FRAUD ADVISORY

FY23-01 Advisory on Phone Scams

Recognizing common phone scams and then ending the scam call protects USDA, its employees, and the public from criminals using evolving tactics to defraud persons of money or sensitive information.

This advisory should be shared with:

- *All USDA employees and the public*

The United States Department of Agriculture (USDA), Office of Inspector General (OIG), is issuing this advisory to alert all USDA employees and the public of the continued evolution of common phone scams.

This advisory provides publicly available information concerning the tactics used in several common phone scams and one particular scam directed at USDA programs and operations.

The purpose of this fraud advisory is to ensure that USDA employees and the public recognize a recent phone scam directed at USDA, as well as other common phone scams, so that they may immediately end a scam call and avoid compromising themselves.

OIG is aware that USDA employees are often the random target of common phone scams directed at their government-issued or personal cell phones. Generally, the goals of common phone scams are to defraud a person of money or sensitive information. Scam callers use countless, evolving tactics, but generally attempt to exploit a person's fear of economic harm, interest in financial reward, or trust that the call is in the person's best interest. Scammers may act friendly and helpful or may threaten or attempt to scare you. Recently, a scam call containing a pre-recorded message targeted a USDA program. USDA employees should be vigilant and immediately end unsolicited calls that request any government or personal information.

USDA employees and members of the public should report to the OIG's Hotline any calls concerning suspected impersonation of USDA employees, solicitation of any sensitive government information, or if they believe they have already been the victim of a phone scam. For other common phone scam calls, USDA employees and members of the public may report to

the Federal Trade Commission (FTC) by calling (877) 382-4357 or online at ReportFraud.ftc.gov.

USDA Phone Scam

Recently, the OIG received a report of a phone scam targeting the Food and Nutrition Service's Supplemental Nutrition and Assistance Program, specifically attempting to compromise Electronic Benefit Transaction (EBT) card accounts and PIN numbers. The scam call contained a recorded message informing the recipient of the call that their EBT card was compromised and deactivated because of fraudulent activity. The message then informed the person to press "1" on their phone's keypad, and then when prompted, enter their EBT card account number and their "old" PIN number. At this point, the scam call had collected the necessary information to cause an account takeover and deplete the funds before the rightful beneficiary could report the fraud and re-establish control of their account.

Common Phone Scams

The FTC works collaboratively with Federal law enforcement partners to collect information about common phone scams and to educate the public on how to avoid and report scams. The FTC website[1] describes several examples of common phone scams:

Imposter Scams
A scammer pretends to be someone you trust — a government agency like the Social Security Administration or the IRS, a family member, a love interest, or someone claiming there's a problem with your computer. The scammer can even have a fake name or number show up on your caller ID to convince you.

Debt Relief and Credit Repair Scams
Scammers will offer to lower your credit card interest rates, fix your credit, or get your student loans forgiven if you pay their company a fee first. But you could end up losing your money and ruining your credit.

Business and Investment Scams
Callers might promise to help you start your own business and give you business coaching, or guarantee big profits from an investment. Don't take their word for it. Learn about the FTC's Business Opportunity Rule, and check out investment opportunities with your state securities regulator.

[1] https://consumer.ftc.gov/articles/phone-scams#examples%20of.

Charity Scams
Scammers like to pose as charities. Scams requesting donations for disaster relief efforts are especially common on the phone. Always check out a charity before you give, and don't feel pressured to give immediately over the phone before you do.

Extended Car Warranty Scams
Scammers find out what kind of car you drive and when you bought it so they can urge you to buy overpriced — or worthless — service contracts.

"Free" Trial Scams
A caller might promise a free trial but then sign you up for products — sometimes lots of products — that you're billed for every month until you cancel.

Loan Scams
Loan scams include advance fee loan scams, where scammers target people with a poor credit history and guarantee loans or credit cards for an up-front fee. Legitimate lenders don't make guarantees like that, especially if you have bad credit, no credit, or a bankruptcy.

Prize and Lottery Scams
In a typical prize scam, the caller will say you've won a prize, but then say you need to pay taxes, registration fees, or shipping charges to get it, but after you pay, you find out there is no prize.

Travel Scams and Timeshare Scams
Scammers promise free or low-cost vacations that can end up costing you a lot in hidden costs. And sometimes, after you pay, you find out there is no vacation. In timeshare resale scams, scammers lie and tell you they'll sell your timeshare — and may even have a buyer lined up — if you pay them first.

Complaints concerning fraud, waste, and abuse regarding USDA programs can be provided using the USDA OIG Hotline Unit submission form located here.

USDA OIG
Hotline Unit
P.O. Box 23399
Washington, D.C. 20026-3399
Phone: (800) 424-9121
Fax: (202) 690-2474