


ARVEST ADVENTURES PRESENTS: SCAMS, FRAUD AND IDENTITY THEFT



Carolyn Grieve, Adventure Coordinator-Arvest Bank

COMMON SCAMS TO AVOID

- ❑ Telephone/text Phishing scams
 - ❑ IRS scams
 - ❑ Grandparent/Warrant scams
 - ❑ Lottery and Sweepstakes scams
 - ❑ Tech support scams
 - ❑ Door to door solicitation/ Home Improvement
 - ❑ Mail Scams
- 

TELEPHONE/TEXT PHISHING SCAMS


Examples:

- ❑ Car warranty- un-solicited offers for things you've never purchased.
- ❑ Home warranty- Must renew now or home won't be covered.
- ❑ Zelle, Apple Pay, CashApp, Banks- Un-solicited or unexpected texts, email, or phone call. Account has been compromised. Accounts you don't even have!
- ❑ Charitable organizations- Could be legitimate, but better to donate through company website.

In November 2021, the financial industry reported actual instances where scammers pretended to be from the fraud department and may even have used spoofed phone numbers to impersonate them to trick customers to act.



WAYS TO AVOID TELEPHONE/TEXT PHISHING SCAMS


- ❑ Know what you have and what you don't have (home warranties and car warranties)
 - ❑ Never use provided links in texts or emails. Always go to the actual website and get phone numbers and contact information.
 - ❑ Only go to the actual website for charitable organizations.
 - ❑ Don't rely on caller ID for verification. Phone numbers are commonly spoofed.
- 

INSURANCE AND MEDICAID FRAUD

- ❑ Debt collectors trying to get payment for services not received.
- ❑ Debt collectors trying to get payment for items not owed.
- ❑ Medical collections notices on credit report that aren't yours.
- ❑ Emails from Medicaid and Social Security requesting account access.
- ❑ Emails requesting transfer of funds (for safe keeping).



HOW TO AVOID INSURANCE AND MEDICAID SCAMS

- ❑ Know your bills and services.
 - ❑ Contact providers directly for payment.
 - ❑ Insurance and Medicaid will not request access to bank account.
 - ❑ These entities usually send letters unless you have requested emails or texts.
 - ❑ Don't click on links in emails or texts, instead contact the companies directly.
 - ❑ Shred all mail and documentation that may include personal identification information such as SSN or Policy numbers
- 

SOCIAL SECURITY SCAMS

As of June 2021, Social Security phone scams are the #1 type of fraud reported to the Federal Trade Commission and Social Security. Over the past year, these scams misleading victims into making cash or gift card payments to avoid arrest for Social Security number problems have skyrocketed. Social Security encourages you to report phone scams to disrupt the scammers and help them reduce this type of fraud, and to reduce the number of victims.



Social Security employees will occasionally contact you by telephone or mail for business purposes **if** you have ongoing business with the agency. However, Social Security employees will not:

- Tell you that your Social Security number has been suspended.
- Contact you to demand an immediate payment.
- Ask you for credit or debit card numbers over the phone.
- Require a specific means of debit repayment, like a prepaid debit card, retail gift card or cash.
- Demand that you pay a Social Security debt without the ability to appeal the amount you owe,
- Promise a Social Security benefit approval, or increase, in exchange for information or money.

Remember that Social Security employees will never threaten you. If there is a problem with your Social Security record, Social Security will mail you a letter. If Social Security needs you to submit payments, the agency will provide instructions in the letter, including options to make those payments.

AVOIDING SOCIAL SECURITY SCAMS

Scammers are using regular mail delivery to send fraudulent letters on SSA letterhead, advertising the recipient to call a toll-free number to activate an increase in SSA benefits, such as a cost-of-living adjustment (COLA). The letters appear to be from an SSA official and are on SSA letterhead.

COLAs are automatic and do not require any kind of activation. THIS IS A SCAM!

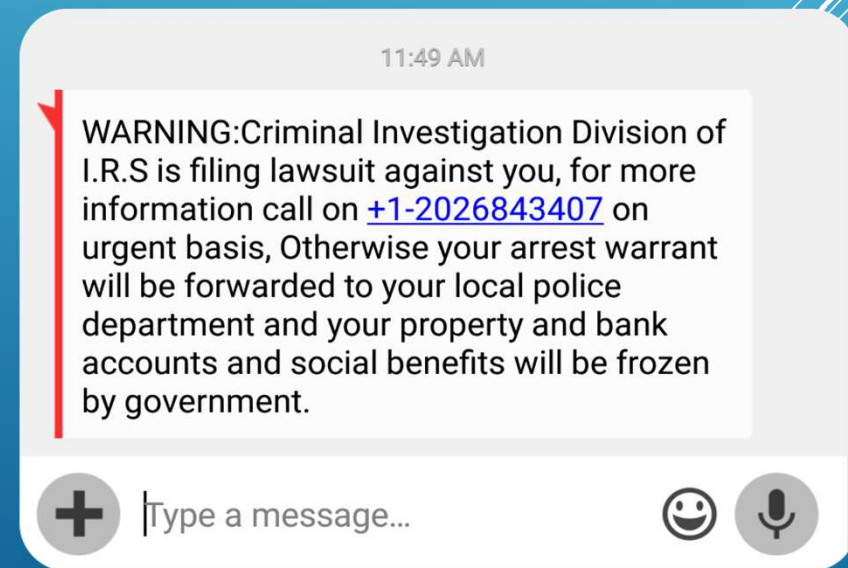
Scammers frequently change their approach, trying new tactics and messaging to trick people. Stay up to date with SSA and Alert for scammers.

Call Social Security Admin. 1-800-772-1213 or the local Social Security office in Fayetteville 1-877-694-5493 if you have any received unexpected mail, emails or calls.


IRS SCAMS

- ❑ Phone call saying you owe back taxes and will be arrested.
- ❑ Text saying the same thing
- ❑ Tax returns filed in your name, but it wasn't you.
- ❑ Emails that look official, but you're not expecting.
- ❑ Demanding payment or you'll be arrested.

Most recently (October 2021) Fake IRS email to claim your Economic Impact Payments



AVOIDING IRS SCAMS


- ❑ IRS will/can only contact you through mail.
 - ❑ The IRS doesn't threaten to arrest you.
 - ❑ The IRS doesn't demand immediate payment.
 - ❑ The IRS doesn't require money orders or prepaid gift cards.
 - ❑ Don't click on links in texts or emails.
 - ❑ Scammers will use spoofed numbers, so call the IRS direct for any questions.
- 

GRANDPARENT/ WARRANT SCAMS



- ❑ These scams are similar and use the same premise.
- ❑ Your grandchild has a warrant or had been arrested and needs bail money.
- ❑ You have a warrant and will be arrested immediately unless you pay your fines.
- ❑ Suspects always try to make the situation urgent...MUST ACT NOW!!!

HOW TO AVOID GRANDPARENT/WARRANT SCAMS


- ❑ Know your own history and know your family.
 - ❑ Jail is not the gulag...they can wait awhile to go through the proper channels.
 - ❑ Jail's and bondsman don't take money orders and prepaid gift cards.
 - ❑ Contact the police or Sheriff's office direct to confirm the accusation. Don't use provided numbers and links.
 - ❑ Some scammers will actually meet in person. Never go alone and always alert police to this kind of activity.
- 

LOTTERY/SWEEPSTAKES SCAMS



- ❑ They offer to give you an advance on winnings you've won.
- ❑ They claim you need to pay a percentage to claim your winnings.
- ❑ If you agree to put money in foreign accounts for safe keeping, then they'll pay you an advance on you're millions.
- ❑ They will ask for bank account information or want to wire money so you can "claim" your winnings.

HOW TO AVOID LOTTERY/SWEEPSTAKES SCAMS

- ❑ If you didn't enter...you didn't win!!!! Nothing in life is free.
 - ❑ No lottery gives you an "advance" on winnings.
 - ❑ It's illegal for a lottery to advertise to put money in foreign banks.
 - ❑ Never click links on texts or emails.
 - ❑ Never give bank account information over the phone or internet.
 - ❑ Never take wire transfers or pay for items with gifts cards.
- 

TECH SUPPORT SCAMS



- ❑ While on your computer or phone a screen pops up. Malware, virus, anti-virus protection, or even software is out of date.
- ❑ Phone calls saying your computer is infected with a virus.
- ❑ They will provide links or request remote access to fix your computer.
- ❑ They will request credit card or banking information to pay for services.

HOW TO AVOID TECH SUPPORT SCAMS

- ❑ Never click on links on pop-ups, emails, or texts.
- ❑ Never give our credit card or banking information.
- ❑ Click the “X” on any pop ups and run a third party anti-virus software such as AVG or Norton.
- ❑ If you clicked on links than malware could already be installed trying to obtain sensitive information. Contact a local computer professional to clean computer.

POSTAL MAIL SCAMS

- ❑ Offers of products, services, or work from home that seem too good to be true.
- ❑ Unexpected checks in the mail that all you have to do is cash them and send a portion.
- ❑ Investment opportunities that have above average returns.
- ❑ Letter threatening action on civil or criminal charges for things you know nothing about.

Note: Since Covid we've seen a serious increase in scams, mail theft and fraud, particularly around Christmas time when checks are being sent to Children and Grand-Children – if you mail a check be sure to write it with Gel Ink – not Ballpoint.

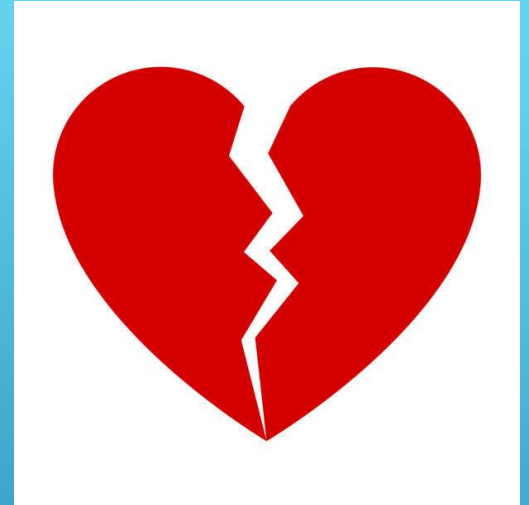


HOW TO AVOID POSTAL MAIL SCAMS


- ❑ If it seems too good to be true...it is.
- ❑ Never deposit or cash checks that you don't know the sender. The bank will hold you responsible.
- ❑ Check out products and companies on official websites like Better Business Bureau and State's attorney general's office.
- ❑ If there is doubt you can bring it by the local PD and we can take a look.

ROMANCE SCAMS

- ❑ One of the most common and highest losses for Bella Vista.
- ❑ Can start with a random text, email, or phone call.
- ❑ This person will live in another state or be out of the country on business.
- ❑ This person will be wealthy, but since they're out of state they don't have access to their own bank account.
- ❑ They will require payment in gift cards or Bitcoin.
- ❑ Plane tickets can only be purchased through their agent.
- ❑ No matter how much money is spent they never show up.




HOW TO AVOID ROMANCE SCAMS

- ❑ If you're going to date or search online, use reputable sites. Don't talk to unsolicited people.
 - ❑ In 2021 everyone has access to their bank accounts around the world with the touch of a button.
 - ❑ Scammers are the only people that require prepaid gift cards.
 - ❑ This scam is VERY common, don't let embarrassment keep you from reporting it.
 - ❑ Almost all of these scams originate overseas and that is where your money is sent. Very little chance of getting it back.
 - ❑ When possible, talk to people face to face and don't carry on digital relationships.
- 

Beware of Mortgage Scams

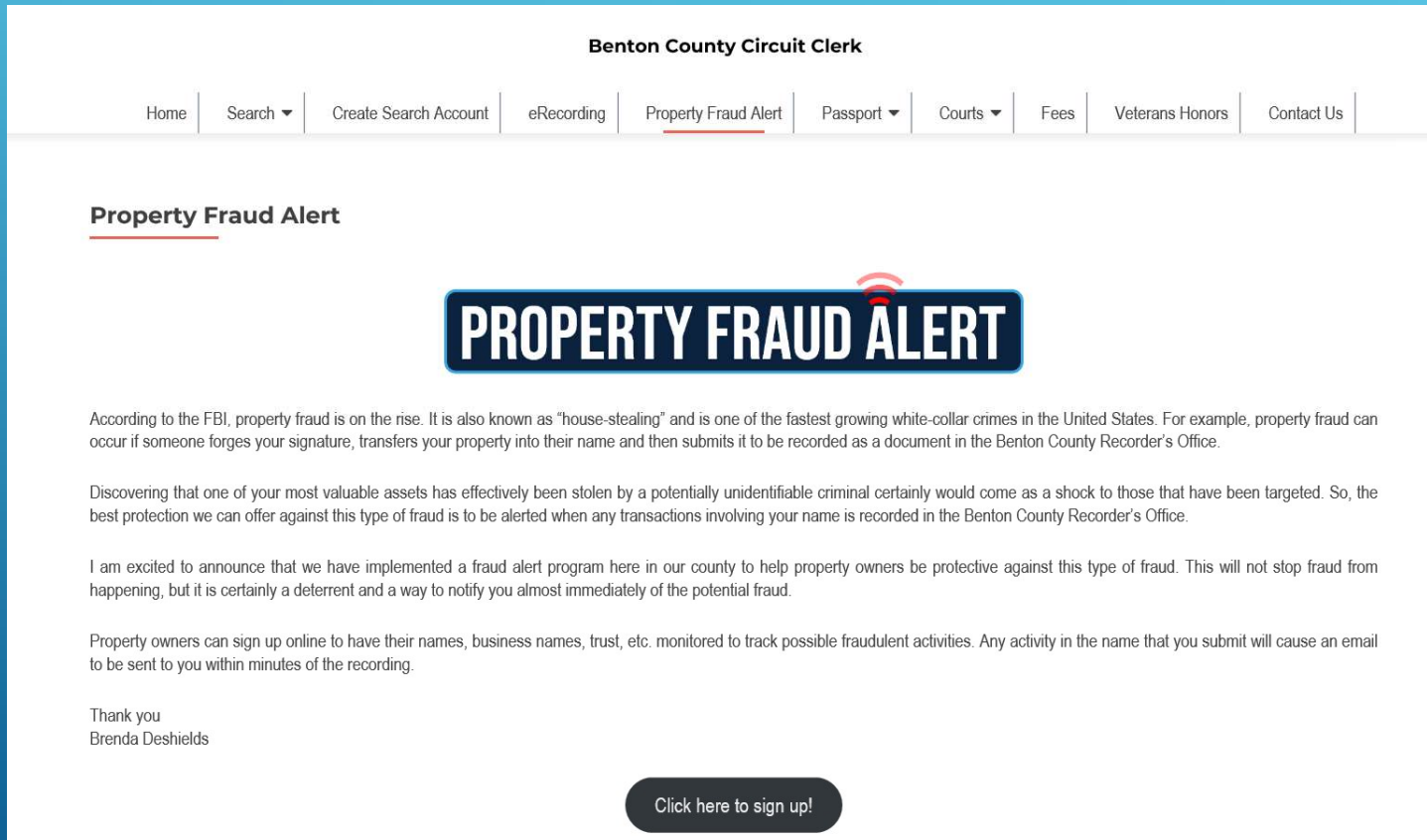
- ❑ Lease-Back or Repurchase Scams promise to pay off your delinquent mortgage, repair your credit and possibly pay off credit cards and other debt. However, in order to do this, you must “temporarily” sign over your deed – trouble is, you have signed over all rights to your property trusting it will be signed back to you. After the scammer takes ownership, he can legally evict you.
- ❑ Partial Bankruptcy Scams – the scammer asks you to give partial interest in your home to one or more persons, you then make mortgage payments to the scammer in lieu of paying the delinquent mortgage or seek new financing. However, the scammer does not pay the mortgage. Each holder of partial interest in your property files bankruptcy without your knowledge causing a delay in foreclosure, which your property is headed for and the scammers have a steady stream of income.
- ❑ Refinance Scams – look out for people posing as mortgage brokers or lenders offering to refinance your loans so you can afford the payments – the scammer presents you with “foreclosure rescue” loan documents to sign, you are told these documents will bring your loan current. What you don’t realize is you are surrendering your home. The “loan documents” are Deed Transfer documents and the scammer counts on your not reading them.
- ❑ Internet & Phone Scams convince you to apply for a low-interest mortgage by phone or internet, extracting personal information such as SSN and bank account numbers. The loan gets approved immediately and you sending wire transfers to the phony company the whole time thinking you are making payments toward your new loan.

HOW TO AVOID MORTGAGE SCAMS

- Know you're dealing with. If you're not sure check with Better Business Bureau or the State Consumer Protection Office .
 - Know what you're signing.
 - Get promises in writing.
 - Make your mortgage payments directly to your lender or the mortgage servicer.
 - Never sign over the deed until you clearly understand what will happen to our rights to your home.
 - Report suspicious activity.
- 

OTHER RESOURCES:

- www.bentoncircuitclerk.com and then there's a tab at the top entitled "Property Fraud Alert".



The screenshot shows the website for the Benton County Circuit Clerk. At the top, there is a navigation menu with the following items: Home, Search (with a dropdown arrow), Create Search Account, eRecording, Property Fraud Alert (underlined in red), Passport (with a dropdown arrow), Courts (with a dropdown arrow), Fees, Veterans Honors, and Contact Us. Below the navigation menu, the page title is "Property Fraud Alert" with a red underline. In the center of the page, there is a large, dark blue rectangular button with the text "PROPERTY FRAUD ALERT" in white, bold, uppercase letters. Above the button is a small red Wi-Fi signal icon. Below the button, there are three paragraphs of text. The first paragraph explains that property fraud is on the rise and is also known as "house-stealing". The second paragraph states that the best protection is to be alerted when transactions involving your name are recorded. The third paragraph expresses excitement about the new fraud alert program. At the bottom left, there is a "Thank you" message from Brenda Deshields. At the bottom center, there is a dark blue button with the text "Click here to sign up!".

Benton County Circuit Clerk

Home | Search ▼ | Create Search Account | eRecording | Property Fraud Alert | Passport ▼ | Courts ▼ | Fees | Veterans Honors | Contact Us

Property Fraud Alert

PROPERTY FRAUD ALERT

According to the FBI, property fraud is on the rise. It is also known as "house-stealing" and is one of the fastest growing white-collar crimes in the United States. For example, property fraud can occur if someone forges your signature, transfers your property into their name and then submits it to be recorded as a document in the Benton County Recorder's Office.

Discovering that one of your most valuable assets has effectively been stolen by a potentially unidentifiable criminal certainly would come as a shock to those that have been targeted. So, the best protection we can offer against this type of fraud is to be alerted when any transactions involving your name is recorded in the Benton County Recorder's Office.

I am excited to announce that we have implemented a fraud alert program here in our county to help property owners be protective against this type of fraud. This will not stop fraud from happening, but it is certainly a deterrent and a way to notify you almost immediately of the potential fraud.

Property owners can sign up online to have their names, business names, trust, etc. monitored to track possible fraudulent activities. Any activity in the name that you submit will cause an email to be sent to you within minutes of the recording.

Thank you
Brenda Deshields


[Click here to sign up!](#)

DOOR TO DOOR/HANDYMAN SCAMS

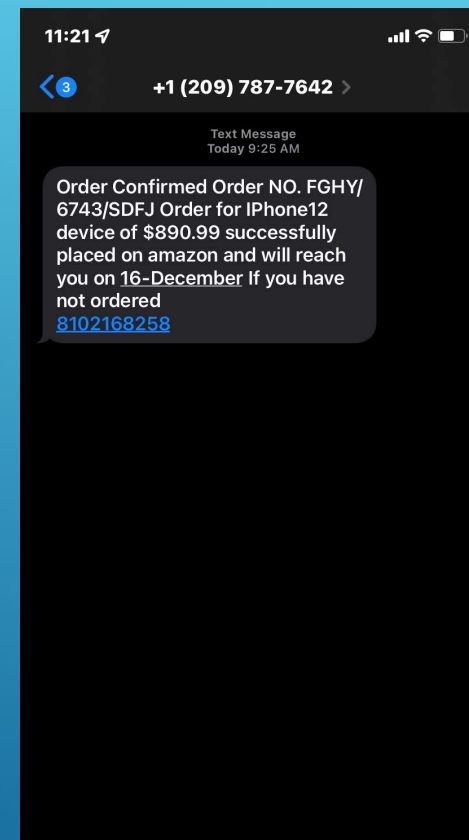
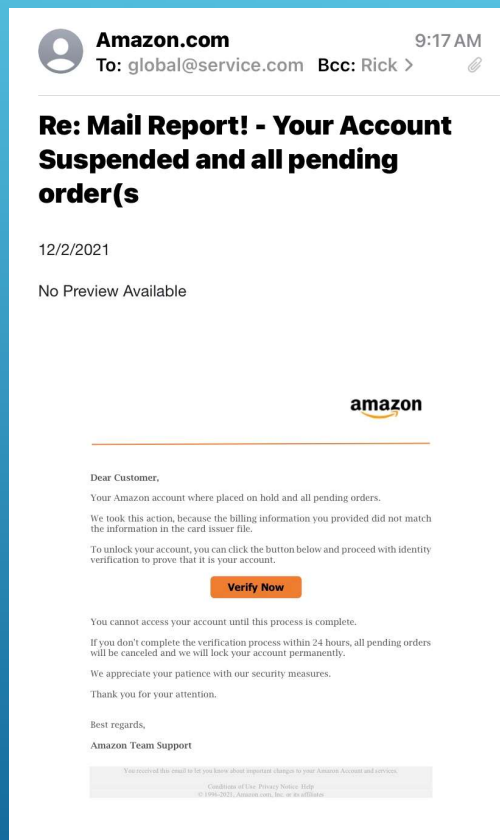
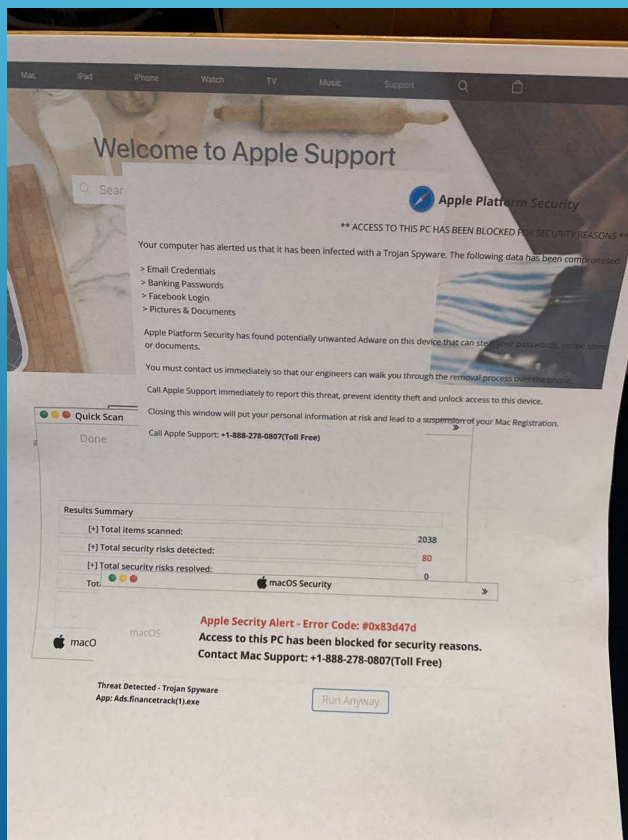
- ❑ People come to your door offering roofing, landscaping, handyman, driveway repair, chimney repair, or magazine sales.
- ❑ Usually want to do the work right away and may even use neighbors as a reference.
- ❑ High pressure sales tactics to intimidate you and make you afraid to say no. May insist on payment up front.
- ❑ They don't provide references or written quotes for the work to be performed.
- ❑ Does anyone remember the August 3 Scam Alert in Bella Vista? warrants were issued for 4 people for scamming an elderly Bella Vistan with Dementia.



HOW TO AVOID DOOR TO DOOR/HANDYMAN SCAMS

- ❑ Just say NO! If they keep pressuring you...call the police.
 - ❑ Insist on references, written quotes, and time to research the company.
 - ❑ Never pay for any work in advance...ever!!!
 - ❑ Take a couple days to make any decisions.
 - ❑ Refuse to hire them if they don't provide the proper paperwork (quotes, references, ect.).
 - ❑ If you already hired them and then discovered you've been scammed, then contact the police.
- 

COMMON SCAMS – DON'T FALL FOR THEM OR ANYTHING LIKE THEM



HOW DO SCAMMERS KNOW SO MUCH? WHERE ARE THEY GETTING THEIR INFORMATION?

- ❑ Social Media Profiles and posts – we've all seen the "Cute" surveys on social media: "if you were a dog, what name would you have?" "What is your best friend's name?" "What's the best H.S. mascot?"
- ❑ Accepting Friend requests from people you do not know
- ❑ Dumpster Diving
- ❑ Fraudsters pretending to be someone you know-Spoofing
- ❑ Mail Theft
- ❑ Shoulder Surfing
- ❑ Pre-texting (responding to surveys from someone you don't know
- ❑ Skimmers – on ATM.s Gas Pumps and other Self Serve equipment

HOW TO REPORT SCAMS

- ❑ Social Security- 1-800-269-0271
- ❑ Postal Inspector- 1-877-876-2455
- ❑ Internet scams- [Reportfraud.FTC.gov](https://www.reportfraud.ftc.gov)
- ❑ Identity theft- [Identitytheft.gov](https://www.identitytheft.gov)
- ❑ Attorney General's office- 1-800-482-8982
- ❑ Bella Vista Police Department- 479-855-3771



NOTE: By not reporting fraud it enables fraudsters to continue taking advantage of others

IDENTITY THEFT

- ❑ You're not getting your normal mail.
- ❑ You receive bills for things never purchased.
- ❑ IRS informs you that you already filed your taxes.
- ❑ Credit report has strange entries.
- ❑ Contacted by debt collectors.
- ❑ Unknown transactions on banking statements.
- ❑ 7-Categories of Identity theft include: Financial which makes up 1/3 of all fraud, Criminal, Medical, Social Security, Drivers License, Synthetic and Child – 2/3 of whom are under age 7
- ❑ According to FTC there were 4.8 Million reports of Fraud and ID Theft in 2020



NOTE: not all ID theft is financial, it can have you arrested, or it can be deadly. A case on file tells about a healthy woman who never used her insurance but someone was able to steal her identity and use her insurance. Their trip to the hospital set up a health record for the rightful owner using the criminal's blood type. When the victim was rushed to the hospital following a car accident and received a blood transfusion of the wrong blood type it killed her. Another instance of ID Theft has a person arrested for criminal activity that was committed by someone who stole their identity.

THINGS TO DO WHEN IDENTITY IS STOLEN

- ❑ File a police report.
- ❑ Contact postal inspector.
- ❑ Subscribe to a third-party monitor like Life-Lock or ID Protect which is available to most Arvest Customers.
- ❑ Check your credit reports often.
- ❑ File taxes as soon as possible.
- ❑ Review bank statements often to catch theft early.
- ❑ Put fraud alerts on bank and credit card accounts.

Question: have you wondered why children are one of the most targeted classes of ID Theft?

Answer: Children are often given SSN's at an early age but typically don't use them or check their credit reports until they secure their first job or enter college.

OTHER TOOLS IN THE THIEF'S TOOLBOX

- ❑ **Credit and Debit Cards** – At restaurants, cards are often taken out of your view long enough for a waiter, waitress or other staff to take pictures of front and back for future unauthorized use or even sold on the dark web. Skimmers can be hard to detect and allow thieves to read your card information from a remote location. Use a Credit card instead of a debit card, at least the money tied up will belong to the credit card company instead of you – it can take 10 days – 2 weeks to resolve card theft.
- ❑ **Malware** – Know your wi-fi source, never connect to public wi-fi or use public USB charging outlets always use a power plug.
- ❑ **Break-ins** – always put valuables out of sight before you arrive at your destination – recent reports of stolen purses and car break-ins can lead to all kinds of fraud.
- ❑ **Postal** –If you plan to write checks use the Uniball 207 Gel Ink pen to prevent washed checks, never put a check in your mailbox with the flag up, always take them to the inside box at the post office where they can't easily be fished out of the box with a long stick and duct tape.