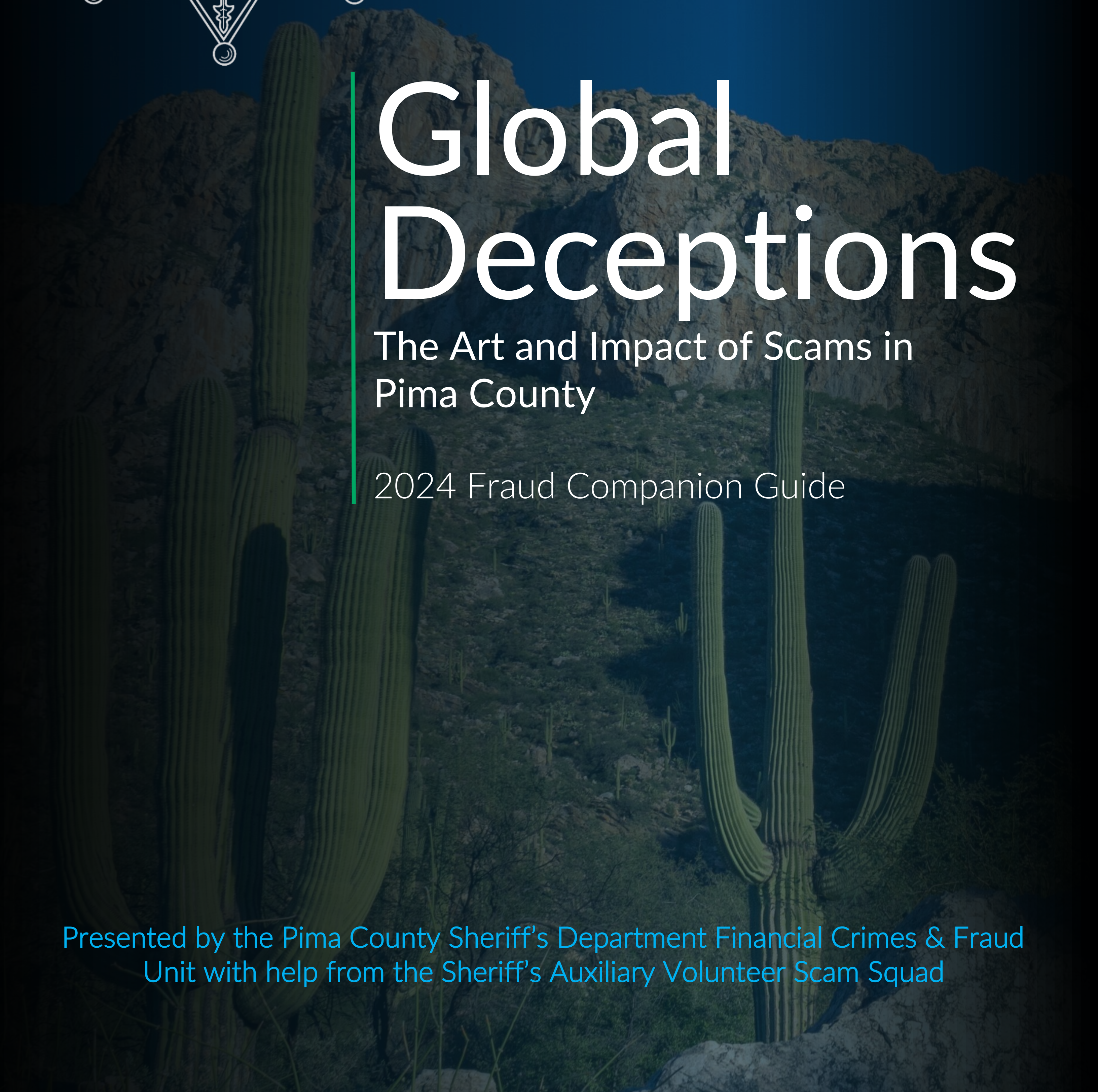


Global Deceptions

The Art and Impact of Scams in Pima County

2024 Fraud Companion Guide

Presented by the Pima County Sheriff's Department Financial Crimes & Fraud Unit with help from the Sheriff's Auxiliary Volunteer Scam Squad

Dear Community Members,

I am extremely proud of the Pima County Sheriff's Department (PCSD) Financial Crimes and Fraud Unit. This unit works tirelessly to investigate and solve a diverse array of criminal fraud cases that occur in our community. As the national data suggests, the number of fraud cases is on the decline; however, the financial losses from these crimes continue to skyrocket.

The causes of the contrasting data points are clear— scammers have only become more efficient. They are creating sophisticated scams which enable them to siphon an increasing amount of money from those in our community. Victims increasingly include individuals of diverse and socioeconomic backgrounds who believe this could never happen to them.

While the work from this unit diligently holds these scammers accountable, oftentimes the perpetrators of these schemes are outside our county, state, and frequently outside of the United States. This distance makes prosecution difficult, with the result being monies that are difficult to recover, and scammers that continue to act without regard for the residents of Pima County.

Fraud prevention ultimately starts with you, and outreach and education continue to be the strongest tools to prevent scammers from taking advantage of our residents. If you know the signs and tactics these scammers use, you can empower yourself and those around you to stop the scams before they start.

To accomplish this, we have created *Global Deceptions: The Art and Impact of Scams in Pima County*, which combines presentations, demonstrations, and resources to give you the tools necessary to prevail against these scammers. We hope the educational resources will provide you the knowledge you need to protect every hard-earned dollar.

The PCSD greatly appreciates your participation in being a scam stopper! For more information please visit, www.pimasheriff.org to learn more.

Respectfully,

Chris Nanos
Sheriff of Pima County

The Pima County Sheriff’s Department Financial Crimes & Fraud Unit

Kevin Gardner

Sergeant

Santiago Hernandez

Detective

Michael Wilson

Detective

Joseph Knipp

Detective

Tyler Rivas

Detective

The Pima County Sheriff’s Department Financial Crimes and Fraud Unit serves the unincorporated areas of our community, with a focus on investigating scams, financial fraud, forgery, among other crimes. Comprised of four detectives and a sergeant, the team contains several Certified Fraud Examiners, an Anti-Money Laundering Specialist, as well as a federally cross-certified Detective who is our liaison to the Federal Fraud Task Force.

You can contact this unit via email at fraud@sheriff.pima.gov or via telephone at (520) 351-3000

The Sheriff’s Auxiliary Volunteers

Visit
gvsav.org
for services in Green Valley

Visit
pcsdsav.com
for other areas in Pima County

The Sheriff's Auxiliary Volunteers (SAVs) are a nationally recognized, award-winning organization comprised entirely of volunteer citizens. The SAVs support residents of Pima County living in unincorporated areas encompassing 9,241 square miles in Tucson, Green Valley and Ajo.

The Pima County Sheriff's Department SAV members perform a number of important tasks vital to the overall mission of the Sheriff’s Department. These operations include Patrol, Crime Prevention, Neighborhood Watch, Field Operations and Emergency Response, Administration, Fingerprinting, Special Activities, and Recruiting and Training.

The Pima County Sheriff’s Auxiliary Volunteers are exceptionally trained individuals who represent the Department in an extraordinary manner. Since 1982, this non-profit volunteer organization has provided over 1 million hours of service to the community. The SAVs extensive contributions make them a vital part of our efforts to enhance the quality of life within the community we serve.

Contents

The National Data:

The Impact of Fraud Across the Country

Visualizing Fraud Nationally...5
Pima County Demographics...7
Importance of Education...8

The Technologies:

Introduction to A.I. and Other Tools

Artificial Intelligence...9
Caller ID Spoofing..13
Voice Cloning...14

The Methodology:

The Common Scams in Our Community

Imposter Scams Detailed...15
Lottery/Company Scam..16
Romantic Interest/Family Emergency Scam...................17

The End Goal:

Turning Victims into Money Mules

Money Mules Explained..18
Visualizing the Process...19
Global Nature of Local Scams..20

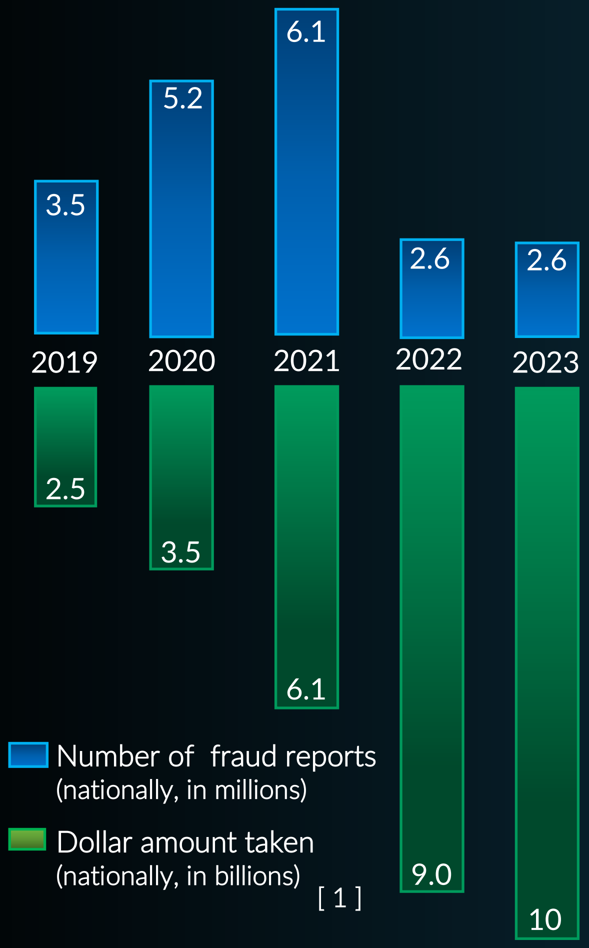
Prevention:

Tips & Tricks to Stop Fraud

Auditing Your Social Media...21
Independently Verify Information...................................22
Creating Stronger Passwords...24

Fraud is a Growing Crime

Each year, more and more money is lost



[1]

The Federal Trade Commission (FTC) has logged data related to consumer fraud for over a decade. In the last five years, a seismic shift has occurred. The number of fraud cases has dropped drastically from their post-covid peak in 2021 at 6.1 million reports, to a “tiny” number of 2.6 million by 2023.

Despite this massive drop in cases, the amount of financial loss has skyrocketed. Scammers did not stop they simply became more efficient, taking more money with much less effort.

5.4

MILLION REPORTS

2.6 MILLION OF WHICH, WERE *FRAUD* RELATED

$10.0 BILLION | $500 MEDIAN LOSS

27% reported a loss

TOP THREE CATEGORIES IN 2023

1. Identity Theft
2. Imposter Scams ❮ Growing Rapidly
3. Credit Bureaus

[2]

It is a common misconception that victims are all elderly. In fact, a plurality of cases that are reported target younger folks. The likely reason older folks are most commonly perceived as victims has more to do with the amount of money lost, not so much the frequency.

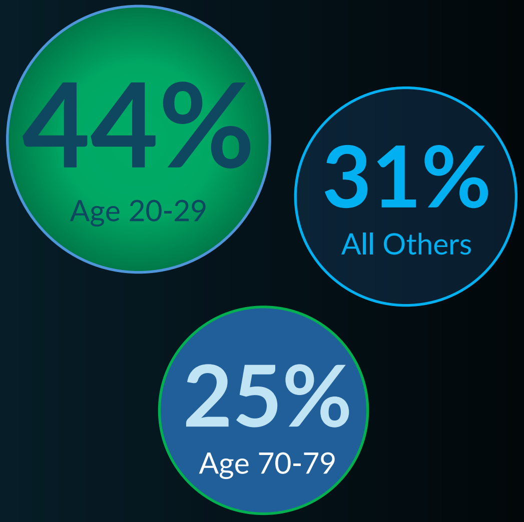
Older scam victims tend to be retired and have spent their lives accumulating a large amount of capital. The access to these funds is actually the difference maker, as when older folks become scam victims, they are losing a lot more money than younger people.

IMPOSTER SCAMS

ABOUT 1 IN 5 PEOPLE LOST MONEY

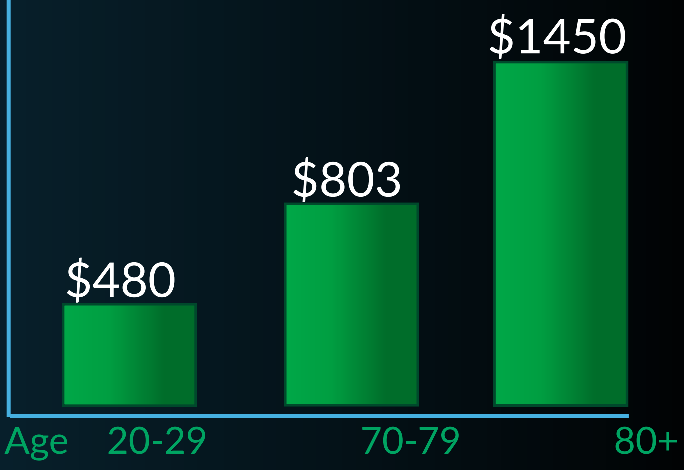
$2.668 BILLION REPORTED LOST | $800 MEDIAN LOSS

[3]



Younger people reported *losing* money to fraud more often than **older people.** [4]

But when people aged 70+ had a loss, ***the median loss was much higher.*** [5]



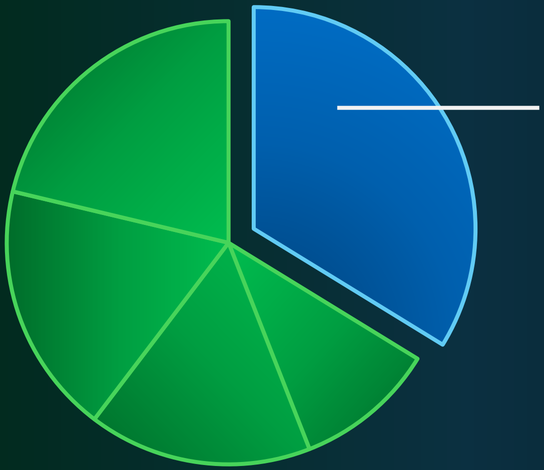
24.2%[6]

Percentage of population reporting household income of $150,000 or more in last 12 months.

Percentage of population over 60:

27.7%

(national average is 23.8)[7]



33.8%

65+ year olds who graduated college studied science and engineering. [8]

High volume of seasonal residents. (Snowbirds)

What Makes Pima County Unique?

You have likely heard it a million times before, but Arizona is a great state for retirees. The warm winter weather and tight-knit communities make Southern Arizona extremely attractive to ‘snowbirds’ as they have come to be known locally. These seasonal residents tend to be older, and that larger demographic is what makes Pima County a hotbed for fraud. With high educational attainment via our science, defense and technology driven economy, there are a lot of financially secure people that call Pima County home. These high numbers make the frequency of fraud attempts much more common, and it is the combination of all these factors that make Pima County ripe for these types of crimes.

Education and Prevention

Increased awareness can stop fraud scams

The good news is that the data suggests the number of reports are down significantly. From 2019 to 2023, we saw a decrease of nearly 60% in fraud cases at the national level.

While a reduction in cases is never a bad thing, it unfortunately was accompanied by an increased amount of financial loss. All this to say that scammers have simply gotten more efficient, likely targeting older folks due to the large access to capital readily available to this group.

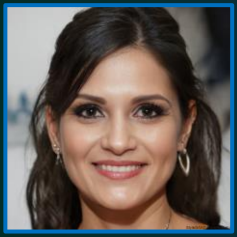
> ***Education is key to stopping this trend, so it is time we increased our fraud awareness.***

Fraud is a unique crime that can be prevented with increased awareness from the public.

What sets fraud apart is that today's schemes typically require a lot of involvement on the part of the victim. Scammers are persuasive in instructing individuals to complete tasks in the furtherance of their overall goal. Because victim participation is so essential, an opportunity exists to counter the scammers actions. A well-informed person can exploit this vulnerability in the scammers plans and severely limit the success of these crimes if they know what to look out for.

Artificial Intelligence

Creating fake people with technology



Pima County is an extremely beautiful and diverse place. None of us would be taken aback by seeing the folks pictured out on the town. We would not blame you if you recognized these faces or believed you have seen these people before. You might even think you know some of them.

Unfortunately, you would be *wrong*.

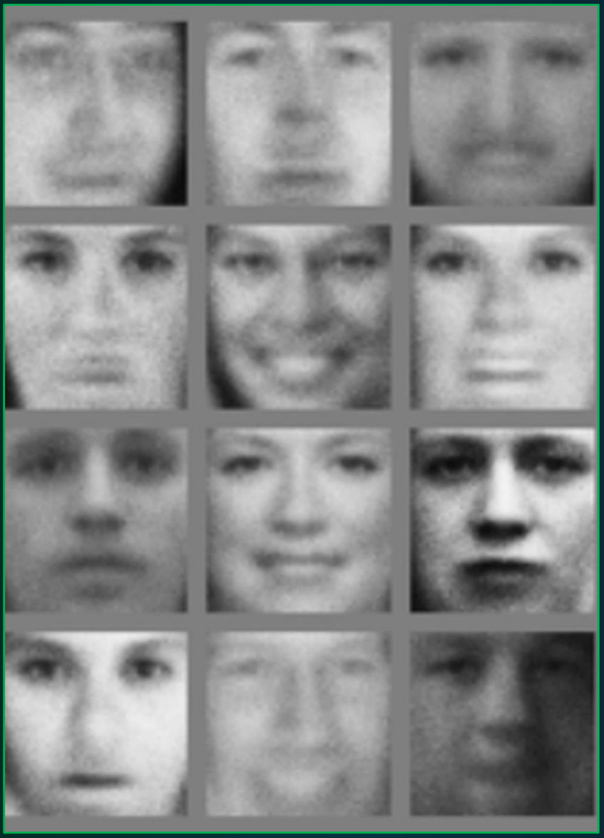
As realistic as these faces look, every single one of them was created with artificial intelligence (A.I.) algorithms. These computer and math-based instructions are just starting to work their way to the public, and have become easily accessible to us all.

The advent of facial creation algorithms has amazing applications for large sectors of our economy. In computer focused fields like video games development, film production, and other creative sectors, these technologies can have a very positive impact on many industries. Like most good things however, once these technologies get into the wrong hands, they can be used for nefarious

[9]

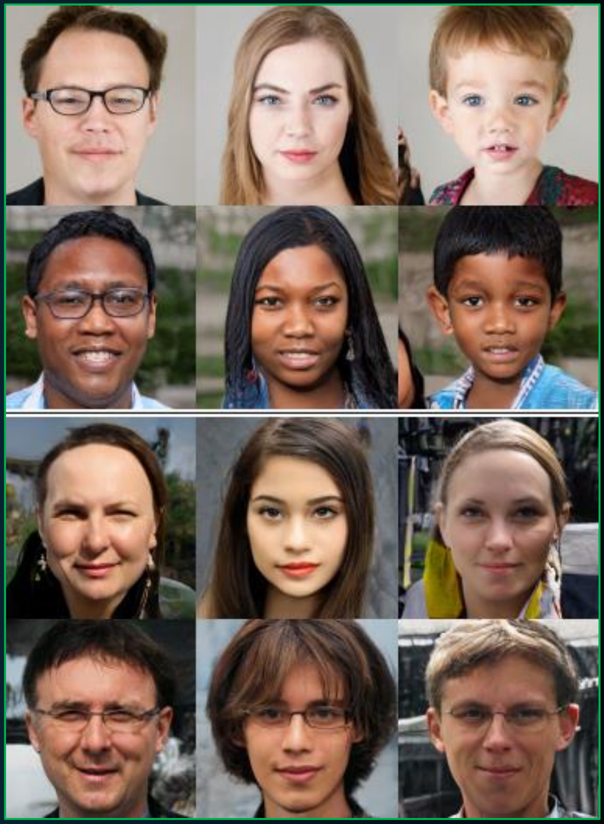
Artificial Intelligence

Creating easy computer-generated imagery



[10]

It took four years of research to go from the faces on the ***left*** to the faces on the ***right***.



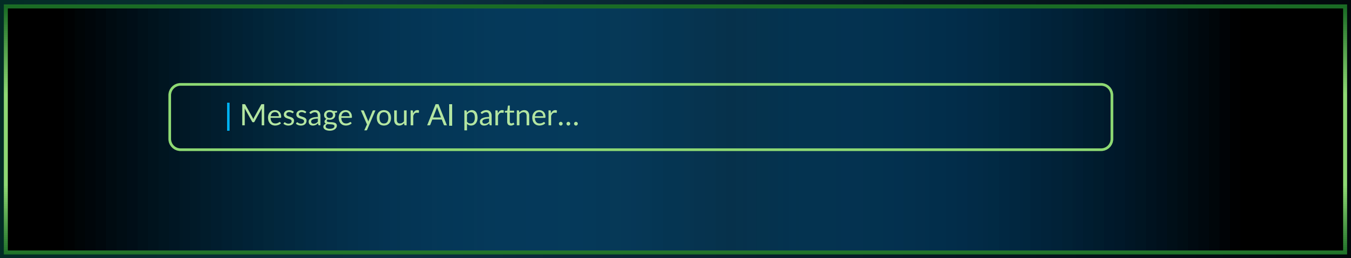
[11]

The technology has advanced so fast that in 2024, ***anybody*** can create high quality faces in mere seconds.

Fake images aren't the only thing that's gotten easier to create. The stories behind them can also be crafted in ***seconds.***

Artificial Intelligence

Writing the stories behind the pictures



| Message your AI partner…

Faces are one thing, but the artificial intelligence you may be most familiar with are the services that can output human-like text with very little informational input. In the past, writing resumes, stories, film scripts, class reports and many other expository ventures, were oftentimes consuming and exhausting. Today, writing these complex pieces is as simple as typing in a simple request to your AI service.

> ***Computers are now capable of outputting text which appears to have been written by a real person, with the generated text appearing in seconds.***

Services like Open AI's ChatGPT, Microsoft's CoPilot, and Google's Gemini (to name a few) are typically free to use and provide a whole host of useful features that may yield amazing benefits for large sectors of our society. Once similar services enter the wrong hands however, they can be used to create anything from fake backstories for dating profiles, to essentially anything that scammers can think of. The high-quality nature of the generated texts means that scams have a stronger appearance of realism. Gone are the days of emails with large swaths of misspelled words that helped us easily identify scam attempts. Modern scams can appear professional and of a high quality, making them difficult to spot and often indistinguishable from real human produced text.

The Scammer’s Goal

Using social media to find victims

okcupid
match.com
tinder

The goal for these scammers has always been the same: find efficient methods to communicate with potential victims and steal their money.

Artificial Intelligence (A.I.) systems have simply assisted them at being more efficient. Scammers must no longer steal real-people’s images to make fake accounts, they can simply create new people instead. These types of services make detection difficult and can result in a more realistic scam experience for victims.

Many of the services above have done well to curb the misuse of A.I. images and text on their services. Unfortunately, not every service is able to stop them 100%. Recognition of this is important because the individuals that slip through the cracks may be able to misuse these services to exploit your hard-earned money.

While scammers may use these emerging technologies to create ‘*new* people’, they use other common tools to conceal and trick you into thinking they are people and services you *know and trust* as well. Let us take a look at *Caller ID Spoofing*.

Caller ID Spoofing

A way to trick you into a sense of trust

Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their true identity.

Scammers can force your device to show any number they want, without you knowing.

Scammers will often spoof local phone numbers so that the incoming call appears to be from a local business or individual. This process is called Neighbor spoofing. They do this because you're more likely to answer calls from your area.

Scammers often spoof numbers that the community knows and trusts such as financial institutions or government agencies.

Voice Cloning

Taking spoofing to new heights

Receiving a phone call from a spoofed phone number is bad enough, but what if when you picked up the call or listened to the voicemail the caller left, you heard a voice that you recognized?

Sometimes, the person on the other end of the line is not the person we believe they are. Unfortunately, the technology exists to now reproduce somebody else's voice.

Welcome to voice cloning, a new way to make crimes even more realistic.

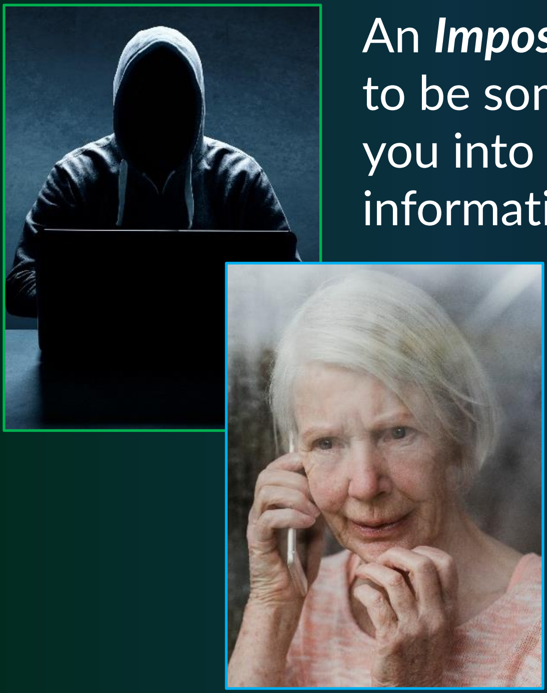
By simply feeding these voice cloning algorithms some sample audio, scammers can make a version of a voice say anything they want, with realistic tones, cadence, and accurate sound. They can do this even though the person never uttered any of the words!

Imagine getting a call from a loved one's phone number, and hearing a voicemail from them telling you they need help and to send money urgently. You may believe this level of realism, and scammers know it.

Now that you are aware of the technology such as phone spoofing, fake faces, fake stories, fake social media applications, and voice cloning, it's time to look at the common scams we see in Pima County, and what role these pieces of technology play in them. Let's look at some specific scams.

Imposter Scams Detailed

What we see in Pima County



An ***Imposter Scam*** occurs when a scammer pretends to be somebody you know or trust to manipulate you into sending money or other personal information when you otherwise would not.

‘*Imposter scam*’ is an umbrella phrase for many different types of frauds where scammers utilize the same method of disguising their identity from the victim. Other agencies may add different scams into this category but the outcome is the same, **to get your money!!!**

Common imposter scams in Pima County fall into two main categories:

Business Scams

- Lottery & Sweepstakes
- Company Impersonation

Personal Scams

- Romantic Interest
- Family Emergency

Common Imposter Scams

Lottery & Sweepstakes

How this works:

You are contacted via a phone call, text message, or email advising you that you have won a large cash prize. During the process of trying to collect your winnings, you will be told that you need to pre-pay the taxes first.

Most common variation:

- Pre-pay taxes on winnings.

Technology Utilized: Call Spoofing
Psychological Tactic: Urgency/Act Fast

Company Impersonation

How this works:

You are contacted via text message or email from a business informing you of some complication which has arisen requiring your attention. At some point in the interaction, they will request you send them money (gift cards, bitcoin, etc..) to help resolve the issue.

Most common variations:

- US Postal Service, UPS, and FedEx: missed packages.
- Sheriff’s Department/FBI: Warrant for your arrest.

Technology Utilized: Call Spoofing,
Psychological Tactic: Urgency/Act Fast + Fear of Punishment/Confusion

Common Imposter Scams

Family Emergency

How this works:

You are contacted via a phone call from a friend or loved one who is experiencing some type of emergency. They need you to send them money quickly or something bad is going to happen to them.

Most common variations:

- Got arrested and need bail money.
- Kidnapped in Mexico.
- Car broke down and need a tow.

Technology Utilized: Call Spoofing
Psychological Tactic: Urgency/Act Fast

Romantic Interest

How this works:

You've been speaking to a possible romantic interest online for some time. At some point, the person wants to visit you but needs money to do so. They will inevitably ask you for money to help. The visit never happens due to some new complication and they continue to ask for more money to help.

Most common variations:

- They want to visit but need travel money.
- They are almost there but got into a car accident.
- Stopped at the border and agents want money.

Technology Utilized: Fake Profile Images, Fake Details
Psychological Tactic: Companionship/Love

Money Mules Explained

How victims are made to move money

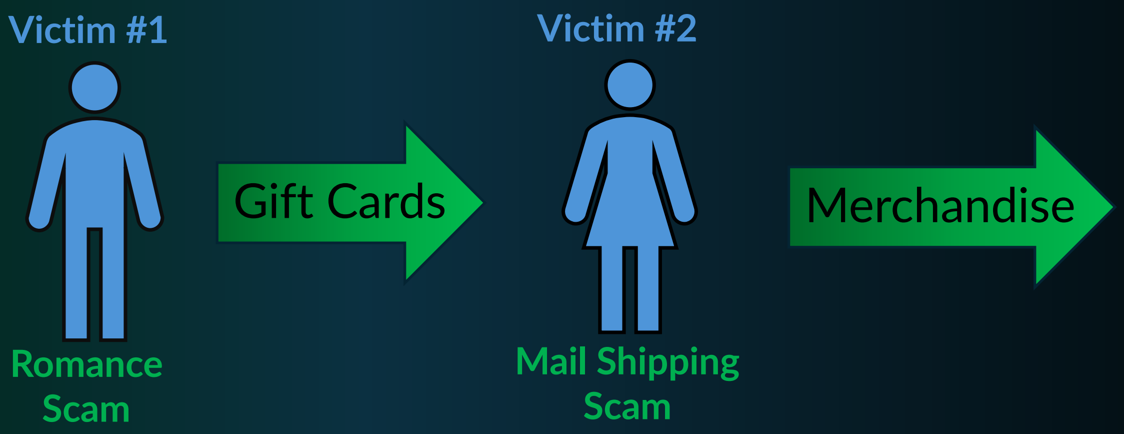
A '***money mule'*** is someone who receives and moves money that comes from other victims of fraud. Some money mules know they are assisting with criminal activity, but most are unaware that their actions are helping fraudsters.

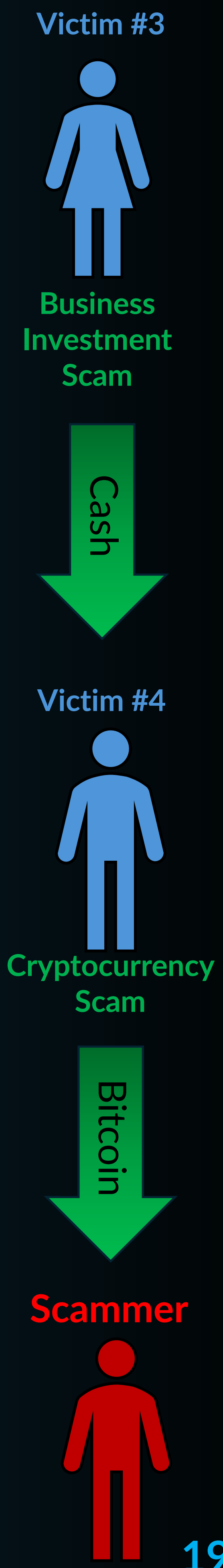
Just as a mule has been bred from a horse and donkey to create a more useful animal, money mules have been methodically crafted by their scammers with the goal of transitioning them into effective tools to move illicit funds. They are great for moving money, just like mules are for hauling cargo.

> *A **money mule** scam usually starts when other scams have run their course.*

This is because victims typically have no more money to be scammed out of, but because they have now been emotionally tied to the situation, they can be easily manipulated to start moving funds.

Money mules add layers of distance between crime victims and criminals, making it difficult for law enforcement to accurately trace money trails.





Money muling is a way for scammers to create distance between the original victim and them. The higher the degree of separation, the more difficult it is to track the funds and ultimately find the suspect.

As the diagram illustrates, money muling typically looks something like this: The first victim loses money as part of some type of scam, in this case it is a romance scam, and is told to send money to somebody else. From the victim's perspective, this money transfer appears legitimate, maybe they believe they are sending it to their online romantic partner for a plane ticket, but in reality, they are sending it to another person in the chain- the first mule.

The recipient of those funds (victim #2) might be the victim of another type of scam. They likely live in another state from the first victim. For example, victims may be told the incoming money is for a mail shipping business they believe they are a part of. They are told to purchase merchandise with the money and mail the purchase to a 'business partner'. This business partner is simultaneously a victim of another scam. This process continues until the last mule sends the funds to the scammer, who is often overseas.

Local Scams Are Now Global

Small cases operate out of other countries

The nature of modern-day fraud makes holding offenders accountable difficult at a local level. If we find a scammer in Pima County, we can investigate, arrest, and prosecute as needed. But what happens when the scammers are in other countries entirely? Well, that's where things can get complicated.

The use of technology makes identifying suspects difficult.

Global reach of scammers means local prosecution is extremely difficult.

Because these scams occur over time, evidence is typically lost.

Overflow of federal cases makes smaller losses less of a priority.

These complexities make the likelihood of getting money back pretty limited.

It is unlikely these complexities can be worked out overnight. Because of this, prevention is key to stopping these scams in the first place.

Let's talk about some small things you can do ***today*** that will have a huge impact in reducing these crimes.

Tips to Prevent Scams

Know the people you are dealing with

Periodically audit your friends lists on social media like Facebook, Instagram, WhatsApp, etc.

Scammers will often add you on social media to gain access to the information you have hidden to the public, but visible to friends.

Smokey Bear
36 mutual friends

McGruff
7 mutual friends

Normal Guy
0 mutual friends

> ***Things to consider during your friend audit:***

Do you know the person in real life?

Can you confirm the profile belongs to the actual person you know?

Any mutual friends? Do they have a low friend count? A lack of friends or no mutual friends could be the sign of a new account, or one created for a nefarious purpose.

Do many of their posts appear to be spam leading you to unusual websites? They may be using click-bait to get you to scam websites.

Overly professional looking photos in limited numbers, or images that are highly cropped are characteristics typically associated with scams as they tend indicate the images might be from stolen accounts associated with real people.

Tips to Prevent Scams

Independently verifying information

If you receive calls from somebody claiming to be with law enforcement, government agencies, lotteries, or other companies, you should verify they are affiliated with the entity they claim to represent before divulging anything.

Common steps for verification

1) Collect as much information about the caller as possible (name, title, badge number, phone number, agency, reference number, etc.)

2) Inform the caller you will be briefly hanging up to verify their information. Resist the pressure of staying on the call.

3) Locate a verified phone number for the entity the caller claims to represent ***on your own***. You can find these numbers online, on bill statements, etc.

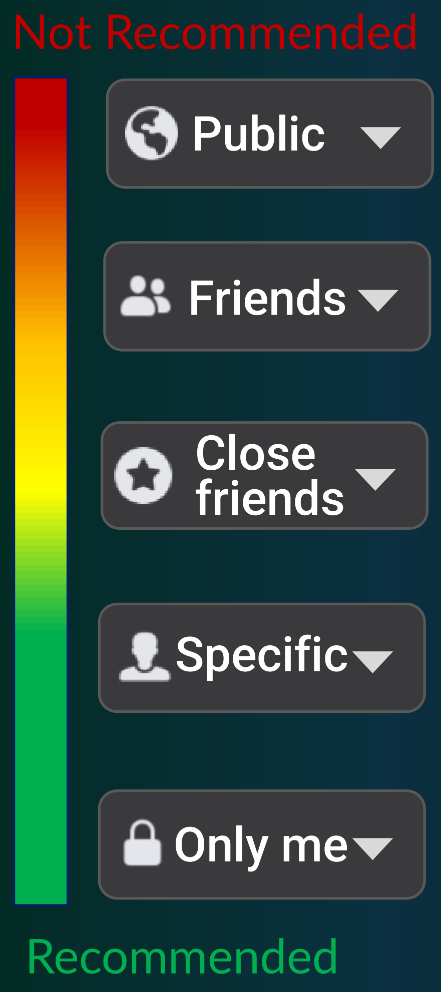
4) Have the entity reconnect you back to the original caller via their own internal means while also confirming the information the original caller provided.

Tips to Prevent Scams

Protecting your personal information

Do not contact the caller at phone numbers they provide. Remember that ***any*** phone number can be spoofed. Just because the original number appears real, doesn't mean that it is.

If you use social media apps like Facebook, Instagram, or WhatsApp, periodically conduct a ***privacy checkup*** in your settings.



Consider limiting posts, photos, and stories which share your real-time location to more restricted groups.

Personal identity information such as birthdays, phone numbers, family members, photo albums, and email addresses should be restricted as much as possible. Publicly displaying this information can make you more vulnerable to identity theft.

> ***Virtually none of your sharing settings should be set to public, if possible.***

Tips to Prevent Scams

Consider unique and complex passwords

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter + number	At least one uppercase letter + number + symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hr	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hr	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

[12]

Use strong, unique passwords.

Data breaches that expose passwords and usernames are common. Scammers will obtain the data and try the stolen information on many websites until they find one that works.

Resist the urge to use the same password everywhere.

Tips to Prevent Scams

Check bank and financial data regularly

> ***Do not be afraid to use mobile banking.***

Many modern mobile banking apps use advanced security methods such as passwords, two-factor authentication, biometric (facial recognition, fingerprints) to safeguard your accounts.

With mobile banking, users can setup alerts to be notified of suspicious transactions, withdrawals over a certain limit, and many more useful features.

Paper statements are slow, and many fraud transactions can occur before they show up in the mail.

They are also not as safe, and when stolen from the mailbox, they can reveal our finances, making us targets for scammers. Consider going paperless.

Tips to Prevent Scams

Consider some alternatives to checks

While checks may be a universally accepted standard for payments, they are highly vulnerable to forgery and account for a very high number of fraud cases in Pima County.

There's a reason the term 'blank check' has become synonymous with unlimited money. Simple fraud techniques can give unwanted access to sometimes boundless amounts of your money.

> ***Checks are no longer the safest way to pay.***

They can be easily stolen, quickly reprinted, and altered on the fly—all with little effort.

New technologies mean we do not have to rely on checks as the only means of financial transactions. Peer-2-Peer services such as Zelle are integrated into most mobile banking apps. These services assist in making quick money transfers to others as simple as typing in a phone number.

Credit cards use funds that belong to the bank, and not your wallet, this can help create additional buffers between your money and potential scammers.

Certified/Cashier's checks and money orders provide the familiarity of checks while also increasing security and limiting access to further funds. Consider these alternatives to limit forgery and fraud.

Tips to Prevent Scams

Gift cards, gift cards, gift cards....

Anytime somebody asks you to purchase gift cards or send them the code on the back of your gift card, it should immediately raise *red flags.*

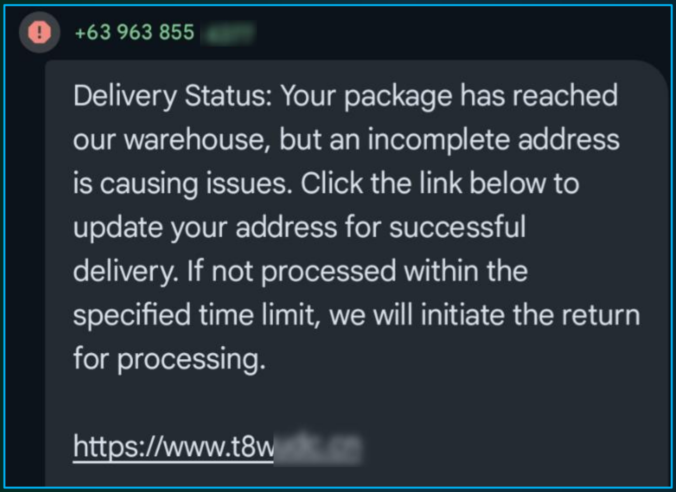
No government agency- to include the IRS, Pima County Sheriff's Department, or FBI- will ever ask for payment via gift cards. But what makes gift cards so special, and why do scammers love to use them?

The answer to that question is simple: gift cards allow for scammers to bypass financial institutions and create ways to immediately access your money. If you have ever made a purchase online, you are likely aware that you never physically swipe your card to authorize a purchase. All that is required is for you to enter cardholder and billing data. The process is the same for purchases made with a gift card except there is no accountholder information at all to enter. All the scammer needs is to access to the gift card code and the funds are now available.

The lack of a name on the card means money is not tied to a person, it is tied to the gift card. This makes it easy for scammers to make online purchases very rapidly, often, and without the need to physically possess the card. They also do not need to know any personal information about the person who bought the gift card.

Tips to Prevent Scams

Five ways to help identify text and email schemes



+63 963 855 [redacted]

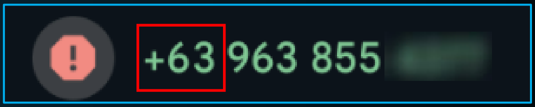
Delivery Status: Your package has reached our warehouse, but an incomplete address is causing issues. Click the link below to update your address for successful delivery. If not processed within the specified time limit, we will initiate the return for processing.

https://www.t8w[redacted]

We've all gotten text messages or emails like the one pictured on the left. While these messages have many variations, they all come with the same goal of trying to take your money. Let's try and identify some common traits of this text message and other emails that can assist you in identifying a scam.

Tip 1: The text message comes from a phone number that has a country code attached to it.

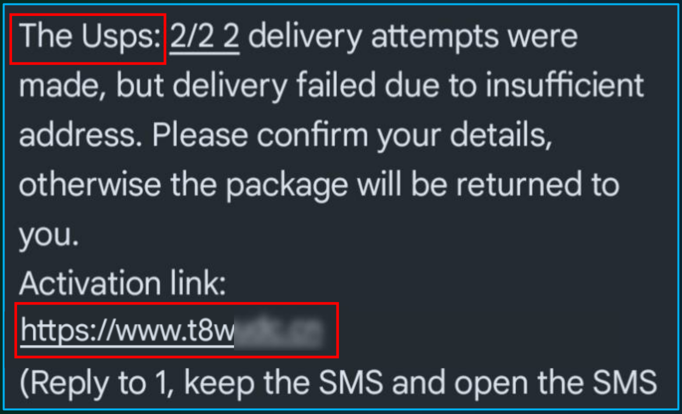
Anytime you see the "+" symbol followed by additional number(s), it likely means the sender had to identify what country they were trying to send the message to. This is usually a telltale sign the sender is outside the United States, as we rarely add this numeric code domestically. This is not true of all messages but can be used to quickly identify international scams.



+63 963 855 [redacted]

Tip 2: The website they include in the message does not match the entity they claim to represent.

Notice this text message claims to be with the United States Postal Service (USPS), but the link they want you to go to is not USPS.com? This is a common deceptive practice used by scammers. Just because they claim they are some entity, doesn't mean they are. Be wary of links leading you to websites you cannot easily identify. Sometimes the link changes can be very subtle, and you might not even spot the difference on first glance!



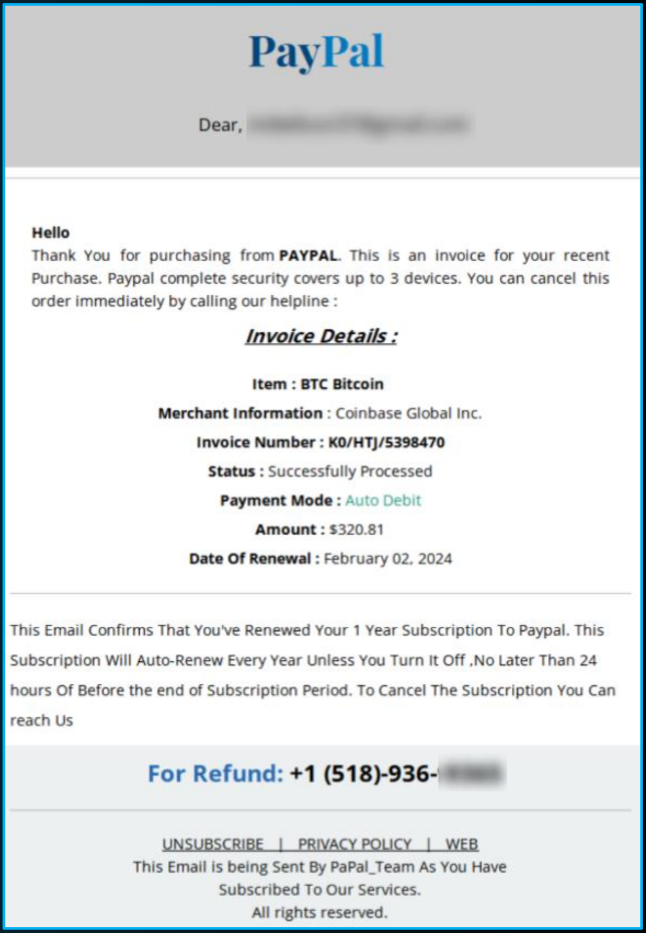
The Usps: 2/2 2 delivery attempts were made, but delivery failed due to insufficient address. Please confirm your details, otherwise the package will be returned to you.
Activation link:
https://www.t8w[redacted]
(Reply to 1, keep the SMS and open the SMS

Tip 3: The email/text message contains many typos and uncommon formatting.

Look closely at this email and you might start to question its legitimacy based solely off these inconsistencies:

- Commas missing where you would expect.
- Words capitalized that should not be.
- Spaces after colons.
- Logos that look unofficial.
- Weird sounding sentences.
- *The list goes on and on...*

This is unfortunate for the scammer, but fortunate for us as it makes identifying illegitimate messages that much easier. Billion-dollar corporations spend a lot of money on accurate messaging – scammers don't. Often, a tell-tale sign is simply a message littered with errors and mistakes.



PayPal

Dear, [redacted]

Hello
Thank You for purchasing from **PAYPAL**. This is an invoice for your recent Purchase. Paypal complete security covers up to 3 devices. You can cancel this order immediately by calling our helpline :

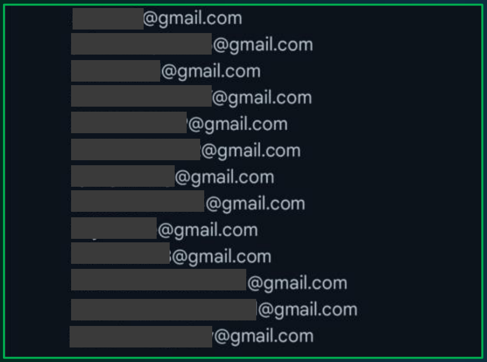
Invoice Details :

Item : BTC Bitcoin
Merchant Information : Coinbase Global Inc.
Invoice Number : K0/HTJ/5398470
Status : Successfully Processed
Payment Mode : Auto Debit
Amount : $320.81
Date Of Renewal : February 02, 2024

This Email Confirms That You've Renewed Your 1 Year Subscription To Paypal. This Subscription Will Auto-Renew Every Year Unless You Turn It Off ,No Later Than 24 hours Of Before the end of Subscription Period. To Cancel The Subscription You Can reach Us

For Refund: +1 (518)-936-[redacted]

UNSUBSCRIBE | PRIVACY POLICY | WEB
This Email is being Sent By PaPal_Team As You Have Subscribed To Our Services.
All rights reserved.

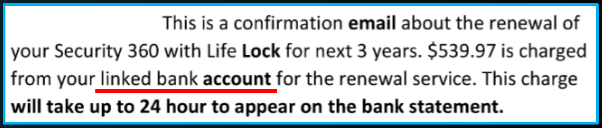


[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com

Tip 4: The email or text message was sent to multiple people at once.

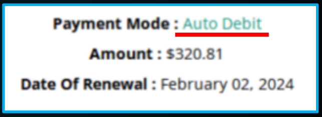
This is fairly straightforward, as the message the scammer sent likely never even mentions your name or personal information. This allows them to send scams out in bulk and hope somebody takes the bait.

Tip 5: The message never identifies which of your credit/debit card, or bank accounts was charged.

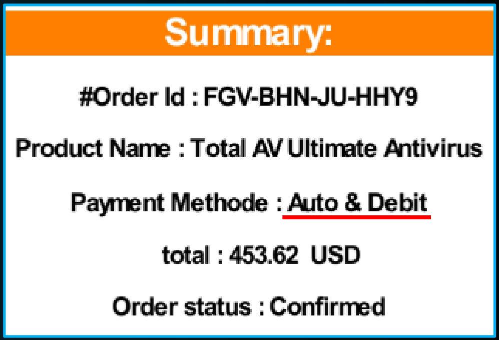


This is a confirmation **email** about the renewal of your Security 360 with Life **Lock** for next 3 years. $539.97 is charged from your linked bank **account** for the renewal service. This charge **will take up to 24 hour to appear on the bank statement.**

Scam emails aim to deceive you about a transaction by sending you a fake invoice that details a transaction you did not make. A sign the invoice is likely fake is that it doesn't identify the actual card or account used to make the purchase. Instead of listing the last four digits of your card or account number like a typical receipt/invoice, the email uses broad terms like 'auto debit' or 'linked account' instead. This is because the transaction is not real, as the scammer does not have your card or account data.



Payment Mode : Auto Debit
Amount : $320.81
Date Of Renewal : February 02, 2024



Summary:

#Order Id : FGV-BHN-JU-HHY9

Product Name : Total AV Ultimate Antivirus

Payment Methode : Auto & Debit

total : 453.62 USD

Order status : Confirmed

Tips to Prevent Scams

Protecting your personal information

ĀURA
IDENTITY GUARD
EQUIFAX
NortonLifeLock
TransUnion
credit karma

Fraud and credit monitoring services are a great way to stay on top of your personal information that is out in the wild. Many of these services will cross-reference your known demographic data with recent third-party data breaches, hacks, and other intrusions and notify you when they find your private information on the internet somewhere you didn't intend.

Many of these services will also monitor your credit, and can alert you when new credit inquiries, accounts, or other financial information has been linked to your name.

The main benefit of this is that you can catch fraud much earlier, and take the necessary steps to prevent further escalation before it gets out of control.

While not all services are free, there are many options (such as the ones pictured above) that offer a whole host of useful services.

Consider the one that is right for you.

Tips to Prevent Scams

Some final recommendations

Do not believe promises of easy money

- Any offer or prize won that seems too good to be true… *probably is.*

Respond with caution

- Do not reply or respond to phone calls, emails, text messages, or other forms of communication from people you don't recognize.
- Be wary of *spoofed* numbers!

Resist Pressure

- Legitimate companies and charities will be open to giving you time to make decisions.
- Demands, and pressure to make quick decisions are *red flags* of a scam.

Use your resources

- Friends, Family, Google, Local Law Enforcement, FTC Response Center 877-382-4357, websites such as the Internet Crime Complaint Center (IC3), and the Consumer Financial Protection Bureau are great tools for scam information

Steps To Consider

What to do if you fall victim to a scam

Don't delete any records regarding what happened— All of that information can be evidence used to identify suspects later.

Contact the Pima County Sheriff's Department (if in unincorporated Pima County) or Tucson Police Department (if in the city) to file an initial report.

Immediately contact your financial institution and file a fraud claim, they may be able to stop pending transactions.

Request your credit report and begin the process of monitoring and freezing your credit.

EQUIFAX

TransUnion

experian™

Do not wait.

Money moves extremely fast today, time is of the essence in these investigations.

Some Additional Resources

Recommended Steps

Contact one of the three credit bureaus to place a fraud alert. You only need to call one of them because when initiating the fraud alert process, they are required to alert the other two bureaus:

Experian.com/help or call 888-397-3742
TransUnion.com/credit-help or call 888-909-8872
Equifax.com/personal/credit-report-services or call 800-685-1111

If someone uses your social security number to obtain credit, loans, phone accounts, or other goods and services, file a report with the Federal Trade Commission:

FTC.gov/idtheft or call 1-877-438-4338

If you believe somebody has used your information to commit unemployment assistance benefits fraud, file a report with the Arizona Department of Economic Security (DES):

Fraudreferralexternal.azdes.gov or call 1(800) 251-2436

To report fraud associated with counterfeit money or goods, contact your local law enforcement agency. They will forward your report to the United States Secret Service for investigation.

To report fraud associated with mail service through the United States Postal Service, file a report with the US Postal Inspectors Service at:

USPIS.gov/report or call 1-877-876-2455 to report mail theft

If there is an emergency, call 911

Sources

This publication:

M. Wilson, J. Knipp, S. Hernandez, T. Rivas, K. Gardner "*Global Deceptions: The Art and Impact of Scams in Pima County*", Pima County Sheriff's Department. March 13, 2024.

References

[1 – 5] Adapted from Federal Trade Commission (FTC) Consumer Sentinel Network, *Data Book 2023*, January 23, 2020, Updated February 8, 2024

[6 – 8] Data Visualizations: U.S. Census Bureau. "AGE AND SEX." American Community Survey, ACS 5-Year Estimates Subject Tables, Table S0101, 2021.

[9] Philip Wang, This Person Does Not Exist. www.thispersondoesnotexist.com, Accessed November 22 2022.

[10] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio. Generative Adversarial Networks. In NIPS, 2014

[11] T. Karras, S Laine, T. Aila et al NVIDIA. A Style-Based Generator Architecture for Generative Adversarial Networks. In arXiv, Cornell University, 2019.

[12] K. Bucholz, Statista, How Safe is Your Password? www.statista.com, Accessed February 25 2024. Adapted from data from security.org

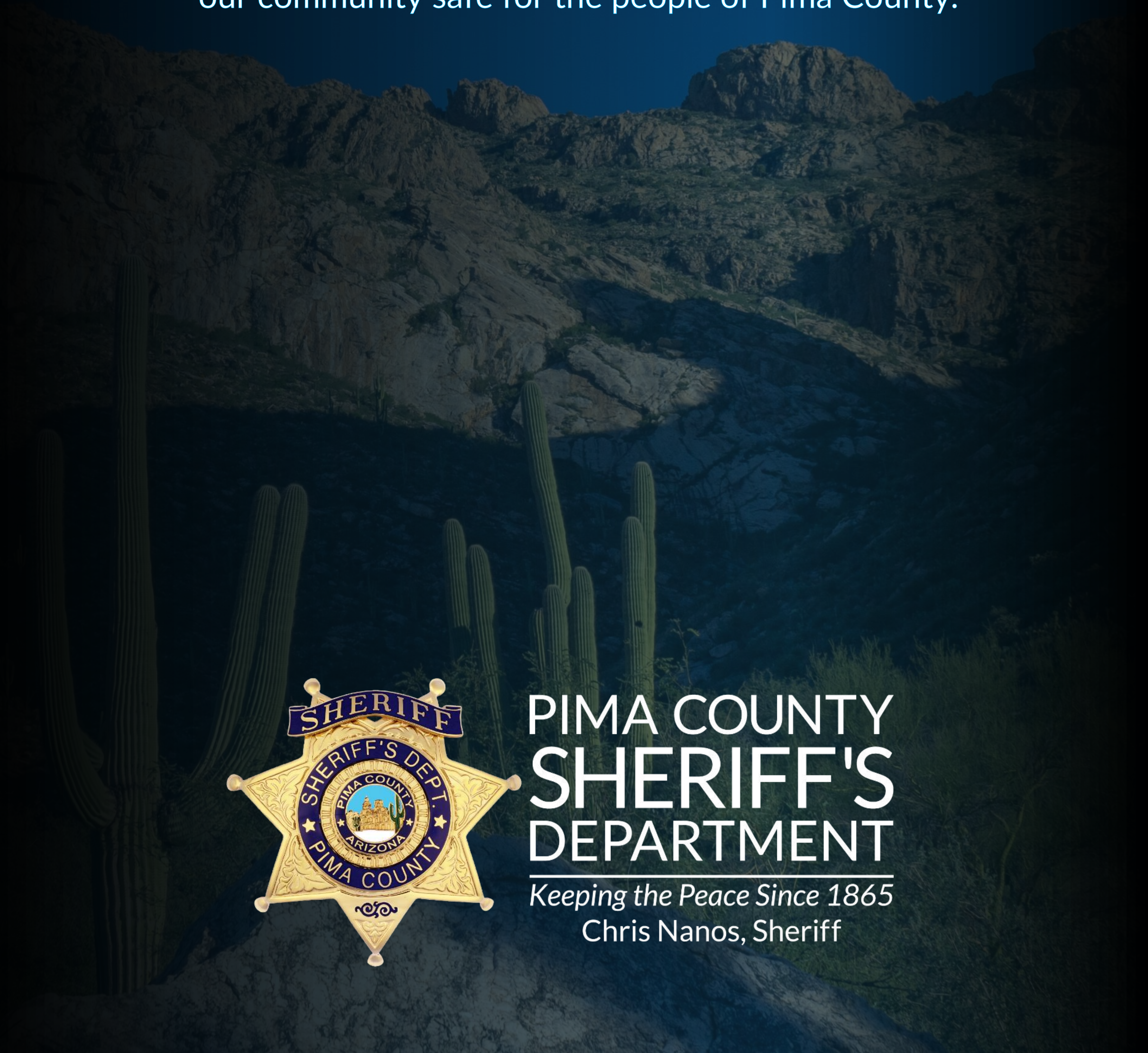
A special thanks to our fraud prevention partners:

Arizona Department of Economic Security
Adult Protective Services

As a leader in public safety, we are committed to serving with

HONOR, COURGAGE, and INTEGRITY

In the fight against crime; and to work relentlessly toward making our community safe for the people of Pima County.



PIMA COUNTY
SHERIFF'S
DEPARTMENT

Keeping the Peace Since 1865

Chris Nanos, Sheriff