

Protecting Yourself From



SCAMS

We could all use more money, right? Whether it's to add to your current income or to be able to give up your 9-to-5 job altogether, it's fun to imagine the possibilities. And it's this exact perception about finances and income that scammers are banking on. Look Below to find the most common kinds of scams and what you can do to protect yourself (information supplied through USA.gov.)

Census Related Fraud

The U.S. Census Bureau is the federal agency responsible for collecting data about the people and economy of the United States. It must collect some personal and demographic information from people and businesses to do this research.

Some scam artists may act as if they work for the U.S. Census Bureau to collect personal information about you to use for fraud, including stealing your identity. These scam artists may send you letters that seem like official letters from the U.S. Census Bureau, or they may come to your home to try to collect information about you.

The U.S. Census Bureau provides tips to help you spot and report these scams so that you are not a victim. To verify if a survey is from the U.S. Census Bureau:

Common Scams

Wednesday, 11 May 2016 17:35 - Last Updated Wednesday, 11 May 2016 18:47

- Call your regional U.S. Census Bureau office if someone wants to visit your home to conduct a survey.
- Call the National Processing Center if you receive a survey by mail or phone.

Charity Scams

Not all organizations that claim to be charities or help people are reputable. Some scam artists set up fake organizations, taking advantage of the public's generosity immediately after a tragedy or major disaster. Follow these tips to help you detect common charity scam tactics:

- Check out the charity with the attorney general or the Better Business Bureau before you give.
- Don't give in to high pressure tactics such as urging you to donate immediately.
- Don't assume that you can get a tax deduction for donating to an organization. Use the IRS's database of 501(c)3 organizations to find out if it has this status.
- Verify the name. Fake charities often choose names that are similar to well established charities or use keywords that elicit sympathy, such as "children", "cancer", or "disaster relief".
- Don't send cash. Pay with a check or credit card.
- If you suspect charity fraud, report it to the Federal Trade Commission. Although the Do Not Call Registry doesn't apply to charities, you can ask an organization not to contact you again.

Financial Fraud

Scam artists use different types of fraud to try to trick people out of their money. Two common types of fraud are banking scams and investment scams.

Popular banking scams include:

- fake check scams, where a scam artist creates counterfeit checks that look legitimate, with watermarks, routing numbers, and the names of real financial institutions. They then try to deposit them in banks, use them as part of other frauds against consumers, or use them to pay companies for products or services.
- unsolicited check fraud, where a scammer may send you a check that you didn't have a legitimate reason to receive. Unfortunately, if you cash it, you may be authorizing the purchase of items you didn't ask for, signing up for a loan, or something else you didn't ask for. The Federal Trade Commission offers tips to help you avoid being a victim of these scams, and recommends what to do if you have been a victim.
- automatic withdrawals. A company sets up automatic withdrawals from your account that you didn't approve.
- phishing. E-mail messages that ask you to verify your bank account number or debit card PIN. By clicking on the link or replying to the email with your account number, you are giving a scammer access to your financial accounts.

Investment Scams

Investment scams prey on your hope to earn interest or a return on investment on the amount of money that you invest. The Securities and Exchange Commission (SEC) offers overviews of many common investment frauds, and tips to avoid being a victim.

If you are the victim of an investment fraud, you can file a complaint with the SEC or with your state's securities administrator.

Lottery and Sweepstakes Scams

Not all lotteries and sweepstakes are legitimate. Before you participate, keep these tips in mind:

- Scam artists often use the promise of a valuable prize or award to entice consumers to send money, buy overpriced products or services, or contribute to bogus charities.
- Legitimate sweepstakes don't require you to pay to collect your winnings.
- Scam operators use the telephone and direct mail to entice U.S. consumers to buy chances in foreign lotteries. These lottery solicitations violate U.S. law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail.

Pyramid Schemes

A pyramid scheme, also known as Ponzi scheme, is an illegal form of multilevel marketing. In these programs, your ability to earn profits is based on the number of new participants you recruit, instead of the amount of products or services you sell. Sometimes there actually aren't any real products that are being sold. These types of schemes are common with investment and independent direct selling opportunities.

These schemes rely on the income from new participants in order to pay fake "profits" to people that have been part of the scheme for longer amounts of time. However, the scheme falls apart when there aren't enough new recruits to pay into the system, so the earlier participants no longer receive earnings.

Tips to Avoid Being a Victim

Take steps to protect yourself from being a victim of a pyramid scheme:

- Be wary of "opportunities" to invest your money in franchises or investments that require you to bring in more investors to increase your profit, or recoup your initial investment.
- Independently verify the legitimacy of any franchise or investment with the Better Business Bureau, your state Attorney General, or any licensing agencies.
- Be skeptical of success stories and testimonials of fantastic earnings.
- File a Complaint

If you've been the victim of a pyramid scheme, file a complaint with your state consumer protection office, state Attorney General, or the Better Business Bureau (BBB). If the pyramid scheme involved securities, you should also file a complaint with your state's securities administrator, or the Securities and Exchange Commission.

Tax-Related Identity Theft

Tax-related identity theft occurs when someone uses your stolen Social Security Number (SSN)

to get a tax refund or a job. These tips can help you prevent and report tax identity theft:

Warning Signs

To prevent tax identity theft, be wary of any Internal Revenue Service (IRS) letter or notice that states:

- More than one tax return was filed using your SSN.
- You owe additional tax, you have had a tax refund offset, or you have had collection actions taken against you for a year you did not file a tax return.
- IRS records indicate you received wages from an employer unknown to you.
- The IRS does not initiate contact with a taxpayer by sending an e-mail, text, or social message requesting personal or financial information.

Should you get an e-mail that claims to be from the IRS, do not reply or click on any links. Instead, you should report it to the IRS. The United States Computer Emergency Readiness Team (US-CERT) provides alerts and tips on how you can protect yourself against U.S. tax season phishing scams and malware campaigns.

Dealing with Tax-Related Identity Theft

If you suspect someone used your Social Security Number (SSN) for a tax refund or a job—or the IRS sends you a letter or notice indicating a problem—take these steps:

Common Scams

Wednesday, 11 May 2016 17:35 - Last Updated Wednesday, 11 May 2016 18:47

- File a report with the Federal Trade Commission (FTC), the lead federal agency for identity theft. You can also call the FTC Identity Theft Hotline at 1-877-438-4338 or TTY 1-866-653-4261.

- Contact one of the three major credit agencies to place a fraud alert on your credit records:

Equifax: 1-888-766-0008

Experian: 1-888-397-3742

TransUnion: 1-800-680-7289

- Contact your financial institutions, and close any accounts opened without your permission or tampered with.

- Respond immediately to any IRS notice; call the number provided. If instructed, go to the Identity Verification Service.

- Complete IRS Form 14039, Identity Theft Affidavit (PDF, Download Adobe Reader); print, then mail or fax according to instructions.

- Continue to pay your taxes and file your tax return, even if you must do so by paper.

Telephone Scams

Every year, thousands of people lose their money and personal information to telephone scams. Typically, phone scammers will try to sell you something you hadn't planned to buy and will pressure you to give up personal information, like your credit card details or Social Security number.

Common Phone Scams

- In telemarketing fraud, phone scammers will often use exaggerated—or even fake—prizes, products, and services as bait. Some may call you, but others will use mail, text, or ads to get you to call them for more details. Types of phone scams include:
 - Travel packages - "Free" or "low-cost" vacations can end up costing a fortune in hidden costs.
 - Credit and loans - Popular schemes include advance fee loans, payday loans, and credit card loss protection.
 - Fake business and investment opportunities - As business and investing can be complicated, scammers take advantage of people not researching the investment.
 - Charitable causes - Many phone scams involve urgent requests for recent disaster relief efforts.

National Do Not Call List

Avoid phone scams by registering your home and cell phone numbers with the National Do Not Call Registry. This national registry was created to offer consumers a choice regarding telemarketing calls. It won't stop all unsolicited calls—but will help stop most.

Report Telephone Fraud

If you believe you have been a victim of a telephone scam or telemarketing fraud, you can file a report with the Federal Trade Commission (FTC).