Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • June 2019 • 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!

Keeping it real

OK, we admit it, we love shopping on Amazon, where we can find anything—including fake reviews promoting some very devious scams. The problem got worse in 2016, when the retail giant saw an explosion of cheap, counterfeit brands (mostly from China) shipped through its Fulfillment by Amazon program. Add in the fake reviews and you have a perfect storm! Amazon has deployed algorithms to detect suspicious review patterns, but this is difficult to fight because devious scam sellers pay for the fake reviews. In addition to financial incentives, these entities are providing detailed, ever-changing instructions on how to make the reviews appear authentic. (One journalist discovered a thriving "fake review economy!") We realize this is a tricky game of Whack-a-Mole, but we hope Amazon (whose record high profits reported in Q1 of 2019 were almost $60 billion) can use some of their wherewithal to take even more steps to solve this problem. In the meantime, shoppers should steer clear of products with loads of reviews posted on the same day, unverified reviews, and reviews that sound suspiciously similar to others. There's also FakeSpot, a website that will scan and analyze reviews and grade products from A (credible) to F (for "fail," or "fake reviews").

Stop the madness!

Robocalls are the bane of every phone owner's existence. Knowing this, and that the

problem is getting worse, particularly as it relates to scam calls "spoofing" (faking) government numbers, our latest *Consumer Action News* is appropriately titled *The Robocall Scourge*! We cover what every consumer should know when dealing with robocalls. For example: Unless they are political or charitable in nature, the vast majority of robocalls are illegal. Perhaps most importantly, we tell you how to block the obnoxious calls. Among your options? Join the Do Not Call Registry, use a call blocker or a blocking app such as Nomorobo, employ the built-in settings on your smartphone to block calls from certain numbers, and/or activate blockers via your wireless carrier. And, you can (and should) call on Congress to pass a bipartisan bill called the TRACED Act, which would force phone companies to adopt tech that alerts consumers/blocks the illegal calls. TRACED would require the Federal Communications Commission (FCC)—which has been slow to take action even though robocalls are *technically illegal*—to actually, you know, regulate. One plus (sorta): Earlier this month, the FCC passed a rule to "allow" (but not require) phone companies to block robocalls without requiring customer sign-off (a service for which the companies will, sadly, be permitted to charge extra). Under the new scenario, if your carrier blocks robocalls and you *want* to hear an artificial voice at the end of the line (who *are* you??), you can opt out.

Get that coin

Step into the light. Wall Street's financial crimes are often hidden, but investigative journalists, regulators and others often can expose them. Wall Street Market (WSM), however, was operating entirely in the shadows. Up until last month, WSM was just another vendor on the "dark web" (the corner of the internet where people go when they don't want to be found or tracked). It allowed people to deposit cryptocurrency (Bitcoin and the like) in digital "wallets" to make (typically illicit) purchases. Cyber-savvy WSM customers realized the seedy operation was pulling a classic "exit scam," however, when they no longer had access to their wallets, and WSM admins began coming up with a variety of excuses as to why, buying themselves time as they drained $30 million in customer funds before disappearing into the darkness. Only, WSM didn't *totally* disappear: An admin with access to the shady seller's database has been blackmailing users, threatening to report them to law enforcement for their (usually illegal drug) buys if they don't pay up with a Bitcoin or two (each worth $7,948 and change at this writing). The feds are constantly arresting dark web vendors (and sometimes their clientele), so putting your coins in this basket may not be wise.

Hop, skip, jump. Hackers have created a website that looks like the site Cryptohopper.com, which bills itself as "the best crypto trading bot currently available." Tech/security news site BleepingComputer posted an image of the fake site, complete with a perfect rendition of Cryptohopper's cute lil' robot dude (who represents the site's automated trades). The image was all they posted, however, as simply skipping over to the fake site is enough to cause information-stealing malware to jump into your computer and begin siphoning off data, such as your browser history, saved login credentials and

payment info, and, of course, your cryptocurrency wallets (which the hackers are assuming you use, if you're visiting a site like Cryptohopper). The criminals have set the malware to upload your info to a remote server, where they harvest it. They've *also* set it to bounce any money you might transfer via your digital wallet(s) to their *own* wallet, which (shockingly enough!) is online for all to see (and, as of this writing, boasts the equivalent of over $258,000 USD).

Bitcoin is gambling. Change my mind. Above, we expose some scary cryptocurrency cons. "But simply investing in Bitcoin is a safe and straightforward way to get in on the game," you proclaim! Through the use of statistics and probability ("the maths"), one CNN reporter revealed that "investing" in this cryptocurrency (over traditional stocks) is actually more like gambling. Your average annual return when playing the stock market is 11.5% (an easy calculation to make by measuring the historic variability of the S&P 500). Basic statistical analysis reveals that you're 95% likely to encounter a swing in returns from –11% to +34% in any given year. Not too terrifying. Now take Bitcoin: According to the Grayscale Trust (a marketplace for buying and selling Bitcoin), in any given year, your Bitcoin (invested through the Trust, mind you, and *not* directly into some unknown, riskier ICO venture that makes off with your money) averages a 60% return. "Sounds great," you say! Except that these investments are 95% likely to give you a return anywhere from –100% and +222% percent! *Negative 100!* Considering the possible losses, a person is generally safer "at the craps table."

Tips!

- **What the Zelle?!** Veteran consumer/tech journalist Bob Sullivan, of the eponymous site BobSullivan.net, is warning consumers to watch out for mysterious bank account charges from Zelle, even if they've never heard of Zelle, let alone opened a Zelle account. If you aren't aware of the peer-to-peer payment system, it's actually so convenient it's giving Venmo a run for its money, since it operates from within a user's bank or credit union account/app. Unfortunately, this makes it convenient for criminals to access the accounts too, by hacking into them, linking Zelle (if it's not already been linked), and adding their own mobile number to the linked accounts to confirm mobile financial transactions. The worst part? Consumers have been reporting difficulties disputing the charges with the banks, as Sullivan reported after contacting Bank of America to go to bat for one man who lost $1,800. Here's a tip: Change your online banking username and password frequently! Use a combo you can remember easily without writing it down, but do not employ credentials using personal details. (Not even beloved Fido's name!)

- **Terrorized in three acts.** What would you do if the government called you up and accused you of having funded a terrorist group like ISIS after you *had* in fact given money to an individual you didn't really know over the internet? Probably freak out and immediately attempt to prove your innocence! Scammers are banking on this. Using the instant

message function through Facebook, dating apps and even the seemingly innocuous Words with Friends, the criminals commence a reign of terror by contacting their targets, chatting them up and asking them for money for a "friend in need." After they've sent the money, these targets receive a call from what appears to be the Department of Homeland Security (a spoofed number), accusing them of *actually* having given money to ISIS, al-Qaida or some other terrorist group, and threatening them with arrest and jail time. The final act? The elaborate scam introduces an "attorney" into the equation, who offers to help the now-terrified victims fight the accusations—for a grand or more.

Home sweet…[groan]. File under "closing catastrophes:" A South Florida family lost $77,000 after wiring closing costs for a new home to someone they *thought* was their attorney. Larry Beach was ready to move into his dream home *near* the beach when his lawyer's secretary—to whom he thought he had wired the money—asked him to…wire the money! What Larry must have felt in that moment, we can only guess. The closing email Larry had been sent looked legit, even (according to CBS) boasting "the right logo, contact information and same display name as the lawyer's secretary." But upon closer inspection, there were a few things…off. According to the CFPB, hackers have been monitoring communications between real estate and closing agents and their clients and creating email addresses that are a character or two away from the real ones. They then email the client close to his or her closing date, posing as the trusted agent. "There's often little that can be done to retrieve the stolen funds once the theft has occurred," the CFPB cautions, before advising consumers not to send funds via email without confirming first via phone. (Better yet, personally hand a cashier's check from your bank made out to the seller over to your agent, old school-style.)

They see me rollin', they hatin'. Jesse Marquez was psyched when he got a text from Monster Energy offering to pay him to wrap his car in the company's battery acid-green branding. If he'd called the energy drink maker to confirm, however, it would have told him the proposition would, like most car-wrap cons, lead him down a winding road of check fraud. All signs pointed to danger ahead when Marquez agreed to the deal and received a check for coating his car in corporation that was way bigger than promised, and that required him to turn around and reimburse the sender for the overage before it had cleared. What could have ended in disaster didn't, fortunately, after Marquez shared news of his "good fortune" with his savvy son, who told him to put on the brakes. Any time you get a check written for "too much," it's a scam! If you're still hell-bent on earning a few bucks driving around in a corporate billboard—*think how awkward it would be to pick up your dinner date!*—there *are* legitimate businesses out there. Compare among several companies and always look for a deal with no upfront costs to the driver. (Those with car loans and leased vehicles need to be super sure they are allowed to participate in ad wrapping.)

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

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