Protect Yourself From the Latest Scams

Investment, mortgage, Internet, and other kinds of fraud are on the rise

Consumer Reports – 2 hours 59 minutes ago

- 

  Yahoo! Finance/Thinkstock - Financial Fraud Research Center estimates the measurable direct cost of financial fraud to Americans to be $40 billion to $50 billion a year.

The economy may be struggling but the fraud business is booming. Although comprehensive data aren't kept, the fingerprints of a crime wave are all over. Fraud and identity-theft complaints tracked by the Federal Trade Commission topped 1.2 million last year, up 19 percent over 2010 and 800 percent since 2000.

Moreover, the FBI says fraud involving investments, mortgages, and the Internet is growing. Government takedowns of multimillion-dollar schemes are common.

"Fraud is as high as it's ever been, because the scam artists are using brand-new channels and technology that didn't exist 15 years ago," says Martha Deevy, director of the Financial Fraud

Research Center at Stanford University's Center on Longevity. The center estimates the measurable direct cost of financial fraud to Americans to be $40 billion to $50 billion a year.

Experts also say the need for law enforcement to pursue terrorists has shifted FBI resources from fraud cases. "After 9/11 the scammers realized, 'This is our time,'" says Doug Templeton, chief investigator for the Pinellas County (Fla.) Department of Justice and Consumer Services, who has tracked criminals in the state for 13 years.

David Vladeck, director of the bureau of consumer protection at the FTC, says, "What we're seeing is 'last dollar' fraud aimed at taking the last dollar from the unemployed or underemployed."

Like a good novel, a scam is all about the story. It must be convincing and, above all, new. Consequently, con artists change their techniques to respond to changing consumer awareness, says the latest threat assessment by the International Mass-Marketing Fraud Working Group.

We interviewed experts, scoured the complaint files of regulatory and consumer-protection agencies, and followed our readers' tip-offs to present the latest frauds making the rounds—and some of the classics. Here's what to watch out for.

1. This solar-energy system pays for itself, cutting your bills by $1,000 a year

A new twist on the home-improvement scam targets folks who want to cut their energy bills with rooftop solar panels or windmills. Solar energy, of course, can reduce your electric bill. But making the big up-front investment is the equivalent of paying for 30 to 40 years of electricity in advance. And lots of variables can confound payback, including living where cloudy weather is commonplace or in the shadow of towering trees, terrain, or nearby tall buildings.

Solar-panel scams. Consumers unfamiliar with those caveats give double-dealers an opportunity to lowball costs and talk up savings. The promised best-case scenario can lure you into paying a big deposit to a contractor who skips town or otherwise never delivers the system or savings. Some victims have been burned for several thousand dollars. Home-improvement companies are the third most complained about businesses, according to the latest survey of consumer-protection agencies by the Consumer Federation of America and the North American Consumer Protection Investigators.

Protect yourself: California is the leader in residential solar, so go to its electric utility website to see whether solar makes sense for you. If it does, work only with licensed contractors specializing in solar installation. Conduct an energy audit and get bids from at least three companies. Check their Better Business Bureau rating and references. Never pay the full price up front or a deposit of more than $1,000 or 10 percent of the project price, whichever is smaller.

2. We'll remove the virus we found for $100

Some scoundrels fly under the radar via telephone. A tech-support person, purportedly from a trusted company like Dell or Microsoft, calls to warn you that its security systems have remotely detected a virus on your computer and offers to remove it—for a fee of $100 or more.

Bogus tech-support scams. Of course, there is no virus, so you pay for unnecessary service. The crook may also take the opportunity to install mock antivirus software that later starts "finding" nonexistent malware. That can cost you a bundle for removal. Worse, the tech may also install software that scans your computer to steal your passwords and hijack your computer to generate ads and spread spam.

Protect yourself: See our June 2012 report on security software to find legitimate antivirus and antimalware software that we've rated, install it on your PC, and keep it up to date. Hang up on anyone outside your home who claims to find trouble on your PC.

3. Confirm the flight reservation you didn't make

You get an e-mail notifying you about airline reservations you didn't make, a package from UPS you weren't expecting, or a problem with your bank account. Just click on this link or attachment.

Phishing and malware scams. If you follow the instructions, you might end up downloading malware designed to take control of your computer and turn it into a spamming robot, harm it with a virus, or mine your files for financial information. Following the link will take you to a site that looks real but is fake. When you log in, it captures your user name and password so that the bad guys can get into your real accounts.

For years, those threats were limited to your PC, which should be protected with security software. But the popularity of smart phones has opened the door to "smishing." (The word combines "SMS," or short-message service—aka text messaging—and "phishing.") Some smart-phone users don't realize that their phone is a computer and prone to the same security risks as a PC.

Those deceptions work. More than 9 million households had at least one member who gave up information to phishers, and 30 million suffered a malware attack in the previous year, according to our latest survey of online households. The Better Business Bureau pegged phishing as its top scam of 2011. Moreover, today's fake sites are more believable than ever.

Protect yourself: Never click on a link to your online accounts through e-mail or call an account-related phone number in a text message someone sends you. Instead, open your PC or mobile Web browser and type in the desired address on your own. And don't click on an e-mail attachment unless you're expecting it.

4. You've just won a $100 gift card!

In this new bamboozle, burglars claiming to be from a local store call to tell you that you've just won the prized plastic, and you must come in to pick it up.

Burglary. The game is to get you out of the house so that robbers can carry out an old-fashioned break-in while you're gone.

Protect yourself: This simple trick works because it catches you by surprise. Always be suspicious when someone promises you something for nothing. The Better Business Bureau, which first warned about this scam, advises "winners" to ask questions: What contest did I win? How was I chosen? Call the store to independently confirm the details. After you determine that it's a scam, notify the police. And take extra precautions to lock up your house, set your alarms, and protect valuables when you do leave, since burglars have clearly targeted your home.

5. Now you really can see who views your Facebook profile!!!

Social-media networks are fertile ground for fakery. You might have received, for example, news-feed messages from Facebook friends raving about an app that claims to let you see who's checking out your profile. Such messages can be spam in disguise, leading to "bait pages." Other bait involves purportedly bizarre or salacious videos. Consumers who take the bait never get the promised software or film.

Instead, the link drives the curious to a fake Facebook website. You're asked to "like" the app or other bait, which forwards the spam to all of your friends. Then you have to complete a survey, which collects personal information and opinions.

Survey scams. The goal is to trick you into filling out surveys for online advertisers, with the person who set up the operation collecting commissions for each one completed by an ever-expanding circle of friends, says Chet Wisniewski, senior security adviser at Sophos, an information security firm. One "clickjacker," Adscend Media of Wilmington, Del., raked in a significant amount of money, according to a lawsuit filed by the Washington state attorney general. The case was settled in May under a consent order in which the company agreed to stop certain marketing.

There's a difference between scam surveys and legitimate surveys, like those Consumer Reports e-mails to subscribers. Our surveys link you directly to the questionnaire; you don't need to "like" us first. And your responses are confidential; they aren't used for marketing or fundraising.

Protect yourself: Don't reveal personal information online to anyone who initiated contact with you unless your trust is certain. Look for the survey company's name and go to its website independently by reopening your browser, or call it. Ignore product promos from Facebook friends. Use caution in granting access to your profile. And think before you "like."

6. Cut your credit-card interest rate to 4.75%

Who doesn't want to cut sky-high credit-card interest costs in today's low-rate environment? An unsolicited caller falsely implying that he's affiliated with your credit-card issuer offers to reduce your interest rate and save you $2,500. The service costs $695 up front, and you must fill out a "financial profile form" with details about your debts, including balances, credit limits, interest rates, and customer-service numbers, plus your name, address, and Social Security number.

Credit-card interest rate-cut scams. The full extent of the "service" typically involves a conference call with the thief, victim, and creditors, during which the shark asks for a rate reduction and the creditor usually refuses. Consumers, of course, can do this on their own—free. One such operation, Select Personnel Management, a Canadian company, and eight associated companies and defendants were ordered by a U.S. District Court in Illinois in 2009 to pay more than $7.8 million and stop telemarketing after the FTC said they hoodwinked more than 12,000 consumers.

Protect yourself: Don't give personal information such as account numbers to anyone who initiates contact with you. Go to donotcall.gov or call 888-382-1222 to register your phone numbers on the National Do Not Call Registry. Hang up on unsolicited telemarketers.

7. Free golf, dinner, and priceless investment advice for savvy retirees

Investment advisers, broker-dealers, and people from other financial-services firms invite wealthy seniors to enjoy fun, food, and access to investment secrets that will add $100,000 to their net worth, get them 40 percent investment returns, or turn $100,000 into $1 million for their heirs. Attendees might receive a sleeve of golf balls or even win golf clubs.

[More from Consumer Reports: Ratings and recommended TVs]

Investment-seminar scams. The main goal of this educational "opportunity" is to sell investment products that generate commissions for promoters, mostly annuities, real-estate investment trusts, mutual funds, and reverse mortgages. That's all perfectly legal.

But the ads, sales materials, and pitchmen can be misleading or promote strategies inappropriate for seniors. Reported problems have included promises of a 38 percent rate of return with no risk, the liquidation of investments without the customer's knowledge or consent, the misappropriation of customers' funds to buy unregistered oil and gas partnerships, and the sale of nonexistent investments to pay a salesman's personal expenses and trading losses.

Protect yourself: Deal only with long-time, trusted financial advisers, never with new "friends" from a rubber-chicken sales seminar. Accept the invite and fun, but provide zero financial information and don't sign blank authorization forms or anything else. And just say no to follow-up one-on-one meetings that will probably be suggested on the pretense of preparing a financial plan.

8. A national family health-care plan for $3 a day

The Supreme Court's June ruling upholding most of the Affordable Care Act is expected to revive this scam, which appeared after the legislation was passed in 2010. An "emergency broadcast" and video of President Obama discussing health care prompts viewers to call a toll-free number to reach one of many telemarketers. They imply that they're selling affordable, government-authorized health insurance that provides "significant" savings on prescription drugs, doctor and hospital fees, and labs coast-to-coast.

Medical discount plan scams. The product isn't insurance; it's a discount card costing an enrollment fee of $29 to $500, plus monthly fees of $90 to $1,300. That's deceptive enough, and the FTC has taken action against more than 50 such operators in recent years. But when ill customers finally need to use the card, many health-care providers don't honor it. Refunds? Fuggedaboutit!

Protect yourself: Discount plans aren't illegal, but we consider them to be junk insurance. They're often sold deceptively as insurance, but unlike real health coverage, discount plans don't pay any of your medical bills. Instead, they amount to a list of providers who may be willing to offer plan members a discount. Think coupons, not coverage, and this poor bargain becomes obvious.

9. We can 'clean-pipe' your car to pass smog inspection

When a car is unlikely to pass a state smog inspection, a technician or other mechanic simply tests a stand-in car that does meet standards, and voilà! The good numbers are used to certify the belcher.

Auto-repair scams. They continue to thrive; auto-repair rip-offs were No. 8 in the BBB's complaint rankings in 2011. Among the most common tricks: Mechanics give a good estimate up front but pad the bill with extra work. Some shops make a business of this by advertising a low-priced oil-and-lube job to suck in customers, then "finding" much more expensive problems that need to be fixed.

Another scam involves counterfeit, used, or substandard parts used in place of the new parts you pay for. Sometimes the mechanic doesn't provide any replacement parts and doesn't do the work. Bogus billing can add up. After a mechanic in Palm Desert, Calif., claimed to have rung up more than $11,000 in parts and labor on one car, inspectors from the California Department of Consumer Affairs Bureau of Automotive Repair said they found something else: fraud.

Protect yourself: The Coalition Against Insurance Fraud says you should always get a written estimate before work is done, ask to see the repairs and discarded parts, use a shop recommended by knowledgeable friends, check the shop's BBB rating and Yelp page, and be wary if the mechanic says he'll help "waive" the deductible on insurance-financed repairs.

10. You could win an iPad, so start bidding!

Hot electronics are commonly used to entice victims into a shakedown. A pop-up ad on your computer invites you to bid on an iPad, laptop PC, or wide-screen TV, but you must include your cell-phone number to play. Submitting your bid sends a text message to your cell phone that, whether you respond or not, may authorize an unwanted $9.99 a month subscription to some useless service. The charge gets tacked onto your cell-phone bill, where you're unlikely to notice it.

Cramming. The auction is smoke and mirrors designed to capture your cell-phone number to place unauthorized charges on your bill, a practice called cramming. Unlike numbers for landlines, cell-phone numbers aren't published in directories, so scammers must be underhanded to get it.

Cell-phone companies, which can collect $1 to $2 commissions per charge, claim that wireless cramming isn't a problem. But we found 480,000 alleged cell-cramming victims in one case, and in 2011 a Senate committee investigation concluded that landline and cell-phone crammers could be fleecing $2 billion a year from consumers.

"We have multiple wireless-cramming investigations under way," says Vladeck at the FTC, "and we're quite quickly seeing the migration of cramming from landline to wireless phones."

Protect yourself: Guard your cell-phone number like a credit card; don't give it to strangers. Demand refunds from your cell provider if you've been crammed. Tell your wireless and landline carriers to block all third-party billing to your account, and check previous bills for cramming charges.

11. Buy a gourmet dog-food coupon worth $61—for just $16

You receive an e-mail that alerts you to a website—not the manufacturer's—where you can purchase high-value coupons. They're not your typical 25 cents off but special coupons for $2 to $60 off or free high-priced products like shaving razors, pricey pet food, diapers, infant formula, coffee, and even restaurant meals. Such giveaways are rarely circulated, but manufacturers do use them to introduce new products or as a goodwill gesture to win back a wronged customer.

Coupon scams. Problem is, there's no way anyone can accumulate enough of those rare coupons to make a business of it, "so they have to be counterfeit or stolen," says Bud Miller, executive director of the Coupon Information Corporation, an industry group that works to stop coupon fraud. Other coupon flimflams involve moneymaking ventures based on inflated earnings promises, in which consumers invest several hundred to several thousand dollars for coupon booklets that are difficult to sell, or they toil at work-at-home coupon clipping.

Protect yourself: Avoid such coupons.

12. I've been in an accident in Canada and need your help, Grandpa

It's the phone call every grandparent dreads: Bad news about a grandchild coming in the middle of the night. Maybe the car has broken down or been involved in a crash, maybe the kin has been unjustly arrested, or a family member in the military has been mugged overseas while on leave. The caller may attempt to impersonate the grandchild or a police officer, lawyer, or doctor. Whatever the details, the family elder needs to wire money ASAP.

Grandparent scams. The caller, however, is not a relative but a cheat who'll collect the untraceable wire transfer you might send, typically to Canada, Mexico, or another country. This dirty deal has been working since 2008 at least, but the Internet Crime Complaint Center reports that scammers have lately become more sophisticated by mining social-networking sites for personal details that make their impersonation more credible. One couple was pinched first for $3,000 when their "grandson" was supposedly caught fishing in Canada without a license, then for a whopping $30,000 more when the drama escalated to Mounties finding drugs and alcohol on the boat, the Michigan attorney general said.

Protect yourself: Ask for details about your last visit that your grandkid should recall and a stranger couldn't. Jot down the caller's location and number. Hang up, and instead of calling Western Union, call the grandchild's parents or the number you usually use to reach him to verify his whereabouts—even if the caller pleads, "Don't call my parents!" Don't send a dime unless you confirm the story.

13. Sweet deal: $15,000 for a car with a $28,000 book value

Hard times nudge many consumers into the used-car market, and some wind up with this bargain hunter's nightmare: Crooks steal a car, then copy the vehicle identification number (VIN) from another car—same make, model, year, color—in a mall parking lot. They use the legitimate VIN to counterfeit VIN dashboard plates and Mylar stickers, slap them on the stolen vehicle, and sell that car to you at an attractively low price. The registration documents are also forged.

VIN cloning scams. Sooner or later, because you must register and insure your car, insurance carriers and state motor vehicle departments eventually figure out that two vehicles are using the same VIN, which draws the police to repossess your sweet deal. You're now out the car and the money you paid to the long-gone criminals. This and many other schemes help put auto sales in second place among the top 10 complaints listed by the National Association of Attorneys General.

Protect yourself: Watch for red flags: a far-below-market price, a private seller doing business in an odd location, a cash deal. When you call a seller, ask for the VIN and check it, free, at vehiclehistory.gov or the website of the National Insurance Crime Bureau. While sizing up the vehicle, compare the VIN you were given with those in several places on the car—dashboard, glove box, side door, in the trunk, under the hood near the radiator post. If there's any mismatch, remain poker-faced, don't confront the seller, walk away from the deal, and call the police.

14. Want a $17.50-an-hour job?

Last May, job hunters using computers at a public library in Columbus, Ohio, to search the want ads were approached by a "recruiter" looking to fill positions at a new store nearby. The sneak used the library to conduct job interviews, and candidates filled out applications with their name, date of birth, Social Security number, and more.

Identity-theft scams. When the applicants later went to the store for training, they learned that the recruiter wasn't associated with it at all. Rather, face-to-face job interviews are a new and brazen way to extract information for ID theft.

Job scams rank seventh on the BBB's top 10 scams list, and such come-ons also involve work-at-home schemes including stuffing envelopes, assembling merchandise, medical billing and claims processing, and reshipping what the victim may not know are stolen goods.

ID theft was the biggest category on the FTC's 2011 complaint list. Thieves use a wide variety of tactics to get you to give up key information that lets them steal from your existing bank and credit accounts or use your Social Security number to open phony financial accounts and commit other crimes in your name. The most effective deceptions appear to come from your bank or credit-card company, a government agency, or other entity that you trust, and they wheedle information out of you by saying they need it to correct an error or prevent a problem.

Protect yourself: Never give your personal information to anyone who telephones, e-mails, texts, or otherwise initiates contact with you. Don't participate in fun-looking online pop-up quizzes that ask for your mother's maiden name, your first pet's name, or other information commonly used to verify your identity. Monitor your financial accounts weekly or even daily, place a security freeze on your credit reports at all three credit bureaus, and file an ID-theft report with the local police if you get swindled.

If someone approaches you with a job, contact the prospective employer to verify that the recruiter and the job opening are legitimate. There should be no need for checking-account and other financial information on your application.

15. Gold prices will peak in the next 60 days. Invest now!

Telemarketers promise senior citizens with assets that gold, silver, platinum, and palladium bars, bullion, and coins are a surefire, low-risk investment and use high-pressure sales tactics to close the deal. In fact, precious metals are a commodity subject to erratic short-term pricing with no guarantee of any net return.

Gold investment scam. What consumers aren't told is that their investment is really a credit purchase. Their money is deposited in an account, and the scammers don't actually buy any precious metals. Instead, the crooks rake off poorly disclosed fees and commissions.

Protect yourself: Hang up on telemarketers who call out of the blue. Deal only with reputable precious-metals dealers. Take delivery of your gold at your bank, where you can keep it in a

safe-deposit box.

16. I overpaid you, so deposit my check and wire me the difference

You post an item for sale on Craigslist or another classified-ad website and you're pleasantly surprised when an out-of-state buyer quickly responds by mailing you payment. But yikes! The buyer has mistakenly sent you a check for much more than he owes. You contact him about the mix-up. No problem: He trusts you to deposit his check and wire the overage to him via Western Union, MoneyGram, or other service. To show how nice you are and to uphold the goodness of mankind, you go ahead.

Overpayment scams. But the check bounces, so you don't get the snake's money; he gets yours. Overpayment fraud was fifth-ranked among complaints filed with the Internet Crime Complaint Center last year. You're also stuck with any returned-deposit fees from your bank.

Protect yourself: Deal only with people you can meet in person, Craigslist warns. (Its founder, Craig Newmark, is on the board of Consumer Reports.) Exchange goods for cash, don't deal with distant buyers or wire them money, and don't accept checks, not even cashier's checks or money orders, which can be faked.

17. National Sweepstakes Bureau calling

In a new spin on a timeworn fraud, you receive mail or a call from a seemingly authentic government agency that is "supervising" the safe transfer of—congratulations!—your sweepstakes winnings. Among the agencies supposedly calling are the fictitious National Consumer Protection Agency, the make-believe National Sweepstakes Bureau, and even the misappropriated FTC.

Sweepstakes scams. Spoofing technology makes the callback number look like it's really in Washington, D.C., and the official-looking documents have lots of gravitas and seem authentic. But it all works to fool you into paying a transfer or processing fee, or taxes and insurance on "winnings" of $20 to $10,000. Of course, there are no prizes, but any lost fee payment is real. Sweepstakes scams are surprisingly popular, ranking third on the FTC's annual complaint list.

Protect yourself: Never pay lottery-win fees, which are a red flag of fraud. Legitimate sweepstakes don't require winners to pay insurance, taxes, shipping and handling, or any other fees. Other tip-offs include high-pressure efforts to get you to wire the fee immediately to beat a deadline. And though governments definitely tax prize winnings, they don't "supervise" delivery.

18. Pay me up front for this repair, or I'll go elsewhere

In the wake of tornadoes and other severe weather, these hustlers take advantage of the surge in demand for repairs. The push is for up-front money.

Storm-repair scams. Once they get your money, these skunks may do shoddy work, delay the work endlessly, or take the money and run. Tina Shelton of Manvel, Texas, a Houston suburb, lost $12,000 to a contractor who bilked her and elderly neighbors after Hurricane Ike swept through their area in 2008. Roofers in general generate more than 8,000 complaints a year with the BBB and rank 15th among all industries for number of complaints.

Protect yourself: Ask your insurer about coverage and to get a correct estimate. Never pay the full price of a job before it's done; pay in increments as work is completed. A down payment of less than a third of the estimated total cost is OK. It allows the contractor to buy materials, which you should see arrive at your home along with invoices indicating what was bought and paid. Pay with a personal check or credit card, which you can keep better track of than cash. Don't do business with contractors who knock on your door; find listed, licensed, and insured local construction companies. Get at least three written estimates.

19. The government wants you to have a scooter

Someone at the door or at a church presentation tells a Medicare beneficiary that the federal health program will pay for so-called durable medical equipment; all you have to do is ask. Motorized scooters and power wheelchairs are the big prizes. The trickster collects info about the person's medical conditions, doctors, and—most important—Medicare account number.

The beneficiary may never receive the equipment or may receive a $500 unpowered wheelchair while Medicare gets billed $11,000 for a feature-laden powered one. Gaming a government program is easy: A 2009 report by the Department of Health and Human Services Office of Inspector General said that 60 percent of standard and complex power wheelchair claims lacked proper documentation.

Medicare scams. Dishonest doctors, nurses, pharmacists, and ordinary cons use your warm body and Medicare account number to steal money from the government. But you might also get stuck with co-pays for things the thief billed to Medicare without telling you. Your identity may also be stolen and sold off, your medical records altered to create a billable phony affliction, and your health may be jeopardized by a resulting false diagnosis.

"Patient brokers" may offer you free groceries, rides, or even cash (which are illegal kickbacks, the FBI says) for your ID number so that they can bill Medicare for medical treatments never performed.

Protect yourself: Never give your Medicare number to a stranger who claims to be a government employee. Check your Medicare Summary Notice for equipment or services that you never received, were double-billed, or billed at a higher price than you were told. Check your credit report periodically for past-due or collection accounts for medical equipment or services never received. Don't sign blank authorization forms. You can get medical equipment, subject to the rules and co-pays of Medicare, but it must be medically necessary and authorized by your doctor.

20. But we already sent your tax refund

No one likes letters from the Internal Revenue Service, but this one is both baffling and terribly worrisome. After you file your income tax return, the IRS notifies you that you've filed more than one return and that someone else has already filed using your identity.

Fraudulent tax return scams. This crime is relatively new but has jumped this year to 940,000 returns filed by identity thieves using other people's names. How do they make money paying your taxes? They use your identity to claim a tax refund, and if you don't have money coming to you, they lie about deductions to concoct a refund—$5 billion in ripped-off refunds this year.

Protect yourself: File an IRS Identity Theft affidavit, available on the agency's website at irs.gov/pub/irs-pdf/f14039.pdf. If the problem persists, you can also get help from the IRS Identity Protection Specialized Unit at 800-908-4490. Be prepared to wait. Howard Shoelson, of Davie, Fla., learned in March that a thief filed a return using his name and Social Security number, and he was still waiting for IRS help when we spoke to him in August. Also report the situation to the Social Security Administration to protect your benefits, which could be at risk.

21. We'll recover the cash scammers stole

Adding insult to injury, "recovery room" operators buy "sucker lists" of people who've already been conned to fleece again—this time on the promise that for a fee they'll recover your losses.

Recovery-room scams. Fees cost hundreds of dollars, and you don't recover the original losses.

Protect yourself: Hang up on anyone who tries to sell, give, or help you with anything. Short-circuit the key step in every scam and never give money or personal information to acquaintances or strangers.

Editor's Note: A version of this article appeared in the October 2012 issue of Consumer Reports magazine with the headline "Scamnation!"