

Using channels like emails, text, and phone calls; fraudsters typically use scams like these.

Romance Scams



Using fake online dating profiles with photos of other people, scammers say they are from the U.S. but are temporarily traveling or working overseas. Most romance scams start with fake profiles on online dating sites created by stealing photos and text from real accounts or elsewhere. Some of the fictitious occupations include working on an oil rig, in the military, or as a doctor with an international organization.

Scammers quickly profess their love and tug at the victim's emotions with fake stories and their need for money. They often request money for reasons such as a plane ticket, other travel expenses, and customs fees – all needed to get back into the country. The victims often wire their "sweetheart" scammers money or share login credentials with them.

Secret Shopper Scams



Members looking to earn extra cash are frequently tricked into participating in the secret shopper scam. If a member accepts the job, he/she receives a counterfeit cashier's check ranging from \$2,000 to \$5,000. They are instructed to cash the check and purchase money orders and gift cards and send them to the scammers. For their efforts they will keep a percentage of the check they receive. The counterfeit check is subsequently returned unpaid and charged back to the member's account.

Advanced Fee Scams



In the advanced fee scam, the scammer informs a victim that he/she has won a large award (think bogus lottery scam) or is entitled to a large inheritance from a deceased relative. However, before the victim can receive the money, he/she must supposedly pay taxes or fees. The victim ends up wiring funds to the scammer to pay the taxes or fees but never hears from the scammer again.

Relief Scams



Scammers attempt to take advantage of times of uncertainty to con people into giving up their money to aid those in need in fraudulent relief funds. Recent scams that have been attempted: flood / disaster relief; Covid-19; Ukrainian assistance; student loan debt forgiveness; and other charity scams.

Social Security, Government, and IRS Scams



Scammers impersonating Social Security Administration employees over the phone to request personal information or money. Imposters may threaten you and demand immediate payment to avoid arrest or legal action. Many scam calls "spoof" official government numbers, such as SSA's National 800 Number, the Social Security Fraud Hotline, local Social Security field offices, or local police numbers. In addition, impostors may use legitimate names and phone numbers of SSA employees.

Similarly, you can get a call from someone who says they're from the IRS. Additionally, the caller may know some of your SSN. They say that you owe back taxes, or you're involved in money laundering, drugs, etc. They threaten to sue you, arrest / deport you, or revoke your SSN or license if you don't pay right away. In order to avoid legal action, you asked for your account info or are asked to send money in the form of gift cards, wire transfer or cash.

Tech Support Scams



Someone calls and says they're a computer technician. They might say they're from a well-known company like Microsoft or Apple, or maybe your internet service provider. They tell you there are viruses or malware on your computer, and you'll have to provide remote access to your computer or buy new software to fix it. These scammers might want to sell you useless services, steal your credit card number, or get access to your computer to install malware, which could then let them see everything.

The **tech support scam losses amounted to more than \$347 million** in 2021 according to the FBI's Internet Crime Report. Additionally, most victims, almost 60 percent, report to be over 60 years of age, and experience at least 68 percent of the losses