Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • August 2018 • 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!

Guilty conscience?

The fact is, a large swath of the public watches online pornography (ahem, "adult videos"). That's what scammers are literally banking on when they send an email saying that not only have they viewed your Pornhub predilections, they've also recorded *you* (through your own webcam), uh, enjoying the stuff, and they're ready to send the recording to all your contacts if you don't pay up. "Not I," you protest. "I am positively puritanical in my internet use!" Hey, we believe you—but you'll still be shaken when the "sextortion" attempt mentions an actual password you've used in the past. These types of emails have been popping up in inboxes by the droves lately. Recently, one was sent to a Consumer Action employee demanding she pay a "confidentiality fee" of $2,900 (in bitcoin). "I'm not planning to break your bank," the email reassured her. "I am just looking to be compensated for efforts and time I put into investigating you." Gee, thanks? So, how are the scammers getting your (often old) passwords? From any number of data breaches that have occurred over the years and leaked the passwords onto the dark web (read: online black market), where crooks buy them before sending their phony accusations to freak you out. In reality, they don't have access to your contacts or webcam. Feel more confident by covering your webcam when it's not in use and updating your passwords frequently. Also, check to see if your accounts have been breached on the modernly monikered "Have I Been Pwned" website. And if you'd like to make the *scammers* sweat, report 'em to the FBI's Internet Crime Complaint Center.

This is America

The Federal Trade Commission (FTC) has launched Operation Donate with Honor to combat "charities" that lie about helping wounded and disabled veterans. A rep for the Veterans Affairs Department summed up exactly how damaging this deceit can be: "Not only do fraudulent charities steal money from patriotic

Americans," he said, "they also discourage contributors from donating to real Veterans' charities." Fortunately, the FTC has publicly outed the scoundrels. *Un*fortunately, shutting down organizations like Help the Vets, Inc. (HTV) is akin to Hercules killing the hydra. The FTC points out that HTV, for instance, was also operating under the names "American Disabled Veterans Foundation," "Military Families of America," "Veterans Emergency Blood Bank," "Vets Fighting Breast Cancer" and so on and so forth. (Multiple pro-veteran-sounding organization names and "lookalike" charity names are standard for this sham "industry.") Unlike the rose, which smells as sweet by any name, the thieving HTV, or whatever it's called, did *not* help veterans. Instead, its corrupt director pocketed a large amount from every donation. But the FTC wasn't fooled. As part of over 100 total recent actions taken against fraudulent veterans charities, it fined HTV $20.4 million, ordered that it give its remaining assets to *legitimate* vets charities (zing!), and banned it from soliciting donations (under any name). And, the FTC has launched a massive public awareness campaign (complete with a shareable educational video and infographic) to teach donors how to differentiate real from fake charities. One of the quickest and easiest ways? Research the group in question on a reputable non-profit ratings site like Charity Navigator (and while you're at it, run their name by the Center for Investigative Reporting's list of "America's Worst Charities"). If you *do* decide to donate, use a check or credit card and keep records.

Binge, purge

All the McNuggets money can buy. Ever wonder why you were never a "big winner" in the McDonald's Monopoly money game (despite gobbling down Big Macs like a depraved Pac-Man)? It might be due to Jerome Jacobson, the man managing the official printing and distribution of the coveted game stickers. From the late '80s on, the ex-cop used his access to head up "a sprawling network of mobsters, psychics, strip-club owners, convicts, drug traffickers, and even a family of Mormons." With Jacobson at the wheel, the clown car of characters cashed in on various winning pieces for a whopping $24 million until the early '00s (when the operation got sloppy and Jacobson got McNabbed by the FBI). What makes the story interesting is that Jacobson had an altruistic streak (even though he often demanded kickbacks from those cashing in): He anonymously mailed a $1 million winning piece to a St. Jude hospital in Tennessee, for instance, and friends in need often found themselves landing on Boardwalk. What makes the story even *more* wild is that one of the (fake) winners (the mobster mentioned above) can be seen boasting about it in a national McDonald's-created Monopoly promotional commercial from 1995 (talk about gall!). The long-standing scam is *so* wild, in fact, that Ben Affleck and Matt Damon teamed up for the Hollywood movie version less than a week after the story broke!

Gag me with a spoon! Passengers around the world have been complaining about a bogus Uber "vomit fee" they've been hit with, even when they were neither sick nor lit. One woman has sworn off Uber after she claims she was wrongly charged $150 for what the embattled company describes as a "Level 4 major bodily fluid mess" that "requires cleaning between the windows, doors or air vents" (or perhaps an exorcist?). Drivers can often get away with filing these types of fraudulent charges because passengers don't check their electronic receipts and/or don't want to engage in disputing the accusations. This makes sense, since Uber only offers a generic "Help" button for those shocked by the outlandish charges and, if the case *does* escalate to a real person, typically puts the victim through more headaches and hassles. One passenger detailed how "every new email [during a dispute about a "vomit fee"] from Uber came from a different representative and always favored the driver." Frustratingly, as the *Miami Herald* points out, "It's unclear what steps local governments can take to stem the fraud, which is leaving Uber customers without needed protection." Given the ridesharing company (and its founder's) history of bad behavior, maybe use Lyft instead? Or, take a cab!

Tips!

- **Mrs. Doubtfire.** The FTC released an alert about nanny and caregiving scams, and no, it's not directed at the parent looking to hire; it's for the person looking to get the gig. Websites like Care.com can be crawling with con artists, some with sob stories about sick children or domestic drama that prompts nice people like this college student to take the bait. Once she responded to the job application, the student was immediately offered the job without meeting the parent (which prompted her dubious boyfriend to warn her that it was a scam and she needed to "get her head out of her butt"). The next step, which is all too common in these cases, involved the con artist mailing the student a (bad) check to deposit and instructing her to keep part, but send the majority of it on to another party. Worried that mommy dearest isn't a legit employer? Any request to send money back should instantly confirm your doubts.

- **At attention!** We somehow *just* discovered this very comprehensive website to "empower active duty and retired servicemembers, military families, veterans and civilians in the military community" by offering free resources, news alerts and more in the fight against fraud. Loads of federal and state lawmakers are involved in maintaining it, so if you're military, definitely sign up for email alerts through the site!

- **Kiki, are you scamming?** Charlene probably thought her boss just wanted his clients to be able to buy a copy of Drake's *Scorpion* (*In My Feelings* is only *the* catchiest song of the summer). Fortunately, after the office manager received an email request (from who she *thought* was said boss) asking her to purchase five $100 iTunes gift cards, she texted him to confirm, to which he responded: "What in the world are you talking about?!" (or something along those lines), saving her from a common scam. Anyway, we're telling you about this to make you aware that scammers are pretty darned sophisticated these days and can easily clone an email address. (And go ahead, listen to *In My Feelings*, but *don't* do the "Kiki challenge." Just don't.)

- **This checks out.** Over the last month, the FTC has announced that it's mailing thousands of checks to those who have suffered at the hands of mortgage relief companies, debt collection agencies and even the ubiquitous Uber. Some of the transgressions are so egregious that we don't know what else to call them but outright fraud! The debt collection company Delaware Solutions, for instance, ignored evidence that the debts they were attempting to collect were invalid. The thugs then "portrayed themselves as process servers or attorneys and falsely threatened arrest or litigation for failure to pay." Then there's the weight loss company NutriMost, which claimed that their (too-good-to-be-true) product not only caused users to drop 20-40 pounds, but also "helped treat or cure diabetes, psoriasis, and other diseases," and another company, aptly named Cedarcide, which claimed it could "stop and prevent bed bug infestations using cedar oil." To see if you qualify for a check, check out all of the ongoing cases here.

- **@fakeDonaldTrump.** Trump's so busy accusing everyone of "fake news" that he may not be aware his *own* name and Twitter likeness is being used in a very real attempt to get people to click on links for malicious sites that would steal their info. According to *Yahoo! Finance*, the Twitter scam, which promises to give away bitcoin or ether "money," has "become so prevalent and recognizable that scores of cryptocurrency enthusiasts have added 'not giving away ETH' [ether cryptocurrency] to their Twitter display names as an inside joke." How does it work? Hackers break into the Twitter accounts of public figures with loads of followers and change the photo and display name to mimic another public figure (e.g., Donald Trump). In the

Trump case, they then reply to a *real* Donald Trump tweet (in order to make the account seem more like Trump's at first glance) and announce the big giveaway, complete with the (malicious) link to claim your private info. Sometimes the scammers simply hack into a celebrity account (e.g., the band Bad Religion—how 21st century!) and reply to another big-deal account, like @realDonaldTrump.

Complicated code. A pregnant Milwaukee woman received a call from a man who asked her, "Are you prepared to care for a kid with autism?" The caller then tried to sell the mom genetic tests for autism (which would cost several thousand dollars, of course). But screening tests cannot tell parents if their child is on the spectrum. (As one wise genetic counselor points out, there are over 1,000 different genes that might be related to various forms of autism, and in many cases there is *no* known genetic cause.) More puzzling than the human DNA code, however, is *how* the scammer knew his victim was pregnant. Unfortunately, there's a multibillion-dollar data broker industry (with virtually no oversight) dedicated to collecting, analyzing and selling the information it gleans from your website visits, internet searches, email content, social media posts, online purchases, etc. It's easy for grifters who gain access to target those who are experiencing big "life events," like having a baby or buying a home. What can you do to stop these scams? Help plug the endless stream of data collection by using an ad blocker and a browser extension to block websites from tracking you, selecting the strictest privacy settings on social networks and opting out of sharing personal data with third parties.

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