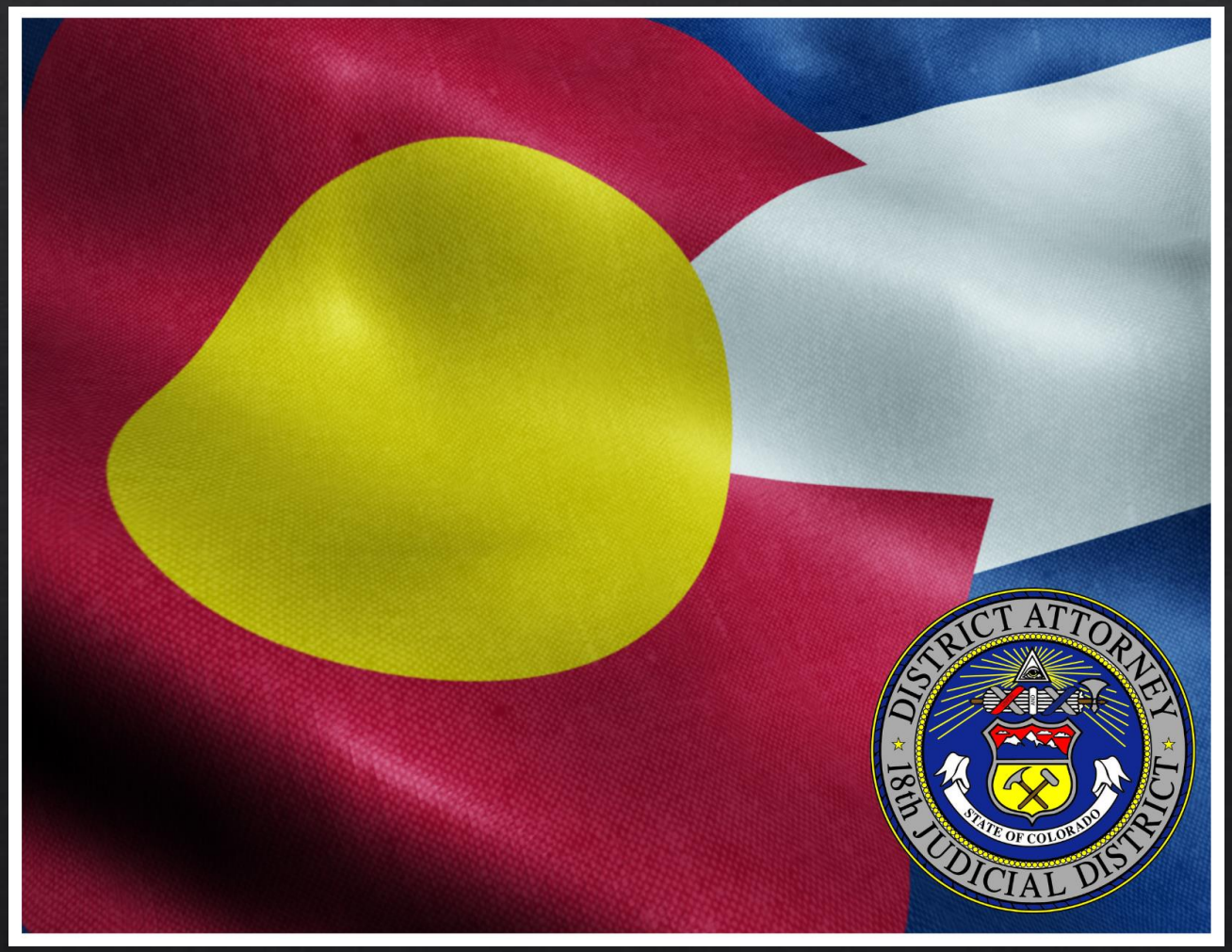
Office of the District Attorney
18th Judicial District

Senior Safety Saturday

Consumer Fraud and Exploitation Protection

September 20th, 2025

US Census Bureau: Age 60 and Over



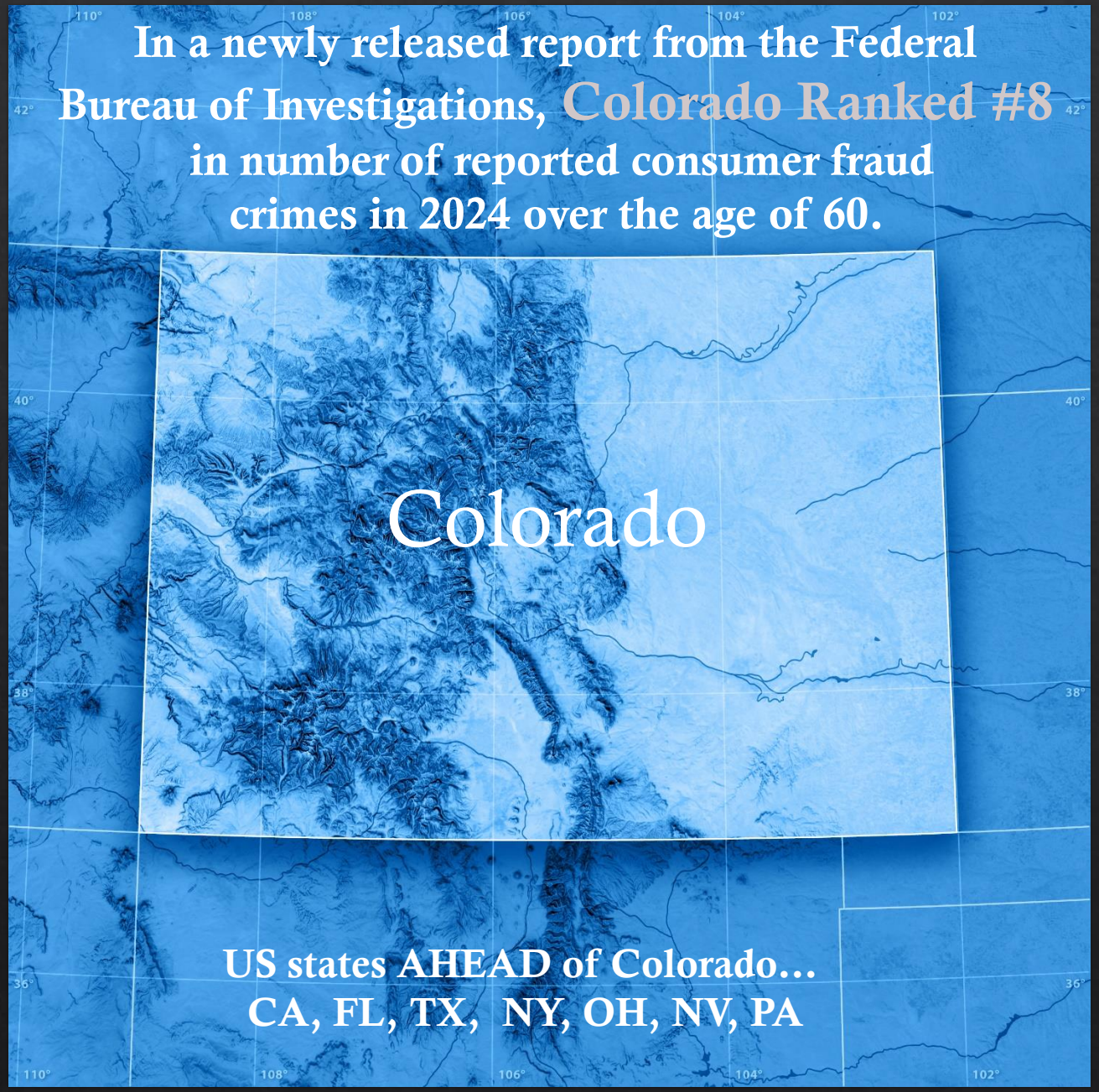
18th Judicial District

Arapahoe County – 128,680

Douglas County – 66,941
Elbert County – 7,040
Lincoln County – 1,467
Total – 204,128

State of Colorado

Total – 1,201,048



Fraud Does Not Discriminate!

Seniors, children, individuals, businesses are all targets, regardless of age, education or income.

Our senior population is often the most vulnerable demographic.

Reasons Why Seniors Are Targeted

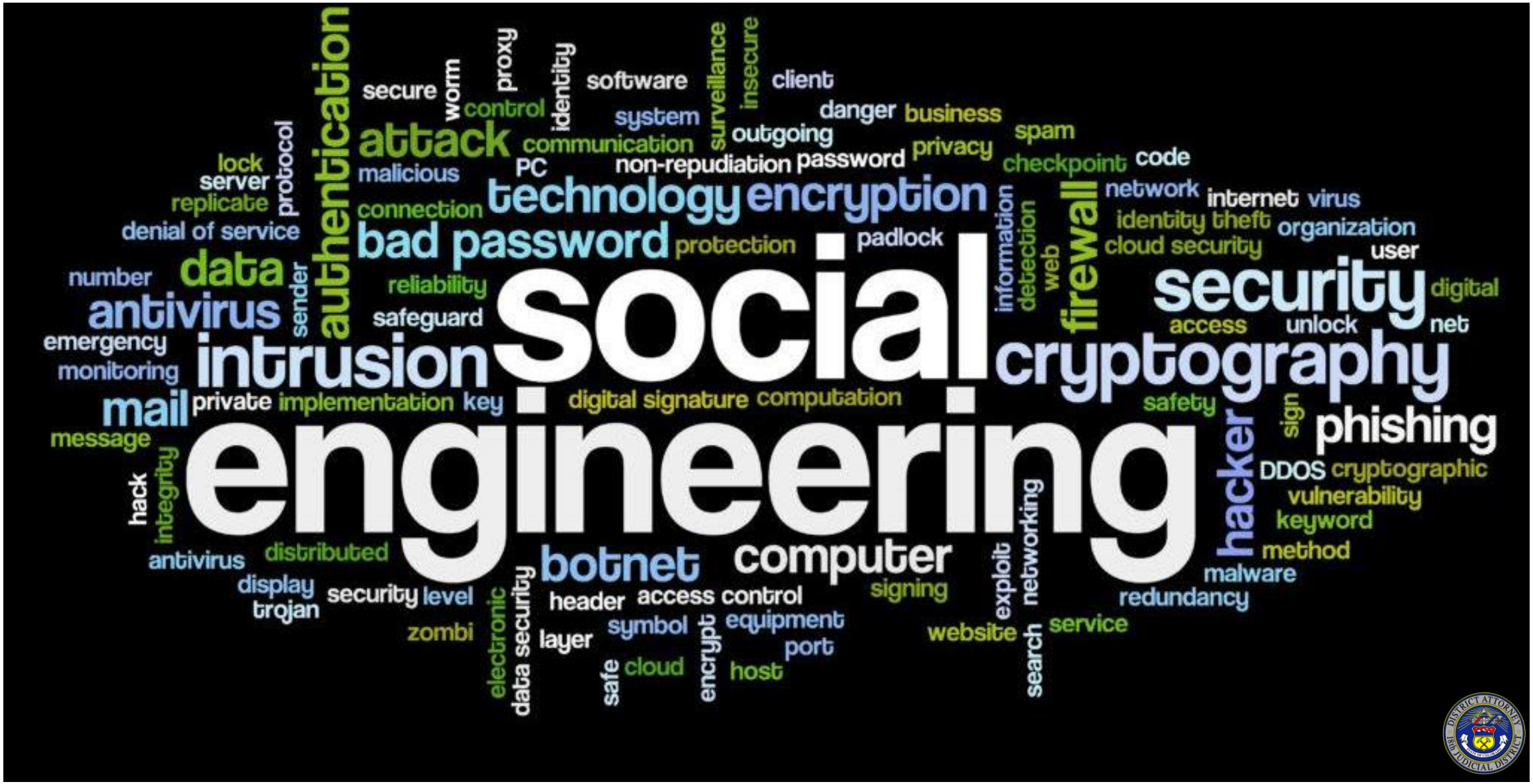
Level of discretionary income and assets

Many individuals are retired-often at home and accessible

Many older individuals may not understand new technology

This generation tends to be more trusting and has a higher degree of respect for authority

Criminals know some individuals may be experiencing memory problems


social
engineering
cryptography
security
intrusion
attack
authentication
technology
encryption
bad password
data
antivirus
mail
firewall
hacker
phishing
botnet
computer
malware
DDOS
cryptographic
vulnerability
keyword
method
redundancy
service
website
search
networking
exploit
signing
access control
header
layer
symbol
equipment
port
host
cloud
encrypt
safe
electronic
data security
zombi
trojan
display
security level
distributed
antivirus
hack
integrity
message
emergency
monitoring
denial of service
number
sender
replicate
server
lock
protocol
secure
worm
proxy
identity
control
software
system
communication
malicious
connection
PC
non-repudiation
password
outgoing
surveillance
insecure
client
danger
business
spam
privacy
checkpoint
code
network
internet
virus
identity theft
organization
cloud security
user
digital
net
access
unlock
safety
sign
information
detection
web
padlock
protection
reliability
safeguard
private
implementation
key
digital signature
computation

Social Engineering

"Social Engineering is the art of manipulating people so they give up confidential information. Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software." - Webroot

Social Engineering is a series of psychological manipulative techniques that exploit human errors and judgments in order to direct people into performing certain actions.

Scammers trick you into revealing personal and financial information, giving access to protected devices, exposing resources – all of which usually result in varying degrees of theft, sabotage or injury. Victims can be either individuals or businesses.

Scammers sometimes make broad-based attacks (known as phishing) or more specific, targeted attacks (known as spear phishing).

A scam = result of a calculated effort to deceive!

Why Do Scammers Do What They Do?

A scammer's model is simple and has a common end goal…

The origins are broad: overseas, domestic, someone known to you, personal, and business.

Scams range from impersonations of federal offices or banks to AI voice cloning that impersonates a family member or friend to pretend romances. The situations scammers create often involve high pressure emotional stakes and tight deadlines—such as claiming a family member has been kidnapped and asking for ransom—which are meant to encourage the individual to spring into action and make choices they wouldn't normally make. The emotional part of the brain really just hijacks our ability to rationally think through the situation.

Scammers do psychological warfare to make you feel either less lonely, or guilty, or afraid. Those core human emotions make us react physiologically instead of intentionally.

It is not always the negative side of emotions. The wheelhouse goes full circle.

Approximately 95% of cyber attacks and events involve preventable human error and behavior weaknesses.

One of the most common statements I hear from complainants on our DA18 Consumer Fraud Protection Hotline is…

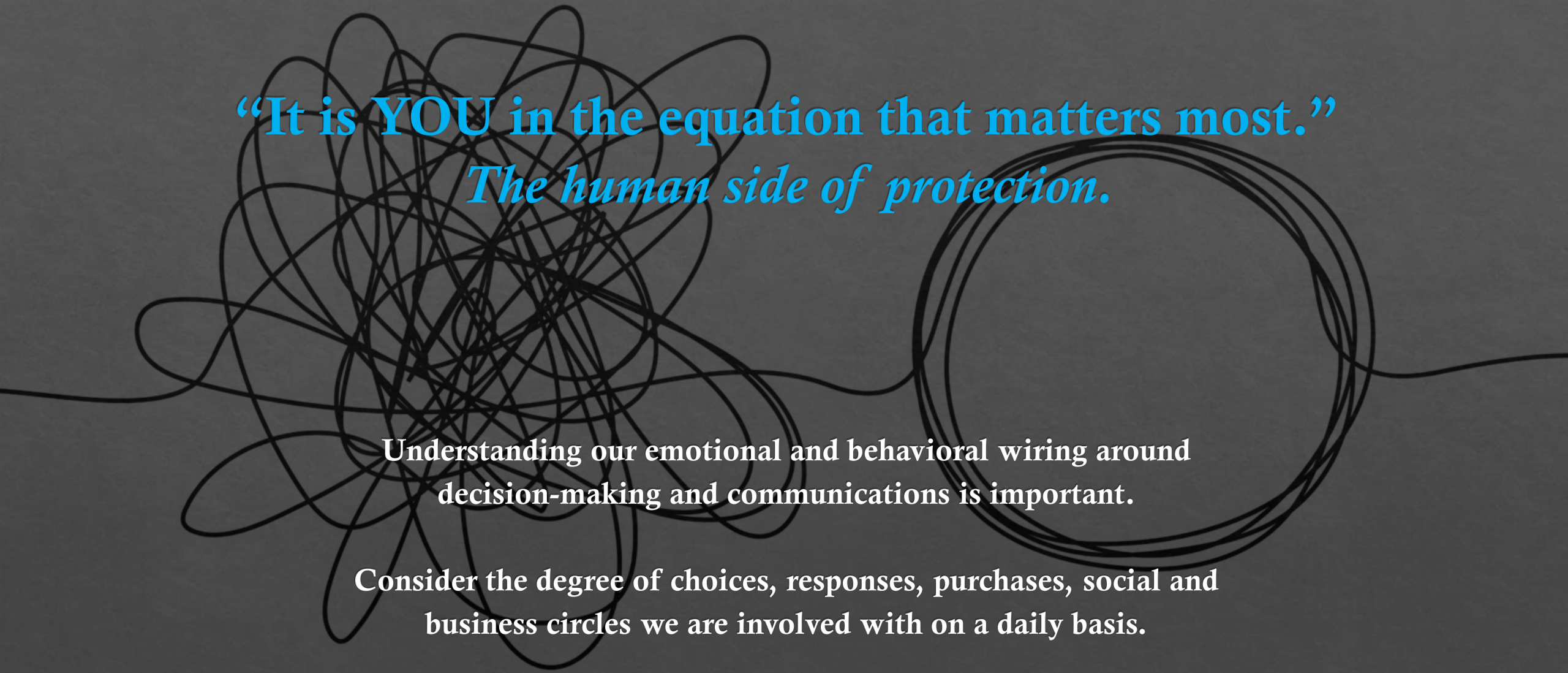
"I knew better than to do what I just did."

The Human Side of Online Protection Protocols

"Online security is about more than just passwords, antivirus software, and firewalls."

While these preventative measures are necessary and can greatly minimize your initial exposure to fraudulent activities, you can do so much more to protect yourself.

Everything starts with your understanding and awareness of the human side – the Emotional and Behavioral properties of the equation.



“It is YOU in the equation that matters most.”

The human side of protection.

Understanding our emotional and behavioral wiring around decision-making and communications is important.

Consider the degree of choices, responses, purchases, social and business circles we are involved with on a daily basis.

Your own personal experience.

How you **REACT** vs. RESPOND.

Specifically, the How, When, Where, Why, and Under What Circumstances do you find yourself in a reactionary state of mind vs. a responsive one.

How do we protect ourselves against a scammer's assault that preys our human side?

Reaction

A reaction is instant. It is a reverse movement or tendency, or an action in a reverse direction or manner. Reactions are done on impulse, without putting much thought into it or considering what the end-result may be. A reaction originates from your unconscious mind, which is usually survival-oriented, and on one level or another, a defense mechanism. While some reactions serve us well, many leave us feeling with some degree of regret.

Most of the DA18 hotline call responses I receive regarding actual scams involve a victim experiencing some level of regret over their reaction to the situation/interaction that played a role in the scam.

"The more reacting we do, the less empowered we become…"

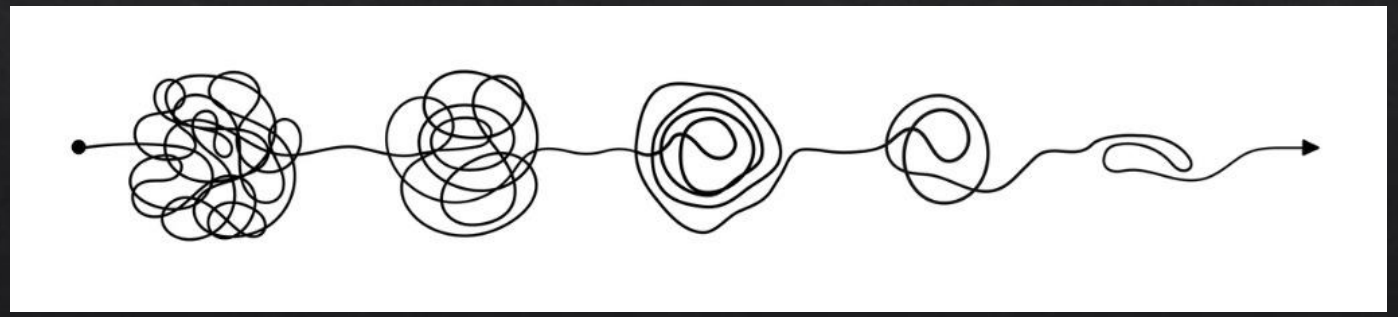
Response

A Response is more thoughtful and done with some degree of reasoning behind it.

In taking additional time to make decisions, you are addressing the long-term benefits and effects of your choices. You also allow yourself to recognize your underlining core values, beliefs, and needs.

You give yourself a chance to see the larger picture. Most things in life do not require immediacy and urgency.

Take a step back, catch your breath, question, research, and understand.



"Learning to respond vs. react can be the difference between falling prey to a scam or outsmarting the scammer…"

Five Psychological Reasons Why People Fall for Scams

You Scratch My Back

Beware the principle of reciprocity. If someone does something for us, we feel more obliged to do something for them.

Like Lemmings Off a Cliff

Research shows that if a person believes other people are doing something, then they feel it must be okay for them to do it too.

Little Steps

People like to think of themselves as being consistent and committed individuals. If we say we are going to do something, then generally we will, as failure to do so may dent our sometimes fragile self-esteem.

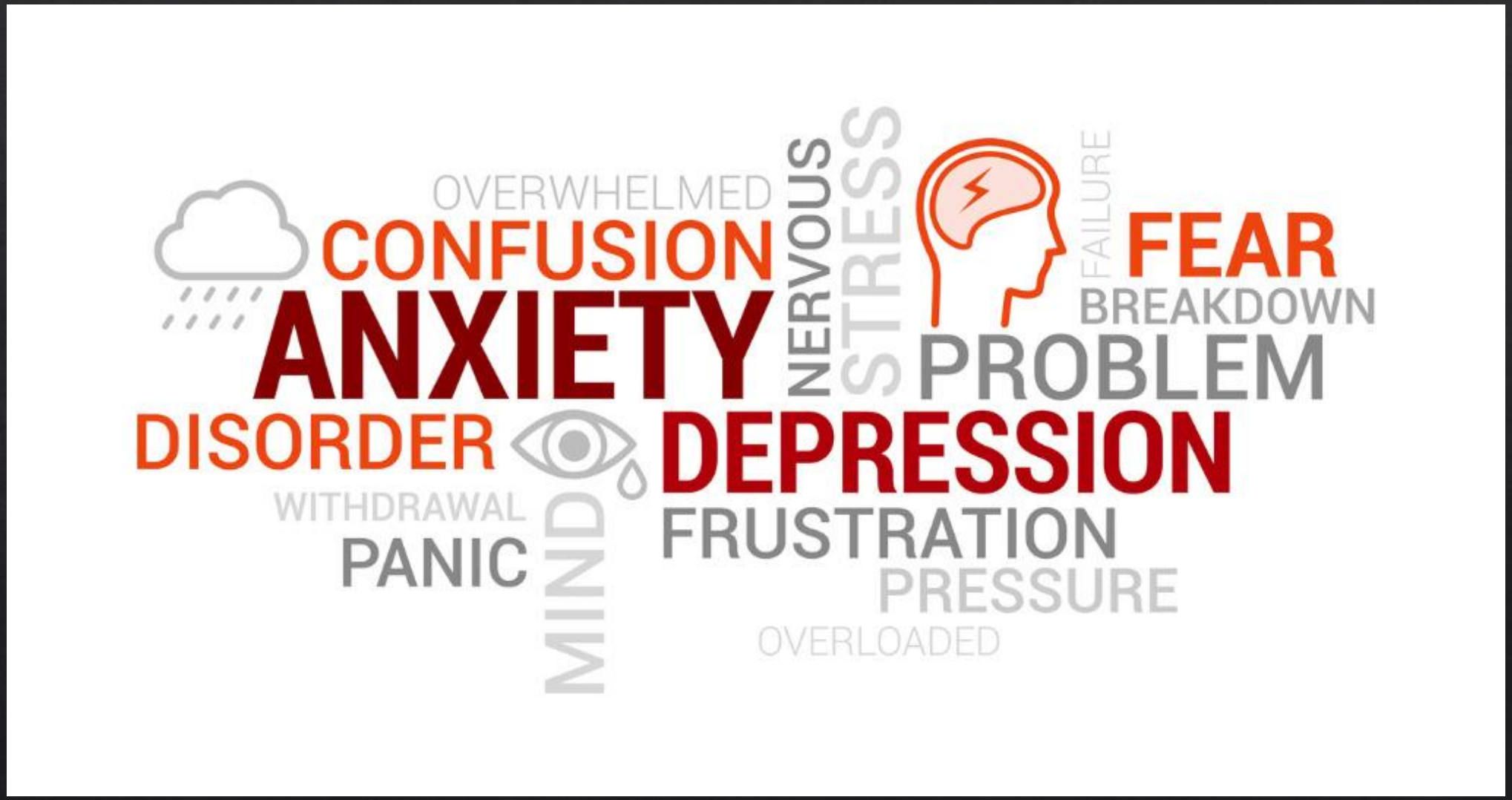
FOMO (Fear of Missing Out)

People are generally worried about missing out on an opportunity, perhaps for "the next big thing". And if such an "offer" is for a limited time only, then the principle of scarcity suggests that people are more likely to be drawn to it.

They Seemed So Nice

The principle of similarity suggests that we tend to like people who seem to be the same as us, and, in turn, we are much more likely to agree to a request from someone we like.

Where Are We In Heart and Head?



The Emotional Side of Being a Victim

Depression and mood changes are common long-term effects. Trust issues and paranoia. Anger. Sense of loss. Shame. Self-blame, self-esteem issues. Anxiety. Insecurity. Decision paralysis. Victims might experience embarrassment, shame, and guilt, not to mention financial stress.

Perhaps most troublingly, many victims are reluctant to seek help or report the scam. This reluctance can stem from shame, fear of ridicule, or a belief that nothing can be done. It's a silent suffering that often goes unnoticed and unaddressed.

The emotional recovery after a scam can be difficult.

Recovery

After Reporting the Scam Incident…

Recovering From a Scam Should Prioritize Emotional Healing

Connecting with others who have experienced similar situations can quickly alleviate feelings of isolation and shame. If that's not an option, confiding in someone you trust can provide valuable support.

Choose People Who Can Help You Process the Experience and Rebuild Your Ability to Trust Others

While it may feel tempting to become overly vigilant or guarded, this approach rarely brings the protection or sense of safety you seek. True safety comes from cultivating trusted connections with those close to you.

Accepting the Outcome Can Help You Move On

You might not be able to change what happened, but you can learn from the experience and protect yourself in the future. If you feel comfortable, you can share your story and help others protect themselves.

Trending Scams Impacting Our Senior Population

Government IMPOSTER Fraud

Scammers are targeting people through emails, calls, or texts and claiming they are from a government department.

The messages may offer grants, special medication rates, requests for updated personal information, or demand money.

Scammers use many tactics to sound and appear credible.

They sometimes provide information like badge numbers, names of actual law enforcement officials and federal judges, and courthouse addresses.

They may also spoof their phone numbers to appear on caller IDs as if they are calling from a government agency or the court.

Romance Scams

Feb.12, 2022 - According to a new Federal Bureau of Investigation report released Friday, more than 200 victims within Colorado and Wyoming lost over $32 million between October 2021 and January. Roughly 60% of the victims are over 60 years old, according to the FBI.

Scammers often claim to live or work in other parts of the country or world to avoid meeting in person.

Donation and Charity Scams

CONSUMER ADVISORY & PROTECTIVE TIPS

The recent tragic event in Boulder, CO will bring out the best of our communities, but it will also bring forth an opportunity for scammers.

Office of the District Attorney - 18th Judicial District

Proudly Serving Arapahoe, Douglas, Elbert and Lincoln Counties

PEOPLE WANT TO HELP

Tragedy has presented itself in our backyard. The Boulder Community, the State of Colorado, and our nation mourn for our recent loss. As individuals and as a community, we want to help those who were directly impacted. We are touched on many levels and want to reach out.

Tragedies, natural disasters, disease, and the need for basic human services offer the call for people and groups to step up and try to fill the gaps. Donation groups and established charities are there to help in the effort, often by pulling in financial contributions. Scammers are there too, especially when the events are extreme, dire, and overly emotional.

SCAMMERS AT WORK

Fraudsters use the misfortunes of others to take advantage of your kindness and goodwill. Fraud will surface through a range of solicitations, including spoofed communications, copy-cat charity websites, malicious links, heart-wrenching images of victims or devastated landscapes. At times, scammers pretend to be the victim themselves or a family member. The speed and depth of technology, an urgency to act, and your empathy play to their advantage.

TIPS

- **If Donating for Boulder Shooting Relief** - *Visit local Colorado news media and local police department websites for a list of legitimate organizations.*
- **Do Your Own Research on Legitimate Charities and Donation Sites** - *Visit CO Secretary of State website, Charity Navigator, CharityWatch, Better Business Bureau's Wish Giving Alliance.*
- **Never Donate Using** - *Gift Cards, cash, wire transfer, bitcoin. Instead, use credit cards or checks.*
- **Never Give Sensitive Financial or Personal Information** - *Social Security#, driver's license#, bank account#, DOB, etc.*
- **Beware of Unsolicited Communications and Links** - *Don't click on unsolicited emails or LINKS within emails or social media sites like Facebook, Twitter, etc.*
- **Beware Payments Through Crowdfunding Sites** - *During major tragedies and disasters, sites like GoFundMe are not always legitimate. Payments to individuals are generally gifts and not guaranteed tax-deductible donations. See website for details.*
- **Urgency and Pressure to Give** - *Beware requests or demands to donate or act quickly. Reputable charities will not pressure you to make a donation on the spot.*

COMMON RED FLAGS

- **UNSOLICITED Phone Calls, Emails, Texts, Door-to-Door Interactions** - *Be careful of organizations, entities or people initiating contact with you.*
- **Sense of Urgency** - *Common scammer tactic. A legitimate charity or cause will always take your donation. End of day urgency to commit or provide is always a red flag.*
- **Non-Traditional Donation Methods** - *Request for donations using Gift Cards, Cash, Wire Transfers, Bitcoin - these types of transactions are difficult to trace. Gift card payment scams are a common issue in Colorado.*
- **Unsolicited Emails with Attachments** - *According to Charity Navigator, it is not typical for legitimate emails from organizations to include attachments.*
- **Being Asked or Feeling Inspired To Donate DIRECTLY Through Social Media Sites** - *Always best to do your homework and investigate on your own. Make sure the group is legitimate and that you are going to charity's legitimate website to make donation.*
- **People That Contact You Online Claiming To Be A Victim** - *Unlikely for a victim of a recent tragedy or disaster to be contacting you directly for assistance. Fraudsters will pose as victims or use their stories and pictures to trick you.*
- **You Receive a "Thank You" For a Donation That You Do Not Remember Making** - *This is an old trick scammers use to relax you into their conversation.*
- **Examine the Web Address** - *Most non-profit web addresses end with .org and not .com.*

SPOOFING

Spoofing is when someone disguises an email address, sender name, phone number, text, or website URL—often just by changing one letter, symbol, or number—to convince you that you are interacting with a trusted source. Criminals count on being able to manipulate you into believing that these spoofed communications are real, which can lead you to download malicious software, send money, or disclose personal, financial, or other sensitive information. - *FBI.gov*

HELPING LOCALLY

Helping those in need is a good thing. Take the necessary precautionary steps to ensure that your charitable gifts are truly going to those who need it. As for recent events here in CO, research current articles from mainstream news outlets and visit local police department sites to see how you can help.

Contact Consumer Fraud Protection
18th Judicial District
Hotline (720) 874-8547 | consumer@da18.state.co.us

Donation and Charity Scams

Tragedies, natural disasters, disease, and the need for basic human services offer the call for people and groups to step up and try to fill the gaps.

Donation groups and established charities are there to help in the effort, often by pulling in financial contributions.

Scammers are there too, especially when the events are extreme, dire, and overly emotional.

Fraudsters use the misfortunes of others to take advantage of your kindness and goodwill.

Affinity Scams and Fraud

"We share the same interests and background. I am like you. You can trust me, right?

I can help you make a lot of money.“

- Said the Scammer -

Gift Card Payment Scams

Message Is Simple

Gift Cards are for Gifts.
NOT for Payments!

Extortion and Cryptocurrency

Beware!

Cryptocurrency…

- Accounts are <u>not</u> backed by a government.
- Payments do <u>not</u> come with legal protections.
- Payments typically are <u>not</u> reversible.
- Values change constantly.
- Some information about your transactions will likely be public.

Only Scammers…

- Demand payment in cryptocurrency.
- Will guarantee profits or big returns.
- Make big claims without details or explanations.
- Never mix online dating and investment advice.

Current Domestic and Global Economic Climate

Government-slashing efforts may embolden criminals if they suspect that agencies won't be responsive to consumer complaints. Uptick in scammers trying to take advantage of federal workers who've been fired as a result of recent "government" efforts.

Dramatic Fluctuation In Stock Market

Cost of Goods

<u>Might Lead To</u>

Unemployment/Employment Scams
Imposter Government/Federal Agencies
Imposter Non-profit Agencies & Resources
Investment Scams

In-Person Advisories

Check Fraud is when someone approaches you with a request to deposit or cash a check but after the check has "cleared" and it's a fraudulent check, the deposit will be reversed on your account. You are responsible for the check amount and any bank fees attached to it.

Sometimes **Family Members** also take advantage of an older adult financially and these are difficult cases due to the family bond. Examples are adult children who feel entitled to their parent's money and take it for their own use. Intimidating or isolating an older adult, name calling or trying to force them to hand over money is a form of abuse.

Guardian or Conservator - this is when a fiduciary (someone you have authorized to take care of you or your money) abuses their role. Bank or credit card activity that is unusual is a warning sign. Only appoint someone you know you can trust as an agent to make decisions about your money and health. It is important to remember you can always change your mind and revoke a POA/Conservatorship or hire a new attorney.

Medical or Caregiver Fraud scams are when your medical information is used to obtain reimbursement for services not provided. Always protect your Medicare and Social Security number. Caregiver Abuse can involve both paid and volunteer caregivers and family members who act as caregivers.

Public Wi-Fi

When in public spaces, we urge you to be very careful when using Public Wi-Fi in places like coffee shops, restaurants, airports, and other public venues.

Public Wi-fi is easy for someone to hack into.

Use your phone hotspot, purchase a VPN (Virtual Private Network) or other secure network.

Do not conduct sensitive, personal or financial inquiries and transactions on public Wi-Fi.

Public Charging Stations

Be Aware

Cybersecurity experts warn that bad actors can load malware onto public USB charging stations to maliciously access electronic devices while they are being charged. Malware installed through a corrupted USB port can lock a device or export personal data and passwords directly to the perpetrator. Apr 27, 2023 – Federal Communications Commission

Tip

Use an AC power outlet instead. The FCC also suggests you bring your own AC, car chargers, power cords, and USB cables with you when you travel. The FCC recommends carrying a charging-only cable, which prevents data from sending or receiving while charging.

TAKE NOTICE

CREDIT CARD SKIMMERS

Credit card skimmers are devices that criminals attach to ATMs and gas pumps to steal your credit card information. Criminals have used skimmers for a long time and the advancements in technology around them continue to improve. Skimmers are becoming smaller, therefore harder to detect. Criminals use blue tooth technology to extract the card and PIN numbers gained once customers use their cards.

The newest trend...skimmers are being detected at SELF-CHECKOUT STATIONS in retail stores. Occurrences are popping up in certain states across the country, including here in Colorado.

Here Are A Few Tips On How To Protect Yourself

Examine the Credit Card Reader Before Using

Look for any signs of tampering or take notice of any loose components. Try tugging on where you insert card to check for oddities.

Use A Contactless Payment Method

If possible, hover or tap your card over the card terminal as a means of conducting a transaction. This is a much safer method than swiping card through terminal.

Use A Credit Card Instead of A Debit Card for Payment

If possible, use a credit card because it is easier to dispute a charge with a financial institution. Always a good idea to use a credit card at gas pumps.

Protect Your PIN # When Entering

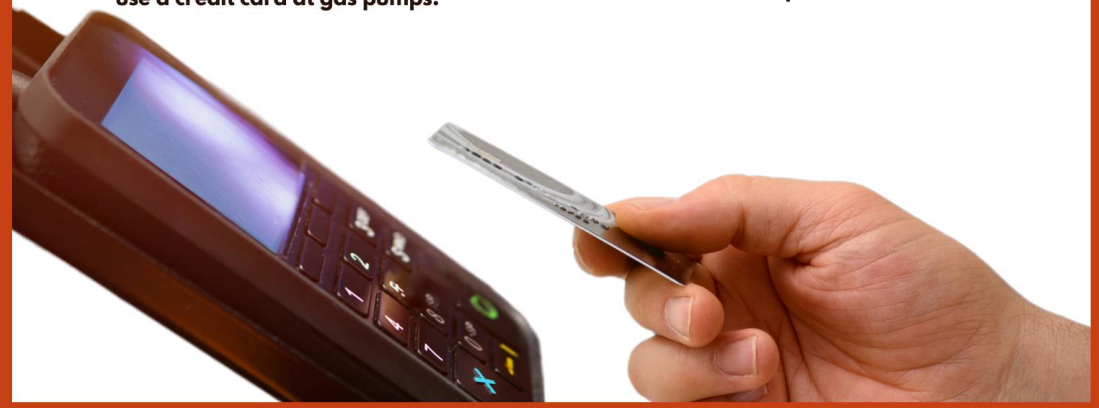
Cover the keypad with your hand or your body to prevent someone from capturing it with hidden cameras or who might be looking over your shoulder.

Check Credit Card and Other Financial Statements for Unusual Activity

Report suspicious activity immediately to your financial institution and the police.

Report Suspicious Activity, Card Reader Oddities to Retail Store,Gas Station or Financial Institution!

Reporting criminal activity helps to protect others and helps to defeat crime.



Spoofing

Definition

Spoofing is when someone disguises an email address, sender name, phone number, text, or website URL—often just by changing one letter, symbol, or number—to convince you that you are interacting with a trusted source.

Criminals count on being able to manipulate you into believing that these spoofed communications are real, which can lead you to download malicious software, send money, or disclose personal, financial, or other sensitive information. - *FBI.gov*

SPOOFING

CAN YOU TELL?

Client@aol.com

CIient@aol.com

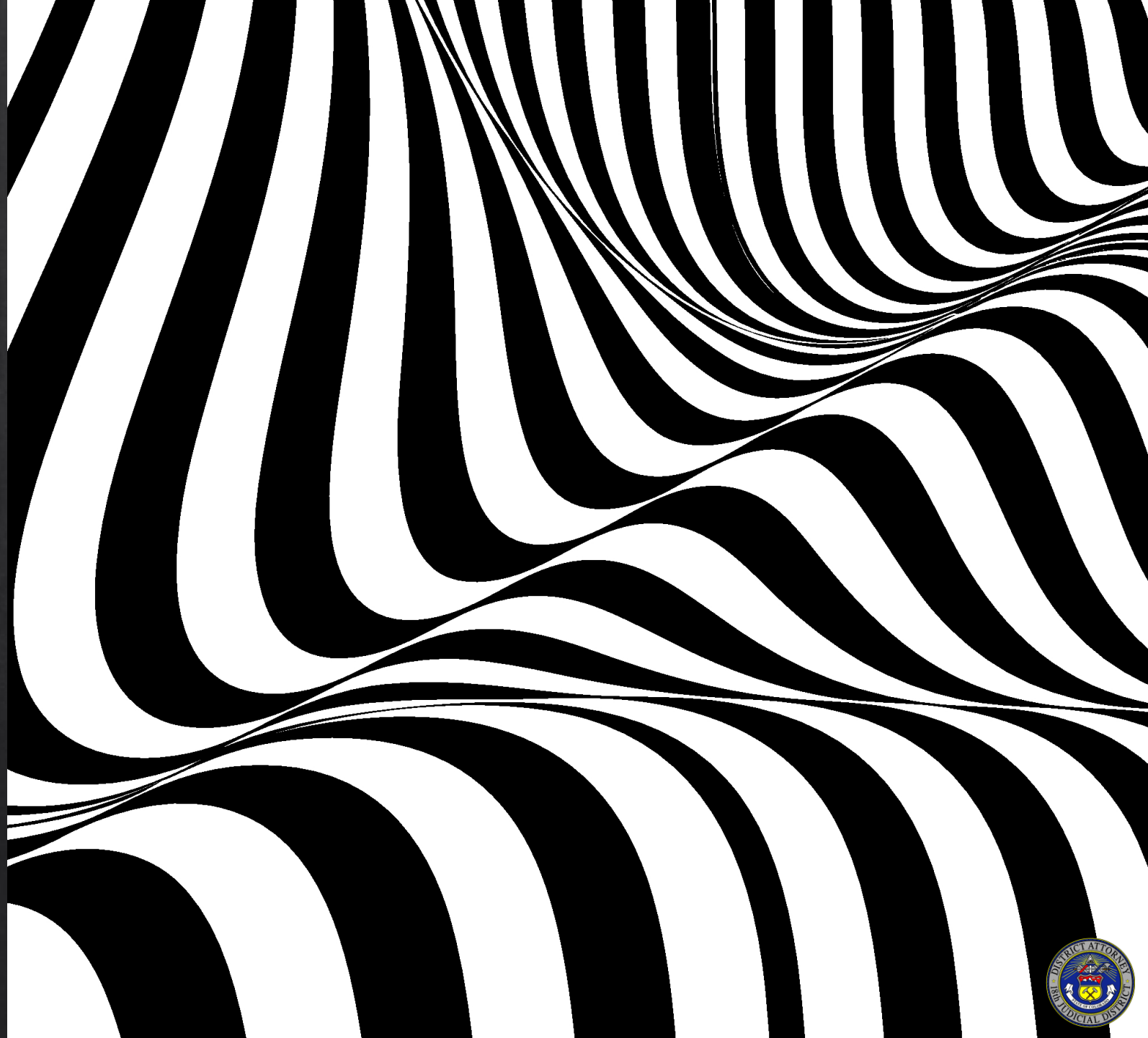
Huckelberrylaw@outlook.com

Huckelberry1law@outlook.com

J0HN.SMITH.LAW@gmail.com

JOHN.SMITH.LAW@gmail.com

L1 1i 0O 11



Recovering Identity

Resolving ID theft is left largely to victims!!

- ✓ File a police report.
- ✓ Cancel all compromised credit cards and close all compromised financial accounts. Select new PIN #'s.
- ✓ Contact the business where your info was misused in writing, let them know there was fraudulent activity on your account.
- ✓ Change your passwords for all your online accounts, including Email accounts.
- ✓ Review your personal profiles on all accounts with financial information; look for changes to addresses, phone numbers and email addresses.
- ✓ Contact the 3 credit reporting agencies. Consider a credit freeze for your accounts.
- ✓ Set up a credit monitoring account.
- ✓ File a report with the Federal Trade Commission at www.ftc.gov.

Protective Tips

Never trust caller ID: Send calls you don't recognize or are not expecting to voicemail.

Do not click links you receive in an email or text: Research official number or website.

Never provide sensitive information over the phone, email, or text. This includes Passwords, PIN #s, SSN, Medicare number, license number, or credit card numbers.

Slow Down! Notice reg flags. Research rather than react. Consult with family members and friends.

Recognize Manipulation: Rarely are things urgent. Recognize threats. If it sounds too good to be true, it is.

Payments: Do not make payments with cryptocurrency, gift cards or wire transfers. Be cautious when making peer-to peer payments like Zelle and Venmo.

Place your sensitive documents under lock and key, a safe or a safety deposit box.

Change your passwords today! Don't reuse passwords. Change your passwords regularly. Use two-factor authentication.

Report all fraud and scams to local law enforcement agency or the District Attorney's Office:
consumer@coda18.gov or 720-874-8547.

Contact Info
Consumer Fraud Protection

Hotline: (720) 874-8547
Email: jsorrells@coda18.gov

Jamie Sorrells
Director of Consumer Protection
& Community Engagement
Office of the District Attorney
18th Judicial District
6450 S. Revere Parkway
Centennial, CO 80111

Proudly Serving Arapahoe County