

If you no longer wish to receive email from Consumer Action, [skip to the end of this message](#) and click the link to opt-out.

[View this newsletter in a browser.](#)



Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • July 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!

Goop be gone

What is *with* celebrity Gwyneth Paltrow's Goop?! It seems that the snake-oil website has been making claims of an increasingly ludicrous (and easy to debunk) nature. The most recent: "Wearable stickers that rebalance the energy frequency in our bodies"—stickers that Goop claims are "programmed" to a frequency that will "fill in the deficiencies in your reserves, creating a calming effect, smoothing out both physical tension and anxiety." (Sounds like a job for Xanax?) The description on Goop made the mistake of adding that the stickers were cut from the same expensive carbon-based cloth used to line NASA's space suits. The space agency quickly [set Goop straight](#), stating that 1) NASA does not use carbon in their spacesuits and 2) Goop's stickers (which sell for \$120 for a 24-pack!) are not made out of NASA spacesuit material. The Goop empire has been known for its bizarre "health" advice for years now, ranging from purchasing a ["medicine bag"](#) full of "magical stones" from "various indigenous traditions" all the way to jade eggs to insert in your lady parts, and SO much more [dubious advice](#) (read the linked article...it's cringe-inducing). And it gets even weirder for the "peace and love" earth-child crowd buying Goop's garbage; as it turns out, Goop's products are eerily similar to ones sold on its polar-opposite website Infowars (which Quartz [calls](#) "a dark corner of the American right, heavy on guns, light on government intervention and still very mad at Obama.") Hmm...sometimes it seems like this whole "lifestyle" thing is really just about making a buck.

Tempting texts

We've talked about the email-based phishing scam technique ad nauseam; less frequently, we've mentioned its equally evil cousin "[smishing](#)." Smishing warrants more than a mention though, as its meteoric rise in popularity has corresponded with the rise in smart phone usage. The 's' in smishing stems from SMS—the technology behind text messaging. As people become more suspicious of emails with potentially dangerous links, scammers have realized that a text message seemingly from your bank, utility

company, favorite store or even friend in need is more likely to appear legit and get a reply. The goal of the scam typically is to convince you to tap on a link in the text, which leads to a fake website (that may look real) prompting you for personal or financial information. The text also might ask you to call a number, or text back directly (which confirms that you're a sucker and pretty much seals your fate: You'll be getting more texts). CNBC provides some great examples of what these correspondences look like (e.g., "Dear customer, Bank of America needs you to verify your PIN number immediately to confirm you're the proper account holder. Some accounts have been breached. We urgently ask you to protect yourself by confirming your info here [links to bogus site].") So how can you avoid the tempting texts? Update your phone's operating system; download antivirus software through an app (yep, this software isn't just for your desktop computer); be cautious with who you give your number to; actually read through your phone bill for any strange charges; and, last but not least, never click on suspicious links (just delete the text immediately). The Better Business Bureau (BBB) is also encouraging you to [report](#) smishing to its Scam Tracker service.

Summertime scams

We're only midway through the summer and the hot-weather scams are piling up. While they are innumerable, we'll list two of the most "popular" ones here. First, there's the vacation rental scam, which occurs when you pay for a beach house or other property only to find that it's not what you bargained for (or doesn't exist at all). The Better Business Bureau (BBB) [gives](#) would-be renters red flags to look out for, including too-good-to-be-true property prices and requests for payment via sketchy avenues like cash or money wire. But let's say you're a smart consumer, doing your research and picking the perfect place. If you're planning on getting a summer job to pay for that vacation, you could be facing another big seasonal scam. Con artists know that college kids and others are often looking for temporary work when the days get long, and they tend to advertise via the same avenues as "real" employers. So how do you know if a job is a joke? Never pay for a position or offer personal information to would-be employers (for "credit checks," W-4s and the like). The job should always pay *you*, and you should at least get to the interview stage before giving up any personal info. For more sizzling summer scams, click [here](#).

Getting theirs

Burning down the fest. The notorious Fyre Fest—or as we called it in a previous newsletter, "Dumpster Fyre Fest"—not only raised the ire of the many millennials who paid thousands to attend what they were promised would be a "luxury" music experience in the Bahamas, only to be stranded on an island with little to no food, water or music, it also raised eyebrows at the FBI. Yes, one of the event's main organizers has now been arrested and [charged](#) with wire fraud after a federal investigation found he "presented fake documents to induce investors to put over a million dollars into his company" (aptly called Fyre Media LLC). The organizer, Billy McFarland, co-founded the ill-fated festival with late '90s hip hopper Ja Rule (who, if you're wondering, is *not* currently under investigation).

Be humble. Sit down. Maybe it's time for maligned "pharma bro" Martin Shkreli to just stop talking. The 34-year-old, who has been accused of enriching himself by raising the prices of prescription drugs owned by his pharmaceutical company by hundreds (even thousands) of dollars, is [facing](#) 20 years for defrauding investors (he's currently on trial for eight counts of securities and wire fraud, to be exact). Most people, when faced with such charges, would watch what they say on Twitter and to the media, but Shkreli has

publically blasted prosecutors in the trial as “junior varsity,” called Congress “imbeciles” after his hearing last year, and claimed that he’s “so innocent” that the judge and jury will apologize to *him*. This probably won’t end well unless he can turn some of his fabled “charm” on the jury.

Paging Dr. Quack. The author of the best-selling book *The pH Miracle* has been [sentenced](#) to 44 months in jail. This shouldn’t come as a surprise: Over the previous couple of years, the good “doctor” Robert O. Young had been convicted of several counts of practicing medicine without a license. There’s also the fact that Young, who received a degree from a non-accredited correspondence school, enjoyed pumping his very ill patients full of baking soda (!?) and, [according to](#) the website QuackWatch, sold dietary drugs of dubious origin on his own website, [phmiracleliving.com](#) (where he also boasted that he “performed live and dry blood analysis on over 15,000 people repeatedly”—whatever that means).

Tips!

● **No money in coffin nails.** In the late ‘90s, the tobacco companies entered into a legal settlement with 46 states, agreeing to pay them for the medical costs associated with icky tobacco-related illnesses. Scammers, who know that the Philip Morrises of the world are still dishing out the big bucks, are [telling](#) retirees that they can claim thousands from the settlement every month—if only they sign up for a newsletter (with a monthly subscription fee, of course). Unfortunately for those looking to benefit from cancer stick fallout, the settlement money is *only* paid to the states (not individuals).

● **Wouldn’t wish this on anyone.** The Make-a-Wish Foundation grants wishes to very sick children (often with terminal cancer and other serious diagnoses), but that doesn’t stop lowlifes from using the organization’s name to deceive the gullible. Specifically, the con artists [claim](#) to be calling with a federal agency on behalf of the charity in order to award the recipient with a cash prize (which, of course, they must pay ‘taxes’ and other upfront fees on to collect because how else would the scammers get paid?).

● **States against student scams.** Eighteen states and the District of Columbia have [filed a lawsuit](#) against Trump’s administration, specifically Education Secretary Betsy DeVos, whose very job entails protecting students, but who has seemingly done everything in her power *not* to. Her office has suspended rules created to shelter students from for-profit schools (known for leaving them with thousands in debt and worthless degrees). If you’re a student, [watch out](#) for predatory schools (and check out our [guide](#) to finding the right job training school). In the meantime, stick it to ‘em, states!

● **An ‘F’ in fake news?** If your ability to suss out fake news were put to a test, would you ace it? Now you can find out. A veteran journalist created [Factitious](#) to help you determine your gullibility level. The test involves reading news articles (both real and fake) and determining if they pass the “objectivity” and “common sense” tests, if the sources are credible and more. Try it out!

● **Scamazons.** There are quite a few Amazon phishing scams going around these days; some even popped up in our executive director’s inbox! (What’s phishing, you ask? This [simple infographic](#) will help you understand.) One claims that the online retail giant is having trouble processing or shipping your order. Another claims that “because of your loyalty as a member” you’re eligible for a \$100 credit. And yet another prompts you to take a survey in exchange for a \$50 reward. There are probably more floating around, but they all have a couple things in common: fooling you into giving up your financial and/or personal information to drain your bank account or steal your identity.

● **Horrible gas.** We know, you're in a hurry to gas-'n-go. But don't be in such a rush that you can't spot a skimmer at the pump. Skimmers are fake readers that collect the financial data from the magnetic strip on your credit or debit card and deliver it to crooks. The Federal Trade Commission (FTC) has some excellent photos revealing what it looks like when someone has tampered with the card reader and installed a skimmer. It's worth the time to check it out [here](#) (and at the gas station).

● **Think of the *children!*** Between toys that spy on your kids, social media that tracks their whereabouts, and school testing services that record and share their performance without your explicit consent, it's become increasingly difficult to protect your offspring from ID theft and other high-tech privacy invasions. The pitfalls inherent in our brave new world could have long-term consequences for your child, which is why modern parenting practically mandates that you read articles like [this one](#) to wise-up on the risks.

● **Frequent Facebook miles.** If you're anything like this author, your Facebook addiction may have led you to stumble across an ad [offering](#) free Delta airline tickets. Needless to say, it and other offerings like it are scams seeking your personal and/or financial info. Remember: The old adage "Nothing in life is free" exists for a reason.

● **Blue screen of death.** You're working from home (or online shopping for those cute summer shoes) and suddenly your computer screen turns blue. Totally, completely blue. You freak! This is way worse than that time the internet went down! Scammers are relying on your panicked reaction to what is known as the "blue screen of death," and they're willing to bring your computer back to life, [at a cost](#). If your screen turns blue and a toll-free number pops up prompting you to call for repairs, don't do it. Instead, keep calm and reboot your computer. Then make sure your antivirus software is up to date, and run it to destroy the malware that caused the blue screen in the first place. If all else fails, you might want to call the makers of your computer or your local tech support guru for help.

● **You can never be too careful.** Credit.com has created an [exhaustive list](#) of ways to avoid becoming a victim of credit/debit card fraud: everything from placing a sticker over your security code to setting up text alerts that list your daily account balance. Follow these rules and not only will you drastically decrease your likelihood of being a victim, but if (heavens forbid) something *does* happen, you'll likely catch it (and be able to put a stop to it) right away.

● **We owe what?** As the FTC [points out](#), scammers know that in many companies "the people who order supplies and the people who pay the invoices might not talk all the time." Of course, the scammers use this knowledge to their advantage, charging organizations thousands for bogus business supplies that they never actually ordered. We know from experience: Consumer Action received a call from "FedEx billing" asking us to pay an "outstanding invoice" just a month ago! Thankfully our razor-sharp admin team realized it was a scam (which they confirmed upon calling back the *real* FedEx number).

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.

nationwide to financially prosper through education and advocacy.



[Manage your email subscription.](#) Choose the content you'd like to receive. You will have to create a password to do so. Lost your password? Use "Forgot your password?"

[Click here to unsubscribe.](#)