Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • January 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!

They say love is blind…

Every Valentine's Day, pictures of flowers, chocolates and even bride-and-groom bliss are increasingly giving way to *being* groomed by scammers. According to the FBI, romance scams account for the largest amount of money lost to online scams—more than a whopping $230 million in 2017 alone! We know, we know…our readers are too smart to fall for some lothario's story—but your parents, friends or even grandparents *may* fall for it. CSO, a website that helps the public stay ahead of cyber crimes, points out that they've received tons of emails lately from the concerned adult children of twitterpated relatives who've fallen hopelessly in love with catfishers and con artists. So how can you help grandma see that her new bae is a faker? Before you rip the blindfold off *Bird Box*-style, perform a Google image search to reveal that her crush bilked his photo from someone else's profile. You also could suggest she message the mystery man for a photo of himself pointing to his nose (or another image that would be difficult to create if he were an imposter). Unfortunately, even after Romeo fails these "tests," the victim still may not listen to reason. (Love is a helluva drug!) Whatever you do, avoid playing the blame game and instead send your loved one articles from trusted sources (like us!). You also can contact AARP or local law enforcement to intercede. The National Center on Elder Abuse offers state resources as well. Finally, the FBI encourages you to head over to its Internet Crime Complaint Center (or IC3 for short) and file a report to teach that fraudster that flattery will get him nowhere.

Gonna "get you arrested"

In a scam that the Federal Trade Commission (FTC) describes as "growing exponentially," people across the U.S. are receiving calls from alleged law enforcement reps threatening to suspend their Social Security numbers (SSNs), claiming that the SSNs (or the call recipients) have been implicated in some sort of crime. Sometimes the callers even say they're helping the person on the other end of the line to avoid financial losses

during the alleged "crime spree" by moving money out of the victim's bank account (gee, thanks!). The FTC has posted one of the calls online. In the oddly-worded, pre-recorded message, a robotic voice threatens the caller if they don't call back immediately, stating: "I have received suspicious trails of information in your name" and "I will issue an arrest warrant in your name" and "get you arrested" (arrest you?). We'd like to think this goes without saying (although the FTC reports that they've "heard terrible stories about people losing lots of money" to the scam), but *never* give your SSN, even just the last four digits, to someone calling and threatening you—*or* cajoling you, *or* offering to help you, *or* professing their love to you, or doing *anything else* to play on your emotions—*even* if the number on the caller ID reflects the real Social Security Administration (SSA) number (this isn't hard to spoof). *Any* time you're asked to give your SSN (or any personal or financial info, for that matter), warning bells should go off. If you're wondering if the SSA is trying to contact you for real (or you've got questions about your SSN), hang up the phone and call *the agency* at 800-772-1213.

Feeling so used

Money mules. You've probably heard of drug mules, but the U.S. Department of Justice (DOJ) wants you to be aware of money mules: average, everyday Joes used by scammers to send and receive currency. The situation often starts innocuously enough with romance scams, when a seemingly handsome fella' convinces his "love" interest to help him manage "his" money because he's working in, say, outer space, and can't access a computer (riiiight!). Sometimes it originates when job seekers believe they've found a legit work-from-home arrangement that involves transferring money. And, according to a recent DOJ report, "Sometimes the money mule began as a scam victim, but when the scammer tapped the victim's resources dry" they found "another way to put the victim to work." (How resourceful!) Foreign scammers love U.S. money mules because the scammers' victims are more likely to send money to U.S. accounts (which may appear more credible). The mules are also urged to "collect and bundle" the proceeds from these scams (whether unwittingly or not) and wire *huge* amounts of money to what appear to be legitimate overseas "business accounts." Worried that you (or someone you love) are acting a mule? The FBI offers advice on how to get criminals off your back.

The gift that keeps on giving. Talk about giving yourself a pat on the back: Some Amazon sellers (usually located overseas) are shipping their *own* products to random homes in the U.S. through fake buyer accounts they create (using the identities/addresses of the residents)—and all this just to write themselves glowing "verified" reviews (which bump up their products in buyer searches). The scam is called "brushing," and as one couple points out, it can be annoying when a bunch of random stuff starts showing up at your doorstep (unless of course, it's that phone charger you were about to order off Prime anyway). Shockingly, according to the FTC, you actually have the legal right to *keep* merchandise you received but didn't order, as a "gift." If you find yourself in the awkward position of receiving gift after gift that you never asked for (or wanted), however, change your Amazon password and contact the U.S. Postal Inspection Service for help stopping the influx. Worried about buying a product that's only rated highly due to brushing? The websites ReviewMeta and Fakespot help you suss this out.

Tips!

- **Trials and tribulations.** An in-depth Better Business Bureau (BBB) investigation of free-trial "deals" reveals what many of us have already learned the hard way: They'll cost ya! The language hidden in the tiny

terms-of-service text governing sample products and trial-period services dictates that, in signing up and entering your credit card info, you're also signing your soul away (or at least your money, and often on an ongoing monthly basis). The BBB gives the story of one woman who agreed to pay $7 to ship some "free" skin cream to her home (it was advertised as having been featured on Shark Tank!). All told, the company hawking the sample ended up billing her $75. And who even knows if it was actually on Shark Tank!? These types of "no risk" trials "often try and trick consumers with deals that seem too good to be true or claim to have an endorsement from someone famous," said Lori Wilson, BBB Oakland's president and CEO. (The BBB report found that free-trial celebrity endorsements, from Oprah to Ellen DeGeneres, are often fake.) Sadly, 72 percent of the victims of scam trials are women (since they're the main buyers of the pills, products and potions that are commonly advertised this way). Don't get trapped in trials!

- **PSA pile-on.** It looks like Best Buy's Geek Squad has taken a break from fixing your granddad's printer to warn you about gift card scams in a common-sense PSA pointing out that gift cards should be used *only* to pay for products or services offered by the issuing retailer, *not* for scams. (We'd be remiss in our duties if we didn't mention that you can *also* trade or sell unwanted gift cards.) What prompts people to give their gift cards up to scammers? "You may get a call or an email from somebody pretending to be a family member in distress or even the IRS [claiming you owe taxes, you'll be sent to jail, yada yada]," cautions AARP. (Since older people are disproportionately paying criminals via gift cards, AARP joined the PSA.) Ultimately, scammers want the number on the card they've scared you into buying so that they can siphon money off it in an untraceable, foolproof way. Cash is complicated for scammers because they'd have to meet up with you to get it, and credit cards are not only traceable, but card payments can also be shut down or reversed by your bank, points out the National Association of Attorneys General (NAAG). (NAAG is *also* featured in the PSA, since your state AG can help stop the bad guys…and also, who's *not* involved in this PSA?)

- **Southern hospitality.** You're watchin' *Dumplin*,' singin' along to Dolly Parton, when an email appears in your inbox warning that your Netflix payment details need updating. You simply *must* know if Willowdean wins the pageant, so you click on what might be obvious to some is a link in a phishing email. Why obvious? Because, like most phishing emails, this one contains misspellings and other oddities (beginning with the charming greeting "Hi Dear"). However, it also boasts an accurate Netflix logo and convincing visual branding, so what's a binge watcher to do? If you're ever questioning if there's some sort of problem with your account (any account, not just Netflix), visit its official website *through* the web (*not* by clicking on the devious link in the phishing email). Then contact the service in question through their website directly or through the contact info listed on their site .

- **Let the right one in.** Ring, ring! It's Apple calling. Or so con artists would have you think; and they're doing a very good job by displaying the company's logo, address and phone number on your phone's incoming call screen. The automated spoofed calls advise you to call back an 866 number that's not Apple's real tech support department—this is the giveaway that the call is a scam. Unfortunately, your iPhone doesn't know this. According to Krebs on Security, iPhones are listing the calls as coming from "Apple." So if you were to, for instance, call the *real* Apple back and get disconnected or call them back again after ending a recent conversation, the fake Apple number looks like the real company in your phone, and is even connected to the series of real Apple calls that just occurred! As Krebs on Security remarks, "it is remarkable that Apple's own devices…can't tell the difference between a call from Apple and someone trying to spoof Apple." And yet…

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.
