

STANFORD POLICE DEPARTMENT



PSA - Fraudulent Schemes

It is hard to ignore the huge impact that fraud and theft have nationwide. Lincoln County and the City of Stanford residents are no exception to being victims to these crimes. In our current technology driven age, residents can be victims where the perpetrator may live in another state or another country.

What kinds of scams target Kentuckians?

Scams have reached an all-time high in Kentucky, and the Office of the Attorney General is constantly working to stay ahead of con artists. Our office has already warned Kentuckians to be on alert for the following scams this year. Go to the link below to learn more about different kinds of scams.

https://ag.ky.gov/Priorities/Protecting-

<u>Kentuckians/Consumers/Pages/Comsumer%20Alerts.aspx#ctl00 ctl00 m g 9a35ad0c 0348 4959 857f 36b03a9c719f ctl02 AccordionList ctrl8 Collapse</u>

If you have an event that you would like the Office of Senior Protection and Mediation to attend please contact the Office of Senior Protection at (502) 696-5300.

Go here https://ag.ky.gov/about/Office-Divisions/OSPM/Pages/events.aspx to find a scam event near you.

What are Fraudulent Schemes?

Fraudulent schemes can occur in a variety of forms. Some of the more common are:

- Lottery Scams. In these cases, the victim usually receives unsolicited notice that he/she has won a contest, drawing, or
 some other prize waiting to be claimed. The victim is instructed to transfer money to claim a prize, often lured by an
 illegitimate check written to the victim by the scammer in guise of a "no cost, no loss" assurance.
- Sales of Used Vehicles, Properties, Personal effects, etc. In these cases, the victim who is trying to sell something of significant value is scammed by the perpetrator who uses transfer of non-negotiable funds to lure the victim into fronting money for a false shipping or storage arrangement.
- Fraudulent Advertisements / Sales. In this scheme, the scammer offers an item or service for sale, never intending to deliver. These scammers often hide their true identity and develop a trust by not requiring full payment up front. They instruct the victim to deposit the money in a seemingly safe place, often using venues such as eBay, PayPal, or well-known banking institutes. The victim loses the money, does not receive the goods, and the perpetrator disappears. Be especially wary of any request asking for transfer of money to a foreign country or foreign bank account.
- **Fraudulent Business and Charity Requests.** These scams often use phone, mail or internet solicitation to victimize people. The victim's contribution is not applied to benefit the indicated purpose, or the victim's personal information is used in an illegal way.
- Fraud Schemes by Covert Attachments to Legitimate Organizations. In this type of fraud, the scammer usually creates a document under the guise and appearance of being a legitimate appendage of a well-known business. It is usually presented as an alert in the form of a questionnaire or demand for immediate action or additional information to gain access to your financial resources, accounts, or account codes / logins.
- **Impersonation.** The method usually used in this situation is a scammer calling the target and introducing himself as a person in authority, such as a security representative with a financial company, a law enforcement officer, a member of

management with the corporation, etc. The scammer wants the victim to believe he is working to right a wrong or inquire into newly discovered suspicious activity involving the victim's account. The goal is to gain specific and vital information through the victim's cooperation.

- Pleas for Personal Hardship Relief. This usually occurs when you are personally contacted by a subject saying he/she is in need and asking for assistance. Often this is a haphazard contact on the local level and frequently is not against the law, unless there is a prohibitive ordinance against panhandling and gestures of this nature. Even though the money you provide may not be used for the implied purpose, this is not considered fraudulent activity but simply a violation of the understanding between the giver and the receiver.
- **Door to Door Schemes.** In this method, a person or persons canvasses your neighborhood as salesman or representatives of various organizations or businesses. The businesses implied often times are made up and the scammer may present documents, sample products and identification associated with the fraudulent cause. His/Her primary goal is to gain an invitation into the residence and begin his/her pitch and to coerce you to either make a purchase or provide personal information.

Internet Crime Complaint Center https://www.ic3.gov/

Common Scams and Fraud https://www.usa.gov/common-scams-frauds

WHAT YOU NEED TO KNOW ABOUT PHONE AND INTERNET SCAMS

Scammers use the internet or telephone to trick millions of people every year into sending money or giving out personal information. Scammers can be polite and charming. They may say they work for a company that you recognize. They may know your name or certain things about you and make you feel special. They promise things like lottery winnings, prizes, friendship, or romance. But they don't keep these promises.

Are you an older adult? Do you have savings? Do you live alone? Then be on the lookout for scammers. The Stanford Police Department wants seniors, their families, and caretakers to know about common phone and internet scams, how to stop them, and how to get help and report them.

HOW DOES A PHONE OR INTERNET SCAM WORK?

Scammers may offer prizes, products, or services. They want you to say "yes" quickly. They say you must act right away. They may even try to scare you by saying you could be taken to court or to jail. Look out for statements like these: You've been specially selected for our offer.

This is a free trial offer.

You'll get a prize if you buy our product.

You've won money in the lottery.

Don't tell anyone that you've won.

You have to pay us now to receive our special offer.

You trust me, right?

We need you to confirm your personal/billing information.

If you don't pay us now, we will sue you (or you will be arrested).

PHONE AND INTERNET SCAMS

<u>Imposter Scams:</u> An "imposter" is someone who pretends to be someone else. Scammers may email or message you and say they are a family member or someone who wants to be your friend. They may even say they love you. They try to win your trust and ask you to send them money.

Grandparent/Grandchild Scam: "Grandma, I need money for bail. Please don't tell mom!"

Romance scam: "I wish I could visit you, but I don't have enough money for a plane ticket."

Government Grant scam: "You've been awarded a grant and just have to pay taxes and fees to get it."

<u>Tech Support Scams:</u> You get an email or a pop-up alert on your computer. It says your computer has a virus or other security issue. You are told you must call a tech support company. This company asks for remote access to your computer so they can fix the problem. Once they have access, they say your computer has many different viruses that

they can take care of—if you pay them a large amount of money. Or they may install malware—a program that steals your personal data, like usernames and passwords, or even whole computer files.

<u>Lottery Scam:</u> Scammers say they are lottery officials or with a sweepstakes company. They tell you you've won money. Then they ask you to pay them upfront to cover fees or taxes. But they take your money and never give you the winnings they promised.

<u>Phishing Scam:</u> Scammers pretend to be from credit card companies or banks. They trick you into giving them your personal information. They may send you an email or text like this:

Warning: We have detected an unauthorized transaction on your account. To ensure your account is not compromised, please click the link below and confirm your identity.

Our records indicate that your account was overcharged. You must contact us immediately to receive your refund. IRS Imposter Scam: Scammers say they are with the Internal Revenue Service (IRS). They say you owe back taxes. They may threaten that you'll be arrested, deported, or have your driver's license taken away if you don't pay them. Or they might say you must give them your bank account number to receive a tax refund. If you receive this call, contact the IRS right away at (800)366-4484, or visit their website: www.irs.gov/uac/report-phishing. Remember, the IRS will contact you initially by mail (NOT email or phone), and will always give you a chance to question or appeal any amount they say you owe. They will never say you will go to jail for not paying.

<u>Utility Bill Scam</u>: Scammers say they're from your local utility company. They say you're behind on your bill and that your service will be cut off if you don't pay right now. They ask for your credit card information over the phone. Remember, utility companies usually send notices of overdue service fees by mail. Always call your utility company using the number on your bill to find out if you really owe them money.

HOW TO AVOID PHONE AND INTERNET SCAMS

Sign up your phone number with the National Do Not Call Registry by visiting www.donotcall.gov or calling 888-382-1222. If you get a telemarketing sales call after you are on the registry it might be a scam. You can also sign up with the Kentucky Attorney General's Office Do Not Call Program, https://www.nocall.ky.gov or call 866-877-7867.

If a caller says you must act right now to receive a special offer, don't do it. Ask them to give you contact information and send you information in writing so you have time to research the organization and review the offer.

If the caller says they're with a company you recognize, but you're still not sure they're telling you the truth, hang up. Call the company using a number from their official website or the phone book.

Look out for websites with misspelled words or logos and pictures that are hard to see or read. They may be fake sites run by scammers. Check the URL (site address) to see if the web address matches the one for the real company.

Only enter banking or other sensitive personal information on secure websites that you trust. The web address should start with https:// and the web browser should display a closed padlock, which means the connection to the server is encrypted. This will protect your information so no one else can see it or use it.

Only share your financial and personal information with callers that you know and trust.

Pay with a credit card. Don't send cash, use a debit card, or send a wire transfer. When you use your credit card, you may have protections against fraud through your credit card company.

WHAT TO DO IF YOU BECOME A VICTIM

Here are some things you can do:

<u>Document It:</u> Write down everything you remember about what happened. Include the names of the companies and people you spoke with. Also write down the dates you spoke with them.

Take Action and Report:

Contact your bank or credit card company right away. Stop the payment if you can.

Report what happened to federal and/or state agencies. Here are some places you can call for free:

Eldercare Locator helpline, (Department of Health and Human Services): (800) 677-1116.

Anti-Fraud Hotline (U.S. Senate Aging Committee): (855)303-9470 between 9 a.m. to 5 p.m. EST, or visit www.aging.senate.gov/fraud-hotline.

Victim Connect hotline (Victim Connect Resource Center, National Center for Victims of Crime): (855) 484-2846.

Federal Communications Commission's Consumer Call Center: (888) 225-5322.

File a complaint with the following state and federal regulators:

Call the Kentucky Office of Consumer Protection at (888) 432-9257 or (502) 696-5389, or visit to file a complaint.

File a complaint with the Federal Communications Commission at www.consumercomplaints.fcc.gov. File a complaint with the Federal Trade Commission at www.ftc.gov/complaint.

File a complaint with the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) at www.ic3.gov. Tell your family, caregivers, and friends: Tell others what happened so that they can help you and protect themselves. How can I sign up to receive alerts?

Go to https://public.govdelivery.com/accounts/KYAG/subscriber/new?topic_id=KYAG_1 to sign up to receive Consumer Alerts via email.

Kentuckians should report scams to the Office of the Attorney General at 888-432-9257 or file a complaint online at https://secure.kentucky.gov/formservices/AttorneyGeneral/ScamReport

Relevant Articles

Help Stop Elder Abuse https://www.floydct.com/opinion/help-stop-elder-abuse/article_221d7732-ce74-11eb-9cc7-074b24baf2bf.html, June 2021

Don't Be Duped https://www.todaystransitionsnow.com/living-your-best-life/caregiver-solutions/dont-be-duped/, Jan. 2021

Spot a Scam https://www.todaystransitionsnow.com/living-your-best-life/featured/spot-a-scam/, Nov. 2020

Employment Scams https://www.nkytribune.com/2020/11/ladonna-koebel-employment-and-work-from-home-scams-prevalent-during-covid-19-pandemic/, Nov. 2020

Scam Concern Resolved http://www.columbiamagazine.com/index.php?sid=109154, Feb. 2020

TOP TIPS to Avoid Scams

Hang up. If someone calls asking for money or personal information, hang up. If you think the caller might be telling the truth, call back to a number you know is genuine. And, avoid robocalls by registering your number on Kentucky's No Call List http://nocall.ky.gov/default.aspx.

Do not pay upfront. Scammers often offer prizes or threaten to take action against you, if you don't pay a fee or provide your personal information. Legitimate businesses and government agencies will not threaten you for upfront payments.

Do not wire money or send reloadable credit/gift cards to people you do not know. Legitimate businesses and government agencies will not require you to use these payment methods. It is almost impossible to get your money back after it has been wired, through services like Western Union. Reloadable cards like MoneyPak, Reloadit or other types of gift cards like i-tunes present the same problem.

Slow down. Con artists prey on fear and want to scare you in to taking action very quickly. Before you issue payment or provide your personal information, verify the business by researching it online – verify their website, contact information, search for customer reviews and company policies. **If it sounds too good to be true, it probably is.** If someone is offering you something for free or a prize you never registered to win, it is more than likely a scam.

RESOURCES

The following websites provide more information on phone and internet scams:

- U.S. Department of Justice, Elder Justice Website: www.justice.gov/elderjustice
- Federal Communications Commission: www.fcc.gov
- Federal Trade Commission: www.ftc.gov/complaint
- Federal Bureau of Investigation: www.fbi.gov/scamsand-safety
- Federal Financial Fraud Enforcement Task Force: www.stopfraud.gov