Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • May 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!

Just as we predicted!

You could say we're psychic (or we just really understand the way scammers think). Last month, we reported that the newly redesigned Medicare cards (the ones meant to be safer, sans Social Security numbers, or SSNs) would open a whole new opportunity for crooks to contact seniors during the card replacement period (happening now through April 2019). Like clockwork, the Centers for Medicare & Medicaid Services, the Coalition Against Insurance Fraud and local police are now reporting complaints of callers demanding that would-be card recipients give them cash for cards, as well as bank account and credit card numbers and even the numbers off their old Medicare cards. *Fox News* reports that scammers are "working overtime" and are "desperately trying to convince seniors to divulge their SSNs before those numbers disappear completely" from the old cards. This is particularly bad news since a new study reveals that, as we age, we become less capable of detecting fraud because we tend to "concentrate more on the positives" in life. Just remember: Medicare *won't* call you about your card; it only operates via snail mail. (And that person who *is* calling—he is bad!) Also, don't let the fact that you haven't received a card yet make you give up the goods; it may be that the card simply hasn't been mailed yet (remember, it could take until April 2019) or that your contact info isn't current (in which case you can log in to your Social Security account here or visit your local Social Security office). You can also sign up to receive an email notification when your card is in the mail. If you still have questions or want to report a scam, call 800-MEDICARE (633-4227) or holla at your local Senior Medicare Patrol office. Finally, when that glorious day arrives and you *do* get your shiny new card, make sure to destroy the old one (lest someone fish it out of the trash and, despite your best efforts, get your SSN *that* way).

Confessions of a shopaholic

We have something to confess: We love online shopping as much as the next person (and have spent *way* too much on late-night Amazon Prime impulse buys). But it's a dangerous world out there for a Windows

shopper, what with online marketplace fraud increasing at an alarming rate (up 30 percent from 2016 to 2017)! Credit reporting agency Experian breaks down the numbers and outlines two major types of fraud: shipping and billing. Shipping fraud happens when criminals instruct that the stolen goods they purchased online be delivered to an address *they* provide, while billing fraud occurs when *your* address is tied to the payment account used to purchase the stolen goods (which are, typically, never shipped to your address). Interestingly, Experian's research revealed that in 2017, Beaverton, OR, had the highest rates of shipping fraud in the U.S. (How's that for useless trivia?) So what can you do to avoid becoming a victim? You're typically better off making your purchases through tried-and-true websites that offer secure protection for your payment/personal info and tracking numbers for your packages. That being said, even Amazon loyalists are currently experiencing "empty box" scams that bank on the retail giant's "guarantee policy" to pay customers back for deliveries from third-party sellers—deliveries that in this case contain naught but air. And even buyers who think they're getting a swell deal from a kindly neighbor on Facebook Marketplace might be shocked to find that no space is sacred: Scammers are now exchanging emails with the buyers and referring them to eBay imposter sites to complete the con.

Parking is crazy!

Americans love to drive. But grifters stand to gain from our gas guzzling ways, particularly if they can approach us in parking lots. As colorful as a Volkswagen Beetle (but certainly not as cute), parking lot scams are driving drivers crazy! One Connecticut woman, for instance, paid $200 to a man who claimed that she injured his hand and damaged his cell phone as she backed out of her parking space. (Of course, the "injured" man did not want her to call an ambulance, or the authorities.) In another case, a scheming couple in St. Louis, MO, approached drivers running errands, interrupting them to point out they had a "broken wheel" (presumably as part of an attempt to get behind the wheel). Throughout parking lots in Texas, one man claimed to need help for his "family" and offered fake gold jewelry in exchange for "food and gas money"; and in Charlotte, NC, a crook pretending to be with a towing company (while conspicuously lacking a tow truck) immobilized cars with various odd "boots, chains and locks" before demanding cash to release them. There's more, but you get the idea (and in case you don't, the Better Business Bureau gives an exhaustive list of the types of scams you might encounter in your average parking lot). If you're approached outside of the grocery store by a shady individual asking for money, threatening you or otherwise trying to engage you in or around your car, keep your head forward and your mouth shut and walk away. If the individual is acting particularly scarily and you feel that you can't get in your car and leave them in the dust, threaten to call the police (loudly, and ideally while walking into a nearby, populated store). The AARP offers more info on how to handle a plethora of possible parking-related problems. (For instance, if you're handed a ticket or you find one on your windshield, independently look up the alleged "issuing agency" online and verify its legitimacy.)

Ain't nothing like the real thing

Never forget. In the wake of 9/11, the government set up a Victim Compensation Fund (VCF) to provide financial compensation to those who were killed or injured due to the terrorist attacks (or in the aftermath due to toxic debris present during rescue and cleanup efforts). Unfortunately, scammers caught wind of the fund and have recently re-upped their efforts to steal money from victims. According to the fund, the lowlifes call to ask "questions about the status of an individual's VCF claim, state that the individual may be entitled to money and/or ask for personal information in order to mail a claim package or file a claim on the

individual's behalf." One firefighter, who suffers from a chronic 9/11-induced illness, recently received a call from a scammer and summed up what we're all thinking: "These guys have an express ticket straight to hell." The scam is so heinous that lawmakers across the aisle have recently joined together to launch an investigation.

Head in the clouds. If you receive a call from Apple letting you know that your iCloud account or Apple ID has been breached and you need to contact Apple support to fix the issue, you might do what most sensible people would and call the number back to make sure that the call is originating from a legit Apple location. *Wait a minute!* Sad to say, clever scammers have managed to spoof the actual phone numbers associated with local Apple retailers across the country. Often, scammers are banking on the customer either pushing a *button* during the call and engaging with them then and there or calling back another number left via voicemail. Regardless, Apple has let customers know that they will not initiate calls with customers, so if you get a call about the cloud, stay grounded and hang up!

It ain't over 'til it's over. Tax season is over, but that doesn't mean that you're not still worried about paying off an outstanding tax balance. Crooks know this, and they're using telephone numbers that show up as IRS Taxpayer Assistance Centers (TACs) on your caller ID to demand payment. If you question their demands, you're directed to look up the real TAC number on the IRS' official "dot gov" website (which might make the whole situation seem credible) before the scammer calls back again from this spoofed number (and you, presumably, fall for the convincing ploy). To avoid this, know that the IRS will rarely contact you via phone about back taxes. If you *do* owe taxes, don't just pay whoever calls you: Check out IRS.gov/payments and initiate payment yourself. (Also, be wary of any companies promising to help eliminate your tax debt.) Learn more about new ways to report tax-related fraud and identity theft.

Will the real Mark Zuckerberg please stand up? What's worse than watching Mark Zuckerberg apologize repeatedly for data privacy violation after data privacy violation? Seeing him (or his comrade Sheryl Sandberg) pop up in your Facebook Messenger inbox asking for money! The *New York Times* has reported on the insane number of imposter accounts on sites like Facebook (and Instagram)—accounts that use the likeness of the sites' top executives to coax money out of the gullible. All told, the *Times* found over 200 such accounts on Facebook and Instagram, "not including fan pages or satire accounts" (which can number in the thousands). These types of imposter accounts, many of which engage in lottery and government grant scams, aren't allowed (according to the sites' own rules), so why is the real Mark Zuckerberg failing to take them down? The *Times* story features some entertaining conversations between scammers and their marks and details how difficult it is for those who get duped to even *contact* Facebook (let alone get their money back).

Tips!

- **Don't bank on it.** If you can't rely on the bank to put a stop to a payment that's clearly fraudulent, who *can* you rely on? This is what one scam victim was left asking herself after she rushed to a Wells Fargo bank branch to notify them (in person) within an hour of realizing that a $6,700 "fee" she deposited in a Wells account for access to a $150k+ "government grant" had ended up in a con artist's account. Upon alerting an employee and noting that the money was still in the account (phew!), the employee rushed to the rescue! Just kidding. That's what you would expect, but not at Wells Fargo. This employee actually did…nothing! Outrageously, the consumer had to sue the bank to finally get them to freeze the account (by which time thousands had already been withdrawn from it). "Banks have a duty to look out for red flags

that their customers are using their accounts to commit fraud or other illegal activity," said a spokesperson for the National Consumer Law Center. Obviously! (And hopefully this scam victim sues the socks off Wells for not doing so!)

- **Taking too much off the top.** When Groucho Marx said he wouldn't want to belong to any club that would have him as a member, he might as well have been talking about peer-to-peer Lending Club, which appears to accept anyone who is willing to sign up for its deceptively marketed loans. Enter the Federal Trade Commission (FTC), which is suing the not-so-exclusive "club" for promising "no hidden fees" while continuing to take hundreds in "up-front fees" off the top of loans it issued to consumers (because, you know, these unadvertised fees aren't technically the same as hidden fees...at least that's what Lending Club would have you think). Perhaps more shocking, however, is that the suit alleges Lending Club "told consumers they had been approved for loans when they had not" and "made unauthorized withdrawals from consumers' bank accounts"! Whoa Lending Club: Slow your roll.

- **Don't it make my cell phone BLU.** While mobile phone maker BLU bills itself as a "pioneering" company that gives consumers "a choice between network providers" while "fulfilling the needs of the everyday person," last we checked, those "needs" didn't include privacy invasion. The FTC just announced a settlement with the U.S. company for allowing a Chinese company to collect not only call logs and other data from its cell phone users, but the actual *content* of users' text messages! The FTC adds that the Chinese company "didn't have a business need for this information" (we contend that there's generally never a "need" to read customers' text messages, period).

- **Mystery "man."** Be wary of any advice you get from website The Student Loan Report and its spokes"person" Drew Cloud. *The Chronicle of Higher Education* published an exposé on Cloud, a ubiquitous presence on the student loan advice circuit (having been quoted in the *Washington Post*, on major national news stations and in popular blogs). The problem? Cloud is "the invention of a student loan refinancing company [LendEDU]" that stands to benefit financially from his recommendations. It would be one thing if The Student Loan Report made it known that Cloud was an "Ask Jeeves" type of character. The Report, however, featured a photo of a (smug bro-ish-looking) dude (allegedly Cloud), who it claimed had "a knack for reporting throughout high school and college, where he picked up his topics of choice." Humanizing a company that makes its money off of students who are up to their eyeballs in debt is, well, kind of inhumane. If you're looking for advice or to set up a payment plan to get out of student loan debt, check out our real, objective guide here (we have nothing to gain).

- **What's in a name?** If you've got a Chinese last name, fraudsters may call you claiming to be with the Chinese consulate. According to the FTC, anyone could become a target of this scam (even if your last name is "Smith"), but if it's "Wu," you're more likely to be impacted since the robocalls are often in Mandarin and the scammers are banking on people of Chinese descent having some connection to the consulate (or embassy). Upon answering the phone, targets are directed to pay for mystery packages, documents or fines (allegedly levied by the agencies), lest they end up "in trouble." One 65-year old Chinese woman in NYC lost a whopping $1.3 million after a series of threatening calls. Just say no to government imposter scams and hang up the phone (even if your caller ID says it's the consulate calling).

- **No room for error.** We lead busy lives (both online and off), which is why it's easy to make a mistake when quickly pounding in the URL for a website that lets us pay our electric bill the day it's due; buy more bulk baby food online (as the baby screams in the background); or rid ourselves of the fine from that ticket we incurred when we parked on the curb with our blinkers flashing (hey, we only ran into the store for a

moment!). Scammers are making money off our harried existence when we make common typos that take us to a site we *thought* we had input correctly. A simple .com instead of .gov could mean the difference between paying a bill and paying some dude named Bill. The National Consumers League's Fraud Center encourages you to slooooow down and learn more about how to avoid what it's calling the "typosquatting" scam.

- **This is a test. This is only a test.** Consumer Reports has created a seven-question test to, well, test your knowledge of modern-day scams like credit card skimmers and shimmers, crowdfunding, "like" farming, and the like. We took the test and got tripped up by at least one of the scenarios; the answers aren't as obvious as you might think. Fancy yourself a con-conscious consumer? Have a go at it and see if you can beat SCAM GRAM's score!

- **An open-and-shut case.** Perhaps emboldened by a 2016 class action in which StarKist settled with consumers to the tune of $12 million for failing to pack their cans full of tuna, two potato chip lovers took chipmaker Wise Foods, Inc. to court on behalf of salty snackers everywhere, alleging that the company had defrauded the public, since Wise's individual-sized bags of chips contained too much air and not enough of the crunchy stuff. The suit went so far as to include visual exhibits of open bags, with rulers measuring the air (or "slack-fill" space) at the top of the bag versus the actual chip depth, and even compared Wise's dimensions to other popular brands, like Ruffles. If you think this is pedantic and awful, you'll be happy to hear that the plaintiffs lost the case.

- **File under: stuff you don't need.** Always at the forefront of trending news, the *New York Times* took on the topic of faddish alkaline water: Does this higher-pH water have any benefits? Should we pay more for it? In short, no. As one particularly blunt doctor stated: "For people to continue to market alkaline water —they're really as bad as the snake oil salesmen of yesteryear." As a matter of fact, the *Times* points out that there are actually *risks* to drinking alkaline water, which "showed impaired growth and damage to cardiac muscle in rat pups" and caused skin burns on humans exposed to it after a municipal water plant in Germany went awry.

- **Last call!** We've mentioned this one before, but time is almost up! The Federal Trade Commission has extended the filing deadline to May 31 for its $586 million settlement with Western Union. Anyone who wired money to a scammer through Western Union between Jan. 1, 2004 and Jan. 19, 2017, is still eligible to submit a claim and get all or part of the money they lost back. (Important: Don't pay anybody to help you file your claim or get money back. Anybody who asks you to pay for your claim or refund is scamming you.)

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.