If you suspect you're the victim of a scam or identity theft...
don't be afraid or embarrassed to talk about it with someone you trust. You are not alone, and there are people who can help. Doing nothing could only make it worse. Keep these phone numbers and resources handy so that you can turn to the appropriate authority, including the local police or your bank (if money has been taken from your accounts).

Fraud Assistance Resources & Information

The Federal Trade Commission (FTC): This federal agency collects information about ongoing scams to share with law enforcement and the public.

FTC Consumer Response Center
1-877-382-4357 • *www.ftc.gov*

FTC Identity Theft Hotline
1-877-438-4338 • *www.consumer.ftc.gov*

Office of the Iowa Attorney General – Consumer Protection Division: This division of the Iowa Attorney General's Office protects Iowa consumers from fraud; educates consumers about current scams and how to avoid becoming a victim; and ensures fair marketplace competition.

515-281-5926 • *www.iowaattorneygeneral.gov/for-consumers*

Federal Bureau of Investigation (FBI) Internet Crime Complaint Center: This is the complaint center within the FBI. Use their online resources found at the website below to report internet fraud, file a complaint, or read the latest warnings.

www.ic3.gov

U.S. Postal Inspection Service: This division of the U.S. Postal Service (USPS) investigates mail fraud and scams. Call or visit the below website to report identity theft or scams that involve U.S. mail.

1-877-876-2455 • *www.postalinspectors.uspis.gov*

U.S. Department of Health and Human Services (HHS), Administration on Community Living: This federal agency is responsible for community support for older Americans and individuals of all ages with disabilities. Contact this organization for more information on elder services and assistance in your area.

1-800-677-1116 • *www.eldercare.gov*

Social Security Administration — Fraud Hotline: This agency is responsible for responding to the various Social Security needs of the American people. Contact this organization to report theft or fraudulent use of your Social Security Number.

1-800-269-0271 • *www.oig.ssa.gov*

Better Business Bureau — BBB Scam Stopper: Use the Better Business Bureau Scam Stopper website to look up businesses to ensure a reputable track record, report scams, and read about new and top scams.

www.bbb.org/council/bbb-scam-stopper

****REMEMBER**** ***If you believe you or someone else is in immediate danger, always call 911.***

CONGRESSMAN DAVID YOUNG
Working for the People of Iowa's 3rd Congressional District | *Young.House.Gov*

FRAUD & SECURITY ALERT

U.S. House of Representatives
Washington, DC 20515
PUBLIC DOCUMENT
OFFICIAL BUSINESS
This mailing was prepared, published and mailed at taxpayer expense.

David Young M.C.
PRSRT STD

IMPORTANT SECURITY INFORMATION FOR IOWANS

Iowa Congressman David Young

IOWA CONSTITUENT SERVICES OFFICES:

Council Bluffs	(712) 325-1404
Creston	(641) 782-2495
Des Moines	(515) 282-1909
Washington, DC	(202) 225-5476

Young.House.Gov

PROTECT YOURSELF FROM SCAMS & FRAUD

A SPECIAL REPORT ON FRAUD PROTECTION FROM CONGRESSMAN DAVID YOUNG

Dear Friend:

As founder of the Bipartisan Congressional Task Force to Combat Identity Theft and Fraud, it is my mission to find solutions to protect your personal security, identity and bank account. In this special report, you will find important information and resources to protect you against fraud and theft.

It is also my hope the official website of my Congressional task force—*IDTaskForce-Young.House.Gov*—will empower you and your family with information and resources to prevent identity theft and fraud, and keep you informed about the threats and scams facing many Americans.

Remember, you can always contact our bipartisan task force to share a story or report a scam to help educate our neighbors in Iowa.

I encourage you to visit *IDTaskForce-Young.House.Gov* to learn more about the information, resources, and services available to you.

Sincerely,

David Young
Member of Congress

TOP TEN TIPS TO PROTECT YOURSELF:

1. As Iowans, we want to be available for friends, and loved ones, but ***if you don't recognize a phone number, don't answer the phone.*** Let the caller leave a message. Often, scammers call just to see if someone answers the phone. Just saying "hello" can make you a target.
2. In our great state, we're known for being "Iowa Nice," but ***don't hesitate to hang up the phone if the person on the line is trying to pressure you*** into a deal or giving away your personal information. If someone claims to be with the government, tell them you need to speak to your loved ones first, or the Iowa Attorney General's Office. ***Ask them for a phone number where you can call them back.***
3. The government, companies, and financial institutions will never ask you to provide payments in the form of gift cards—***never buy a gift card to pay off supposed debts or payments someone claims you owe.***
4. ***When shopping online always use a credit card and not a debit card***—credit cards have safeguards in place to help you get your money back if someone steals your information while debit cards do not.
5. ***If a deal sounds too good to be true, it probably is.*** You can often save yourself from falling victim to a scam by doing a quick search online to see if it checks out.
6. I've heard from Iowans about folks coming to their homes claiming they're with the IRS or Medicare. These agencies very rarely come to a person's house. ***If you're unsure of who's at the door, don't answer it***. Ask for official identification, or tell them you'll call their office and set up a time that works better for you.
7. As Iowans, we're respectful of our friends' and neighbors' privacy. Equally important to us is protecting them from harm. If they tell you about a deal, someone they met online, or other questionable activity, ***never shy away from asking your loved ones for more information***—you may save them from falling victim to a scam. We all have to work together and look out for one another to stop fraudsters and scammers.
8. ***If you get questionable offers or deals in the mail, contact your local postal inspector.*** Postal inspectors can help combat scams and fraud sent through the mail. Learn more at *www.postalinspectors.uspis.gov*.
9. Arming yourself with knowledge of current scams is key to fighting off identity thieves. ***Visit my website www.IDTaskforce-Young.House.Gov for periodic updates*** on the common fraudulent activity in our communities.
10. ***Remember, you have a friend in this fight.*** If you are ever unsure of where to go or what resources are available, don't hesitate to contact me! You can find my contact information by visiting *Young.House.Gov*.

DATING AND ROMANCE SCAMS

Known as "catfishing," in this scam, a con artist targets you through a dating website, app, or through social media platforms. The thief may appear as a suitor or admirer, someone looking for a friend, or sometimes a lonely active duty service member looking for a connection back home. Once a relationship with you is established, which may occur after a long period of time, the con artist usually asks for money for an emergency or business idea, before ending all contact with you.

Top Targets:
- Everyone

How to Protect Yourself:
Always be careful when interacting with others over the internet, and be extra cautious when someone requests money from you, for any reason. A simple search of the individual may point to a legitimate web presence, but it's also a good idea to conduct an image search to help determine if photos are genuine. Also, if you decide to ever meet the individual in person, take care to tell your family or friends, and always meet in a public place.

GET RICH QUICK SCAMS

Whether you get an unsolicited offer to invest in something with unbelievable returns, a business opportunity requiring minimal effort for maximum reward, or even if you win an outrageous prize or sweepstakes which you don't remember entering—if it sounds too good to be true, it probably is.

Top Targets:
- Everyone

How to Protect Yourself:
Be mindful of alerts or notices announcing unexpected money or winnings, for these can sometimes be an easy way for scammers and fraudsters to steal your personal or bank account information. If you are offered a business opportunity by mail, online, or by phone—double check with the Better Business Bureau that it is a reputable organization. Be wary of unsolicited offers or investment opportunities, and always thoroughly research the seller to ensure the legitimacy of their claims. If you deem the seller is genuine, make sure to research the investment thoroughly before handing over your money.

TRAVEL SCAMS

In these scams, con artists will target you with unbelievable travel deals, typically bundled as packages. These sham companies will usually require you "act now!" or will have a quickly approaching deal expiration, requiring you to book your travel without adequate research or investification.

Top Targets:
- Families
- Students

How to Protect Yourself:
Always research the companies with whom you seek to do business, especially if they are unfamiliar companies or organizations. It is usually a good idea to check with the Better Business Bureau before taking any action to book a trip.

IRS SCAMS

Phone calls from criminals impersonating IRS agents remain an ongoing threat to all taxpayers. Scam artists call and threaten taxpayers with arrest, deportation, and license revocation, among other things, if they don't provide payment over the phone.

Top Targets:
- Everyone

How to Protect Yourself:
Remember, the IRS, or any other federal agency, will never contact you demanding payment over the phone. If you receive a call like this, hang up and call the IRS Treasury Inspector General for Tax Administration hotline: 1-800-589-3718. The IRS will also never call you to discuss a tax situation or ask for personal information without first mailing you a notice or bill. Question if the caller is really from the IRS and record the employee's name and badge number. Then, hang up and call the IRS at 1-800-366-4484 to verify if the caller is truly an IRS employee with a legitimate need to contact you.

GIFT CARD SCAMS

This type of scam can come in many different forms, and occurs when the con artist asks for money through iTunes gift cards or other gift cards. Usually, the caller poses as a federal agent, such as one from the IRS, or a grandchild or child needing money because they're in trouble.

Top Targets:
- Seniors
- Students

How to Protect Yourself:
Always be wary of anyone asking for money in the form of gift cards or wire transfers. Not only will federal agencies never contact you to demand payment by phone, they will never ask you to purchase gift cards and provide serial numbers, or wire transfers, as a form of payment. Scammers use this technique because gift cards are often untraceable and once you provide the serial number, you cannot get your money back.

CHARITY SCAMS

In this scheme, donations are solicited for fake charities, often after major natural disasters. Scammers succeed by tugging at your heartstrings and taking advantage of your desire to help those in need.

Top Targets:
- Seniors

How to Protect Yourself:
Never make donations over the phone, no matter how nicely the caller may ask. No charity will run a phone-only fundraiser, so ask the caller to send you more information. If it's a legitimate organization, this won't be a problem.

FINDER'S FEE / INVESTMENT SCAMS

Here, the con artist calls and tells you they have found a large sum of money and they are willing to split it with you if you make a "good faith" payment by withdrawing funds from your bank account. Similar scams peddle outrageous and unbelievable investment schemes, sometimes even from a foreign business partner looking for your help in an opportunity, or to claim an inheritance or foreign prize winnings. Often, a second con artist is involved, posing as a lawyer, banker, or similar official to request your bank account number, or a wire transfer.

Top Targets:
- Seniors

How to Protect Yourself:
Remember, if an "opportunity" sounds too good to be true, it probably is. Never give unknown individuals information about your bank account, credit card, or even numbers from prepaid debit or gift cards. If you are thinking about investing and have any questions, do not hesitate to call the U.S. Security and Exchange Commission's Office of Investor Education and Advocacy at 1-800-732-0330.

SOCIAL MEDIA SCAMS

In these scams, con artists use social media websites such as Facebook, Twitter, LinkedIn, or Instagram to target you and your friends. These can come in the form of fake accounts, fake online surveys or contests, online discount scams, and more.

Top Targets:
- Seniors
- Students

How to Protect Yourself:
Fake accounts of real businesses may offer deals or discounts, but they exist to steal your personal information. Double-check the company's official website to ensure the social media profile is real, or look for a "verified" check mark next to the account name to confirm it is legitimate. Scammers can also post links in comment sections which drive you to surveys, contests, and more. Before you can access the content you're seeking, the website requires you to enter personal information. Don't enter this information—that's the prime opportunity for scammers and fraudsters to steal from you.

HOME IMPROVEMENT SCAMS

In these scams, con artists posing as home improvement professionals will come to your home, offering services to improve your lawn, repair your roof or driveway, and more. By asking a reasonable price, these "professionals" may seem like commonsense hires, but be wary of anyone going door to door soliciting their home improvement services.

Top Targets:
- Seniors
- Families

How to Protect Yourself:
While you may need a home improvement professional or contractor to complete some of the projects around your home, seek references from family and friends to ensure a job well done. Always get an estimate and contract in writing, and check with the Better Business Bureau if you're unfamiliar with their work or company. And, if you're simply unsure of someone knocking on your door—don't open it! If they need to contact you for legitimate reasons, they will find another way.

MILITARY PERSONNEL SCAMS

Beware of scams targeting military members and their families. In these scams, con artists may pose as U.S. Department of Veterans Affairs (VA) employees and ask for the military member's personal information. Other scams include phony security systems marketed towards families of active duty service members, guaranteed military loans with hidden fees and high interest rates, fake housing deals for military members, and more.

Top Targets:
- Military Members
- Families

How to Protect Yourself:
Before agreeing to purchase any good or service from a company, check with the Better Business Bureau to ensure a reputable track record. Be wary of unsolicited deals or offers and don't be afraid to check with family and friends before taking any next steps. Also, keep in mind that federal agency employees, including individuals from the VA, will not contact you by phone to demand payment.

PHISHING/VISHING SCAMS

In these scams, victims receive a call or email telling them to call a customer service telephone number, or visit a website to "fix a problem" with their bank or credit account. The phone number and website are fake. Victims are prompted to enter their bank account numbers, credit card numbers, and personal identification numbers (PIN), or even their passwords, to gain access to their account.

Top Targets:
- Seniors
- Students

How to Protect Yourself:
Do not respond to any suspicious emails, phone calls, or voice mails which request personal or financial information, especially ones which use pressure tactics or prey on fear. If you have reason to believe a financial institution actually needs information from you, call the institution yourself using a number you have on file or in the phone book—do not use the information the email or phone call provides. Also, do not click on a link in an email or social media message supposedly sent by a financial institution. Fraudsters have been known to create fake websites to trick their victims. While a linked website looks real, it likely isn't—so don't click the link.

LOTTERY SCAMS

Phony lotteries and sweepstakes use the promise of an unbelievable prize or payout to steal your hard earned money. Scammers often use this approach to target you by phone, direct mail, or even online.

Top Targets:
- Everyone

How to Protect Yourself:
If a prize or payout sounds too good to be true, it probably is—be mindful and question winning any contests or sweepstakes you do not remember entering. Lotteries and legitimate sweepstakes also never require you to pay a fee in order to collect your winnings.