Popular Scams

Scams aim at stealing your money or personal information and involve a variety of techniques. This list includes some of the more common scams:

- **Advance-fees scams** – With these scams, the crook baits you by getting you all excited about **receiving some large amount of money or a wonderful "free" prize.** But before they can send you your treasure, there are certain "fees" that have to be paid "in advance." The first fees are usually small (e.g., "for postage and handling," "for taxes"), and you might be tempted to pay them. But it's never the last fee and the amounts of the fees keep rising. Some victims have paid millions in these "fees" (yes — millions!) without ever receiving a thing.
- **Wire-back scams** – In this situation, the crook **sends you a check or puts money in an account in your name.** You are then **instructed to wire some of that money out** (the crooks always give a very logical reasons for this). The payment for the funds they sent to you is returned because they were fraudulent to begin with, and you're left to cover the amount of their fraudulent payment. The funds you wired are long gone, and you're left holding the bag — an empty bag.
- **Check cashing scams** – Helping someone new in town is considered neighborly. Crooks often take advantage of people's goodwill by posing as a new friend and then asking for help with cashing a check. You take the crook (who you believe to be a friend) into your bank, you cash the check for them on the strength of your relationship with the bank, and you give the cash to the friend. The check is eventually returned, and since you endorsed it by signing the back, you legally guaranteed your own liability for the check. Your new friend is nowhere to be found, and you're left having to repay the bank yourself.

Stealing Your Information

Many people — especially young people — believe that because they don't have a lot of money or assets themselves they don't have to worry about criminals bothering them. This is an erroneous and dangerous assumption. Sometimes your good name is exactly what a crook is looking for.

Next to cash, a crook's most valuable asset is a good and real financial identity. Many crimes require the use of an unblemished identity, and for that reason they've become a major black market commodity.

There are usually two sets of crooks involved with identity theft: the one who steals and then sells your identity, and the one who buys and uses it.

There are two general categories of **Identity Theft**:

- **Account takeover** – This is when crooks take over your bank accounts. The person gets the information needed to convince the bank that they are you, and the bank gives them access to your money or line of credit. This can include all of the information associated with your account: account numbers, card numbers, passwords, PINs, security codes, social security numbers and other personal information.
- **True-name fraud** – This is when crooks get the personal information they need to establish an account in your name, such as a credit card, a new bank account, renting or buying a property, obtaining medical insurance, or establishing a utility service. You may never know about these accounts until they become delinquent and the collection agency comes calling, or you're refused a loan because of "unpaid debts" you never knew you had, or until you're arrested because there's a warrant in your name. Or perhaps you're mistreated during an emergency medical situation because your medical records show the records of the criminal rather than yours. While some of this may seem unbelievable, all of these scenarios happen all too often.

The "Ishings" – Phishing, Vishing and Smishing.

With the advent of digital services, cybercriminals have created devious new ways of stealing victims' personally identifiable information (PII). The terms used to describe this type of fraud follow a fishing theme (i.e., baiting a hook

and casting a line in the water, hoping to lure fish to bite). First seen in emails, the technique has evolved, using the same basic bait-and-hook technique, customized as needed to work through phone and text messaging services.

PII is no longer the only thing at risk to an "ishing" attack. It is also used to lure victims to web sites where their electronic devices can be infected by Trojans or viruses. To add insult to injury, these techniques are only successful if the victim voluntarily complies with the crook's request, not recognizing that these requests are illegitimate.

To avoid becoming a victim, don't respond to these directives immediately. Question all unexpected requests for PII, instructions to call unrecognized phone numbers or directions to click on links. Contact authentic organizations through other channels and make sure the contacts and requests are legitimate before responding.

- **Phishing** – Fraud operators bait victims by sending emails that appear to be from a reliable source, asking the recipients to respond to the email in various ways, e.g., send a return email with information or click on a link in the email. Those recipients who respond become victims. Able to send a large number of phishing emails in mass distributions, the crooks need only a small percentage of recipients to respond in order to make it a worthwhile catch.

  Example: Victim receives an email from his bank telling him that he needs to update his password immediately or risk having his online banking service shut down. The victim clicks on the link in the email, which takes him to a fake ("spoofed") bank site where he is instructed to enter his username and current password. He complies and in so doing, gives the fraud operator his on-line banking login information.

- **Vishing** – Since Voice of Internet Protocol (VoIP) technology became available as an option to traditional telephone services, criminals recognized an opportunity to collect victims' numeric PII (e.g. credit and bank account numbers, PINs, security codes, SSNs, dates of birth) through their telephone devices, by creating the illusion that they were interacting with a legitimate organization.

  Example: Victim receives an automated phone message that there is a suspicious transaction on her credit card account and to please call a number to confirm the transaction is legitimate. The victim calls the phone number given and is asked to enter her credit card number and security code on the key pad so she can be "authenticated" as the real customer, which is how the crooks get her card information for future fraudulent transactions.

- **Smishing** – It wasn't long before smart phones and texting became a popular communication channel, and with it, scoundrels saw the chance to use SMS – Short Messaging Service – to convince texters to respond to fraudulent texted communications.

  Example: Victim receives a text message that he is about to be charged for a service the victim never ordered. He is told that he needs to contact the company immediately to cancel the order or be responsible for the charge. The text includes a hyper-link, which the victim clicks on, taking him to a fake website that triggers the download of a program that breaches the security features of his phone.

Types of Payment Fraud Scams

- **Auction scams and advertising scams (sellers)** – In a "wire-back scam," often seen with auctions and classified ads (both print and online), a crook buys what you have to sell and gives you a check for much more than the amount of the item with some rational excuse (e.g., they were unsure of the shipping amount or thought there might be additional shipping fees associated with the purchase). The crook asks you to wire back whatever you don't need. Sounds simple enough, so you send the item and wire back the extra money. But when the check returns as fraudulent, you're out the amount you wired and probably also the item you sold.
- **"Call-back" scams** – You get a call, a letter or an email directing you to call a number for some compelling reason. So you call, and after listening to a long message, you're put on hold for a while. What you don't realize is that you've dialed an expensive overseas pay-per-minute service that charges an exorbitant fee for every minute you're

connected. (Often this is an “809” or a “900” number.) You may not know you’ve been scammed until you get your whopping phone bill.

- **Charity scams**– Americans in general are generous people and when they hear of someone in need, they are anxious to help. Crooks take advantage of this generosity by creating all sorts of heartbreaking stories to open people’s hearts – and wallets – relying on your trust that the bogus organization they’re describing is legitimate. The causes these crooks say they are representing most often include:

  Sick or missing children

  Hospitals needing life-saving equipment

  Overcrowded orphanages

  Victims of earthquakes, floods and other acts of Nature

There are legitimate needs out there, but be sure you are dealing with a reputable organization.

- **Fake government scams**– Any contact from any government agency is bound to make us anxious to please, but government agencies do not use email to initiate contact with people, nor do they ask for personal or financial information.
- **FBI scams** – The FBI will never email you to notify you of an inheritance or of money recovered from a drug sting, nor do they assess fines by email.
- **IRS Scams** – The IRS does not discuss tax matters online or ask for personal or financial information via email.

  Social Security scams – Like the IRS, the Social Security Administration will never request personal or financial information via email.

The lesson is the same with other government organizations: an email contact is unlikely to be legitimate, and any contact should be verified with the purported agency first by using a phone number from the telephone book or dialing 411. Do not use a phone number supplied in the letter or email to verify the agency’s legitimacy.

- **Handyman scams** – Someone comes to your door and offers to do some needed maintenance like cleaning gutters, raking leaves, or shoveling snow, for a very attractive rate. They will ask for a check for payment, which gives them your name, address, the name of your bank and your checking account information. Elders are particularly attractive targets for this type of scam. (By the way, this is also a technique used by burglars to “case” a house as part of planning for a break-in later.)
- **job scams**– We’ve all seen the “work from your home” advertisements on online job boards and in the newspaper. With these, just filling out the application is a risk. If you’re asked for personal information that identifies you, like your social security or driver’s license number, or if the so-called employer wants to deposit money into your bank account as part of the job, move on. These are usually some form of “wire-back” scams. Examples of common job scams include:

  Mystery shoppers – In this scam, the crooks ask you to test their “customer service” when using payment services. First, they send a check and ask you to cash it so that you will not have to use any of “your own money” for the job. You’re also given a number of wire service locations (or other electronic payment services) and instructed to pretend to be a customer by sending some of the money to a name and address at each location. At the end of all this, they tell you, you’ll be asked to “rate your customer service experience.” Your wires will go through, returning the money to the crooks, while the check initially deposited into your account will be returned as a fraudulent payment and charged against you.

- **Lottery scams and sweepstakes scams** – If you didn’t enter, you can’t win!! Especially foreign lotteries or sweepstakes. And if you did enter, you wouldn’t be required to send them money to pay taxes or anything else before receiving your prize. This is a classic “advance-fee scam.”
- **Nigerian or “419” scams** – Among the most notorious “advance-fee scams,” “Nigerian”-type scams now originate in many other countries, but they are still named for the country where they started (“419” refers to the Nigerian

criminal code that makes them illegal). The essence of these scams is to represent that there is a substantial amount of money that the perpetrator — supposedly a dignitary of some type — must route out of their country to a safe haven, and that they would gladly **let you have a percentage of the money if you would only let them transfer the money into your account**for safe keeping. In the beginning, the Nigerian scammers were just trying to get victim bank account information so they could then drain the victims' accounts, but it wasn't long before they realized the opportunity they had to get the victims to willingly send them the money. Since their inception – and with the increasing recognition of the traditional "Nigerian" scam – the scam stories have morphed into:

Orphan scams – The crooks represent themselves as youngsters who have just lost their parents and need to get their inheritance out of the country before a nefarious aunt or uncle gets control of the money. For a percentage of the inheritance …

Assassinated official or "coup" scams – With these, a high-ranking public or military official has been killed mysteriously (often in a plane or helicopter crash) along with their families. The message urges the recipient to allow them to wire money before the coup gets ahold of it …

Inheritance scams – If neither you nor your relatives have ever heard of the person or know of anyone else in the family related to them, no, you don't have a long-lost relative who decided to leave you their fortune in another country.

- **Social engineering scams**– "Social engineering" is a fancy term to refer to the way criminals convince people to do things that then allow the crook to commit a crime. In this age of immediacy and a desire for relationships (upon which social networking depends), trusting souls become all too vulnerable to these types of scams, which include:

Friend's friend scams – A friend introduces you to a new friend of his. A couple of weeks later, that new friend needs helping cashing his "paycheck." Your mutual friend isn't around, he tells you, so can you help him? You take him to your bank and cash the check for him on the strength of your relationship with the bank. When the check returns for "forged endorsement" (or another reason) and the bank charges your account, your friend's friend can't be found to pay you back.

Sweetheart scams – You meet someone who's new in town. You think they're wonderful and you date for a while. Maybe you even move in together. Then one day your sweetheart asks if you'd help cash a check at your bank since she doesn't have a local account. You do, and that's the last time you see her. The check bounces a few days later and the bank comes to you for the money. Let's just hope the money is all you've lost.

Relative-in-distress scams – This is one of the newer scams. Grandparents (or aunts or uncles) get a sudden urgent call or email from a "grandchild" saying they've been falsely arrested somewhere and they need money wired immediately for bail. The message asks to "please don't tell mom and dad …"

Scams Perpetrated Against Seniors

Like anyone else, seniors can fall prey to almost any of the scams posted on this site, including identity theft, charity scams, relative-in-distress, and telemarketing fraud. However, some scams seem more often targeted toward vulnerable seniors such as:

- **Power of Attorney Fraud** – The crook seeks to obtain a Limited or Special Power of Attorney, enabling them to access funds and other assets, including bank accounts and real estate, and make legal decisions that are not in the best interest of the victim.
- **Unsolicited Work** – Fraudsters coerce, intimidate or otherwise manipulate individuals into agreeing to home repairs they often do not need. Sometimes they offer a very attractive rate and then perform a shoddy or

incomplete job and leave the home in disarray, insisting on more money to complete the work and return the home to order. Frequently, they insist on cash and on accompanying the victim to the bank to withdraw funds.

- **Companion Scam** – a stranger enters the victim's life to win their affection and gain influence for the sole purpose of financially exploiting the senior victim. The perpetrator uses undue influence including threats (or real) physical and emotional abuse. Seniors, overwhelmed by intimidation, the fear of be left alone or the embarrassment of being duped, are less likely to report the activity to trusted family or law enforcement while there is still a chance to recover at least some of their assets.
- **Theft of Income** – A perpetrator, who can sometimes include an unscrupulous caregiver or even a family member, commits theft by obtaining access to the senior's pension or Social Security check, checking, savings or money market accounts, or credit or debit cards, repeatedly draining the victim's funds every time they are replenished by the next month's payments.