Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • October 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!

Odious opportunists

Scammers know no bounds when it comes to exploiting horrific events. Last month it was widespread hurricane destruction; this month, the mass shooting in Las Vegas. The tragedy sadly but predictably brought scammers out from under their rocks. A throng of bogus GoFundMe and other crowdsourcing pages sprung up in its wake (as did a number of fake charities), leading attorneys general in multiple states to issue warnings. (Pro tip: GoFundMe is vetting legitimate pages to support Vegas victims and listing them on its site.) It's not just online operations defrauding the compassionate—be wary of "fundraising" attempts by phone as well. If a telemarketer calls claiming to be with firefighters or the police, for instance, let the caller know you'll call the department back directly (and don't give any personal or financial info to the solicitors). And if you get a text prompting you to donate (the American Red Cross is known to use this outreach tactic), make sure that it's really the organization you want to help by verifying its number. In summary: Always double check by directly contacting the organization you're interested in donating to. And be careful: Even a trusted organization's website can be mimicked by slightly altering the URL (for instance, reddcross(dot)org with two "d"s—see how easy that was?). If you're worried about the website, there are *many* ways to confirm that a charity is real, as the Federal Trade Commission (FTC) points out. But what if a shameless charlatan *has* contacted you? If you think they're operating locally, let your state attorney general know. If the operation's even bigger (read: national), let the FTC know.

Netflix and bill

It's a brave new world out there, one with video and audio streaming, the sharing economy, online shopping, and other modern conveniences ripe for scamming. If it's not Amazon in a con artist's crosshairs then it's Netflix (or another company)—and this month it's Netflix. If you get an email from supportnetflix(at)checkinformation(dot)com, you should back away faster than you would from an episode of "Fuller House." The email will tell you that there's been a "billing" error and, of course, you need to

update your payment details (sigh…typical). Click here to see what the dreaded email looks like. (But don't click on the email itself. If you do, it pops up in your inbox and they have you.) In a nutshell, the email will prompt you to click on a link to a look-alike site or to respond with your credit card number or banking info (once you do, the rest, of course, is history). Note: Netflix will *never* prompt you for your email, your password, financial information, Social Security number or any other information that scammers typically want. And if you're worried that you haven't paid and you're about to be shut out of your account and miss the much-hyped "Stranger Things 2," by all means log in to Netflix ASAP and make sure that you're squared away. (Don't call Netflix based on a phone number that pops up when you Google it; scammers have that one covered too and are posting phony customer support contact info online.)

Bitcoin buyer beware

They say that no press is bad press, but that may not be true for Bitcoin. The cryptocurrency has been getting a lot of negative publicity lately, with both the Wolf of Wall Street and the CEO of JPMorgan (ahem, they're two different people) calling the digital dollars a "fraud." The investors' concerns stem from the fact that the increasingly popular monetary system currently has no government backing and is based on "artificial scarcity." Despite this lack of government support, federal regulators are certainly taking notice of Bitcoin. Last month, the U.S. Commodity Futures Trading Commission charged a hedge fund company with fraud, misappropriation, and issuing false account statements in its operation of what they called a "Bitcoin Ponzi scheme" that bilked $60,000 out of investors. Meanwhile, the Securities and Exchange Commission recently charged both a real estate and diamond sales company with defrauding investors after prompting them to sink money into an "initial coin offering" (ICO), the first of its kind. A *New York Times* columnist described ICOs: "Imagine that a friend is building a casino and asks you to invest. In exchange, you get chips that can be used at the casino's tables once it's finished. Now imagine that the value of the chips isn't fixed, and will instead fluctuate depending on the popularity of the casino, the number of other gamblers and the regulatory environment for casinos. Oh, and instead of a friend, imagine it's a stranger on the internet who might be using a fake name, who might not actually know how to build a casino, and whom you probably can't sue for fraud if he steals your money and uses it to buy a Porsche instead." Buyer beware!

Just deserts for loan sharks

It's high time unscrupulous payday lenders got called out for what they really are: professional defrauders. While payday lending isn't illegal, consumers need protection from the all-too-common loans charging upwards of 300% interest rates and trapping consumers in a cycle of debt. Fortunately, the government is finally getting serious about cracking down on the debt traps. The Consumer Financial Protection Bureau (CFPB) issued its final payday lending rule earlier this month. And the Justice Department has gotten on board, charging payday loan shark Charles Hallinan with racketeering, conspiracy, money laundering and fraud. Hallinan maneuvered to get around sensible state and federal regulations and charge those in a bind 800+% interest rates on loans (through a myriad of companies, like "Tele-Ca$h," "Instant Cash USA" and "Your Fast Payday")—pretty par-for-the-course in the payday industry. We're currently working with a big coalition to stop people like Hallinan, and you can help by contacting your reps in Congress to voice your support for the CFPB rule protecting consumers from the payday loan treadmill (learn more here).

Serving up food fraud

But Gatorade's got electrolytes! In what could be a scene straight out of *Idiocracy*, the makers of Gatorade decided to get creative and create a mobile video game called "Bolt!," featuring a cartoon character of Olympic runner Usain Bolt. In the game, Bolt runs faster when he touches sugar-laden Gatorade icons and slower when he reaches plain ol' wholesome water, with text reinforcing the message: "Keep your performance level high by avoiding water." The game was heavily promoted to children and teens on social media. Eventually, its "misleading [water] statements" trickled down to California's attorney general, who sued and reached a settlement with the company (to the tune of $300,000) for violating the state's consumer protection laws and engaging in "beyond awful" advertising to children. The settlement also forbids the sports drink maker from talking smack about H20 in future ads.

Made with love. The Food & Drug Administration (FDA) had to give a bakery the bad news that a human emotion cannot be a listed ingredient in a food product. Massachusetts-based Nashoba Brook Bakery got cutesy and added "love" as one of the ingredients in its granola. The company's chief executive is describing the government's subsequent cease-and-desist warning as Orwellian and accusing the cold-hearted regulators of failing to see how "nice" it is that an artisan bakery can claim a product is made with love. Unfortunately, Nashoba's products might also be made with bugs (lovebugs?). The FDA's inspection of its premises noted numerous health violations, including a "crawling insect" hanging out with the "focaccia breads, 7-Grain rolls, and brioche rolls."

Damaging more than your waistline. Decadent bacon double-cheeseburgers and banana cream pie shakes aren't the only things SONIC, America's Drive-In is serving up. If you've visited the chain recently you may have also bought yourself some identity theft. SONIC joins the disgraced ranks of Equifax, Yahoo and many other companies that have been impacted by massive data breaches. SONIC's payment systems were hacked, resulting in up to five million credit and debit card accounts potentially being "peddled in shadowy underground cybercrime stores," according to security site KrebsOnSecurity. If you've pulled up to SONIC's drive-in, it's time to pull up your credit and bank account statements to see if there's been any illicit activity.

Tips!

- **It pays to be picky.** Online hotel booking scams upset on average around 15 million bookings annually. In our excitement to score a good deal, it's safe to say we may be rushing things a little, and it's leading us to fall for the first (bad) deal we find. The problem of scam hotel sites is so ubiquitous that Congress recently took up legislation to stop criminals from bilking $1.3 billion from consumers annually (the current rate of money lost in bad bookings). Before clicking the mouse and agreeing to make a reservation, make sure that the site you're on is legitimate and dependable (you know, like an Expedia or a Hotwire), or just book directly with the hotel (many will match the price you found online). And remember, even if a site has a trusted logo, it could be a fake. So check, and then double check, before you check in.

- **BS detector.** Did you know that some wireless phone carriers offer scam detection for free? Often, getting it is as easy as asking for the service, which warns you with a phrase like "scam likely" when an incoming call originates from a sketchy number. From AT&T to Verizon, the website Lifehacker outlines the different phone companies, what they offer and if it's gonna cost you. Check it out and see if your phone is covered!

Seize the day! Hope you didn't think the Equifax debacle was over, because scammers are in it for the long haul, milking the massive data breach for all it's worth. Currently, they're calling credit holders pretending to be with the beleaguered company (but we wouldn't be surprised to see email and text solicitations soon as well). The opportunists claim they must "validate your account information"—and they're good impersonators, so even if the number on your caller ID says "Equifax," hang up! The company won't be calling or emailing you out of the blue; they've got their hands full with millions of angry customers and an FTC investigation that we hope leads to some real action against any company that fails to protect customer data. At any rate, for *real* info on how to protect *your* info from the breach, click here.

Imaginary friends. If you click on an ad because you're looking to buy a puppy, you may fall down a rabbit hole instead. According to a new BBB report, a whopping 80 percent of online pet sale ads are fake! Scammers often steal photos from real breeders' websites and create their own sites (which the ads will direct you to). These sites come complete with bogus testimonials, health and vaccination guarantees and more. The pages are convincing and the prices are enticing, but if you pay for the nonexistent pet, the scammers typically demand more and more money (for fees, dog crates and all manner of bogus nonsense) and may even threaten to report you for "pet abandonment" if you stop sending the cash! The BBB cautions would-be animal buyers to visit breeders in-person (or just go to your local pound and adopt instead of buying), check references and never, ever wire money (always use a credit card so that you can dispute charges). Still looking to buy a Weimaraner on the World Wide Web? You can view a list of pet scam sites here (and report any others you come across).

Forget Jeeves; ask James. Think it's a con, but want a counselor to confirm? The National Consumers League (NCL) has a dedicated staffer to help you avoid falling for a scam or, in case you already have, dig yourself out. "The best calls are from someone who is suspicious of an offer before they've acted on it, and I have a chance to intervene and help them avoid falling victim," NCL fraud counselor James Perry says. He also works to recover lost funds, explaining, "Helping consumers devastated by fraud is what I love most about my job." So ask James—he's a solid guy.

Afraid of change. These days, the USPS may change your address even if you don't move. As a matter of fact, scammers can go online and do it. When this couple received a letter confirming an address change, they thought it was just junk mail, until they found out that a criminal had been diverting their mail to another address and applying for credit cards and loans in their name. If you suspect this may be happening to you (particularly if you stop receiving mail at your address), call the post office and contact the credit bureaus ASAP to find out what's going on.

Self harm. Remember when your older sibling used to hit you with your own hand and claim, "I'm not touching you"? The latest phone scam is kind of like that. Crooks are using "you" to do their dirty work. They assume you're more likely to pick up an incoming call coming from your own number (and they're usually right). As amusing as it is to get a call from yourself—many on Twitter are joking that it's their future selves—picking up and responding just lets scammers know that you're here in the present (and vulnerable).

Leave 'em in the dust. We recently wrote about gas station "skimmers": undetectable chips that thieves connect to credit/debit card readers to steal your information when you run your magnetic strip at the pump. It turns out there's now a way to fight back, in the form of a free Android app called Skimmer Scanner that can detect the nasty little things (by the Bluetooth technology they use to swipe your data)

and alert you if there are any nearby. So gas up and go, without the 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.
