Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • July 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!

Sun, sand and rental scams

Marie Claire is calling it "the summer of scam" and the *New Yorker* has dubbed it "grifter season." It's true, we're swimming in a sea of scams, with some of the worst occurring when we would rather relax on the beach. Those renting properties, from summerhouses to beach bungalows, are easy targets for thieves who excel in intercepting the cash flow between adventurers and their accommodations. The Federal Trade Commission (FTC) points out that this can happen in several ways: "Some scammers…take off the owner's contact information [from a real rental listing], put in their own, and place the new listing on a different site….In other cases, scammers hijack the email accounts of property owners on reputable vacation rental websites. Other scammers don't bother with real rentals—they make up listings for places that aren't really for rent or don't exist." This company, which went so far as to offer property tours for make-believe properties (which it advertised on Craigslist, naturally), was just busted by the FTC to the tune of $5.2 million! Complex rental arrangements—particularly those with confusing terms—are big business for scammers, which is why it behooves the wary wayfarer to get everything in writing (including any fees or refund policies) before agreeing to do business. And doing your due diligence (research!) is a must (you can even ask for references!). Not allowing yourself to be rushed into a decision that involves the transfer of money is also a no-brainer, no matter how eager you are to hit the beach. Finally, below-market rates or too-good-to-be-true opportunities are always a good indicator that a deal is really a dud.

They've got your number

There's a new scam in town, and it's particularly scary. Why? Because unlike credit card fraud, there's no real infrastructure in place to stop cell phone account fraud, which occurs when someone links "you" to an existing or new cell phone account. According to Consumer Reports, by the time this someone's ensuing crime spree

catches up to the *real* you, "your bank account may be drained, credit card companies may be after you for unpaid bills, and the police may be investigating you for crimes committed in your name." So how does this scam work? There are two major ways: First, your personal data (Social Security number, etc.) gets into the hands of criminals (perhaps they buy it from hackers who scored it in the massive Equifax data breach). Next, they use the info to open a new cell phone account (and if they need to present ID at the Verizon counter in the mall, well, they've got that forgery thing down). Another way criminals get your phone number is by having the existing one *transferred* to another account (a practice known as "porting"). Once they've done this, they're now the ones getting authentication texts from your bank, credit cards, etc. to log in to your accounts. One *super* easy way to avoid this whole debacle is to establish a PIN (which only the real you would know) with your mobile carrier. You can also freeze crooks out of your credit information by contacting the big three credit reporting agencies to place a security freeze on your file (and as of this fall, freezing your credit will be free!) A lot less time-consuming than the big freeze? Simply keep your phone number off social media. Whatever you do, don't end up like a consumer by the name of Megan, who didn't realize her number was ported until her phone was no longer working (ultimately resulting in a loss of around $3,500 and a stressful, time-consuming fight with T-Mobile to recover her identity).

With friends like these…

Devious doppelgängers. One sharp-eyed *SCAM GRAM* reader, Carol, recently emailed us to tell us about how her real-life friend Dorothy, who she believed friend-requested her on Facebook, turned out to be a fake. She thought she was already friends with Dorothy, but accepted the request anyway (just in case she was wrong). "Dorothy" began messaging her about how she'd been busy lately with "financial planning," but her nonchalant tone became more serious when she claimed she had discovered a foundation that gave out loans for common expenses like paying bills and buying a home. The story turned even stranger when Carol's "friend" claimed to have received $20,000 free and clear! We did a little digging and, sure enough, the Better Business Bureau recently disseminated an alert about an increase in government and other grant scams, specifically coming from cloned Facebook friends. Fortunately for Carol, she kept this friendship casual. If you don't, according to the BBB, "eventually you will be asked to supply personal information and a payment for [grant] processing fees." The BBB says that consumers reported over 500 government grant scams with losses totaling over $360,000 in the last few years. Carol dodged Dorothy's bullet, but you may not be so lucky unless you immediately unfriend any accounts you suspect are cloned. And, while people do sometimes create new Facebook accounts, receiving a friend request from someone you are already friends with is a real red flag!

All the single (50+) ladies! We've written about romance scams before, but in doing research for this month's newsletter, we realized that not only are they alive and (un)well, but older female consumers are continuing to lose LOADS of money to them! Catfishing is when a scammer (who probably really looks like Trump's "400-pound hacker") uses a fako studmuffin photo to entice the lovelorn. In the case of Pat here, the catfisher also wrote bad poetry, promised to "make love" to Pat and to "buy a bigger house with her" before developing a relationship that ended in her wiring him $5,600 so that he could "come to the U.S." and, presumably, live with her happily ever after. Then there's Ronda, who wired her "boyfriend" around $35,000, believing he was an offshore oil rig worker who had won a big court judgment and needed Ronda's assistance to pay fees associated with procuring the winnings. Last but certainly not least, there's 77-year-old Mary, a grandmother who ended up losing a whopping $130,000 to a man who also (interestingly) told her he was in the oil industry and added, "I love you…even just looking at your picture." How did Mary lose so much? "This is one of the few

times in my life I have been lonely," she said. "It makes you very susceptible to all kinds of things." According to the FBI, 82 percent of romance scam victims are women over 50. So, "women of a certain age," learn more about how to spot a romance scam!

Tips!

- **Your guide to grift.** We've developed a free resource to help you recognize the telltale signs of a scam, which include emails or calls coming from random contacts, manufactured urgency, a request for money or personal information, a threat or enticing offer, or a demand for an untraceable/unrecoverable method of payment. (It's pretty darn comprehensive, if we do say so ourselves.) *And* we don't just tell you how to *recognize* these things, we also tell you what to *do* about them. Consider this your one-stop-shop to avoiding scams. (Oh, and send it to your grandma, too!)

- **Hot-rod hoax.** The FBI has teamed up with auto sales site Edmunds.com to issue a warning to those in the market for a new (or used) set of wheels. It's not a new phenomenon for scammers to take these consumers for a ride, but it's the way they're doing it that has become increasingly sophisticated. Edmunds is warning the public that: "The link to the vehicle history report [of the car you're considering purchasing] may be a legitimate vehicle history report for a legitimate car. It's just the person who put the ad in doesn't own it." Yikes! And here we were, thinking you can always trust a vehicle history report. There are still ways to avoid the fraud: As usual, never wire money to anyone for any purchase, and think twice about any car sale that's done entirely online. You DEFINITELY want to test-drive that Corvette (*and* check the VIN, *and* buy your own vehicle history report—do not rely on one the seller provides!).

- **Tech support with a twist.** We've written time after time about the tech support scam: Someone calls you up claiming your computer has a virus, or somehow freezes it, and gains access to it under the guise of "helping" you fix it. Like the auto scam above, this too has evolved to keep up with an increasingly aware public. Now, "tech support" is calling to say that scammers have purchased products using your account and they'd like to issue you a refund; they just need your personal/financial info to do it. Or maybe access to your computer. Or maybe the numbers off the backs of prepaid cards they want you to purchase. Of course they do. Sigh.

- **Disappearing your debt (and your dollars).** The National Consumers League's (NCL) helpful Fraud.org site has issued a warning about supposed friends, would-be employers, online lotharios, associates and others who ask you for access to your credit card account to help you pay it down. This scam is particularly clever because the con artists, in many cases, really DO pay down your credit card, but with stolen credit or debit cards! NCL tells the story of Pete, who, after having his card paid off, trusted the scammer, gave him access to his bank account, and, well, the rest is kind of complicated but involves gift cards (of course) and Pete losing quite a bit of money. Oh, and his "paid off" credit card balance? It was put right back on the card as soon as the card issuer discovered the payments were fraudulent. Don't end up like Pete—learn more here.

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