Top Ten Scams of 2014

The FTC's Consumer Sentinel Network Data Book identified the top 10 scams of 2014 based on consumer-filed complaints. The AARP Fraud Watch Network's scam guide can help you protect yourself from identity theft and scams.

1. Identity Theft

How does it work? Someone takes your personal information—like your Social Security number or credit card account number—to steal your money or open new accounts in your name.

ID theft can be low-tech—picture a scammer digging through your mailbox or trash for credit card statements or other financial information— or high tech, like hard-to-detect email or text phishing scams that unleash malware on your computer or trick you into voluntarily disclosing personal information.

What should I do?

- Shred sensitive documents before placing them in the trash.
- Check your financial accounts frequently to see if there's any unusual activity.
- Don't click on any links in emails from people you don't know.
- Get a free credit report annually through one or more of the major credit bureaus.
- Be careful about sharing personal information on social media. Set your Facebook privacy settings so your profile is visible only to known and vetted friends and only accept friend requests from people you know and trust.

2. Debt Collections

How does it work? Scammers pose as collection agents, repeatedly calling to threaten garnishment of your wages or seizure of your assets, all the way up to arrest and jail time if you don't pay on the debt right away.

These criminals do their homework so they appear to be "collecting" on debts that you actually owe, often demanding a wire transfer or prepaid credit card for payment.

What should I do?

- Ask the caller for his name, company, address, phone number, and professional license number.
- Refuse to discuss any debt until you get a written "validation notice" including the amount of the debt and the name of the creditor you owe.

- Do not give the caller personal or financial information, putting yourself at risk for identity theft.
- If you're concerned about the status of an unpaid debt, hang up and call the creditor back yourself at the phone number provided on your loan paperwork.

3. Impostor Scams

How does it work? Impersonating police officers, federal agents or financial service companies, scammers use their "authority" to scare you into paying them. Or, they pretend to be a friend or loved one in trouble who needs money. Examples include a phone call from an IRS official ordering you to pay back taxes, or someone pretending to be a grandchild stranded in a foreign country in need of money from you to get out of trouble.

What should I Do?

- Don't wire money or provide personal data over the phone to anyone claiming to be from a government agency like the IRS. Real federal agents don't email or call to demand immediate payment -official correspondence will come by U.S. mail.
- If someone calls claiming to be a family member in distress, check the story with other family members or ask the caller questions that a stranger couldn't possibly answer.

4. Telephone and Mobile Services

How does it work? Mobile phone cramming is the practice of placing unauthorized, misleading or deceptive charges on your telephone bill from a third party, not your mobile carrier. Charges, which show up on your bill typically range from $1.99 to $19.99.

What should I Do?

- Understand and read the terms and conditions of your mobile service plans.
- Regularly check all your phone bills for charges you didn't authorize.
- Call your phone company to ask about any fees you don't understand.
- Ask your phone company to block third-party charges, but be careful, this might prevent you from purchasing a new favorite app.
- Don't respond to unsolicited text messages from unknown senders.

5. Banks and Lenders

How does it work? When looking for a loan online, you stumble upon a fake website similarly named to a legitimate financial services business. You are instructed to fill

out paperwork and told upon submission that you must pay advance fees in order for the company to negotiate on your behalf or so that they can "protect" you from loan delinquency or foreclosure. Funds must be paid by money order or wire transfer. The scammer then pockets the "fees" and walks away without providing any loan.

What should I Do?

- If someone says they can get you an easy loan, but you need to pay some cash up front, walk away.
- Understand the terms and fees of your financial agreements before you sign anything; get help from a lawyer, accountant, or family members if needed.
- Review all of your financial statements on a frequent basis; you are likely to see any discrepancies with your accounts before anyone else.
- Check out the financial professional's background (sec.gov or finra.org) and know who you are dealing with.

6. Prizes, Sweepstakes and Lotteries

How does it work? A person is told by phone, mail, or email that they have been awarded a fake (and sometimes "free") prize, sweepstakes, or lottery. Usually the scammer asks the person to wire an up-front fee to receive their winnings to cover things like insurance, shipment, or taxes.

What should I Do?

- Don't pay to play; legitimate sweepstakes are free and by chance.
- Don't wire money. It's like sending cash, once it is gone, you can't trace it or get it back.
- Be especially cautious about foreign sweepstakes; many fraudulent sweepstakes companies that target U.S. consumers are located in other countries.
- Be suspicious if you get an email saying you have won a prize for something you never entered.

7. Auto-Related Complaints

How does it work? The most common problems involve a lack of disclosure or understanding around terms when buying or leasing a car; for example, details about special offers and promotions may be buried in the fine print or may not be included at all.

What should I Do?

- Read the documents you get very carefully, especially the credit or lease contract.

- Don’t sign, and don’t leave the dealership with a new vehicle, until the terms you and the dealer negotiated are on the contract, and you are clear about your obligation, including all your payments.

8. Shop-at-Home and Catalog Sales

How does it work? A common scam is the selling of weight-loss or nutritional products, which can be notorious for misrepresentations; the more outrageous the claim, the more likely the product will not live up to it.

What should I Do?

- Determine the company’s refund and return policies, the product’s availability, and the total costs.
- Research the company to make sure it is legitimate; and dig deep for reviews and comments as people are sometimes paid to post phony positive reviews.
- Don’t wire money; if it goes to a fraudster you won’t be able to get it back.

9. Television and Electronic Media

How does it work? The most common problems include: problems with installation, billing, and promotions for cable/satellite providers; miscellaneous issues with music/DVD/video game purchases; as well as complaints about television programming or advertisements.

What should I Do?

- Compare and research service providers to make sure you are dealing with legitimate entities and to see if there are any complaints lodged against them.
- Read the fine print of any service contract and make sure you understand any requirements and fees.

10. Internet Services

How does it work? One of the more common examples is malware, when viruses and spyware get installed on your computer or mobile device without your consent, allowing criminals to steal personal information, send spam, and commit fraud.

What should I do?

- Don’t open attachments in emails unless you know who sent it and what it is to avoid malware.
- Download and install software only from websites you know and trust.