Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • March 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!

Senior scams are getting old

#TimesUp for senior scammers! (Specifically, scammers who target the elderly—not old scammers.) The Department of Justice (DOJ) just orchestrated the largest nationwide "elder fraud sweep" in history, with a particular focus on criminals who trick seniors into giving them computer access through "tech support" calls. Last year alone, the Federal Trade Commission (FTC) received more than 140,000 complaints regarding these scams, and people 60+ were five times more likely to be the ones making them—people like Don Holmes. There's no shame in Don's game: He was not only brave enough to share his story with his community, he let it fly in cyberspace. "I realized that if I didn't…I would have shrunk into myself." One day, when the unsuspecting Don saw a popup on his computer screen saying he needed to call a number to fix a virus, he complied. When the voice on the other end asked him for his password, again he obeyed. "When I went back to my computer the next day, I couldn't access my files," Don laments. The good news? Don's friends can relate: "They're not amateurs, Don," one commiserated. And this is far from the only scam seniors are falling for. The DOJ says seniors are helping fraudsters transfer and hide the money they "earn" by acting as "money mules." A new BBB report illustrates, specifically, how scammers often make donkeys out of those looking for love online.

Cryptocurrency calamity

Don't you just *hate* it when you're about to flee the country and authorities nab you at the airport? So close! Or so it was for brother and sister Konstantin and Ruja Ignatov, the leaders of a massive cryptocurrency con. The digital "dollars" in this case were called OneCoin—trash "tokens" that the Ignatovs concocted and sold to naive people around the world for a total of $3.7 billion between 2014 and 2016 alone. Investors probably should have been skeptical since OneCoin lacked a fundamental of blockchain technology—an open, distributed

ledger that would allow the cryptocurrency to be validated as it's bought and sold. How did the Ignatovs get away with such massive fraud? According to one district attorney, they "executed an old-school pyramid scheme on a new-school platform [the internet]." OneCoin, in other words, had no real value. Despite this, it spread like a virus by operating like a multi-level marketing (MLM) scheme; supporters were recruited to sell more worthless OneCoin, and so on and so forth. When U.S. investors finally met up with Konstantin and told him they were interested in cashing out, he reportedly told them: "If you are here to cash out, leave this room now, because you don't understand what this project is about." (You can say that again!) Think this is a one-off situation? It closely mirrors another multi-billion dollar cryptocurrency scheme that toppled about a year ago: BitConnect, an ostentatious "company" that flew too close to the sun, generating one helluva meme and one of the largest coin value collapses in history. In fact, the FBI is *still* looking to connect with BitConnect victims in an ongoing investigation. Bit-buyers beware: Cryptocurrency isn't regulated by any central bank or government. Still interested in investing? The Better Business Bureau (BBB) has tips for navigating this digital frontier.

Let me count the ways

The dirty dozen. Each week leading up to April 15 (when your taxes are due), the IRS will release one in its series of "dirty dozen" tax scams. So far, the "winners" include: fake 1099-MISC forms (and other bogus documents) ostensibly used to help taxpayers "pay down debt" with their returns; phone and email phishing fraudsters purporting to be from the IRS; and misdeeds committed by taxpayers claiming credits they're not owed. The IRS is also warning taxpayers about "ghost preparers" (learn more about these spooky scammers here). Also, pro tip: If you make under $66k annually, you can file your taxes online for free using the IRS' Free File tool—no payment to TurboTax necessary!

The five riskiest. The Better Business Bureau outlines "the Amazon effect" in its recently compiled top five riskiest scams, generated from the data victims contributed to its Scam Tracker reporting tool in 2018. Employment scams are numero uno, with hoaxers leveraging the hype from the expansion of Amazon and other big companies to lure jobseekers into "work from home" and other "opportunities" that involve paying for the privilege. (Silly us, we thought you were supposed to be paid to work!) The four other scams? Online purchases, fake checks or money orders, home improvement and upfront "fees" charged on money loaned (but of course, never issued). Interestingly, men reported losing almost *twice* as much in the scams as women! Click here for the full report.

A third party. In what should be titled "Anatomy of a student loan scheme," *MarketWatch* outlined bit-by-bit how a third-party "debt relief" company used the name of a legit income-driven federal student loan repayment program to direct a woman to make her payments to *it*, as opposed to the U.S. Department of Education (DOE) directly (which is what she *should* have done). Hindsight is 20/20. Unfortunately, the woman is now caught in a three-year contract with the company, which dictates she pay "fees" for its completely unnecessary "services" (even if she bypasses it and begins paying the DOE directly). If you're looking to enter an income-driven student loan payment plan, do it directly through the DOE. "This is not like hiring a tax preparer to prepare your taxes," the wise(r) woman now cautions. "The [DOE] income-driven repayment form is a few pages long, and you can fill it out in a matter of minutes."

Tips!

- **Minor threat.** A little-known law that went into effect last year is allowing the parents (and legal guardians) of teens and children to freeze the minor's credit. The law addresses what's been a major problem: Con artists can get away with using a child's identity for *years* before anyone knows about it (which usually occurs when the now-adult victim first applies for credit). And foster care kids are *especially* vulnerable to identity theft, as their personal information is regularly exposed to all and sundry employees of the foster system (from caseworkers to court employees and beyond).

- **Something's fishy.** Cue the vomit emoji: In what must've been a stinky endeavor, the non-profit group Oceana collected 449 samples of seafood from restaurants across the country and DNA tested them to find out if they were, in fact, the species the restaurants claimed. To the surprise of probably no one reading *SCAM GRAM*, Oceana discovered that a substantial number were not as advertised, and that one out of every three stores and restaurants scrutinized was selling mislabeled items. And it's not like seafood lovers are getting Alaskan halibut when the fish is labeled tilapia: Au contraire, the product is typically "lower quality" (and should be less expensive) than what's advertised.

- **What's more terrifying?** When the Department of Homeland Security (DHS) isn't busy putting kids in cages, it's busy battling scammers pretending to be a federal agency that would put kids in cages. DHS has issued a fraud alert warning the public not to be scared of it, or, at least, the fake "it." If someone calls claiming to represent the agency or to be a U.S. immigrations employee, hang up (even if the caller ID is spoofed to display a real DHS number).

- **App-solutely fake.** You know that "Log in with Facebook" option that pops up to facilitate your opening an app or website that you've linked with the social media giant? Unfortunately, artistic fraudsters know it all too well. They've managed to clone it perfectly (right down to the shadow effects on the buttons at the bottom; check out their masterpiece here). Once they've captured your login information, there's no telling what they might do from inside your account—anything from pretending to *be* you and messaging friends and family for money, to stealing financial info you've linked to the account, to gaining access to damaging messages or photos. (We can imagine some truly grizzly scenarios…)

- **Worst buy.** Don't have the money up front but want one of those dope new 4K QLED TVs? Best Buy might *not* be your best option. The giant retailer will soon be introducing a lease-to-own option that makes an expensive TV cost even more—over *twice* as much in the long run, according to consumer news reporter Bob Sullivan. Sullivan lays out the rent-to-own ripoff: A $1,000 TV, paid off over the course of a 12-month lease, would ultimately cost $2,169 because "Best" Buy can charge consumers $1,169 in interest (at an appalling annual percentage rate of 195%)! Adding insult to injury, Best Buy's CFO seems to believe the company is doing customers with bad or no credit a favor by giving them the *opportunity* to saddle themselves with such debt! Our recommendation? Boycott Best Buy.

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.