Sector 1: Reference of Terms
AARP Links to Scam Articles
As of March 29, 2026

The world of scams is varied and complex. But it's unified by the fact that every scam is only about taking money from unsuspecting, vulnerable people. AARP is an excellent source for people, especially seniors, to become educated in the scam industry: the various types of scams, the tactics that scammers employ and how to protect themselves from being among the thousands who have been bilked out of small and large sums of money.

SCAM Category	Description	Example
Business Impersonation scams	Criminals try to imitate how businesses communicate to their customers	https://www.aarp.org/money/scams-fraud/latest-amazon-impostor-scams/
Romance Scams	Criminals develop relationships with targets, use false identities and when opportunities present, they steal target's money	https://www.aarp.org/money/scams-fraud/what-is-catfishing/
Shopping Scams	Criminals use tricks like financial problems keeping pets or offer expensive pets for sale at steep discounts	https://www.aarp.org/money/scams-fraud/pet/
Services and cars	Criminals pose as gov't authorities and claim unpaid tolls are due	https://www.aarp.org/money/scams-fraud/toll-road-texts/
Charity Scams	Criminals pose as represent a legitimate charity and appeal to target's patriotism	https://www.aarp.org/money/scams-fraud/veterans-charity/
Government and Celebrity Imposters	Criminals pose as IRS agents; threaten fines and or arrest for "unpaid Taxes" due immediately	https://www.aarp.org/money/scams-fraud/irs/
Investment and Tax scams	Criminals may take months to establish trust with a target and then find a way to steal money	https://www.aarp.org/money/scams-fraud/what-are-pig-butchering-scams/
Real Estate and Home Related	Criminals pose a fake moving companies, take money in advance or steal and resell furniture	https://www.aarp.org/money/scams-fraud/moving/
Travel, Gambling, Entertainment	Criminals pose as lottery representatives, claim a fee is needed to claim a prize. There is no prize.	https://www.aarp.org/money/scams-fraud/sweepstakes/

Sector 1: Scam tactics from AARP: How scammers do what they do.

As of March 29, 2026

Scam Tactic	Explanation
Check Scams	"There is an alleged overpayment for goods and services. The person who is writing the check claims fraudulently that they have overpaid, and they ask the person accepting the check to send back or refund them the overpayment. There is no legitimate overpayment at all."
Data Breaches	Your information is all over the Dark Web. Criminals can put together a profile of you with this information and find a way to trick you into parting with your money
Gift Card Scams	criminals drain the value of gift cards before they are purchased. They'll steal cards sitting in unattended store racks, record the numbers and PINs, then repackage and replace the cards. When someone buys and activates a card, they swiftly drain the value.
Card Skimming	Devices placed in credit and debit card readers that capture data from the card's magnetic strip
Catfishing	Catfishing occurs when people use fraudulent information and images to create false identities, then attempt to attract people through dating apps, messaging apps, and social media.
Financial Grooming	Scammers connect with you online, form a relationship perhaps over months or longer, then lure you into bogus cryptocurrency investments.
Gold Bar Payment Scams	Scammers pretend to be representatives of a bank or other financial institution. They convince a victim that their account is compromised and tell the victim to withdraw everything and buy gold bars. Once the victim has the bars the scammers dispatch someone to pick the gold up – claiming that they will take it to safe storage.
Identity Theft	Criminals use a variety of methods to obtain your information. Some are low-tech, such as mail theft. A scammer could also steal your information with such simple tactics as handing you a clipboard and asking you to sign a petition that requests your Social Security number. Some are large-scale: Hackers steal information from companies such as banks and retailers with large databases.
Love Bombing	overly affectionate behavior, usually at the start of a romance, in which one party 'bombs' the other with over-the-top displays of adoration and attention. This creates vulnerability and helps scammers steal a target's money
Money Mules	Money mules are people enlisted, often unwittingly, to serve as conduits for illegal gains, receiving scam proceeds from other targets and passing them along to the criminals. By acting as intermediaries, the mules give criminals a cheap way to move money and cover their tracks.
Robocalls	Robocalls are prerecorded voices, often made through automatic dialing technology. While not all robocalls are scams, over 6 billion scam robocalls were made in 2024

Scam Tactic	Explanation
Phishing	Phishing is a tactic that scammers use to acquire valuable personal and financial data, such as your Social Security number, credit card details or passwords for online accounts, and to steal your identity, your money or both. They are mostly associated with email but can come in many forms, including: social media messages, pop-up ads
QR Codes	QR codes are those black-and-white squares you can scan with your phone. They are used in ads make it easy to access a website; they're on product labels and business cards. Scanning a code might lead you to a page with more information or a coupon. It also could lead you to a fraudulent domain in order to steal your money.
Smishing	Smishing is the use of text messages that aim to manipulate people into revealing payment or sensitive data such as Social Security numbers, credit card numbers and account passwords or providing access to your laptop.
Wrong Number Texts	These are intentionally messages sent to someone with the intent of eliciting a response which can then lead to the victim's becoming friendly with the scammer and providing personal information