HOW TO PROACTIVELY AVOID FRAUD

In a recent Town Hall for Eldorado residents, Santa Fe County Sheriff Adan Mendoza cited reassuring statistics about our community's generally low crime rate. The highest incidence of crime was fraud.

People of all ages and backgrounds can fall prey to fraud, especially in a moment of distraction. If you are upset about something, you are more likely to panic and click on a link in an email or a text that says something about your computer being compromised, or a problem with an online order. Always take a moment and breathe deeply, and question what you are reading before you take action.

PHONE

If possible, don't answer the phone to numbers you don't recognize. If you have a landline without caller ID service, let your phone go to a message machine on which you can monitor the call, or to voice mail. For those who have landlines with Century Link, you can get "No solicitation" service that tells callers to hang up if they are a solicitor or to press 1 if they are not. This greatly cuts down on robocalls and scam calls. You can add 25 numbers to a list of callers who can bypass the system.

Your cell phone should have a setting that allows only numbers in your contacts list to ring through, sending the rest to voice mail. If you run a business or are expecting an important call from someone not on your list like a bank or government entity, you would need to turn this feature off, but otherwise it cuts down on annoying distractions. If it's a legitimate call, they will leave you a message.

Some people subscribe to Robokiller or other paid services to further cut down on scam robocalls. Cell phone providers automatically screen out robocalls, but these systems are imperfect at best.

You can block numbers, but scammers just keep changing them and you could spend time every day blocking numbers.

If you do answer the phone to a scammer, hang up right away unless you want to do a comedy routine with them. Social Security or Medicare is never going to close your account, and will contact you by old-fashioned letter if there are important issues you need to know about. And you don't need to speak to anyone about problems with your computer—especially a brand that you don't even own.

Some phone scams play on the heart, saying that one's grandchild is in some kind of trouble. In these trying times when people might not be in constant touch with distant family members, one could momentarily fall for such a scam, though you probably know your grandchild did not lose his or her passport in Siberia recently.

NEVER give out personal info—especially your Social Security number, Medicare number, or any credit card or bank account numbers—to an unknown caller. If a bank or credit card company calls or texts regarding a fraud, be suspicious and make sure you call the number on their website just in case it is a fraudulent call.

The bottom line is to always err on the side of caution.

You can put all your numbers on the national Do Not Call registry, which is a great idea that doesn't seem to do much. Perhaps we would get even more robocalls and scam calls if it didn't exist, so it's worth a try. https://www.donotcall.gov/

ONLINE
Spam filters catch most, but not all, fraudulent emails. Look carefully at the email address for oddities in the domain name and delete immediately if you are suspicious. If you are not sure whether an email is legitimate, contact the bank or other company online through their website.

Spamsters change and evolve their methods constantly. One of the latest seems to be about an Amazon order of some rather expensive item you know you didn't order. Until you notice the weird domain name and the misspellings in the message, you might for a moment be tempted to click on the "if you did not order this" link. Delete, delete.

If you have any suspicion that you have been defrauded, it's a good idea to change all 100+ of your passwords.

SOCIAL MEDIA
We all know that social media is data-mining us, but there are even more sinister threats. Fake friend requests are incredibly common if you choose to have a public page. If you don't need a public page for your business, it would be wise to tighten privacy settings.

It's easy, and sometimes humorous, to recognize fake friend requests. They are from someone you've never heard of, they are new accounts, and most of them have no friends at all. But some may have a number of friends, including some of your online friends. If you think it might be a legitimate request, for example if you seem to have a business, interest, or affinity connection in common, check with your friends to see if that person is a legitimate friend or if they just accepted the request without thinking.

If a social media "friend" becomes an online stalker or starts harassing you in a creepy way, report it to the social media company. If it continues or is actually threatening, report to law enforcement, in this case our County Sheriff.

TEXTING
"Smishing," referring to scammers on SMS messaging services, commonly known as texting, is becoming more common. Research shows that people are more likely to click on a link in a text without thinking than a link in an email.

The same principles apply to texting as to other forms of communication. If you don't recognize the number and the message doesn't make sense to you or is just a link, delete immediately. Do not under any circumstances reply or engage in any way.

CREDIT
You should check your credit report at least once a year. Many companies offer paid services that check monthly and give you quarterly reports. If you have ever been part of a massive fraud of millions of people like shoppers at a certain chain or patients at certain large medical facilities, they will contact you and tell you that they are giving you free credit monitoring for a fixed period of time.

RESOURCES

AARP (American Association of Retired Persons) has a Fraud Watch Network that offers excellent resources and tips on avoiding being defrauded. Anyone over 50 is eligible to join, but you don't have to be a member to report suspicion of fraud or to sign up for their free email Fraud Watchdog Alerts. If you are active on social media and have the time and inclination, you can even become a volunteer digital fraud fighter.

https://www.aarp.org/benefits-discounts/all/fraud-watch-network/

The non-profit Consumer Reports has frequent articles on avoiding fraud, such as this one on avoiding credit card fraud, especially during the pandemic:

https://www.consumerreports.org/scams-fraud/protect-yourself-from-credit-and-debit-card-fraud/

If you suspect you have been defrauded, report it to both the local sheriff's office and place a fraud alert on the Federal Trade Commission site:

https://www.consumer.ftc.gov/articles/0275-place-fraud-alert

Here are tips from the Consumer Financial Protection Bureau of the US government on recognizing Social Security scams:

https://www.consumerfinance.gov/about-us/blog/five-ways-to-recognize-social-security-scam/

Debra Denker
Eldorado Safety Education Task Group