

## Common Scams

**1. Bogus Health Products.** Since the 1800s! Talk to your doctor before using any “new” health product – especially those marketed directly to consumers and which make outrageous claims.

**2. Advance Fee Loans** – People search the Internet for a lender who will help them. Instead, they find fraudulent websites promising easy credit and loans. The offers are bogus; people never receive their loans and wind up worse than they were before. If a loan company asks you for payment upfront, they’re not legitimate.

**3. The Nigerian Scam** – Since the 1980s, this scam has defrauded scores of U.S. consumers. Via email you learn a rich foreign relative has died or is trying to get funds out of a war-torn region. You have to give *them* money upfront. Payment occurs via wire transfer; sometimes a fake check is sent. Checks bounce and people are out the money they wired.

**4. The Grandma Scam** –Victims receive a call from a “grandchild” in distress in another state or foreign country. Grandparents are told to wire money to “the police.” The best defense is to remain calm. Make them give you their name. Insist on calling your son or daughter. Chances are, you’ll find your grandchild safe at home.

**5. Foreign lotteries or sweepstakes:** A check comes in the mail—to cover “taxes, fees or insurance.” You’re supposed to cash the check and wire back funds to claim your prize, but the check is no good. Remember, it’s illegal for U.S. citizens to enter foreign sweepstakes or lotteries. If you have to send money, even if they send you a check, you haven’t won anything.

**6. Overpayment Scams** – Your KSL or Craigslist ad receives an email expressing interest in the item. The mystery buyer’s English is poor. They want the item delivered through a shipper. They offer to overpay for the item and want you to wire the excess funds after the check is deposited. Never accept a check for more than the selling price and never agree to wire back funds to a buyer.

**7. Charity Scams:** Fraudulent solicitations come over the phone with scammers pretending to be affiliated with legitimate charities. Other scams involve bogus websites created to fool people into providing credit cards. Use charities’ own websites directly. You can investigate unfamiliar charities online at [www.bbb.org/us/charity](http://www.bbb.org/us/charity).

**8. Employment/Mystery Shopping Scams:** Red flags to watch for include:

- Requests for an upfront fee.
- Unsolicited job offers or employment offers that promise exorbitant pay for working just a few hours a day or from your home.
- “Companies” that seek sensitive personal or financial information for credit or background checks.

Regardless of the reason or excuse given by the employer, you should never give out his or her Social Security or bank account numbers over the phone or e-mail.

Mystery Shopping Scams operate just like lottery scams and overpayment scams—here is a check; do a job, wire money back to your “employer.” The checks are no good and you’re out any money you send away.

**9. Phishing:** Scammers, masquerading as a legitimate organizations, send official-seeming email to get you to reveal sensitive data. If you get an email or pop-up asking for personal or financial information, don’t reply. Don’t click any links. Contact the organization mentioned using a phone number you know is genuine, or open a new window and type the company’s correct web address. Use regularly updated anti-virus and anti-spyware software, as well as a firewall.

**10. IRS or Law Enforcement Scam:** You are contacted by someone claiming to be an agent of the IRS or a police officer stating that you have committed a crime or that you have an outstanding warrant. They state that you will be arrested if you do not pay them immediately using a credit card, Western Union, or a Walmart Blue Dot Card. Never give out any information over the phone. If it is a legitimate agent or officer, they will arrange to meet you in person and will never accept payment directly from you. If you are victim of the IRS scam, please contact: [www.treasury.gov/tigta/contact\\_report\\_scam.shtml](http://www.treasury.gov/tigta/contact_report_scam.shtml)