Park County Sheriff's Office
PO Box 604
Fairplay, CO 80440
719-836-2494
Sheriff Tom McGraw

Current fraud/scams to be aware of

Scammers are like viruses: They continually evolve in response to the latest news and trends, using them for new ways to separate us from our cash.

These criminals "*are so adaptable, they're going to just follow the headlines*," says **Amy Nofziger, director of fraud victim support for AARP.**

As she and other anti-fraud experts note, scammers have proved ingenious when it comes to updating traditional criminal operations such as the romance scam or the Ponzi scheme with new twists to make them more convincing and effective. And like the rest of society, scammers are increasingly going online.

"*Most con artists have taken a digital-first approach to scamming,*" says **Josh Planos, vice president of communications and public relations for the Better Business Bureau (BBB).** He notes that **the vast majority of today's scams originate through a digital on-ramp, such as social media or email.**

Source:
https://www.aarp.org/money/scams-fraud/info-2023/top-scammer-tactics-2023.html

Recently in Park County, we have seen a number of scams in which a pop-up window appears on the victim's computer screen telling them their computer has a virus and they need to call the phone number on the pop-up window immediately to get it fixed. The victim then calls that phone number and is instructed to send money in various ways including wire transfer, sending gift cards or even creating another bank account which is then accessed by the criminals and drained.

Several scams have begun by the criminals telling the victim they are federal law enforcement or representatives of their bank. **Law enforcement will never call to tell you that there is a warrant for your arrest or request money to prevent a warrant being issued. Banking officials will also never contact you requesting your PIN, passcodes or personal information.** If you ever receive a phone call from a person claiming to be law enforcement, banking officials, etc. hang up, look up the phone number to that entity and call the listed phone number.

Never call the phone number they give you to call!

If a scam has ever happened to you, call your financial institution immediately so they can **suspend your accounts and begin a fraud investigation.**
Change all passwords on your accounts and computer.
Report the fraud to https://reportfraud.ftc.gov.
If the fraud took place over the internet, report to ic3.gov.

There are several types of scams and they are ever evolving, but a few to watch for are:

Crooks combine crypto scams with old-fashioned romance scams, **posing as internet love interests** so they can cajole their targets into downloading an app and investing in fake crypto accounts. "They claim that they're even putting some of their own money into your fund," explains former Federal Trade Commission official Steve Baker, who publishes the Baker Fraud Report. While the app displays data that seems to show your wealth growing, criminals are just taking your money.

How to stay safe: Carefully scrutinize any investment opportunity, even if you think you're a sophisticated investor. "*People think it's not going to happen to them, but it is happening to many, which is why you have to keep your guard up,*" Nofziger says.

Criminals exploit the inflation squeezing workers by offering **fake payday loans** that they claim will help people settle their bills, according to Nofziger. Loan applicants are told they'll need to prepay a fee. The money goes into the crooks' pockets, and the applicant gets nothing.

How to stay safe: Be wary of anyone who asks you to pay any sort of loan fee **with a gift card or some other nontraceable form of payment**.

Credit reporting company Experian warns that scammers utilize bots — automated programs — to deceive people into sharing the two-factor authentication codes sent to them via text or email from financial institutions (or from companies such as Amazon). **The bot will make a robocall or send a text that appears to come from a bank, asking you to authorize a charge, then it asks you to enter the authentication code you've just been sent if the transaction isn't yours. It's actually the bot that's trying to log into your bank account, and it wants the code that the bank sent to you as a precaution, so it can get in.**

How to stay safe: **Never share authentication codes,** or provide other information, in response to an unsolicited phone call or text.

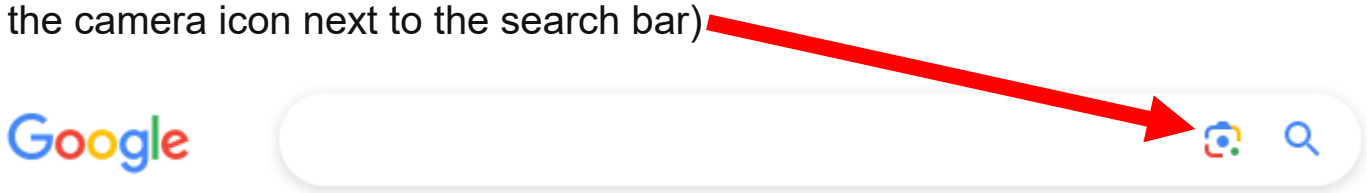
The Biden administration's plan to forgive student loans faces an uncertain future after being tied up in the courts, but that hasn't stopped scammers from trying to take advantage of people who may not have heard it's on hold. **They've built phony application sites aimed at stealing applicants' Social Security numbers and bank information**, and sometimes they contact targets by phone, pressuring them into applying and charging a fee for their help. The scam still has legs, "*because there's so much debt that people are carrying and they're looking for a way to get rid of it,*" explains **Michael Bruemmer, vice president of the data breach group and consumer protection at Experian.**

How to stay safe: Go to the Department of Education's student aid website to keep track of the proposed forgiveness program's status. (https://studentaid.gov/)

Scammers try to exploit dog lovers by offering cute puppies for sale on the web. In one instance documented by the BBB, a woman paid $850 for a Dalmatian puppy, only to receive additional requests for money — first $725 for travel insurance for the dog, then $615 for a special crate. In the end, **the buyer lost $2,200 and never got the puppy** — which didn't actually exist.

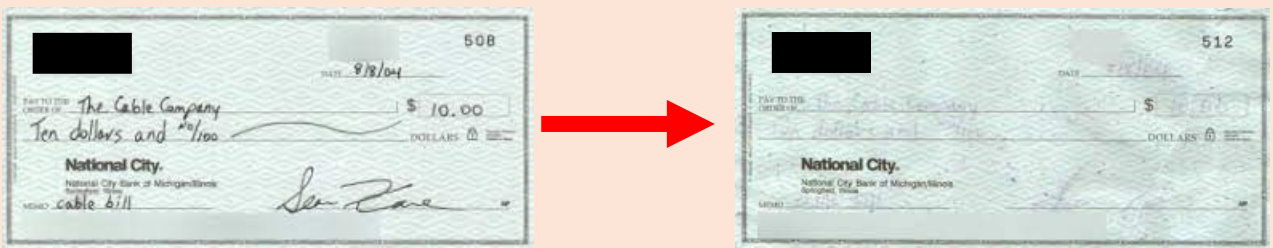
How to stay safe: Go to an animal shelter and check out the dogs available there, before you search online. If you spot a puppy you like on a website, do a reverse image search to make sure it's not a photo stolen from some other site. Insist on seeing the pet in person before paying any money.

(You can perform a FREE reverse Image search by going to google.com & selecting the camera icon next to the search bar)



Though other payment modes are replacing them, checks are still used often enough for scammers to exploit. One trick is "check washing," in which crooks steal checks from mailboxes and bathe them in household chemicals to erase the original name and dollar amount, leaving blank spaces they can fill in. **It's possible to convert a $25 check to one for thousands of dollars.**

How to stay safe: The U.S. Postal Inspection Service recommends **depositing your outgoing mail in blue collection boxes before the day's last pickup**, so it doesn't sit for as long. At home, **avoid leaving mail in your own mailbox overnight**, and have your mail held by the post office or picked up by a friend or neighbor if you're going to be away.



This is a variation on a basic QR code scam that the FBI warned about: Scammers put fake codes over real ones to exploit the convenience of the barcodes people scan into their phones to see restaurant menus or make payments. Experian's Bruemmer says scammers may call and say they're going to send a QR code to your phone, so you can receive a free $100 gift card. **In reality, the QR code may take you to a malicious website.**

How to stay safe: If you receive a QR code out of the blue, contact the person or company that supposedly sent it, to make sure it is for real. **Use a phone number you know is authentic.**

This is an example of a QR code, this one will take you to our website Forms that include some of these useful forms:

Accident Reporting, Fraud & Forgery Victims Packet, Identity Theft Victims Packet, & More.

Seemingly misdirected messages are increasingly the start of a scammer's ploy. **A text message addressed to someone else pops up on your phone.** It seems urgent — a rescheduled business meeting, or maybe a romantic get-together. You text back, "Sorry, wrong number!" The scammer keeps up the friendly texts, and may eventually invite you to join an adult website to see revealing pictures so you hand over credit card info and money, or try to convince you to make a cryptocurrency investment (and take your money).

How to stay safe: Don't respond to texts from numbers you don't recognize. **Don't click on links in them or respond with "STOP" if the messages say you can do this to avoid future messages. Block the phone numbers they come from.**

Beware if you've lost money in a cryptocurrency scam: Criminals set up **fake "get your crypto cash back" websites, including one that looks like it's from the U.S. Department of State.** After luring targets, they contact those who respond by phone, email or social media and ask for personal ID information, including account numbers and passwords, plus an advance fee for their services payable by gift card, cryptocurrency or wire transfer. **You get nothing, warns the FTC.**

How to stay safe: Crypto investments aren't insured by the government the way bank accounts are. For the most part, funds lost to crypto scammers are gone. "*Don't trust anyone who contacts you saying they can get your money back*," says **Frank McKenna, chief fraud specialist for the fraud detection company Point Predictive**.

Let's say you've set up your bank or credit card online accounts so you can access them only with a live code sent from the institution. And let's say a criminal has your bank or credit card username and password login and wants to steal from you. What would he or she do? In this increasingly common fraud, they call you, **claiming to be from your bank and warning about a problem with your account.** The caller tells you they're emailing or texting you a "onetime passcode" for logging in and asks you to read it back to them for verification. In reality, **the scammer's login attempt triggered your bank to send you the passcode.**

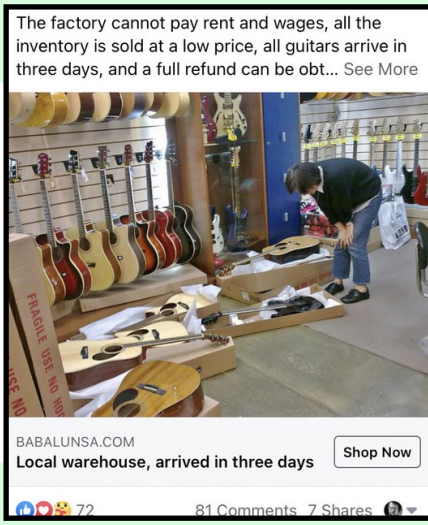
Handing it over gives criminals full access to your account.

How to stay safe: **Never give your onetime passcode to anyone who calls you!!**

Hang up, **find your institution's phone number on a bank statement or on your credit card, and call. Ask if there really is a problem and report the con to the bank's fraud department**, McKenna recommends.

New **package delivery scams** include texts and phone calls purportedly from a professional-sounding delivery driver who can't find your house. Didn't order anything? They may try to convince you someone's sent a gift. Or **you may receive an email about rescheduling a drop-off or a fake "package delivery attempt" sticker on your front door.** Their goal? To get you to provide personal information or simply click on a link they provide. That link then downloads malware that will harvest passwords and account info from your computer.

How to stay safe: Contact the seller or delivery service using a verified phone number, the FCC recommends. Don't use numbers or links provided by potential scammers.



Scammers often place **fake ads on social media sites** for products at too-good-to-be-true prices, take your order and payment info, then tell you the item's not available right now. Your refund is on the way, they promise, but it never arrives. And you can't reach anyone at the company about it.

How to stay safe: Research businesses online before you buy, and only shop on secure websites with a lock symbol in the browser bar and an internet address that begins with "https://" And pay by credit card, the FTC recommends. That way, you can withhold payment pending an investigation.

Source: https://www.aarp.org/money/scams-fraud/info-2023/top-scammer-tactics-2023.html

These are just a few of the scams, but remember, you can always protect yourself and your assets by verifying information. Never click on links sent to you and never call the phone number that is provided to you. If they are conveying a sense of urgency and making you feel that you need to send them money immediately, IT IS A SCAM!

Stay Safe, Stay Secure, & Stay Vigilant.

Park County Sheriff's Office