Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • January 2018 • 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!

The thought that didn't count

If you're like this author, "presents" this holiday season consisted mainly of gift cards from loved ones baffled by what to get you. While gift cards are the "safe" option gift-wise, they also have a dangerous side, particularly if you're trying to resell them to someone who appreciates dining at that chain restaurant more than you do. (Seriously, mom, Chili's?!) But before you sell the card, beware! The National Consumers League (NCL) reports that they see "a spike in scams involving the resale of gift cards" each January. How do these scams work? Sellers often find "buyers" (i.e., scammers) on popular sites like Craigslist or eBay. Once the buyer pays, the seller emails them the code on the back of the card. The crafty con artists work fast, however, and will cancel the electronic payments they've initiated and drain the card's funds before you can say "store credit." To avoid falling victim to this scheme, NCL's Fraud.org recommends you only sell your gift cards via a legit website dedicated to such sales (e.g., Cardpool or GiftcardZen). You could also think about donating said cards or simply trading cards for one store (like Walmart) for credit at another store (like Target). And remember, if you're the one buying someone else a gift card, don't purchase the in-store varieties directly off the rack (scammers could have already written down the card codes). Click here for more information on how to avoid gift card grift.

I'd rather die than fall for this!

The "hitman scam" is heating up around the country, and while it's horrifying, it's also easy to not fall for the extortion attempt once you're aware of what's happening. Put simply, a person contacts you claiming that they've been hired to kill you (or will otherwise end your life, perhaps without even being paid to do it, in some cases). Fortunately, the scammers behind this one usually aren't the brightest bulbs—one dummy even emailed the CHIEF OF POLICE (!) of a New York town telling her that her life would be spared in exchange for what amounted to $6,639 (.40 in bitcoin currency to be exact). The "hitmen," who know that you'll probably be freaking out after the death threat (and wanting more info), will sometimes promise to

reveal who “hired them” to kill you if you pay up. Another strategy? A countdown. One popular email version of the scam gives recipients a mere three days to pay up (talk about pressure!) before, tick tock, time’s up. And of course, reporting the scam will allegedly get you killed. The scammers are relying on you to react emotionally. But you, oh loyal *SCAM GRAM* reader, have learned to *stop, think and react logically* anytime someone is issuing threats and making demands. Whatever you do, do not respond to these hitman scams with any personal information.

A Nigerian Prince in Louisiana?

An elderly Caucasian man who is (clearly) neither Nigerian nor a prince has been implicated in hundreds of the infamous “Nigerian prince” email scams. According to *Vice*, Michael Neu of Louisiana’s arrest is “notable because—while the Nigerian prince scam has reached a certain level of cultural saturation—very few perpetrators get caught.” You’ve probably heard of the scam (which is so old it predates email): An African royal or government official emails to tell you that you’re due some sort of huge inheritance, but first you’ve got to give up your bank account information (or send money directly) to receive the windfall. It’s amazing that people are still falling for the almost prehistoric scam, which the *New York Times* points out existed even “before we started getting all-caps proposals in our inboxes,” when “con men in West Africa plied their trade by fax and paper letter.” As police in Louisiana learned, however, the con men can be closer to home. They charged Neu with 200+ counts of wire fraud and money laundering associated with victims across the country. To Neu’s dubious credit, he *did* have real connections in Nigeria, to whom he wired the money. Click here for more information on the scam (which hopefully will be a little less ubiquitous now that Neu’s no more).

Band of brothers

Making money moves. Would-be e-commerce entrepreneurs should take note of recent lawsuits that Amazon and Washington state’s attorney general have filed against a major seller of “business opportunities” that allegedly help people make loads of money selling goods on Amazon.com. The suits allege that two brothers who live in Massachusetts engaged in deceptive marketing and sales practices by promising that their company, FBA Stores, LLC, would enable sellers to make tens of thousands of dollars (for one hour of work a day, natch). The brothers offered webinars and in-person seminars, where they’d aggressively market—wait for it—more coaching and seminars, including a $20,000 "Master Mentor" program! If you’re into making money from online sales, financial empowerment website The Balance has advice on *actually* profiting on Amazon. While you’re reading, we suggest you also check out the U.S. Federal Trade Commission’s article on avoiding business opportunity scams.

Not buying the backsplash. Your dear author has a confession: If she received a message saying she’d been chosen for the beloved HGTV show Property Brothers (in which two tall twins come in, essentially take a wrecking ball to your home, and upgrade you with an open floor plan, modern grey paint and shiny kitchen appliances), she might have fallen for it. But you won’t, because now you know that scammers are contacting the reality show’s fans and promising home makeovers (via Facebook, in this instance, and not in a particularly convincing manner at that). HGTV has advised anyone who thinks they’ve received communication from the brothers to confirm its authenticity “by sending your name along with a scan of the letter or email you received to castingverification@scrippsnetworks.com.”

All in. If you’re willing to risk it all on a high-stakes scam, you could go Oceans Eleven on a casino—but

you'll probably get caught (and may even get your knees broken by a Joe Pesci lookalike). It's probably safer to stick to reading Casino.org's list of some of the most "popular" gambling scams. The article includes a scam employed by a pair of criminals who called themselves the Roselli Brothers. The brothers managed to hack into casino computers and steal the identity of regulars with stellar credit, before withdrawing *huge* amounts of money from the victims' lines of credit. Other common casino scams to watch out for include card counting, using counterfeit coins and even employing radio transmitters to manipulate roulette balls. Don't take any chances on games of chance!

Tips!

- **Western Union pays up.** If you lost money to a scam that involved a Western Union wire transfer between Jan. 1, 2004 and Jan. 19, 2017, you have until Feb. 12, 2018, to submit a claim here and see if you're eligible for a refund. Why? The government found that Western Union had aided and abetted scammers' wire fraud efforts. Common cons involving wire transfers include lottery scams, grandparent scams, romance scams and so many more ways of tricking you to give up your money!

- **I'll take mine black.** We might as well call this Goop Gram, since Gwyneth Paltrow's "lifestyle" website Goop is in the headlines practically every month for hawking some nonsense product or another. This month it's (drumroll please)…coffee enemas! The website promises that the $135 enemas will "supercharge your detox," when in fact (super ouch!) they could perforate your colon. The Mayo Clinic notes that "coffee enemas sometimes used in colon cleansing have been linked to several deaths."

- **"Raw" water?!** We're of the mindset that clean water is safe water. Unfortunately, that can't be said of those trying to make a buck by selling the "health conscious" on what they're calling "raw water": untreated H20 (often sourced from who knows where). While straight-from-the-spring water *can* be safe, experts point out that "the cleanliness of the water depends on things you can't see—whether herds of elk or moose or caribou have relieved themselves in a stream that you're drinking from and left it full of parasites" (that can cause a very unpleasant gut disease called giardia). Or "whether there has been groundwater contamination from naturally occurring elements such as arsenic, radon or uranium, or from pesticides and other chemicals." So think twice before paying for a "health" product that might just make you sick.

- **Putting the 'BS' in BCBS.** We've always known scammers are sick; maybe that's why they're trying to get your health insurance information? Whatever the reason, they've increasingly been calling and pretending to be with Blue Cross Blue Shield insurance. When a target picks up the phone, they'll say that they need to replace an insurance card, collect payment on a past-due bill or otherwise obtain personal information because there's a "problem with the account" or they need to "update the records," "confirm your address," etc. We've said it before and we'll say it again: Never give your information to some rando on the other end of the line (no matter how convincing the pitch may seem). In the case of insurance questions, whip out your insurance card and call the number on the back for more info.

- **Uber Eats (your food?)** Seattle-based writer Kelly Clay has reason to suspect Uber Eats drivers might be grazing on your greens. After placing a recent Uber Eats order, Clay waited for her Cobb salad to arrive, only to watch on the app as the driver passed her home without delivering it. When she approached Uber about the problem, she was told she would not receive a refund for the purchased food. This led her to wonder, can a delivery driver's low pay, long drives and hunger make it more appealing to dash off and dine on your food than deliver it? Maybe. It seemed like the perfect crime, and Clay even found an online

Uber driver forum where sticky-fingered deliverers discussed ways to abscond with the customer's grub. In response, Clay has provided a couple of tips to help ensure your food ends up in the right place (*your* belly): Check Yelp reviews for reports of Uber Eats delivery problems, and order from local spots that will still be open at the scheduled delivery time (in case you need to resubmit your order). Bon appétit!

Using the drug users. If a loved one is hooked on opioids, you might be desperate to help 'em wean off and stay off. Unfortunately, uncaring opportunists get referral fees (aka kickbacks) to send people (often with health insurance) to worthless, unlicensed "treatment programs" that don't curb the cravings. Once the customer (or a loved one) realizes the program is trash, they may have already used up their insurance benefits or (god forbid) even mortgaged a home to pay for the costly (non)treatment! The problem is big in New York, Florida and other states. Here, a representative for New York's Office of Alcoholism and Substance Abuse Services tells consumers what to look out for. He recommends you speak to your insurance company first, consider carefully if you're going to exceed any out-of-network benefits, make sure the program you're considering is licensed by the state, ask for a breakdown of the fees (and what services they're going toward) and find out the treatment philosophy.

Keep it to yourself. Scammers are all up in your businesses, so why make it easier for them to steal your personal information? That vacation photo you posted on Facebook or the snap of you posing in front of your home can pose a real privacy risk (as Kim Kardashian and Colts Long Snapper Matt Overton famously learned). Fortunately, the Consumer Federation of America created a new blog post with tips for protecting personal information, both in the online world and—you may still be familiar with this—the *offline* world. The article offers advice for the secure use of public Wi-Fi, as well as safe mobile app and social media use. It also gives real-world suggestions to help you keep thieves away from your mail and other sensitive hard copy documents and information.

99 problems, but my computer ain't one. The holidays are over, the New Year is here, and many of us are finding our wallets lighter and our pants tighter. The *last* thing we need is to "fix a problem we don't have," as ABC points out in its coverage of a new Better Business Bureau (BBB) report on tech support scams. Scammers apparently are more geared up than ever to take our money in exchange for "fixing" our already-functioning computers. If you think you're insusceptible to the ruse, ABC disagrees, noting that the question is not *whether*, but when you will become a target of these widespread scams. So educate yourself for the inevitable: Read the BBB's report on how scammers reach their victims (through pop-ups, calls, emails and internet search results) and check out the tips for impeding their access to our computers (not to mention our bank accounts).

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.