Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • February 2020
www.consumer-action.org

Click here to view this newsletter in a browser.

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!

An outbreak of opportunists

As the Coronavirus (renamed COVID-19) continues to spread throughout China (and in other countries via isolated cases and clusters), people across each continent are prepping for the worst. Con artists are feeding off this fear in a variety of ways, from more traditional phishing email attempts, to the sale of (often never delivered) overpriced face masks, to the promotion of false "cures" ranging from herbal teas to kimchi to cow dung. (Yes, cow dung.) Sick scammers are also pretending to be government officials, such as those from the Centers for Disease Control and Prevention (CDC), and asking for Bitcoin "donations" to fight the virus, or sending emails promising updates on the "local" spread of COVID-19. The end goal of the emails? To get the recipient--who is, ironically, attempting to *avoid* catching a virus--to click on a link or attachment that downloads a *computer* virus and locks victims out of their machine unless they pay a ransom. Sometimes the downloaded malware runs covertly in the system, siphoning off the recipient's banking info, passwords, etc. as they are entered. As GovTech points out, we can expect to see more of these successful scams because, "Unlike natural disasters which typically last for a few days or possibly a week as a global top story, the coronavirus facts are changing daily and new warnings and alerts can be expected for weeks, if not many months." Yes, the prognosis is grim when it comes to widespread paranoia and poor choices, but we may pull through: Many with public platforms are already taking the meaningful action necessary to inoculate consumers. Zuck, for instance, is trying to defeat the disease of

misinformation on Facebook and Instagram, including the particularly virulent claim that "drinking bleach" cures COVID-19. (Which is a stretch unless you consider death by bleach consumption a "cure.")

Putting off until tomorrow what criminals will do today

Waiting to file your taxes? You're not the only one. Early data released by the Internal Revenue Service (IRS) reveals that significantly fewer people are filing early this year, which means that it's likely we'll see lots of taxpayers waiting until the eleventh hour. Unfortunately, this bodes well for the criminals looking to commit tax identity theft by using filers' Social Security numbers (SSNs) to beat them to the punch and file "on their behalf" (gee, thanks) in order to collect the refunds. (It's funny how scammers never want to *pay* your taxes if you *owe,* though.) As the Federal Trade Commission (FTC) points out, "You may not find out [tax identity theft] has happened until you try to file your real tax return and the IRS rejects it as a duplicate filing." The good news? Just in time, the IRS has created Identity Theft Central--an online one-stop-shop offering advice on how to: steer clear of email phishing attempts (a common tactic used to steal your identity); secure your data and protect your computer and phone from criminals; determine if it's *really* the IRS contacting you (or, as is too often the case, *not*); and remediate the situation if you *do* become an identity theft victim, which, if you're a *SCAM GRAM* reader, shouldn't happen. You can also find out if you're eligible for an identity protection PIN--a six-digit number that makes it harder for criminals to pretend to be you. The best way to avoid tax identity theft is to file early. And if you're using the services of someone else to file, make sure that *they're* not a scammer: Learn about fraudulent preparer red flags, and how to check out a preparer's credentials, here. For more information on common tax scams, check out H&R Block's Tax Information Center.

The grift that keeps on growing

Booming breaches. The non-profit Identity Theft Resource Center (ITRC) has not only "reached a milestone" in the number of publicly disclosed data breaches it's tracked in the U.S. (over 10,000, by its count), it has also unleashed a report showing a disturbing 17% increase from 2018 to 2019. Alongside these sorry stats, ITRC has set loose some good news: It appears that companies are doing a *much* better job of keeping your personally identifiable information from getting into the hands of criminals when their networks *are* breached, with 65% fewer "sensitive records" exposed over the same time frame. Worried that your data has been involved in a breach? (Hint: You should be.) ITRC's got a free app for you that even offers live chats with an advisor who can help you sort things out.

Legions of lockdowns. Ransomware attacks: The *New York Times* has ranked these computer network captures as "among the the scariest and

most costly online assaults." And they're growing at an alarming rate. In a ransomware scenario, hackers take over an organization or government's computer files and lock that party's own administrators out, so that they cannot access their customer, employee, public or other files or even their payment systems. In the vast majority of cases, the only way a target can regain access to the critical data needed to conduct their business is to pay a ransom, and, sadly, more often than not, they do. In addition to a 41%increase in the number of ransomware attacks from 2018 to 2019, the ransoms criminals are demanding have grown by leaps and bounds, typically ranging from tens of thousands to millions of dollars. If you're a small business owner or city administrator, you need to be particularly concerned about how a ransomware attack could ruin you, and take the steps to keep it from happening. (The old adage "An ounce of prevention is worth a pound of cure" *really* applies here.)

Soaring scams of all sorts. The Federal Trade Commission (FTC) last month released its most recent Sentinel Data Book, which compiles millions of consumer reports of fraud, identity theft and the like to reveal what's new, what's trending and what to watch out for each year. Perhaps not surprisingly, imposter scams came in at No. 1, based on the latest 2019 data analyzed, with consumers losing around $667 million to criminals pretending to be a government official, an online love interest, a distressed relative, a customer support tech, or, well, the sky's the limit! Credit card fraud has been lucrative for scammers as well. More than 271,000 consumers complained to the FTC that new accounts had been opened in their names, or that someone misused their existing cards. Perhaps most surprisingly (depending on your age and outlook), the data book reveals that 20-somethings report losing money to fraud *way* more than septuagenarians, at a rate of 33% to 13%! Also shocking: Florida *didn't* come in first with regard to having the highest rate of statewide fraud. It came in second (beat out by Nevada for the top slot).

Tips!

Let it lapse. In addition to the usual obnoxious "Social Security Administration" robocalls, this month many of us have *also* received obnoxious warranty robocalls claiming we "should have received mail" to extend our coverage before our vehicle "reaches a certain mileage." The recordings say the alleged warranty has "expired" or is "about to expire." There are a few variations on this tired scam; the Federal Communications Commission (FCC) has posted another from an obvious bot named "Shasta"--or "Shuh-sta," as it mispronounces the name. Shuh-sta claims she's with a specific automaker (Volkswagen), which makes her call more dangerous--if scammers hit the mark and guess or know your auto info or details about your warranty, the con can be much more convincing. Don't fall for it: If you're

wondering if the warranty's up, *you* should initiate contact with the dealership from which you bought the car (or another same-make dealership). (Head's up: You'll likely need to provide the VIN number, which can be found on your auto insurance documents or on the driver's side of your vehicle's dashboard.) And be aware that even if the manufacturer's warranty has expired, third-party extended warranties usually are a waste of money.

Dirty deeds, done dirt cheap. As our email inboxes become increasingly stuffed with spammy messages, found-in-the-mailbox paper communications are an inexpensive--and often more credible-seeming--way for scammers to reach us with their malevolent messaging. We recently alerted consumers to the latest mass mailing: "Offers" to sell homeowners copies of their own property deeds. The official-looking solicitations would have the recipients believe that the government requires that they immediately purchase certified copies of the legal documents (*wrong!*). Often, the mailings state that homeowners must pay outrageous amounts of money for the copies, which, in actuality, can be obtained from local government for a nominal fee, if you need them.

'McSting' catches shady scammer. Looking for something new to binge watch? HBO's docuseries *McMillions* makes for some entertaining viewing. This is primarily due to its main interview subject, FBI Special Agent Doug Matthews, who is basically the human equivalent of a particularly excitable and gregarious golden retriever. Matthew's candor (uncharacteristic for an FBI agent) regarding the infamous McDonald's monopoly game scam--which anyone who collected the game pieces in the '90s or early 2000s was marginally involved in--and the inner workings of the FBI taskforce charged with taking the man behind the operation down has set the internet a'chattering. "Anytime he's on screen to make fun of a particularly sweaty winner or brag about his golden [McDonald's-yellow] suit, this already bonkers story crackles," *Decider* writes.

Louder for the people in the back. The FTC's new alert pulls no punches, stating: "If you remember nothing else from this blog post, remember this: Sellers that peddle cures must have scientific proof to back up their claims." Preach! Regrettably for it, however, the company that claimed its ReJuvenation pills could treat everything from brain damage to blindness by increasing a consumer's stem cells paid no heed to the FTC's "reminders," resulting in the FTC laying down the law. The company has now been directed to pay $660,000 to the consumers it defrauded. Boss Bureau of Consumer Protection Director Andrew Smith laid it out for criminal companies: "If you make [ReJuvenation's] kinds of claims, you'd better have credible science to back it up or the FTC is coming for you." Boom! We still have one question for the FTC though: When are you going after Goop? Gwyneth's tone-deaf "wellness" brand is *still* not hearing you.

Not so sweet. The National Consumers League's latest alert on sugar daddy/sugar baby arrangements may vindicate the cynics who steered clear of flowers, candy and sentimentality this Valentine's Day. Contrary to how it's supposed to work, "sugar babies"--younger people looking for money and gifts in exchange for bestowing their, uh, affections on older, wealthier people--are ending up the ones who pay in what ends up being a *very* dysfunctional relationship. Scammers have created convincing sugar daddy (and sugar momma--hellooo, Mrs. Robinson!) profiles on websites like Seeking.com, which has a whopping 4 million users looking for "love"--and maybe Daddy Warbucks. The way the scammers work is kind of complicated; it involves them fooling the sugar babies into believing they've paid off their credit card debt before they coerce them (the sugar babies) into sending gift cards in return (to show their "gratitude"). Read NCL's description if you're inclined towards these not-so-saccharine scenarios.

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

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