Scam Gram!
Keep the sharks at bay

A Consumer Action News Alert • October 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!

Breach of trust

Facebook users (so, pretty much everyone, unless you're a teen on Snapchat trying to avoid your parents) are a bit freaked out by a massive data breach that began logging them out of their accounts earlier this month. The breach is the largest in the company's history (impacting 50 million), and the question on all our minds is: What happens next? Facebook claims they've fixed the vulnerability, but users should still change their password (and the passwords to any linked accounts, like Instagram, etc.). They *shouldn't*, however, be worried about the spam-y messages from friends warning them of cloned accounts. (Cloned accounts have always been an issue, but, as of this writing, there's been no increase post-breach.) What you really need to be worried about is "imposter scams," since, in the words of the late, great Notorious B.I.G., scammers now know "what your interests are, who you be with, things to make you smile, what numbers to dial." There is an upside to all the recent breaches, however. The Senate just had a hearing to consider (*finally*) implementing a national consumer privacy law. (One downside, though: That hearing had zero representation from privacy advocates.) And the hammer is falling on companies that don't treat breaches seriously. Uber (ever the paradigm of ethical business practices) is now paying out "the largest multistate penalty ever levied by state authorities for a data breach" for not only waiting a full year (!!) to disclose a 2016 hack that impacted 57 million, but *paying the hackers* $100,000 in hush money. Our take: Real consequences for corporations that fail to protect against breaches or inform consumers post-breach is what's gonna keep 'em honest, so call Congress and demand a law at *least* as strong as this solid one that California just enacted. (And while you're at it, voice your support for the Cali law, which is under attack by companies that would love to see a weaker national law preempt it.)

Social (in)Security

Repeat after us: Social Security accounts do *not* get suspended. Social Security accounts do *not* get suspended. This is important to remember, since you might be getting a call soon (if you haven't already) from a crook claiming to be with the Social Security Administration (SSA). You could hear a real person on the line, or the call could be automated. It may appear to come from the Washington, DC, area, or a government agency. Either way, the voice on the line is going to tell you that your Social Security account or number has been suspended due to some sort of illegal or suspicious activity and—here's the clincher—that your assets will be frozen if you don't give the caller your personal and/or financial information. (And you know what happens if you go down this dark path: identity theft.) Just to keep you on your toes, SSA scammers sometimes alter their approach and, instead of calling, send an email (using a pretty convincing email address, like "no-reply" @ssa.gov) directing you to a lookalike website. Either way, it's important to know how to *really* check on your Social Security funds: If you haven't already, create a "*my* Social Security" account with the SSA online and you'll be able to check your benefits anytime. Need help? You can call the SSA at 800-772-1213. And if you're contacted by a con artist, it would benefit everyone if you reported it to the SSA Fraud Hotline by phone (800-269-0271) or online.

Uncle Sam wants YOU (to know better)

Electoral knowledge. Officials in various states are warning the public about voter fraud. No, not the type involving one political party gerrymandering districts or suppressing entire demographics (as bad as this is); the type involving calls to collect your voter registration data (i.e., your personal info) in order to commit identity theft (of course!). You may be fired up over recent political happenings, but don't let your frustration lead you to "register" to vote in the November elections with some rando over the phone. Know that legit organizations will *never* register you based on a phone call. Click here to *legitimately* register in your state (there's still time in at least half the states, but don't delay). Finally, if someone calls and pressures you about your civic duty, show 'em where they can stick their ballot by hanging up!

Driver *mis*education. Third-party DMV-lookalike websites across the country are driving drivers crazy by misleading them, collecting their personal information (to sell to private businesses) and personally profiting off their confusion. As one San Francisco-area news station summed it up, the sites "charge customers trying to complete applications for new driver's licenses, identification cards, DMV appointments and other online transactions." Sure enough, one eagle-eyed SCAM GRAM reader from the Bay Area wrote us to say that he was handed a flyer when he visited the DMV with instructions to visit a site that would have him pay by credit card (including a $23 fee) to conduct DMV business that would otherwise be free on the real site. This reader was too smart to fall for it; we're covering the con to make sure you are too.

Tips!

- **Check yourself.** Maybe it's because Millennials are accustomed to using PayPal, Venmo and other electronic forms of payment, but they're the population most apt to fall for check fraud these days, according to a new Better Business Bureau (BBB) study. Since Millennials are also accustomed to 140 characters or less, we'll keep it short: Check fraud occurs because banks (in an effort to please customers) cash your check before determining if it's fraudulent. (Phony checks mimic cashier's checks or those for legitimate business accounts.) The money *appears* to be in the account, but if you spend it (for instance, to send part of the check back to a crafty scammer who claims he cut the check for too much), it'll come back to bite you when the check bounces. *You're* on the hook for the money, *not* the scammer. Learn more here about fake check scams.

Woebegone wages. Ah, direct deposit: keeping employees everywhere from ever having to wait in a bank line. Unfortunately, you may find yourself sitting on the street instead if you fall for the latest scam, which the FBI says is predominantly targeting employees in the education, healthcare and commercial airway industries. Workers are being warned to watch out for emails that claim to come from their place of employment and contain links leading to pages asking for their employee login credentials. Once usernames and passwords are obtained, cyber criminals can reroute future paychecks. Don't be puzzled come payday; the FBI is providing tips for deterring payroll diversion.

Lock down your login. The U.S. Department of Homeland Security and the non-profit National Cyber Security Alliance have dubbed October "Cybersecurity Awareness Month." The organizations recommend six steps to "gain peace of mind and more control over your online security," with each step outlined in detail on their easy-to-navigate website, which aims to help the public "stop and think" before they connect. The steps outlined include how to protect your mobile device, use strong authentication tools and avoid phishing attempts (like the one mentioned above).

Freezing out fraud. In case you haven't heard, last month the government made it free to freeze your credit file, a valuable tool in the fight against identity theft (particularly during an age of seemingly endless data breaches). Put simply, a credit "security freeze" keeps others from opening new credit accounts in your name (i.e., buying a car or a house). It's a good idea to place a security freeze on your credit file if you have no immediate plans to open new accounts (and it's a lot quicker and easier to unfreeze than it was in the past). Consumer Action issued an alert explaining where to get "frozen," and the FTC has published some helpful FAQs pertaining to free freezes and how you can freeze credit on behalf of someone who you care for (e.g., a minor, an incapacitated or elderly person, etc.).

Scram, crammers! Cramming isn't just something you do before a test. It's also what scammers do when they bombard your cell phone with useless, unwanted text messages, resulting in unauthorized charges to your mobile account. In a welcome twist, the FTC will now be "bombarding" those who lost money to these mobile cramming operations with useful and wanted cold, hard cash (well, refund checks to be exact). The average refund is $92.95. You can click here to view all of the cases resulting in FTC refunds (who knows, you might just be owed money!).

Just because. Consumers in Texas, beware! Someone is calling and impersonating…wait for it…the late Burt Reynolds?! Typically we don't write about scams of a hyper-local nature, but this one is just too weird to pass up. Burt always had an electrifying presence, but that still doesn't explain why the mustachioed man would be calling utility customers demanding they pay their energy bills (in cash or via gift card, no less). Besides, the only person who should be impersonating Burt Reynolds is Norm McDonald (as Turd Ferguson, of course).

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