



# Scam Gram!

Keep the sharks at bay

---

A Consumer Action News Alert • December 2016 • [www.consumer-action.org](http://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!

## Online shopping (for victims)

---

If you're like many shoppers, you like to avoid the seasonal hustle and bustle and stay away from the crowded malls. Enter: shopping from home with online mega retailer Amazon. Unfortunately, scammers are all too aware of the site's popularity and are [doing their own](#) online shopping—for those eagerly awaiting the arrival of holiday gifts. The scammers send Amazon shoppers a credible-looking email warning them that their purchase “cannot be shipped” ([here's](#) an example of it). The recipient is likely to break into a cold sweat, worried that the goods won't show up in time. This prompts them to click on a link, which takes them to a site that mirrors Amazon's own and directs them to enter personal and financial information. After they've entered the sensitive info, this bogus site *redirects* the consumers to Amazon's real site (tricky, tricky), making the whole debacle seem all the less suspicious. So, how do you know if the email is fake to begin with? First (and perhaps most obvious), if the sender is anyone other than “Amazon.com,” then the sender is a fraudster. (Place your cursor on the sender's name or click on the arrow next to it to see the actual “from” email address.) Second, any link in the email should direct to a site that starts with “https” (the ‘s’ is for secure) and not just “http.” Since the scam is pretty sophisticated, though, you're probably better off just not clicking on any email links and instead simply going to the real <https://www.amazon.com> in your browser, where you can get updates on the status of your package, and, if any questions still remain, can call or email the company directly through the info provided on the site.

## Money pit

---

Let's say you're fortunate enough to buy a home. You sign all the paperwork, get the keys and finally breathe a sigh of relief. Welcome to the world of homeownership! But wait, not so fast. From the minute you begin the move, scammers are looking to pad their pockets with money that should be going toward your new mortgage. The investigative journalists at FairWarning wrote an in-depth [article on the corrupt moving companies](#) that promise to deliver your belongings at one price, only to hold them hostage until

you pay more. “It’s just like being robbed....You have no choice [but to pay],” said one exasperated consumer who gave a now-defunct company over \$2,000 for an interstate move down the East Coast only to have them demand over \$2,000 more. Other scam movers collect without ever showing up, or show up only to steal your stuff. Once you finally move in, you might think the threat is behind you, but new owners often [become the target](#) of thieves posing as home security professionals for real companies (like ADT). They may come to your door and ask you to let them in to “check out how secure your house is.” *Don’t do it!* They’re probably only there to case the joint (and eventually rob you). Slam the door and call the cops instead. As if this weren’t enough, you might also have to worry about scams surrounding all of the (many) new utility bills you’ll have as a homeowner. These [types of scams](#), usually conducted via phone, increase as the weather turns chilly and the threat of the heat being turned off makes many a consumer cough up an “overdue” payment without question. Again, *don’t do it!* Instead, hang up and call the gas, electric or water company and ask them if you really are delinquent on any payments.

## ***Don’t mess with Mother Nature***

---

A couple of major events from the first decade of the 2000s—Hurricane Katrina and the BP Horizon oil spill—have come back to haunt those who capitalized off the natural and man-made disasters. Some fancy footwork allowed State Farm to escape payouts to thousands who lost their homes or livelihoods in the hurricane. But the Supreme Court earlier this month unanimously [ruled](#) that the insurer had committed widespread fraud when it shifted claims for damage caused by wind (that should have been paid from its own coffers) to federal flood insurance in the wake of Katrina. Two sisters, both insurance adjusters, reported the fraud and filed the charges (on behalf of the U.S. government) against State Farm, which was ultimately required to give the sisters 30 percent of the initial \$750,000 it was fined in damages (proving that doing the right thing pays off). Meanwhile, a Southern California woman just was [ordered](#) to pay \$600,000 in restitution, and to serve four years in prison, for helping hundreds of Florida residents file false claims that bilked the BP disaster fund.

## ***Eat, drink and be wary***

**It’s the thought that counts.** Think twice about any gift exchange coordinated through social media, even if your friend is the one prompting you to join. There are [two major gift exchange scams](#) floating around Facebook right now, and both could reveal your personal info to crooks. (Even your esteemed correspondent, an avid oenophile, stumbled over the seasonal “Secret Wine Bottle Exchange” pyramid scheme at the behest of a friend and almost drank it up.)

**Open your heart, but use your head.** If you’re giving to the less fortunate this holiday season, first, kudos to you from us at Consumer Action. Second: Don’t forget to make sure that the individual or charity you’re considering helping is legit. The Federal Trade Commission just [issued an alert](#) outlining three major ways to avoid letting scammers steal your holiday cheer (and your generous donation).

**Up, up and away!** When it comes to busy holiday travel, any technology that helps us avoid the long airport lines sounds amaaaazing! A word of caution about the scannable QR codes on both paper and online passes, though: The gate attendant might not be the only person with access to the data they contain. Anyone with a smartphone can use a bar scanning app and immediately reveal the personal information associated with your pass. *USA Today* [shows](#) travelers how shockingly easy this is, particularly if you leave your printed pass lying around.

## Tips!

---

- **Hook, line and sinker.** Last tax season saw a dramatic rise in email phishing scams, which prompted the IRS to [issue a warning](#) that will probably be at least as relevant this coming season. Don't get hooked by phishers: Stay vigilant for emails that appear to come from the taxman or take you to bogus look-alike IRS sites. And remember: The IRS does not request personal or financial info via email, text or social media.
- **Frantic for-profits.** One clue that the college you're interested in is a scam school: aggressive, borderline insane recruiting tactics. NPR spoke with former ITT Tech employees and [found that](#) the disgraced for-profit had been looking for customers who were "likely to be kind of desperate to enroll." The college recruiters, who often received names and phone numbers from third-party lead generators that engaged in some serious profiling to identify desirable prospects, were encouraged to badger those who expressed interest via telephone a *minimum* of three times a day!
- **Big brother is watching.** Did you know that the government has a huge Financial Fraud Enforcement Task Force led by U. S. Attorney General Loretta E. Lynch, and that you can report everything from Social Security fraud to cybercrime through their [one-stop website](#)? No? Well, now you do.
- **Getting to the root of the problem.** In this brave new world of social media, citizen journalism and extreme partisanship, reports of fake news and bogus claims abound. A new site, [RootClaim.com](#), promises to help you determine what's real and what's not by using "probabilistic models" to "correct for the biases and flaws of human intuition." We'll see how this turns out.
- **NOT a deportable offense.** "In light of increased fear and anxiety in immigrant communities as a result of the current political climate" and a documented rise in complaints to immigrant rights groups, the New York attorney general [issued](#) a fraud alert warning those who immigrated to the country of deplorable hucksters who would capitalize on their status by threatening to deport or report them or by offering bogus avenues to citizenship, "legal advice" and more.
- **Computer therapy.** Hi, Mom. If you're still reading, then this one is for you: Stop talking to those people [who call](#) and tell you that they're with computer tech support! I know your computer is in a state of perma-broken due to various ([self-inflicted](#)?) issues that you harangue me about every time I come over to your house, but please, hang up the phone on these guys. One of these days I will help you "fix" everything, I swear!

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.*