

Kentucky Fraud Awareness and Prevention



Office of Senior Protection

LaDonna Koebel, J.D.
Executive Director



Attorney General
DANIEL CAMERON

Kentucky Office of the Attorney General Office of Senior Protection

Scam and Fraud Assistance for Victims: Our team assists victims with next steps to protect from further harm

- Education & Outreach
- Consumer Mediation Services
- Scam and Fraud Assistance
- Data collection/ Investigation



How consumers Report: ag.ky.gov/scams or by calling the Consumer Protection Hotline 1-888-432-9257



Attorney General
DANIEL CAMERON

Consumers reported losing nearly \$8.8 billion to scams in 2022: FTC

Investment scams and imposter scams proved to be costliest for American consumers
Reported fraud losses increase more than 30 percent over 2021

Americans lost \$10.3 billion to internet
scams in 2022, FBI says



Attorney General
DANIEL CAMERON



Email scheme led City of Lexington employees to send \$4 million to scammers

ARREST & INDICTMENT



Hacker steals \$185,000 in ethereum from Bill Murray after NFT charity auction

Published: Sept. 4, 2022 at 3:26 p.m. ET

By [Mike Murphy](#) (Follow)

Donors rally, reportedly make up for stolen funds



Attorney General
DANIEL CAMERON

Commonly Reported Scams

- Identity Theft
- Social Security Scams
- Unemployment fraud
- Romance scams
- Grandparent scams
- Lottery/ Sweepstakes scams
- Tech support & banking scams
- Text scams [your Amazon package is waiting]
- Fake check scams [never send money back]

It is estimated that **only**



senior scam victims report their victimization.



Attorney General
DANIEL CAMERON

Top Scams of 2022 reported to OAG [Money lost]

- 1) Investment Scams
- 2) Real Estate/Rentals
- 3) Identity Theft
- 4) Romance / Social Networking
- 5) Sweepstakes / Lottery Scams

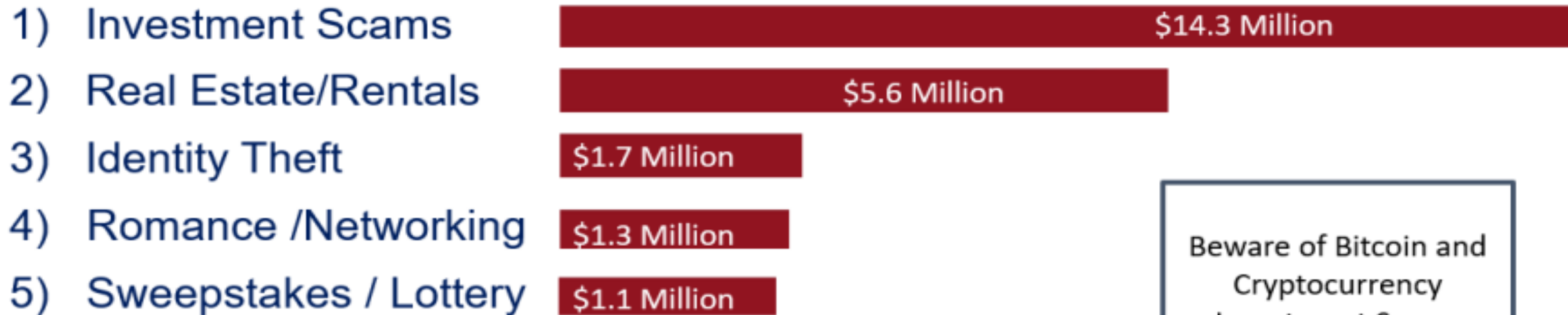


**Since the pandemic began, Kentucky seniors have reported losing nearly \$30 million to scams



Attorney General
DANIEL CAMERON

Top Scams of 2022 [Dollars Lost]



Beware of Bitcoin and
Cryptocurrency
Investment Scams




****Disproportionate impact on Kentucky's elderly**
Since the pandemic began, Kentucky seniors
have reported losing nearly \$30 million



Attorney General
DANIEL CAMERON

Most Common Scams - 2022

- 1) Business Impersonation
- 2) Identity Theft
- 3) Online Purchase
- 4) Arrest Threats / Warrants
- 5) Sweepstakes / Lottery
- 6) Fraudulent Collection Agency



**61% of
Scam
Victims
are younger
than 60**



**39% of
Scam
Victims
are over
Age 60**

Impact of COVID-19 – Scams on the Rise

2019 622 scam reports: \$1,682,931.43

2020 1,734 scam reports: \$5,111,943.94

2021 7,027 scam reports: \$12,775,233.49

2022 2,167 scam reports: \$31,799,253.67



2022 Victims by Age Group



Age 25 and under: 95 reports
\$83,530 in Losses



Age 26 – 39: 325 reports
\$4,762,357 in Losses



Age 40 – 59: 735 reports
\$6,000,617 in Losses



Age 60+: 846 reports
\$19,247,230 in Losses



Not all complaints include an associated age range—those without this information are excluded from this table. Reports with unknown ages: 166 reports representing \$1,705,520 in Losses



Attorney General
DANIEL CAMERON

Business Impersonation

Amazon tops list of impersonated businesses



- Impersonators get your attention with messages to call about suspicious activity or unauthorized purchases on your Amazon account.
- When you call the number, a phony Amazon representative tricks you into giving them remote access to your computer or phone to supposedly fix the problem and give you a refund. But then—whoops—a couple of extra zeros are keyed in and too much money is (supposedly) refunded. They tell you to return the difference. In fact, some people have reported that the “representative” even begged for help, saying Amazon would fire them if the money wasn’t returned.

Increase in Text Scams - Smishing



Text Message
Saturday 7:58 AM

Your Amazon Account has been locked. We recently received multiple failed login attempts to your account.

Recovery your account immediately click link below:

<http://xn--d1amfhmr.xn--p1ai/authcust/>

Please take action on your account within 48 hours to avoid permanent suspension.

Regards,
Amazon Service

The sender is not in your contact list.

[Report Junk](#)



Text Message
Today 8:12 PM

[Information]

Your Netflix account has been suspended, because we're having some trouble with your current account information.

Recovery your account immediately by click link below:

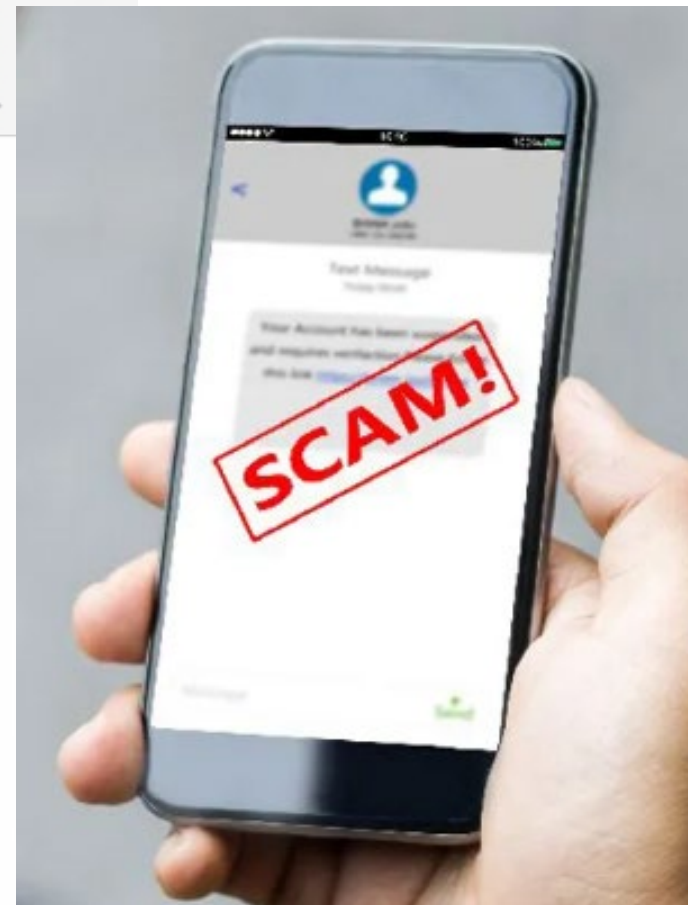
<https://recovery ffm.to/d7m39ez>

Please take action on your account within 48 hours to avoid permanent suspension.

Netflix. Inc

The sender is not in your contact list.

[Report Junk](#)



Attorney General
DANIEL CAMERON

WASHINGTON, March 16, 2023-

FCC ADOPTS ITS FIRST RULES FOCUSED ON SCAM TEXTING

New Action Requires Wireless Carriers to Block Texts from Illegitimate Numbers and Looks to Develop More Ways to Combat Growing Robotext Problem

The Report and Order adopted today requires blocking of text messages that appear to come from phone numbers that are unlikely to transmit text messages. This includes invalid, unallocated, or unused numbers. It also includes numbers that the subscriber to the number has self-identified as never sending text messages, and numbers that government agencies and other well-known entities identify as not used for texting. A second rule will require each mobile wireless provider to establish a point of contact for text senders, or have providers require their aggregator partners or blocking contractors to establish such a point of contact, which senders can use to inquire about blocked texts.

FCC Shuts Down Illegal Robocaller After Repeated Warnings

The agency orders the first robocall-related ban to block calls from a repeat offender.



David Lumb 

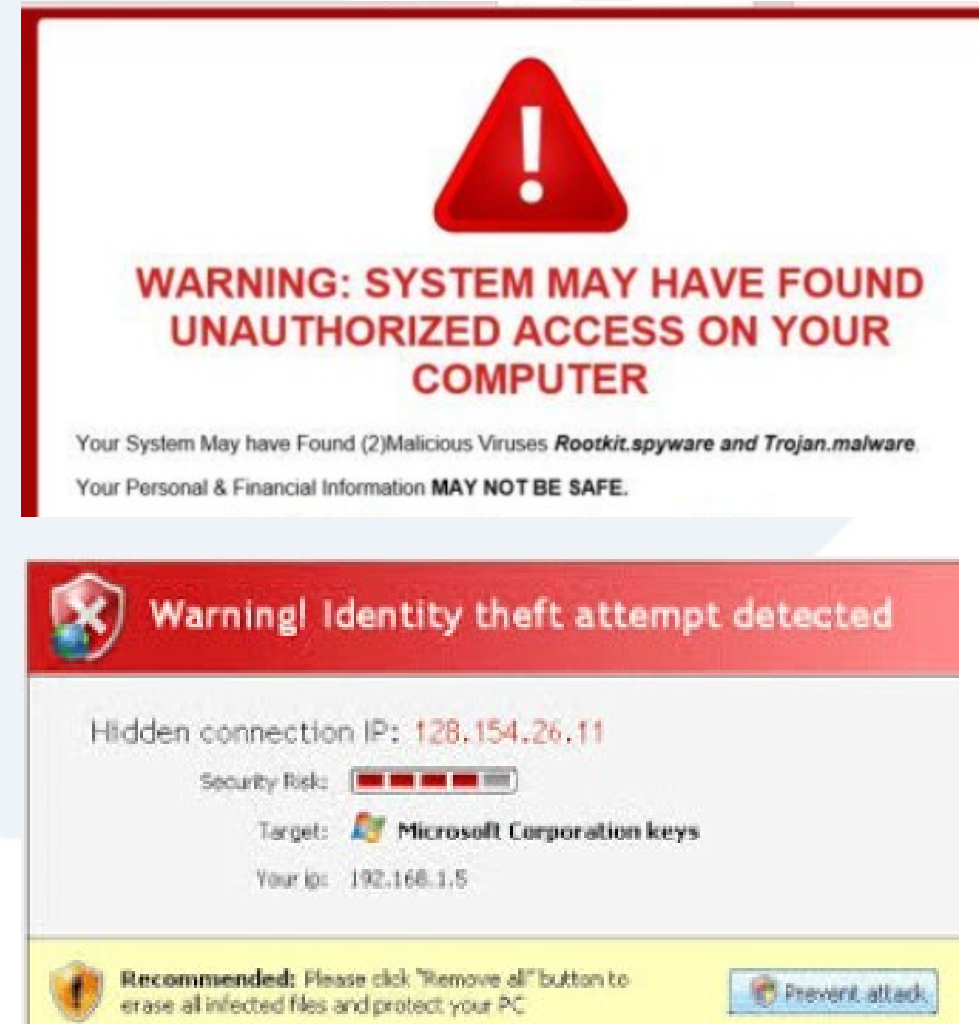
May 11, 2023 4:26 p.m. PT

2 min read

Business Impersonation Tech Support Scams

Tech support scams — Pop-up warnings

Tech support scammers may try to trick you with a pop-up window that appears on your computer screen. It might look like an error message from your operating system or antivirus software, and it might use logos from trusted companies or websites. The message in the window warns you about a security issue on your computer and tells you to call a phone number to get help.



Government Impersonation Scams – Usually by Phone

Utility Company Imposters - Utility company impostors will typically **contact customers with a telephone call** claiming to be a representative from the local water, electric, or gas company. They will demand payment or threaten to shut off service within the hour.

HANG UP and call the real utility company at a verified telephone number.



Attorney General
DANIEL CAMERON

Social Security Scams

- Caller claims to be from the Social Security Administration (your caller ID may even show this - due to spoofing)
- You're told that there's an issue with your SS direct deposit and asks for your SSN or bank account

DON'T FALL FOR IT!



Attorney General
DANIEL CAMERON

Government Impersonation Scams – Usually by Phone

Social Security Scams – As with other Government imposter scams, just remember: The government **will not** call you and ask for personal information, payment, or threaten to cut off your account.



Whether it's a mailed letter, email, text message, or phone call, the scammer will present an unexpected problem or situation and then offer a solution with a hefty price tag. Don't fall for it!

Online Shopping Scam Tips

Pay by credit card

Greater protections! Credit cards are safer than a debit card, cash app, or gift card. If you never receive the item, you can dispute charges and limit the damage if it turns out you were scammed.

Must dispute within 60 days! This time limit is established by the Fair Credit Billing Act, and it applies whether you're disputing a fraudulent charge or a purchase that didn't turn out as expected.



Attorney General
DANIEL CAMERON

Protect Yourself Against Scams

- Know who you are dealing with
- Be cautious of wiring money
- Gift cards are for gifts only
- Don't click on links / text messages
- Treat your personal information like cash
- Protect your Social Security number
- Protect Medicaid / Medicare / Insurance information



COMMON TACTICS OF FRAUD

- Gaining victims trust and confidence
- Try to elicit an **emotional** & quick response
- Shhhhhh.... Don't tell [Scammers don't want you to tell anyone, you must act Now!]
- Getting money in untraceable/
difficult to track ways



What is Caller ID “Spoofing”?

Number spoofing is when a caller uses **technology to display a different caller ID number than the one they are calling from** to mask their true identity.



Why are numbers “spoofed”? The idea is that people are more likely to answer or respond to texts if they see the name of a government agency, bank, law enforcement, or a utility company on their caller ID, or if they see a local number versus an out-of-state or 800 number.

Spoofing makes it IMPOSSIBLE to know if you’re talking to a real government employee or a scammer! Hang up and only call verified numbers from a billing statement or reliable source.

Tips for Scam Calls

Don't answer calls from unknown numbers. Let them go to voicemail.

If the caller claims to be from a legitimate company or organization, **hang up and call them back using a valid number** found on their website or on your latest bill if you do business with them.

Don't click or say "Yes": If you answer and the caller (often a recording) asks you to press a button to stop receiving calls, or asks you to say "yes" in response to a question, just hang up. Scammers often use these tricks to identify, and then target, live respondents, or to use your "yes" to apply unauthorized charges on your bill.

Be Aware: Caller ID showing a name no longer means it is necessarily the identified caller.

Common Theme: Scammers Want Money You Can't Get Back - CASHLESS TRANSACTIONS

Scammers are increasingly looking for cashless ways to scam victims, making it difficult to recover money for victims.

Gift Cards are for Gifts!!!

Never send a picture of the code on the back of the card! The money likely can't be recovered.



CASHLESS TRANSACTIONS USED TO FURTHER SCAMS

- Bitcoin & Cryptocurrency
- Cash Apps
- Wire Transfer Services



Online Shopping Tips

- **Pay by credit card (NOT debit card).** Greater protections! That way you can dispute charges and limit the damage if it turns out you were scammed.
- **Research unfamiliar retail, travel and charity sites online** Search to see if their name is associated with terms like “scam,” “complaints” or “reviews.”
- **Look for return and refund policies** when shopping on an unfamiliar or suspicious site, and make sure they are clear. Be sure to look for service contact information.



Bitcoin and Cryptocurrency Scams

- Investment and Business Opportunity Scams
 - **Scammers guarantee that you'll make money.**
 - **Scammers promise big payouts with guaranteed returns.**
 - **Scammers promise free money.**
 - **Scammers make big claims without details or explanations.**



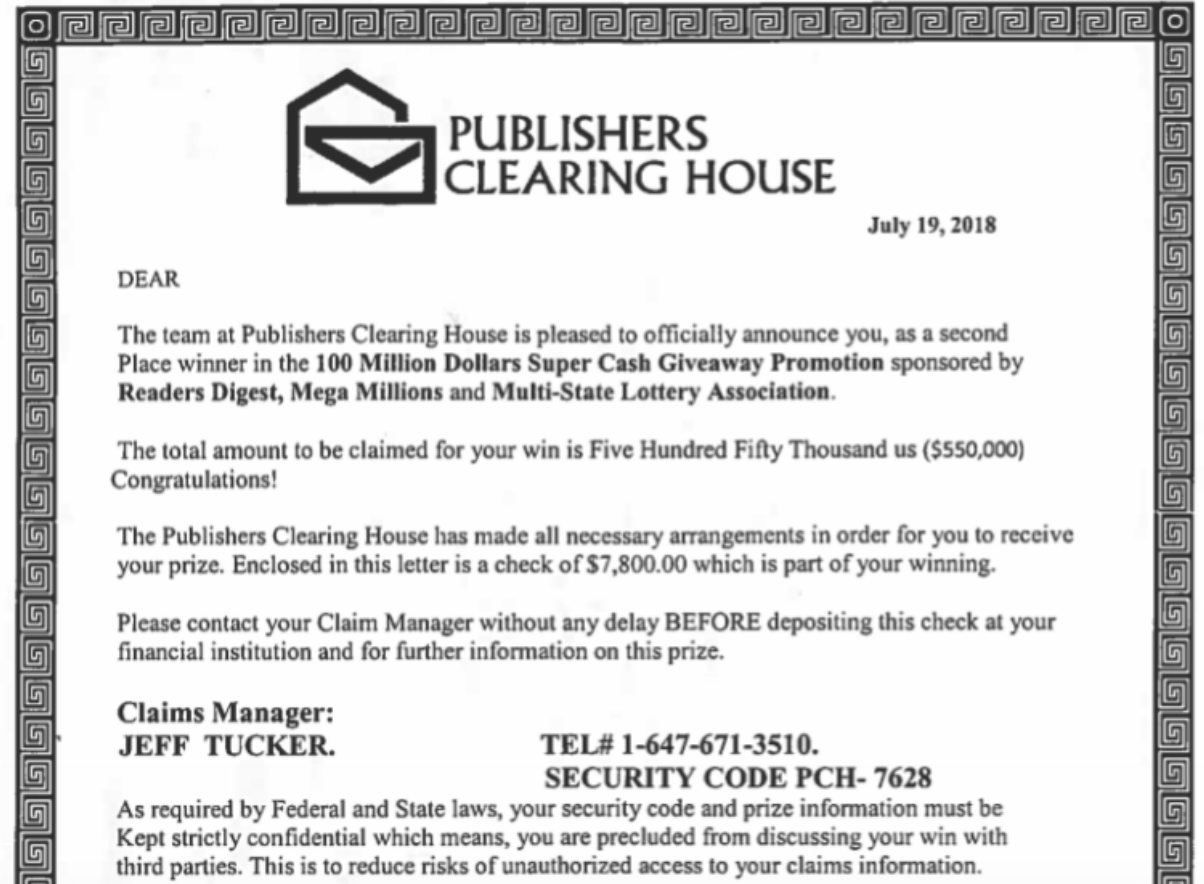
TIPS FOR AVOIDING CRYPTOCURRENCY SCAMS

- ➔ Be very wary of anyone offering to make you quick money with little risk.**
- ➔ Scammers can pretend to be your friend on social media by hacking into their accounts. Always check directly with the person before clicking a link or paying them money.**
- ➔ If somebody claims to be a broker, check them on FINRA's BrokerCheck tool.**
- ➔ Never use an online payment system to pay somebody you don't know.**



Sweepstakes and Lottery Scams

- You didn't win the lottery
- Legitimate sweepstakes **NEVER** ask for money to collect a prize!
- Never give bank account or Personal info by phone

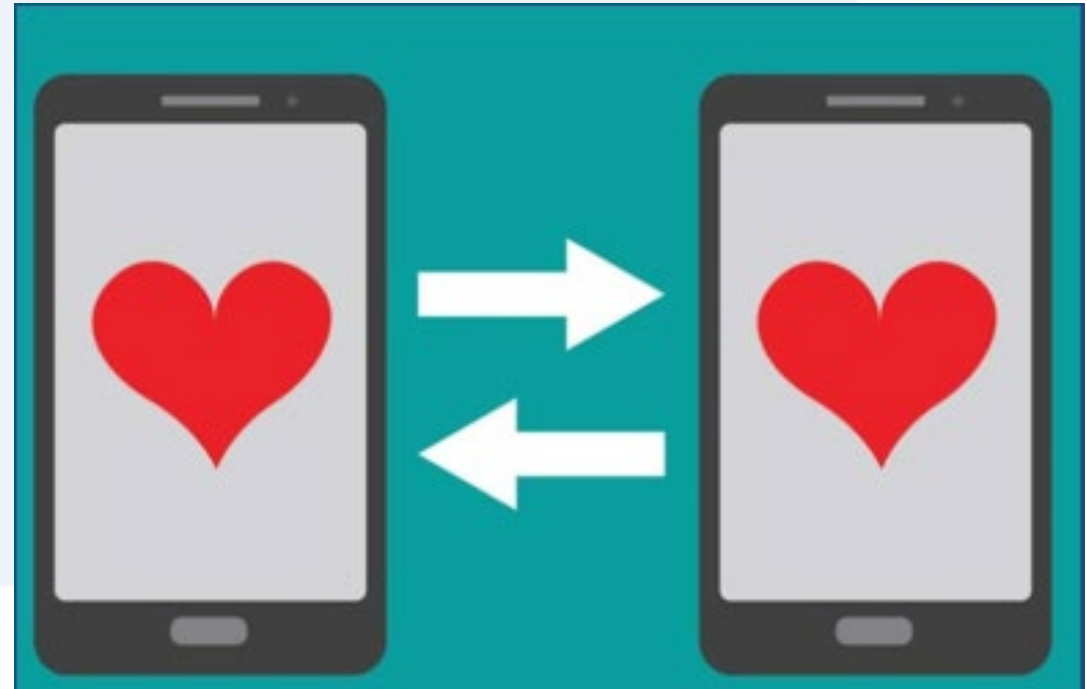


ONLINE DATING SCAMS

Scammers use dating site, online platforms, and chat rooms to meet potential victims.

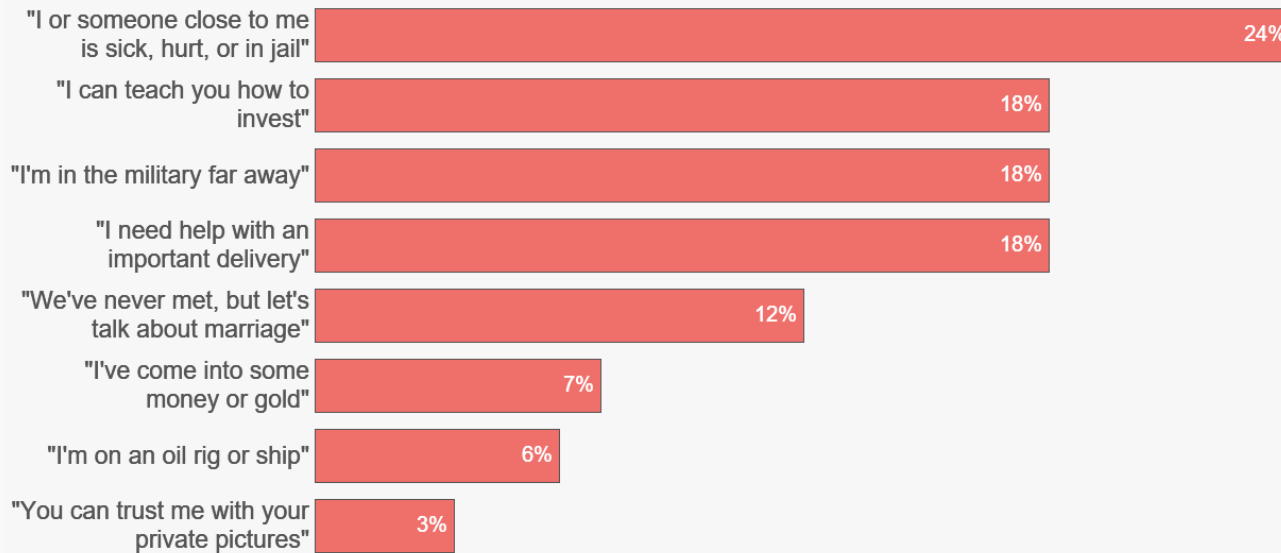
Scammers create fake profiles and create a relationships (usually more than one)

Eventually convince the “loved one” to send money



Top Romance Scam One Liners

Romance Scammers: Their Favorite Lies by the Numbers



Figures are based on 8,070 2022 romance scam reports that indicated a dollar loss and included a narrative of at least 2,000 characters in length. Lies were identified using keyword analysis of the narratives.

The data spotlight also highlights a growing tactic used by romance scammers: sextortion, when a romance scammer convinces a consumer to share explicit photos and then threatens to share those photos with the consumer's social media contacts. The spotlight notes these reports have increased more than eightfold in the past three years, with consumers ages 18-29 six times more likely than older consumers to report this form of romance scam.



Attorney General
DANIEL CAMERON

As a general rule, if the person to whom you're talking asks for money in any context, **they're a scammer.**



Don't fall for emotional manipulation with phrases like, "I thought you loved me."

Don't be afraid to tell family members about your relationship and get their opinion on it.



Attorney General
DANIEL CAMERON

Grandparent Scams

“Grandchild” imposter calls with a frantic plea to send money for an emergency.

Story often involves grandchild being involved in an accident or being detained by police (sometimes it will be the “lawyer” on the phone).

Money is needed immediately and grandparent is told not to contact child’s parents.



Protect yourself from scams on social media

- Try to limit who can see your posts
- Opt out of ads if you can
- Only scammers demand payment by cryptocurrency, gift card, or wire transfer



Actions we're taking to protect victims:

- ▶ Assisting victims
- ▶ Investigation of COVID-related fraud and scams;
- ▶ Education & Outreach;
- ▶ Working with Community Partners
- ▶ DOJ Elder Justice Initiative



Attorney General
DANIEL CAMERON



PROTECTING SENIORS FROM
SCAMS

ATTORNEY GENERAL'S OFFICE
OF SENIOR PROTECTION
502-696-5300

CONSUMER PROTECTION HOTLINE
888-432-9257



Attorney General
DANIEL CAMERON



Let's put a stop to scamming.

Since the start of the COVID-19 pandemic, Kentuckians reported over \$17 million in losses from scams. Follow these tips to avoid scams:

- Hang up on callers asking for money or personal information.
- Don't wire funds or provide gift cards to anyone you don't know.
- Don't act quickly to provide money or information.
- Never send money to receive a prize.

**BE A
FRAUD
FIGHTER!**

Suspect a scam?
Visit ag.ky.gov/scams

This project was supported by Grant Numbers CESF-2020—OAG-0012 and CESF-2020—OAG-0082 awarded through the Kentucky Justice and Public Safety Cabinet by the U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of the

Report Scams

Consumers can report scams to the Attorney General's office online:

ag.ky.gov/scams

Consumer Protection/Scam Hotline
1-888-432-9257



Attorney General
DANIEL CAMERON

QUESTIONS



Attorney General
DANIEL CAMERON