charity Registry | Give.org |
| Charity Navigator | CharityNavigator.org |
| Guide Star | GuideStar.org |
| Federal Trade Commission | FTC.gov |
| Free Annual Credit Report | AnnualCreditReport.com |
| Contractor Registration Verification | DOL.Nebraska.gov |
| Mail and Email Preference Service | DMAChoice.org |
| Opt Out (Opt out of credit and insurance offers) | OptOutPrescreen.com |
| Federal Motor Carrier Safety Administration | FMCSA.DOT.gov |

Questions?

Call us at (402) 471-2682 or send us an email at AGO.Consumer@Nebraska.gov.
If you would like to hear more, schedule a free educational presentation at ProtectTheGoodLife.Nebraska.gov.



Nebraska Attorney General's Office

Consumer Affairs Response Team

1445 K Street, Room 2115

PO Box 98920

Lincoln, NE 68508

(402) 471-2682

ProtectTheGoodLife.Nebraska.gov