Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • November 2017 • 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!

"A virtual network of American e-mules"

In what federal investigators are calling "a virtual network of American e-mules," Nigerian scammers swindled thousands of victims (the e-mules) out of millions of dollars using essentially the same enticing script from a "new-to-online-dating" paramour, which was "blasted out" over online dating websites. The scam ran unfettered for years, before one woman reported to police that her online boyfriend suspiciously sent her a box filled with cell phones and told her to ship it to Africa. (Whatever happened to good ol' fashioned flowers and chocolate?) According to the Department of Justice, "that one phone call took down a massive fraud network." After the call, investigators spent years tracking down the criminals behind a variety of related cons involving an American man named Sam West, whose online identity the scammers had stolen to "catfish" tons of women (and men) into doing their dirty work—from cashing fake checks (and ultimately wiring the money back to Africa) to shipping goods bought with fake credit cards. As MSN points out, these "finely tuned" and "sophisticated" modern operations are not your mother's Nigerian prince scams. Instead, they involve lots of people "working together to separate you from your money" and reeling you in with tidbits they find on social media and dating sites. The good news: The investigation into "Sam West" led 12 scammers to plead guilty. The bad news: A number of the scammers are still at large, and as *MSN* reveals, the investigators' recent discovery is "just the tip of the iceberg." Thankfully, the Federal Trade Commission offers information to keep you from falling for a Nigerian Prince Charming.

The real users

Adding to the already difficult and complex situation of opioid abuse, unscrupulous people are infiltrating drug rehab centers and hurting those looking to be helped off the substances. *NBC Nightly News* released an exposé on the problem of "sober homes" in the state of Florida, which one mayor calls "the Wild West… completely unregulated." As the news segment explains, young people often look to recover from addiction in a supportive environment. All too often, however, the "drug-free" rehab they rely on is, according to one

Florida mayor, run by “convicted felons, people that are trafficking drugs while they’re supposed to be supervising kids in recovery.” Another Florida attorney calls the problem the “number one” criminal justice and public health issue facing the state. And a previous sober home resident adds that even when the industry hasn’t been infiltrated with dealers pushing drugs on residents, it’s still “all fraud. You go to these places under the impression there is going to be treatment, and really you go sit in a room and talk and watch movies and your insurance gets charged hundreds of thousands of dollars." It’s safe to assume that corruption in the rehab industry is not just limited to Florida, and it’s sad to see users prey on those looking for treatment (particularly since there’s no easy solution to opioid addiction, which can be fueled by a variety of complicated factors, from genetic predispositions to experiences of childhood abuse). Addressing the underlying issues of opioid abuse is critical, as is understanding what *doesn’t* work: Criminalizing people who are addicted to opioids, offering them quick-fix programs or punishing the wrong population (i.e., those impacted by chronic pain) by cutting them off from much-needed prescription meds. Scientific research *does* show that people struggling with addiction and looking to stay off opioids are best served by a methadone or buprenorphine-type drug maintenance program to keep them from craving the drugs, along with long-term behavioral therapy and support. So if you’re looking to join a therapeutic community to help you stop using, do your research and make sure *they’re* not using *you*!

The gift that keeps on taking

Scammers flock to the holidays like your aunt to the spiked eggnog during a stressful family get-together. And let’s be honest, she (and you) have enough to worry about this season without adding gift fraud to the list, which is why we’re issuing this year’s warnings early. Look out for online sales scams in particular. Amazon.com warns of common gift card scams in this cutesy cartoon video that essentially alerts the public not to pay sellers, or anyone, really, with gift cards, and never to give out gift card claim code numbers. Speaking of Amazon, you’re best buying from legit sites like the online giant and never sending money to sellers operating outside of what you are certain is an official website/app (beware of copycat sites). And if you’re ordering gifts online, make sure that the seller (from any site) has a history of, well, delivering, and is reviewed highly (since delivery fraud—orchestrated by seedy sellers—is a real peril these days). If you get an email pertaining to a missed delivery, don’t click on the link; instead go to the merchant or shipper website and log in to your account to verify (drivers will also often leave paper tags on your actual door with contact information to arrange another delivery). If you can’t be home to accept a package, it might be best to have it delivered to your place of work to avoid theft. (Yes, Scrooge-like criminals will steal the presents right off your doorstep!) Finally, be wary of online greeting cards from unknown friends and admirers—instead of bringing the holiday cheer, they may bring computer viruses or links that take you to sites designed to phish for your personal or financial information. Click here for more common holiday scams, and remember: ‘Tis the season to be wary!

Oh, the lengths they’ll go…

What’s worse than a dead baby scam? Dead baby jokes are tasteless; dead baby scams, even more so. A heart-wrenching sign featuring a cute baby and asking for money for “burial donations” got two California women in trouble with the law last month. They were initially arrested for panhandling on the street. When police looked into the handmade signs the women had been holding, they learned that the “dead baby” featured did not belong to either of them and that, fortunately, no burial funds were needed.

How about a *live* baby scam? We've heard of adoption scams, but this one takes the cake for cruelty. An Alabama woman promised her (real) unborn child to at least four families across the country, sending sonogram photos and encouraging the would-be parents to pick out names for the promised baby boy (and to send financial support as the pregnancy developed). The mendacious mother-to-be was busted when multiple adoption agencies and attorneys compared notes about their clients' suspiciously similar circumstances. Unfortunately, each of the families had lost at least $6,000 by the time the jig was up. Currently, there are no laws in place to protect adoptive parents from losing money in these types of shameful scams, although the fertile soon-to-be-felon is looking at two to 20 years in prison.

Joy(less) ride. A 34-year-old man was sentenced to eight months in prison in connection with 50(!) car crashes that he and a group of accomplices organized with real—but dishonest—policyholders over the course of several years in order to bilk almost $100k from insurance companies. How'd he do it? By running into trees, fences and other "victimless" objects on remote roads, jumping out of the driver's seat after the impact, and switching with the policyholder accomplices (who would then call for help). In addition to the property damage, sometimes the insured would fake bodily injuries and file those claims as well. Conveniently, there were never any witnesses. And of course, the crash-happy con man got his cut. Our take: When this guy's done his time in the slammer, someone please hire him as a stuntman!

Sick, sad world. The Red Cross has released chilling details on how unscrupulous employees and even a Sierra Leone bank stole over $6 million in funds earmarked to fight the deadly 2015 Ebola outbreak. Collusion between the bank and employees resulted in the disappearance of over $2 million, while the rest was lost to overbilling, fake invoices, inflated payrolls and other fraud. Donors who trust the Red Cross to be responsible, upstanding stewards of their money are no doubt upset to hear the news. The non-profit, to its credit, has been forthcoming about the internal investigation, which reviewed how it handled a total of $124 million to combat the epidemic that, all told, caused the (horrific) deaths of over 11,000 extremely unfortunate people.

Tips!

- **We're wired about these refunds!** Did you wire money via Western Union only to lose it to a scam? If the unfortunate incident occurred between Jan. 1, 2004 and Jan. 19, 2017, the Federal Trade Commission (FTC) has ruled that Western Union must provide you a refund (but first you have to file for one, and soon: by Feb. 12, 2018). How did this justice come about? The FTC filed a lawsuit against Western Union after finding the company guilty of knowingly allowing fraudulent money transfers to occur with impunity and of ignoring federal requirements to report said lawlessness. These transactions ran the gamut from hucksters claiming they needed money for "family emergencies" to criminals promising lottery winnings once they received (bogus) associated fees. Learn more about how to file a claim here.

- **Another day, another Netflix phishing scam.** *Inc.* is calling it "a genuine work of art as phishing goes." The con? An official-looking email scam that's convinced thousands of Netflix users to click on a link to sort out a "billing issue." The link prompts the users to "restart" their membership and takes them to a website that really does look like the real deal, complete with promotions for Netflix shows like *The Crown* hovering in the background behind the "log in" button. Once an unwitting victim logs in, the hackers steal their username and password. If they then "validate" their payment information, the hackers steal their personal/financial info. *Inc.* has more on how these criminals have used technology to keep the bogus site

up for some time now.

Close to home. The Northern California wildfires have hit close to home for many, even impacting Consumer Action employees who live in the region. Fortunately, our staff *hasn't* experienced the identity theft that other area wildfire victims have dealt with. According to the Federal Emergency Management Agency (FEMA), scammers have beaten some homeowners looking to file claims to the punch, using breached personal information to file fraudulent ones in the homeowners' names and collect on the damage. Those who have received a notice or visit from an inspector (but did not register for assistance) should call the agency at 800-621-3362 to cancel any fraudulent registration. Fire victims should also be wary of anyone claiming to be an insurance adjuster and offering to "help" them in exchange for a percentage of the claims money.

A lose-lose situation. A former NASA engineer posted a fascinating video in which he explains the physics behind carnival games, which "employ a bunch of little tricks to make you overestimate your chances of winning, in some cases to such an extent that it's basically a scam." In the video, he outlines three types of competitive games: random chance ones like Plinko (known for offering the player lightweight balls that will not end up in whatever hole they're aiming for); skill-based ones like basketball (with hoops set at a different distance/height than the player would be used to on a traditional court); and ones that are pretty much impossible to win, like those involving throwing tiny rings around the tops of bottles (which are almost as thick as the ring diameter). Even if you win these types of games, you're still losing: As the engineer points out, the junk you might win costs way less than what you're paying to play the game.

Hitman scam. Sinister new scams have grown along with the use of social media and the rise of "oversharing." A New York *CBS* affiliate interviewed one man who was the target of a "hitman scam." The man received an anonymous email threatening to murder his family if he didn't pay $3,000. Fortunately, he realized the threat was idle; the sender didn't know anything about his family. Some scammers, however, do their homework, combing through your online history to find names and locations of loved ones. Other people have been receiving text messages from "hitmen" allegedly hired to kill *them*. The senders say they can only be dissuaded if the recipient pays thousands. As difficult as it may be, just ignore these types of messages, since replying to a scammer and letting him know you're gullible is what really puts a bullseye on your back.

Buyer's remorse. It's a simple yet clever phishing technique: Scammers have been sending emails that appear to be from PayPal, thanking people for purchasing a product that they know nothing about. In the video here, a woman talks about receiving unexpected word of a $171 camera purchase from eBay. In her haste to cancel what she thought was an erroneous charge, the woman was quick to click on the link listed in the email in order to "log in" to PayPal and set everything straight. Big mistake: Rather than ultimately gift the scammers with her personal/financial info, she should have instead, as any savvy SCAM GRAM reader can tell you, gone directly to PayPal's site and logged in to see if any charges were actually made. Remember, check it out before you click!

For-real realtor. We wrote about this one a while ago, but it certainly bears repeating: If you're closing on a home these days, you need to be *super* careful who you send your closing funds to. It's been a very lucrative year for those preying on homebuyers: In 2017, buyers lost or almost lost nearly $1 billion in closing costs scams (a huge rise from the year prior)! The *Washington Post* sums up the scam: "Hackers find an opening into a title company's or realty agent's email account, track upcoming home purchases

scheduled for settlements—the pricier the better—then assume the identity of the title agency person handling the transaction." If you've got plans to purchase a new crib, learn more here.

When dogs fly! If you're looking to fly Fido across the country on Delta airlines, *do* look further than the website DeltaPetTransit(dot)com. The real Delta has filed a lawsuit against the site, which uses its logo and photos of its planes to mislead customers into thinking it will ship and deliver pets. Delta says the site does no such thing, and instead steals money from hapless consumers looking to transport or even buy dogs. Even worse, there are other sites with similar names (like DeltaPetAirways, for instance) doing the same thing (and likely colluding with phony online pet sales sites). If you run into a puppy scam, there's a new way to report it through a site called PuppySpot, which also helps connect dog lovers to legit breeders (or you could, you know, adopt a puppy from your local pound).

To catch a predator. Imagine you're on a dating site chatting it up with what you think is a twenty-something match, only to be told after she sends some risqué photos that your new friend is in fact underage. This is what happened to one man who promptly got calls from what he thought were local police and even the girl's *father*, threatening him with jail time. The man in this story knew something was up, however, when the "father" demanded money to send his "daughter" to counseling. Unfortunately, many men don't realize these types of extortion scams are just that: scams. Some pay hundreds of dollars in hush money, some are too embarrassed to speak out and live in fear, and others are so distraught they even commit suicide! Before you go online looking for love, check out these safe online dating tips from *Psychology Today*.

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.
