Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • July 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!

Seeing is believing?

Deepfake—a blend of "deep [machine] learning" and "fake"—is the buzzword being used to describe realistic looking fake videos, typically posted online for nefarious purposes. Deepfakes took off with scorned dudes mashing up the faces of ex-girlfriends with the bodies of adult video stars. (Fortunately, states are now criminalizing this type of revenge porn.) The videos are made possible through artificial intelligence: Basically, the more images a computer is fed, the more it can "learn" a person's expressions and movements to create a convincing replica. As the technology to create deepfakes becomes more accessible to the masses, so do the videos. Undoubtedly, scammers also will increase their use of deepfakes to coerce victims into sending money. Picture "Wire me $10,000 or this video of [choose your own adventure] goes to [choose your target audience]." The sky's the limit with deepfakes: How about a video of "you" snorting some mystery powder at Lindsey Lohan's beach house (sent to your mom)? Or one from your "boss," Skyping to tell you to wire money for a payment to a "client"? Or a video of your kidnapped "grandchild" begging you to send a ransom? You get the (awful) picture. Twitter and other major online platforms still lack policies governing the removal of the videos. It's not all bad news though; there are bipartisan bills in both houses of Congress to counter the counterfeit content (S 2065, HR 3600) and, as cyber security site CSO says, "At the end of the day, the hype around deepfakes may be the greatest protection we have."

Playing god

The Pastoral Medical Association (PMA) has produced some pretty ungodly "healers" in its mission to "restore bible based wellness and counseling services." The sham organization has (for a fee, of course) "licensed" many "spiritually-minded" humans who believe that chronic illness is caused by "the displacement of God and self-responsibility." (There are many factors contributing to chronic illness—including autoimmune, genetic and anatomical/structural issues—but "God's wrath" is *not* among those accepted by legitimate medical practitioners.) PMA's convenient claim that "regulation of the Almighty's health care concepts is outside of the jurisdiction of…secular regulatory boards" has produced such horrors as Martin Riding, who was just charged with 64 counts of practicing medicine without a (real) license. PMA's website listed its protégé Riding as practicing "raindrop therapy" and ZYTO body scans(!?), but appears to have neglected to mention his "thermographic breast exams" and inappropriate amateur photography "treatments." Looking for a (non-quack) doctor? Make sure their credentials are legit.

If it quacks like a duck…

It all stems from… A shocking 700+ clinics in the U.S. provide unproven stem cell injections to "cure" conditions ranging from a herniated disc to cancer. For the uninitiated reader, there's only one type of stem cell transplant approved by the U.S. Food and Drug Administration (FDA), and it's very specific: hematopoietic (to treat certain blood disorders). So why was the *Journal of the American Medical Association (JAMA)* able to identify 351 companies marketing the procedures (and often not for approved blood disorders) at 570 U.S. clinics (with the largest number of clinics located in CA, FL and TX)? And why, out of the 157 clinics employing an *actual physician*, did only 52% have one on staff with the formal stem cell training required for the procedures they provided? Unfortunately, desperate consumers are listening to unscrupulous clinics and purchasing the treatments—which are typically not covered by insurance—for thousands of dollars (and, in many cases, being told they need multiple treatments!). The sheer number of clinics even appears to have caused the FDA frustration in stopping the phenomenon, which means "buyer beware." Still interested in an infusion? Consumer Reports has more info to help protect you from stem cell scams.

You don't have to be a brainiac. AARP's Global Council on Brain Health (GCBH) has released a new report revealing what many of us already know: "Buying supplements to benefit your brain health is likely a waste of money." Unfortunately, these types of vitamins, minerals, enzymes, pills and potions are often advertised to the 50+ crowd, who may be worried about declining cognitive health as they age. About a quarter of these folks regularly take brain supplements, which generated $3 billion in global sales in 2016. The products *technically* are not legally allowed to make outlandish claims (such as preventing Alzheimer's), but they still do. So, smartypants, what can you do to improve the ol' noggin? According to the GCBH, it's easy to understand: "For most people, the best way to get your

nutrients for brain health is from a healthy diet."

Billion-dollar back surgery. The fallout (and lawsuits) from Operation Spinal Cap—a massive healthcare fraud investigation that began in 2013—continue, with victims from Southern California coming forward with devastating tales of the horrific pain caused by shoddy screws surgically implanted into their backs at the behest of devious doctors. From the mid '90s to the mid '00s, doctors, chiropractors and others involved in the scheme got kickbacks for referring patients with back issues (many of whom didn't need surgery, and all of whom were covered for the pricey procedures under workers comp insurance). Perhaps most disturbingly, documents have revealed that the man who ran "Spinal Solutions," the company distributing the cheap, counterfeit hardware, has supplied it to other states as well, including Wisconsin, Texas, Nevada and Maryland.

Tips!

- **Hot tub crime machine.** Desk jockeys sitting at the computer with painful muscles are likely to click on a too-good-to-be-true hot tub ad that's been plaguing social media sites. And scammers, who know their audiences, are banking on wishful thinkers like Lia Pennington of California. Lia saw the ad for what was being billed as a $399 tub marked down to $20. Unfortunately, these offers have been swirling around social media for a while now, and those who jump in are lighter by 20 bucks but never actually receive the hot tub.

- **Bad blood.** Quest Diagnostics (where you may have gotten a blood test) could have bad blood with patients after the company's debt collection service (the American Medical Collection Agency, or AMCA) suffered a major data breach. It appears the only thing the hackers who breached the system *weren't* after was patients' medical info. Like most digital criminals, they instead wanted financial and personal data (read: Social Security numbers, names, addresses and the like)—undoubtedly to commit identity theft. If you've been a Quest lab customer (particularly one who owed the company a debt), you're probably looking into another kind of "result" now—to see whether or not your data has been breached. How will you know? If so, Quest and the AMCA say you'll receive a letter in the mail (from the AMCA). For more info on what you can do in the meantime, click here.

- **Bogus "bargains."** The non-profit Consumers' Checkbook has organized 17 major retail stores' so-called "bargain" prices into the bins "usually," "often" and "sometimes" misleading. (Sadly, a final category—"legitimate" prices—contains a mere two stores.) Many of the stores engaging in what Checkbook calls "sales-price chicanery" either offer the seemingly-limited sales year-round or advertise clothes, purses and other items as "40 (or some other) percent off," when, in fact, better deals can be had elsewhere. The stores want to push consumers who are into that new pair of kicks to get 'em while the gettin's good, but would-be buyers should always shop around: There's probably a better deal out there.

- **Host(ile).** Small business owners (and website operators of any sort), beware! A self-employed architectural renderer who hosts a website advertising his services contacted our Complaint Hotline to report that he had received a snail mail solicitation in the form of a realistic looking invoice from "Web Host Agents"—a sham company attempting to bill him $180. The company claimed that "failure to renew" hosting services by the deadline listed in the letter "may result in website outages." These "phishing" attempts appear to be prolific; the letters have been sent to people across the U.S., from New York to California—we even received one at our DC office! The con artists who send them clearly hope the victims will bite if they own a website (and aren't clear on what company actually hosts it).

- **Cruel, cruel summer.** This summer, sunblock isn't the only protection you need—break out the common sense! There are three major phone scams heating up now: text alerts that appear to be from your bank (Bank of America and BB&T come to mind); calls spoofing U.S. Marshals and threatening you with jail/arrest; and a spoofing attempt from 1-800-APPLE targeting iPhone owners and claiming that there's a threat to your phone or computer. None of this communication is from the party it claims to be from, and each seeks to separate you from your money. What else do these contacts have in common? They all deserve to be hung up on/ignored and/or reported to the Federal Trade Commission.

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.
