A man with glasses and a beard, wearing a light blue denim shirt over a white t-shirt, sits on a light blue tufted sofa. He has his arm around a woman's shoulder. The woman, wearing a white and blue striped button-down shirt and blue jeans, is looking at a laptop. They are in a modern living room with a wooden shelf in the background holding books and a small potted plant. The text "PROTECT THE GOOD LIFE" is overlaid in the top left corner.

PROTECT THE
GOOD LIFE

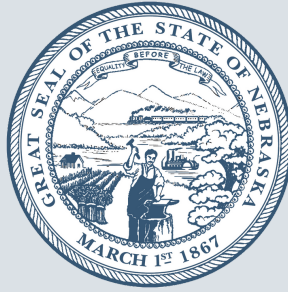
Recognize and Report Scams

Nebraska Attorney General's Office

Nebraska Attorney General's Office

Consumer Affairs Response Team
2115 State Capitol Building
Lincoln, NE 68509
(402) 471-2682

[ProtectTheGoodLife.Nebraska.gov](https://www.ProtectTheGoodLife.Nebraska.gov)



Dear Fellow Nebraskans,

We enjoy a state with strong roots, hard-working citizens, and plentiful resources. Given these strengths, it's no surprise to discover scam artists eagerly target and attempt to defraud us daily. While this is especially true within our state's senior population, Nebraskans of all ages report ongoing frustration and concern with scams.

Education is the best weapon we have in preparing people to protect themselves. This guide includes important information on recognizing and reporting scams if you or someone you know is subjected to one.

If you have a question or concern, please call our Consumer Affairs Response Team, and let us help. We're here to educate and protect you.

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
Puppy Scams: Sarah's Story	10
Identity Theft	11
Veterans Scams: Jeff's Story	13
Home Repair Scams	14
Moving Scams: Robert's Story.....	15
Moving Scam Red Flags	16
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

Nebraska fares favorably compared to most states for identity theft and scams, ranking among the ten safest states in the country according to the Federal Trade Commission.

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 often times the methods used are 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.



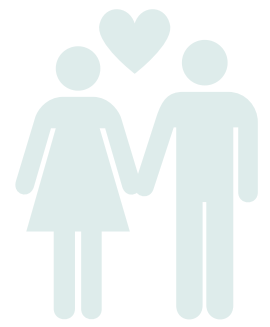
These scams may seem challenging to combat but can be avoided with common-sense tactics. The following pages explore types of imposter scams and how to avoid them.

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.



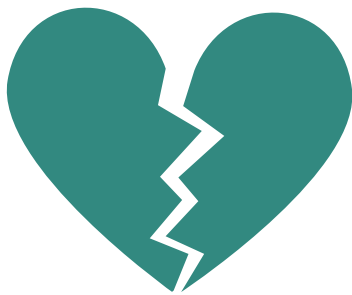
Avoid Romance Scams



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 that 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

Early in the relationship, if you become invested in an online profile, ask to video chat or set up a date in person.

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 taken from other profiles.

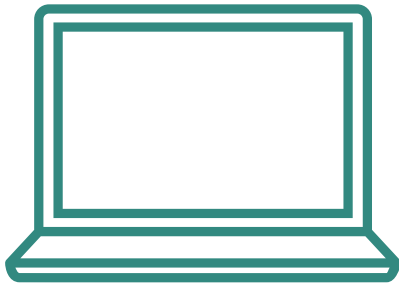
Stop Tech Support Scams



What Is a Tech Support Scam?

Tech support scammers reach out through pop-up messages and phone calls. They pretend to be technicians from a well-known company who can fix a non-existent problem with your computer. 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 computer and ask for large sums of money to "protect you" from legal trouble.

Common Tactics of a Tech Support Scam:



- **Phone Calls:** "Hi, this is Joe from Microsoft Tech Support. Your computer has been sending spam emails. We believe you have a virus we can remove."
- **Pop-Up Warnings:** A pop-up window appears on your computer, warning you about a security issue with a number to call for help.
- **False Advertising:** Scammers run phony online ads hoping you'll contact *them* for tech support only to be scammed.

What You Can Do:

- Seek recommendations from trusted people regarding computer repairs.
- Don't share payment info, or send gift cards, cryptocurrency, wire transfer, or mail cash to anyone who calls you with an urgent tech support issue on your device.
- Routinely update your computer's operating and security software. Contact a local company for help.
- Be skeptical if anyone offers you unsolicited computer repairs.

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 a government official. The government will always contact you by mail rather than by phone.



Don't trust the number on your caller ID without further verification. Your caller ID can be easily tampered with by scammers.



Do an internet search with the phone number or information from the suspected government agency along with the words "scam" or "fraud."



Don't give payment information to someone who contacts you claiming to be a government official.



Don't pay for services with gift cards, cryptocurrency, wire transfer, or cash. Scammers often request forms of payment that are hard to track and even harder to reverse.



Do let a family member or friend know your suspicions about a potential scam. Take your time to read reviews and ask around before paying for anything.



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



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, "Hi, Grandpa," assuming you have a grandson. If you ask, "John, is that you?" the scammer will say, "Yes!"

Lines the Scammer May Use:

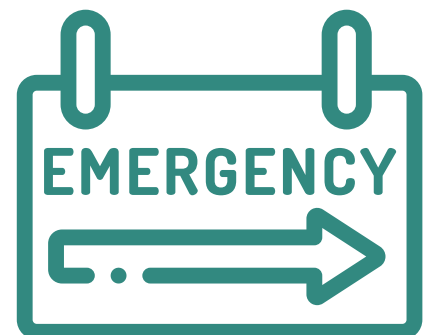
"Hi Mom. I got into a car accident, and the police officer arrested me. Can you send bail money right away?"

"Grandpa, I need help. I traveled to Mexico, and now a customs agent is saying I need to give them a thousand dollars to enter the U.S. again, and I don't have the money."

"Hi, it's your neighbor. I'm in the hospital. Can you help me pay for medical care?"

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 unsolicited 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 alleged "overpayment" that you made. This is a scam.
-  **Don't** pay for services with gift cards, wire transfers, cryptocurrency, or by mailing cash. Scammers often request forms of payment that are hard to reverse.
-  **Do** check with the business directly regarding a call about a wrong order, a refund due, or some other pressing issue. Search the company's contact information on their website to make sure you are not contacting a scammer.

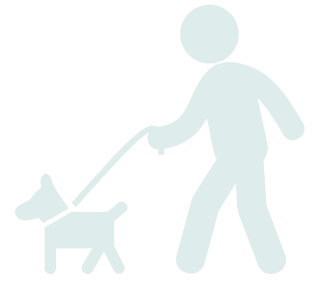
What It Sounds Like:



An email stating "it's time to renew your subscription" or "your subscription is about to expire" from a scam account posing as a well-known company.

"Hi, this is Walmart Customer Service. We are issuing a refund for your recent order. Log into your computer with remote access to verify."

Puppy Scams: *Sarah's Story*



Sarah found a great deal online for a puppy from a breeder several hours away. Typically, similar puppies sold for twice the price, so she felt like she needed to reserve one quickly. The breeder asked for a deposit for the last puppy in the litter.

Though Sarah was surprised the seller would only handle communication by email or online chat, she received so many adorable photos of her puppy that she ignored her uneasy feelings. The only forms of payment the seller accepted were wire transfers or a digital payment app. Once she paid, the breeder stopped responding. Her puppy was never shipped, and her payment was never refunded.

To avoid a pet scam, do your research on what your chosen breed typically costs. Verify the breeder's physical address, phone number, and meet them in person. Do not purchase a puppy sight unseen and use a credit card to make the purchase.



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.
- **Look for "https"** at the beginning of the URL to verify a web address has a secure connection.

Did You Know?

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



Veterans Scams:

Jeff's Story



Jeff received a call from someone claiming to work with 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 reverify his information to determine eligibility. The caller asked Jeff for basic information like his name and address, but also for 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 for the project. Keep a copy of the contract and your receipts.
- Negotiate a reasonable down payment. Pay in full only when the project is complete.
- Verify all claims made about insurance coverage with your insurance company.
- You have the right to cancel a contract within three days if you signed it at your home or at a contractor's temporary location.





Moving Scams: *Robert's Story*

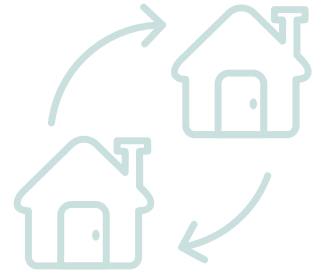
Robert was moving to a new state to take a new job, so he found movers online. He entered information on a website, and an employee gave him an estimate on the phone.

The moving company arrived and loaded his items. Once they loaded Robert's things on the truck, they hit him with the real price of the move and asked for a large deposit upfront. If Robert didn't pay, they threatened to sell what was on the truck to cover the contract. Robert had sold his house and had no choice but to pay the deposit.

It took weeks for the moving company to arrive. When they finally did arrive, the balance due had increased again due to "unforeseen costs." The moving company refused to unload the truck without being paid in cash. Robert noticed many items either missing or broken when the truck was unloaded.

The best way to avoid a moving scam is to get several estimates, preferably one that is binding, meaning the price quoted is the amount you pay. Pay by credit card, not cash, and only upon delivery, not upfront.

Moving Scam Red Flags



Moving scams have been reported in Nebraska. Many times, a scam moving company does not deliver the items at all, and the consumer is at a loss for the majority of their household possessions. The company may also deliver items broken or with pieces missing. A scam moving company will claim you owe them more than you originally agreed to. Here are some red flags of moving scams:

- The moving company's website has no local address or DOT number.
- When you call the mover, they answer with generic names like "moving company" instead of a specific company name. They may have a generic email address.
- The moving company gives you a price without an onsite inspection.
- The company requires you to pay with cash, wire transfers, or money orders.
- The moving company arrives with a rental truck, not a company-owned vehicle.
- They may make unsolicited calls to push you into quick decisions.
- The mover attempts to get you to sign blank documents before loading your goods.

Tips for Researching a Moving Company:

Tip 1

Do your research and visit [FMCSA.DOT.gov/Protect-Your-Move](https://www.fmcsa.dot.gov/Protect-Your-Move)



Tip 2

Use the Federal Motor Carrier Safety Administration's website to search the registered mover database. You can even search by state to see a list of moving companies in Nebraska, how many trucks they have, complaint history, and more.

Report:

If you encounter a moving scam, report it to the FMCSA at 1-888-368-7238.

Avoid Online Shopping Scams

Shopping online can be convenient, cost-effective, and give 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:

Use Secure Websites

Look for "https" at the beginning of the website URL to ensure it is encrypted and secure. This protects your personal info.

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 don't appear professional, have misspelled words, or look similar to other well-known companies.
- Be wary of suspiciously 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.
- If you are shopping from a link posted on social media, double-check that the website is legitimate.



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.com, or GuideStar.org.
- Ask the charity for their address, phone number, and a copy of their IRS tax-exempt status.
- 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



Register Your Numbers on the National Do Not Call Registry
1-888-382-1222 or online at DoNotCall.gov

Ask Your Phone Company about Custom Calling Features
Many companies offer features to help reduce unwanted calls.

Unwanted Calls on Your Landline?

Dial These Star Codes:

Selective Call Rejection (*60) - Allows you to program your phone to block unwanted calls from numbers placed on your rejection list.

Anonymous Call Rejection (*77) - Stops your phone from ringing when callers have blocked their number.

Selective Call Acceptance (*64) - Allows you to limit incoming calls to a preapproved list of phone numbers.



Consider a Call-Blocking Device

These devices come with a spam call database, so you can block hundreds of calls instantly on your landline. They can reject calls shown as private, international, unknown, or fake numbers. Some permit you to block a state, area, or international country code.

Call-blocking devices are available at major retailers and online.

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.



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)



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 buyers 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 in clear terms 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.

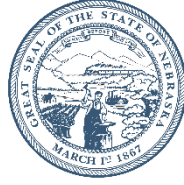
You have a friend in the Nebraska Attorney General's Office. Submit the Scam Report attached in this guide by mail, online at ProtectTheGoodLife.Nebraska.gov, or call our Consumer Affairs Response Team during business hours at (402) 471-2682

By reporting a scam, you could help identify fraud, bring them to justice, 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 Office	402-471-2682
Nebraska Attorney General's Consumer Affairs Response Team	800-727-6432
State Unit on Aging	402-471-2307
State Health Insurance Information Program (SHIIP)	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





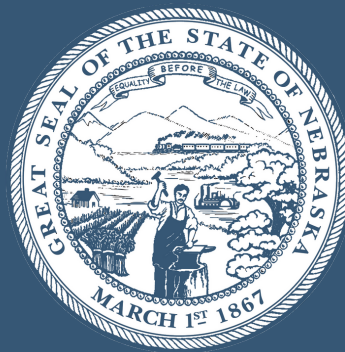
Important Online Resources



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
2115 State Capitol Building
Lincoln, NE 68509
(402) 471-2682

ProtectTheGoodLife.Nebraska.gov