Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • April 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!

Dubious disability

The feds recently indicted a number of seemingly respectable professionals in a massive and complex disability fraud case that the *Washington Times* summarizes as a "brazen scheme [that] involved a lawyer who recruited bogus [disability] applicants and faked their medical forms, crooked doctors who signed off on the false forms and a handpicked administrative judge who would spot the applications in the system, grab them and approve them." All told, the men netted $600 million in government payments. Now that you know the cast of characters, you should understand how disability fraud works: If you claim that you're too disabled to work (due to crippling back pain, mental illness or any number of ailments), you (and your doctor) better be able to prove it, because the government gets pretty angry if they launch an investigation and find out you're faking sick. As a matter of fact, it's NOT a good idea to swindle money from taxpayer-funded programs, whether they be disability, Medicare or food stamps.

Living large off public largesse

It's hard to shed tears for a massive charity charade that has ended in two sham cancer non-profits dissolved and the ringleader of said non-profits (one James T. Reynolds Sr.) banned from ever working in the sector again. Cancer Fund of America Inc. and Cancer Support Services Inc. benefitted from public sympathy (and generous donors) to the tune of $75 million. The charities, which promised to help breast cancer patients and dying children, fed the money directly into the pockets of Reynolds (pictured here), who had already been busted by the Federal Trade Commission last year for operating a network of *additional* bogus charities (some people never learn). Reynolds used the donations to purchase everything from luxury cruises to Disneyland trips and dating website memberships. Officials have ruled that Reynolds must now surrender his "artwork, two pistols, and sale of a pontoon boat"—living large, indeed. You can check for charity scams by looking up any group you are considering donating to at CharityWatch.org.

Homebuyer beware!

Buying a home can be an exciting time. You've spent months house hunting, so it's understandable that you're eager to settle on that perfect three-bedroom with the white picket fence. But before you're handed the keys, you need to undergo one more step in the process: paying the closing costs. Many people just want to close, and will believe that an email sent (seemingly) from their real estate agent with instructions to wire the closing money is legit; unfortunately, it's another example of a new, crafty scam. Typically, homebuyers bring a check to their closing, but recently they've been bilked out of hundreds of thousands of dollars as hackers broke into the email accounts of their real estate agents, dug for information on upcoming transactions and posed as the agent or title company. Let this be a lesson: Always call and make sure that any deviations from agreed-upon payment plans are legitimate. And, call your title company before sending any money!

April fools

There's no such thing as a free dinner. Quite a few Florida seniors were duped by slick marketing materials and the promise of a free meal at a Tampa restaurant. Fraudsters advertised themselves as investment experts offering seminars (and food). Any money the con artists were given, however, was "invested" right into their own pockets. According to a new study by the non-profit Investor Protection Trust, nearly one in five seniors has been swindled in one way or another.

Pray the con away. How much would you pay for someone else to contact the one upstairs on your behalf? The answer appears to be between $9 and $35, or at least that's how much over 125,000 people sent to the popular "Christian Prayer Center" (and its nonexistent pastors). The holier-than-thou website promised a direct connection to the Almighty, who would (allegedly) help the defrauded win the lottery, get a clean bill of health or pay off the mortgage.

It could happen to anyone. Even high-ranking federal officials whose very jobs involve regulating corporate data security practices can fall victim to well-crafted phishing scams. To her credit, this Federal Trade Commission employee isn't too ashamed to speak out and warn others about the type of "deeply sophisticated" scam she fell for—ironically, she opened a hacker's email because it came from a man she knew who heads up a pro-consumer, pro-open internet group!

Tips!

- **Tax scams? There's an app for that.** Good news to all you procrastinators out there: Taxes actually aren't due on the 15th; you have until Monday the 18th. The bad news? Tax scams are up 400 percent this year! Fear not, however, for when the bogus taxman cometh, there's a new app to block his calls.

- **Fake festivals and foodie events.** Turns out that "Groupon" deal you snagged for the crab feast might be even scarier then a bowl of lukewarm crab dip. While scammers are busy advertising discount tickets to all sorts of nonsense events this festival season, Consumer Reports is busy issuing warnings to help you make sure your Bonnaroo ticket is legit, dude.

- **It's as simple as Fraud.org.** The National Consumers League just introduced their new and improved

Fraud.org website. The easy-to-navigate site offers tips for preventing fraud, advice for those who've been scammed, and a special portal dedicated to helping you understand the growing data breach epidemic.

- **Thumbs down on Facebook 'like-farming'.** If you're the type to 'like' everything on Facebook (from that adolescent FarmVille game to that annoying motivational quote) we've got bad news: You're more likely to get duped into promoting malicious content that ends up at the top of your friends' Facebook feeds. Avoid a mass unfriending and learn about how scammers use "like-farming" to steal identities, money and the like. Your friends will thank you.

- **Struck by spear phishers.** You've probably heard of phishing (when a scammer poses as a legitimate organization and sends a fraudulent email message in order to bilk you out of money, etc.), but have you heard of *spear phishing*? It takes phishing a step further by incorporating an often more personalized fraudulent message from a "friend" or some other entity that you (think you) know and trust.

- **I'm too sexy for my scams.** If someone promises that you'll be America's next top model after spending a little dough, think twice before striking a pose. Sometimes the request isn't so obvious at first—perhaps a talent agent or casting director invites you to a photo shoot and then asks for the cash. Read up on how to identify scam scouts and let them know that flattery will get them *nowhere*.

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.
