



Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • September 2016 • www.consumer-action.org

SCAM GRAM is Consumer Action's monthly e-newsletter alerting you to the dirtiest players in the world of tech fraud, credit card scams, ID theft and general con-artistry. Don't be fooled by liars, cheats and crooks—wise up with SCAM GRAM!

One tough lesson

Students interested in getting an education are instead finding themselves graduating from the school of hard knocks, as scammers capitalize on youth hungry for knowledge (and a degree). Educational perils are rampant in the U.S.: Traps can be found at for-profit colleges ([See](#) ITT Tech's recent closure and public shaming); job training programs (Did [someone say](#) Trump University's real estate "seminars"?); and fake schools (check out [this woman](#) who convinced foreign students to sign up for a bogus university in exchange for visas). If you're considering going back to school this fall, first check to make sure any post-secondary education program is accredited through the Council for Higher Education Accreditation or the U.S. Dept. of Education (which offers a handy [guide](#) to filing complaints against both public and private schools who engage in corruption). Before you enroll, you should be aware of the full price of the program you've selected, the difference between public and private student loans, grants that may be available to you, and any other financial implications. Also, be aware of fraudsters posing as "loan counselors," and *never* pay for student loan advice. Need more guidance? We recently released a [publication](#) outlining some of the most critical questions to ask, because, hey, they don't teach you this in school.

Hungry for a heist

Over a dozen Baltimore-area retailers have been [charged](#) with engaging in massive food stamp fraud, costing the government more than \$16 million in Supplemental Nutrition Assistance Program (SNAP) funds meant for low-income people. SNAP is supposed to work like this: A mother goes to the store and buys approved food items like bread and milk for her children through a debit card that the government issued to her. The government, through the U.S. Dept. of Agriculture (USDA), then reimburses the retailer for the funds spent by the mother. Only, there's a catch: A customer might receive \$50 worth of groceries, while the USDA is charged \$100 by the grocer, netting the shop owner a \$50 profit. This profit margin gives shady shop owners incentive to hand customers cash for SNAP benefits. Unfortunately, the problem is

rampant and nationwide, with one U.S. attorney proclaiming that the USDA is “playing whack-a-mole” because the “stores just keep popping up every time they disqualify them and shut them down.” Hopefully these Baltimore grocers, who will be heading to court soon, have a better argument than this group of polygamous Mormon sect leaders in Utah who, after being charged with similar fraud, are [claiming](#) that they were only acting in the interest of the Almighty.

Election year madness

This campaign season has been wild, and opportunistic scammers are only adding to the insanity. Equal opportunity hucksters are [calling](#) the electorate and pretending to be with a political party (parties, conveniently, are not restrained by Do Not Call registry rules). They may claim that they’re fundraising (in order to steal your money over the phone), or they might say they need you to re-register to vote (in which case they’re trying to get your personal information, most likely to commit identity theft). They even may say they’re conducting a political survey and offering a monetary reward if you participate (another way of getting your credit card number in order to “cover the fees,” or some other nonsense associated with sending you the “reward”). No matter how fired up you get leading into November, remember: Think before you act. If you get a suspect call, the smart thing to do is hang up and call your local election office to verify it. If you want to make a donation, you also can visit the candidate’s website. Finally, remember that election law in every state prohibits voting via telephone, so if someone calls and says they’re taking your vote, tell them to take a hike.

Heads up!

Careful who you tweet to. Fraudsters have been [monitoring Twitter](#) for PayPal customers who tweet @PayPal for tech support. The customers, who are expecting a response from the money transfer website, are more likely to fall for the fake “PayPal” phishers when they respond and direct them to a counterfeit PayPal website (in order to nab their username and password and gain access to their finances). Many companies respond to tweets but rarely offer concrete advice about your account via the social medium— usually they ask you to direct message them your phone number or give you a number to call.

A storm’s a-brewin’. This hurricane and flood season, it’s raining scammers. The Federal Emergency Management Agency (FEMA) is [warning](#) those affected by natural disasters of scammers who call and ask for money or personal information in exchange for filing insurance claims, performing housing inspections or awarding grant money. Those who need assistance should instead call 800-621-FEMA or visit [DisasterAssistance.gov](#).

Netflix and bill. Consumers of online media have [been getting](#) fake emails purporting to be from Apple. The emails tell them that they’ve been billed for Netflix subscriptions and other digital fare through the App Store. Shocked to see items that they never bought, the victims click links for refunds, only to be taken to a fake Apple website that “phishes” for (and catches) their financial info.

The pusherman. Do you bank with Wells Fargo? You might have some money coming your way. The Consumer Financial Protection Bureau [busted the bank](#) after thousands of employees opened millions of secret accounts (without customer authorization) as part of a program that rewarded them with financial incentives for pushing costly (and often unnecessary) financial products on customers. If you were

financially harmed as a result of this debacle, you're probably eligible for restitution.

Lost in the mail. Have you been missing any mail lately? The U.S. Attorney's office just [charged](#) 33 people, mainly USPS employees, with theft, possession of stolen mail, conspiracy, embezzlement, bank fraud, and the list goes on and on. Even the president of the National Postal Mail Handlers Union was charged with stealing over 150 mobile phones from parcels and trading them on the World Wide Web.

Tips!

- **It pays to tattle.** A former Monsanto employee was just [rewarded handsomely](#) for alerting the U.S. Securities and Exchange Commission (SEC) to “misstated earnings” associated with the company’s controversial Roundup weed killer. The SEC gave the unnamed whistleblower over \$22 million after the accusations led to an \$80 million settlement, in accordance with a program the agency launched in 2011 to award money to those who report corruption. Hmm... got any dirt on your employer?
- **Another top 10 list?** The Federal Trade Commission seems to know that people can’t get enough of Top 10 lists, so they’re offering their [latest resource](#) in the form of a helpful, free brochure on, you guessed it, the top 10 (count ‘em!) ways to avoid fraud.
- **Fishy business.** You think you’re eating fancy-pants wild Alaskan cod but it’s really just plain ol’ boring tilapia. According to a new report, you’ve probably been the unwitting victim of this type of seafood swindle more than you’d like to believe, which is why you should click [here](#) to learn how to be “seafood smart” and certain of what’s on your plate.
- **Friend to the defrauded.** Victims of fraud, identity theft and other financial crimes now have a powerful ally in the National Center for Victims of Crime. Have you lost money to hucksters and criminals? Do you want justice? [Visit](#) the Center’s website and allow them to simplify what is often a complex reporting and recovery process.
- **Repent, scammer!** Maybe the next time you get a call from a scammer, you should try this woman’s [strategy](#). Not only did she do such a great job acting the role of damsel in distress, she managed to manipulate the man—who claimed he was calling to collect on behalf of a “department of revenue”—into admitting the call was a scam and kindly reassuring her that there was “no need to worry”!

Thanks for reading SCAM GRAM and, as always, feel free to send us your questions, comments and tips. [Click here to email us.](#)

Use our ["Tell a Friend" page](#) to let your friends know they can sign up for their own copies.

Consumer Action empowers low- and moderate-income and limited-English-speaking consumers nationwide to financially prosper through education and advocacy.
