Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • April 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!

CBD: A cure-all, a con or a question mark?

Disclaimer: We're not trying to harsh your mellow, dude. But we *do* think you should know the facts about cannabidiol (CBD) supplements. Late last year the government (finally!) legalized the commercial production of hemp (derived from the marijuana plant). As a result, the non-intoxicating "medical" hemp-derived CBD industry exploded. We put medical in quotes because CBD is marketed as a dietary supplement, not a medication (despite medical claims), meaning it can skirt meaningful FDA regulations around product purity, quality control, etc. In fact, a 2017 *JAMA* study of 84 CBD products revealed that less than a third contained the amount of CBD stated on the label. Complicating things further, CBD sellers tend to make *lots* of claims about CBD's medical benefits, the vast majority of which have yet to be backed up up by peer-reviewed human studies. While studies *do* show that CBD has proven helpful for decreasing some forms of epileptic seizures, insisting that it will cure cancer or Alzheimer's—not to mention generally work better than traditional painkillers or antidepressants for the management of complex medical conditions—can be damaging to consumers/patients. This led to the Federal Trade Commission (FTC) and the Food and Drug Administration (FDA) warning CBD companies earlier this month to stop making claims that can't be backed up by science (for instance, that CBD is "an effective and safe treatment alternative" for serious inflammatory conditions like lupus). One of the companies the agencies wrote to (Nutra Pure, LLC) claimed that CBD is "slowing the progression" of Alzheimer's. Another (Advanced Spine and Pain, LLC) stated: "CBD improves the symptoms of schizophrenia." Yet another (PotNetwork Holdings, Inc.) said that CBD "has shown the ability to kill cancer cells directly." Want to tell the FDA what *you* think? They're holding a public hearing on May 31.

When it rains, it pours

As if they didn't have *enough* to worry about, victims of the recent California wildfires and Hurricanes Harvey,

Maria and Irma have now become victims of failure by the Federal Emergency Management Agency (FEMA) to protect their personal and financial data. The agency allowed a "major privacy incident" (its own words) to occur by giving way too much information on the nearly 2.3 million Americans needing temporary housing post-disaster to a private contractor (which, oddly, remains unnamed). FEMA tasked the contractor with helping to set up short-term hotel housing for the survivors, and, rather than give it the basic information it would need to facilitate this, FEMA shared not only the names of program participants' financial institutions, but also their electronic fund transfer numbers and bank transit numbers (talk about giving away the keys to the castle!). All told, the agency exposed 20 unnecessary data fields to a third party that itself had a number of "security vulnerabilities" and was found to be at "moderate risk" for a data breach, according to a government report. FEMA's PR people are reporting that it's "unclear" if the vulnerable data has been accessed by scammers and used for identity theft/fraud. (Since the contractor only retains the data for 30 days, it's hard to say if any data was breached prior to the 30 days of stored data FEMA was able to analyze.) If you're a disaster victim who used FEMA's Transitional Sheltering Assistance program, we recommend you obtain your free credit report now and continue to monitor your bank account. You also can freeze your credit for free (learn more here).

Comeuppances

Fatal error. The FTC has fined Office Depot $25 million for straight up *lying* to customers about their computers being infected with viruses (in order to sell the confused consumers on tech support services). The company based its "PC Health Check" assessments on people-like-your-grandma's affirmative answers to questions during a virus scan (such as whether their computer ran slow or had virus warnings)—*not* on the presence of actual malware. The penalties will go toward refunding customers.

Affirmative action. Lori Loughlin's *Fuller House* co-stars may be supporting her, and the Abbotts' "blunt-smoking son" may be supporting them, but the 33 wealthy parents charged with various counts of mail fraud in the notorious college admissions scandal known as Operation Varsity Blues aren't likely to receive much support from the judge. While some involved in the scheme have agreed to rat out others in exchange for lesser sentences, the court is likely to take action even against those who are apologizing and pleading guilty, including issuing jail time and/or stiff fines.

Boy, bye. Robocalls: The notorious annoyances are so prolific that *Last Week Tonight with John Oliver* dedicated a lengthy segment on ending them (with a particularly creative solution). Robocallers generally are prohibited by law (without express consent) from placing robocalls to cellphones or sending telemarketing messages to numbers on the National Do Not Call Registry, yet robocallers persist because scammers don't give a darn about the law. Fortunately, the FTC is hunting down illegal robocallers and their ilk like Predator. In addition to releasing a nifty video on "what to do about robocalls," last month the agency announced it had stopped the sham charity "Veterans of America" from robocalling sympathetic donors and collecting millions; banned a company that's historically supplied the autodialers used to make robocalls (and fined them more than a million); issued a "telemarketing ban" on a credit card debt-relief scam company; and more. Read about it all here!

Tips!

SMH, Facebook. It's hard not to shake your head over Facebook's data privacy fiascos, they just keep on coming. First, Krebs on Security discovered that FB was keeping unscrambled user passwords in a database that, if (when?) hacked, could lead to disaster for millions of users. (Keeping plain text passwords is a n00b move, and not something expected from a social media giant.) Second, FB's partners (who have had access to *way* too much of its user info over the years, as evidenced in the notorious Cambridge Analytica scandal) have been storing *tons* of user data (including passwords) on publicly accessible Amazon cloud servers. (We're thinking now might be a good time to change your password!) Third, for months FB was unaware of a barrage of scam ads plaguing its site. The ads, which featured photos of President Trump and recognizable public officials from just about every state, prompted viewers to click on a link and enter their utility account information for "tax breaks" for installing solar panels on their homes. Sigh…

A lethal loophole. Since greedy automakers won't compensate dealers for recalled used cars and the dealers have a hard time moving them off the lot, the auto industry (led by the questionable ethics of the industry group Automotive Trade Association Executives) has pushed *hard* for legislation that allows the dealers to continue selling dangerous recalled used cars (without fixing them, and without fear of a lawsuit if someone is hurt by the death traps), so long as the dealers "disclose" the recalls. This "disclosure" is meaningless, as Rosemary Shahan, president of Consumers for Auto Reliability and Safety (aptly acronymized CARS), points out, since it's often "hidden in a stack of documents and presented to the consumer only after they have already test-driven several cars, chosen a car, negotiated the price, applied for credit and signed a purchase or lease contract." CARS offers advice on how to check for recalls *before* you're about to buy and avoid getting stuck driving a "ticking time bomb." We recommend reading it. And contacting your rep in Congress to demand a ban on the sale of recalled used cars.

Lose the Noom. Trying to lose weight? You might want to lose Noom, an increasingly popular weight loss app that advertises incessantly on Facebook. (Full disclosure: This writer signed up for it and paid $127 before demanding her money back after finding it to be, well, less than advertised.) Noom promises a lot of things, including a personal health coach (who wasn't that available and whose answers to user questions seemed suspiciously bot-like); a weight loss support group (that this user was told she could not join until three weeks into the program, a strange caveat *not* mentioned in Noom's promotions); and, perhaps most egregiously, the promise that "no food is forbidden," with ads featuring snacks of delicious-looking pancakes slathered in butter and syrup (nom!). As nice as eating pancakes and losing weight sounds, Truth in Advertising (TINA) points out that "gut check" claims like Noom's are what the FTC warns marketers to specifically avoid, stating: "Let's face it: When it comes to dieting, there are no easy answers. If a product promises weight loss without effort and sacrifice, it's bogus."

Tax-time tricks. Just because you're done with your taxes doesn't mean scammers are done with you. Au contraire: Your filing with the IRS opens a whole new world of opportunity for these scoundrels to say they *are* the IRS calling to rock your world. Savvy scammers are now claiming to be reps from the Taxpayer Advocate Service (TAS). Since TAS is an actual organization within the IRS, and the callers are spoofing its actual phone number, this is one convincing con. Regardless, if you get a call from anyone demanding any tax-related payment over the phone, just hang up and contact the IRS directly for clarification.

'Can I borrow your phone?' Next time a stranger asks to use your phone, think twice—or at least monitor the user carefully—particularly if you use Apple Pay, Venmo, Cash App and the like. Fast-acting fraudsters are claiming they need to text a friend or relative to get out of a bind, turning the phone away from its owner, opening the owner's money transfer app (typically linked to a debit card or bank account) and

sending themselves money. One woman lost the $1,430 she had saved in Venmo to buy a wedding dress after a seemingly “sweet” man borrowed her phone, taking it to his car so he could “look up a number”. She’s now warning others and recommending they put money transfer apps in hidden folders on their phones. Experts also recommend users require a thumbprint or a PIN each time a transfer is requested, and to link apps like Venmo to credit cards, not a bank account (as this gives victims a higher chance of recouping any lost money).

Several rings. We covered the fake Social Security Administration (SSA) and Chinese embassy phone calls in prior issues of SCAM GRAM, but they’re worth mentioning again since both scams are widespread and show no signs of letting up. As a matter of fact, the FBI has said that the (mainly Chinese immigrant) victims of the embassy call have lost a combined $40 million to the Mandarin-speaking menaces on the other end of the line. Meanwhile, the SSA scam continues to evolve, with targets being told to “press 1” to speak to an SSA agent regarding “suspicious” activity on their account. (Note: It’s the call itself that should raise suspicions.) Don’t think you’d fall for it? Read this reporter’s account of how she almost fell for it when a “fraud investigator” left her “shook” by his calm demeanor.

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.
