Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • October 2016 • 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!

Interception!

We know you're excited for football season, but don't let scammers score a major touchdown by selling you counterfeit tickets to see your favorite team throw the old pigskin around. When purchasing tickets online, the Better Business Bureau (BBB) cautions you to go through a legitimate website (like the team, college or university's); a verified ticket broker that resells gameday tickets; or a person physically located at the stadium's box office. The BBB also warns fans to watch out for related scams, like those involving counterfeit merchandise sales (online or on the street) or people posing as parking attendants (who could take your cash and direct you to a lot where you might get towed…or not direct you at all). Don't get tackled for a loss like these Vikings fans, who bought real PDF tickets only to find that scammers had altered the seat locations to make them appear closer to the field, or this Buckeyes fan, who thought she could get $100 tix for $20 (too good to be true). And if anyone instructs you to pay for your tickets via wire transfer, cash, prepaid card or other forms of payment that are difficult or impossible to trace, make a 40-yard dash in the other direction!

A big turnoff

Consumerist has issued an alert warning men (and their partners) to think hard before purchasing any of the erectile pills found at gas stations and drug stores. As the helpful consumer news source reports: "An Alabama man has been charged with intentionally defrauding and misleading consumers for importing a drug [called Zhen Gong Fu] sold as a 'male enhancement product' that contained sildenafil, the active ingredient in Viagra." So what's so bad about using essentially the same thing as prescription Viagra, you might ask? For starters, it's not the same thing. There might be "too much of a good thing" in the unregulated products. Sildenafil also can dangerously lower blood pressure in men on other medications. Want more reasons? The pills and powders can contain "untested and unstudied pharmaceutically active ingredients," according to the FDA, which dedicates an entire page to "tainted sexual enhancement

products." Then there are the disconcerting names and descriptions of the products, like Black Ant supplements, which purported to contain actual black ants. Closing thought: If your idea of a fun night starts with eating black ants, then you need more than the help offered in a packet hanging next to the 7-Eleven counter.

Keeping tabs on the Kardashians

It's hard to imagine enduring the terrifying experience Kim K. went through earlier this month when she was robbed of $10 million in jewelry at gunpoint (let alone owning $10 million in jewelry). But while it's difficult to relate to the celebrity's costly accoutrements, even us common folk can learn from her ordeal. As CNN points out, Kim (like many of us) is "a prodigious poster on Twitter, Instagram and Snapchat" and "was posting much of what she was doing leading up to the robbery—including her whereabouts at Paris fashion shows." This is a big no-no, and one that we at Consumer Action have been actively advising consumers against. No matter how much you want to show off your shiny new sports car, interior design skills or expensive bling, never post public photos of the cool stuff that you own, the inside of your home or information on your whereabouts and travel plans that might make you more attractive to scam artists or thieves. As Kim well knows, "haters gonna hate"; don't make it easier for them to identify what's yours and make off with it.

Takedowns

A web of lies. As part of its excellent ongoing investigation into international mail fraud, CNN reporters spent months looking into a small but suspect Canadian payment processing company called PacNet Services, Ltd. As it turns out, the U.S. Department of Justice (DOJ) had their eye on the company too. In late September, the DOJ announced that it's coming down hard on little ol' PacNet, which has actually been behind one of the largest global mail schemes in the history of mankind (!), processing payments for a web of scammer-customers around the world—customers who, over the years, have defrauded the elderly and vulnerable out of untold millions. Peace out, PacNet!

The epicenter of IRS calls. Another one bites the dust, this time in the form of several seemingly dull office buildings in India that, Indian authorities say, housed over 700 people who made thousands of phone calls a day to U.S. citizens—citizens they would threaten with arrest for "failure to pay taxes." More than 8,800 people have been conned out of over $47 million in these types of scams over the years. Indeed, IRS scams impact everyone, from young, green students attending their first day of university to college-educated IT consultants in their sixties. Hopefully we'll be seeing a lot less of this scam, though, as the call centers have been shut down and 70 people have been arrested, with more under investigation.

Wells Fargo fallout. The notorious Wells Fargo debacle continues, and now the ex-employees (many of whom attempted to flag the fraud internally years ago) are suing the bank for wrongful termination after they failed to meet the ridiculous "sales quotas" that got Wells in hot water to begin with. The bankers have gone public, telling compelling tales of how they were coerced into signing customers up for account after account under the threat of "working for McDonald's." Sen. Elizabeth Warren put it best during her faceoff with the Wells CEO: "Your definition of 'accountable' is to push the blame to your low-level employees, who don't have the money for a fancy PR firm to defend themselves." Here's to the employees getting that money—from the lawsuit.

Tips!

- **You've been warned.** Surfing the internet is getting a whole lot safer, at least if you use Google Chrome. Starting in the new year, Chrome will explicitly label sites that collect passwords or payment information as being "more secure" due to their use of HTTPS (as opposed to old-school, non-secure HTTP). Simply put, the extra 'S' means that these sites are harder for outsiders to access (and steal information from).

- **Thanks for nothing!** If you get an email purportedly from the IRS with a CP2000 notice attached, don't even bother opening. What's a CP2000, you ask? It's a document that the IRS snail mails you (*never* emails) when it believes that some of the information you reported on your tax return may be wrong. Scammers are sending the fake notice requesting more information (and money) related to healthcare coverage under "Obamacare" (i.e., the Affordable Care Act).

- **Lock it down.** Think your email, banking, social media and other online accounts are secure because you log in using a strong password? Think again. Every two seconds, another person becomes a victim of identity theft. Fortunately, there's a quick and easy way to make sure you're not one of them: strong authentication. This tool allows you to use biometric data, security keys and one-time codes to become more bullet-proof then Luke Cage. Learn how to #LockDownURlogin here.

- **Nothing new under the sun.** While it seems that scammers are always thinking up new ways of committing crimes, often their cons are just twists on tried-and-true classics. Such is the case with the fake check scam. Back in the day, a consumer would be tricked into depositing a bad check and sending the scammer cash or money orders withdrawn or purchased against the "value" of the value*less* piece of paper. Nowadays, in an effort to make the transaction seem more legitimate, scammers are instructing their victims to physically visit a bank to deposit the money into an account controlled by the scammer. As Fraud.org sensibly points out, there's never a legitimate reason for someone to give you a check and then ask for part or all of the money back.

- **Prepaid protections.** The Feds have created standards to protect prepaid card account holders (and those with digital prepaid accounts like PayPal or Venmo) against withdrawals, purchases or unauthorized transactions that happen when lost or stolen prepaid cards are reported to the issuer. The rules limit your liability for fraudulent charges and require issuers to reimburse you for those over $50, *if* you report the issue within two days of becoming aware of it. Prior to this, if your card was stolen and the balance was used up, your only option was to suck it up. This and other new rules for prepaid cards go into effect in October 2017.

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

Use our "Tell a Friend" page to let your friends know they can sign up for their own copies.

Consumer Action empowers low- and moderate-income and limited-English-speaking consumers nationwide to financially prosper through education and advocacy.

Manage your email subscription. Choose the content you'd like to receive. You will have to create a password to do so. Lost your password? Use "Forgot your password?"

Click here to Unsubscribe (but, hey, we hate to see you go!)