Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • August 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!

I love a man in uniform

The *New York Times'* latest exposé on Facebook fraudsters is just…wild. Spoiler alert: It ends in catastrophe for a middle-aged woman who was defrauded out of $30,000-plus by a handsome soldier she met online. As the *Times* points out, social media platforms Facebook and Instagram are teeming with imposter accounts for studly soldiers, including a whopping 120 results for the top three U.S. generals! Bad people, typically living overseas themselves (but not on a military base; more like in Nigeria) use photos of attractive or prestigious American servicemembers found online to create new social media accounts in their names in order to reach out to women. They then court them to hoodwink them out of their money, sometimes over a period of years. The phenomenon has "entangled the U.S. military, defrauded thousands of victims and smeared the reputations of soldiers, airmen, sailors and Marines." And, neither Facebook/Instagram *nor* the military has adequately addressed the scams. For instance, when the *Times* reported 46 imposter accounts to Instagram, the social media platform responded that none violated its rules, "without explaining why," noted the *Times*. But let's get back to the unfortunate victim: She initially paid over $5,000 to fly her love interest back to the U.S. And, as a testament to how convincing these scammers are, she *kept* paying to get her man-in-uniform home even *after* she realized (upon arriving at the airport to pick him up) that his flight never existed, having been assured by another imposter (this time an Army "general") that her soldier had been "injured in war." Before you fall in love online with a man in uniform, do a reverse image search on him—chances are you'll find he's stolen someone's identity.

You also can join groups like Advocating Against Romance Scams to petition Congress and social media companies to stop the madness!

Lambs to the slaughter

Talk about wolves in sheep's clothing! According to the Federal Trade Commission (FTC), scammers are pretending to be your friendly neighborhood "pastor, rabbi, priest, imam, or bishop" and sending emails to their "flock" (sometimes containing misspellings, including of the name of the not-so-godly sender and/or adherent being addressed). How do they know what religious institution you belong to? Unfortunately, as an FTC rep points out: "A lot of worshippers' contact info… is publicly available [to scammers]—it's on the church website or the parish bulletin." The emails request contributions in the form of—*you guessed it*—gift cards! Specifically, these devious devils want the numbers on the backs of cards you're commanded to purchase from major retailers like Amazon or iTunes. WWJD? Not fall for it. Anytime anyone asks you to pay for anything with a gift card, it's a major red flag. Want more info? The Holy Name of Jesus Cathedral in Raleigh, NC, which was the target of a recent "worship scam," sent an email to its congregation with instructions on how to say, "Not today, Satan!" Unfortunately, nothing is sacred to scammers; not even the houses of worship. The St. John XXIII Catholic Church was duped out of $500,000 when a church employee was solicited (again, via email) by a clever con artist claiming to be with a construction company that was, legitimately, doing work to renovate the church. Why do people keep falling for these kinds of cons? The email addresses the criminals create are shockingly similar to the real ones (so PastorJo(at)gmail.com becomes PastorJo(at)gmail.com). If you've already been on the receiving end of one of these secular scams, the FTC asks you to report it.

No time like the present (to freeze your credit)

Just the facts on Equifax. By now, you've probably heard that Equifax has been compelled by the FTC to give victims of its massive 2017 data breach a choice of up to $125 ("up to" being the operative words) or free credit monitoring renewable for 10 years. While we were as excited as AOC, who urged her Twitter followers to file for an easy $125, it didn't take long for all of us to learn that if all 147 million breach victims claim the dollars, each will receive only cents. Still, regulators can (and should) give this type of financial spanking to companies with lax consumer data protections, which, at the very least, might give the companies incentive to clean up their acts. (Although we'll add: We need stronger data protection laws at the federal level in the U.S., in general.) In short: While we believe that the better deal is the credit monitoring (and you can click here to learn how to *change* your claim, if you've already claimed the cash), your best bet is to put a full-on *freeze* on your credit to stop thieves from stealing your identity and, say, buying a boat in your name. Also, if you were particularly unlucky and a victim of the Capital One data breach as *well*, you may be eligible for free credit monitoring through Cap One instead. (Read on for more.)

What's in *your* wallet? Equifax isn't the only game in town when it comes to major breaches (far from it!). Earlier this month, a troubled Capital One employee was arrested after openly boasting on social media about her ability to access the credit card company's unsecured databases (located on Amazon's cloud services). Capital One stated that, out of the 100 million-plus cardholders/applicants breached, none of the "card numbers or login credentials were compromised." It turns out that approximately 140,000 Social Security numbers and 80,000 linked bank account numbers *were*, however, as well as names, addresses, email addresses, birthdates, self-reported incomes and even credit card purchases. And while the company promises to make free credit monitoring and "identity protection" available to everyone impacted, as *USA Today* points out, there will always be risks when hosting sensitive information in the cloud. (KrebsOnSecurity has more info on these risks.) The best step to take if you were a victim of this (or any) breach? Freeze your credit!

And while we're on it… Speaking of data leaks, consumers run the risk of being the ones to leak their *own* data to scammers who, opportunists that they are, have already created fake Equifax settlement websites to collect personal info from those looking to get paid (or get free credit monitoring) from the $575 million Equifax settlement. (Capital One sites are likely next.) Make no mistake: Ftc.gov/Equifax is the correct (and only) website you can use to file an Equifax claim. For more info on what this entails, click here. And, if you think you've suffered *any* sort of data breach (and who hasn't these days?), click here for more information on what to do. Note: You can get free credit reports from each of the three major credit bureaus—yes, including Equifax—at AnnualCreditReport.com (no settlement claims required).

Tips!

¡Ayúdame abuelo! Scammers are bringing the drama to your mama…and your papa, and your grandparents too! Pablo Colón of Connecticut outlined how criminals called not one, but *two* members of his family on the same day—pretending to be his nephew and claiming the college-aged student had been in a car accident, hit a child and needed money to get out of jail. "Abuelo, it's your favorite grandson," the scammers pleaded with Pablo's father. There's also chilling audio from similar calls made to a mother and father in Arizona on the same day, who were told their daughter had been in some sort of accident (the husband received the call at work; the wife got the call as she was driving). "It's me, your daughter," a young-sounding female repeatedly cries to the father (who knew the call was a scam and recorded it). Unfortunately, the wife "truly believed" her daughter was in trouble. If you get one of these calls, stay calm, ask a tricky question that only the "family member" calling would know the answer to, hang up when they can't answer it, and report it to the FTC and law enforcement. Also, call other close family members and warn them, as they may be getting the calls at the same time!

The currency of cons? We miss when "Libra" was the answer to "What's your sign?" Nowadays, using Libra for criminal purposes seems written in the stars. Savvy scammers are promising "early access" to Facebook's recently-announced digital currency Libra through official-looking websites they've created in order to steal the money and personal info of eager early adopters. Some criminals even are claiming they've purchased the currency and are looking to sell it. Libra, truth be told, hasn't launched yet (the plan is to roll it out in 2020)—and even when it does, we advise extreme caution. (Given this month's piece on Facebook's scam profile problem, there's little reason to think Libra won't be a vehicle for more fraud.) Interested in how Libra will differ from Bitcoin and other cryptocurrencies? CNBC has an informative article on the somewhat complex topic.

Mystery shopper. Getting paid to dine at fancy restaurants and peruse the makeup counter as a mystery shopper is a real gig, just not one that you should ever pay to have the privilege to perform. Don't dish out the dinero for a mystery shopper "certification" or "guarantee," and don't even *think* about getting any gift cards for a company that's directed you to purchase them from the stores they've "assigned" you to shop at. Finally, never send any "overage" money back from a check that the company you're "working for" tells you to deposit. (The check they send will bounce, and you'll be left footing the bill with your bank.) There are some *legit* mystery shopping positions available; the Mystery Shopping Providers Association lists over 100 non-sham companies offering them in the U.S. alone. (But don't expect to get rich this way.)

Liar, liar? Report what's transpired. Showed up for that BOGO sale, only to discover it was bogus? We're so not here for it. And neither is the non-profit Truth in Advertising, which offers a convenient online resource allowing you to select your state for a snapshot of its written laws around false advertising; the penalties for violating them; advice on where you can file a complaint (hint: usually with your state's attorney general); how to get copies of existing complaints against bad businesses; and, in worst-case scenarios, how to take a bad business to small claims court (to recoup your hard-earned dollars). Go get 'em, tiger!

Every day I'm hustlin'. This one's for the movie buffs out there: Cardi B, Constance Wu and J Lo are starring in a film (based on a true story) that may or may not glorify bad behavior (the trailer makes it appear that the perps' crimes catch up with them). The group plays strippers turned hustlers (the name of the film) who rob their rich Wall Street clientele. The film is based on the true story of a crew of exotic dancers-turned-scammers who slipped ecstasy and ketamine drugs into the drinks of their wealthy victims, ran up their credit cards (by thousands) and banked on them not telling the police (even if they remembered the night-from-hell), because once a victim "weighed the cost of filing a formal complaint, of telling his wife and the police what he actually *had* done, he'd conclude it was too steep." Whether you see the movie as a cautionary tale or an operating manual on how to pole dance, it looks to be entertaining.

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.