Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • September 2019 • 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!

Where's Will though?

Robocalls in general are a scourge on society (with Americans receiving a whopping 47 billion last year alone!), but one type in particular stands out for its persistent and widespread nature. The call is from a casual-seeming dude named "Will," who offers to "make an offer on your property, if you've thought about selling." Will just bought a property near you, you see, and he'd "love to hear from you." Unlike the robotic voice in many robocalls, Will sounds like a real person—someone you'd meet at a backyard BBQ—and he's just trying to help you out, bro. As a *Philadelphia Inquirer* reporter points out, however, "Will" is basically an automated audio adaptation of a "We Buy Houses" sign, which, like the unsolicited robocalls, are also illegal, and also prey on vulnerable people (particularly those in bad financial situations). So what happened when the *Inquirer* reporter called back and asked to speak with Will? He discovered an underground network of scammers, many named…"Pat!" (When the reporter asked why they were all named "Pat," one said: "We're all Pat. We all go by Pat to keep it easy.") [Shudder] Regardless of whether they call themselves Will or Pat, this borg-like hive mind wants to buy your house for next to nothing. What can you do? For one, hang up if you get a call from "the Collective." Do not assimilate. Instead, join the Do Not Call Registry. And click here for more ideas, including call-blocking tools/apps and smartphone settings to stop Will and his ilk. Whatever you do, don't hitch your wagon (or house) to Will!

Don't call me, I'll call you

AARP, the Better Business Bureau (BBB) *and* the Federal Communications Commission (FCC) are *all* warning about a rise in Medicare scams, particularly since the Centers for Medicare and Medicaid Services recently sent Medicare beneficiaries updated cards that are supposed to be *more* fraudproof. New cards, however, equate to new opportunities for criminals, who are desperate to learn the cards' random number combos. (The cards, wisely, no longer contain Social Security numbers.) Medicare can be a cash cow for con artists, who commit identity theft and make medical claims in the names of elderly cardholders like Judy Craig, a Memphis-based cancer survivor who was promised a "free home cancer detection kit" if she would turn over her Medicare number. Craig knew better (maybe she's a SCAM GRAM reader?) and shut the argumentative scammer down, telling the caller she'd give them exactly "nothing" before hanging up the phone. It's important to know that Medicare will never contact you for your number (unless you asked for and are expecting a call back), and they certainly aren't trying to sell you products or services. Your motto with Medicare should be "Don't call me, I'll call you." If you're not sure about the origin of a call (and remember, scammers can spoof the incoming call, making it appear that it comes from a legitimate Medicare office number), hang up and call back the *real* office at 800-MEDICARE (800-633-4227), or click here for the official (dot)gov webpage.

Tried and true

Winners and losers. The old adage "Gotta spend money to make money" simply isn't true in tried-and-true sweepstakes and lottery scams. These types of cons are among the "Top 10" reported to the FTC because criminals apparently have an easy time convincing people to fork over cash for big "winnings." So how can you avoid becoming a statistic? Alarm bells should go off any time you're being told you've got to *pay* to collect—whether the source appears to be Publishers Clearing House or a lucky immigrant who needs your (financial help) to cash her lottery ticket. Remember: You only *lose* when you pay to win.

Caught with your pants down. Perhaps you've already received one of the many creepy emails in circulation featuring your usernames and passwords (no doubt acquired in a data breach) that threaten to expose internet users' online, uh, proclivities unless they fork over some Bitcoins. If so, your pulse probably began racing faster than it would have if you were doing what the email accuses you of doing, which, according to the BBB, includes "watching or utilizing pornography." Scammers will claim that they've hacked your webcam, and often threaten to "reveal images and videos" of your private life. Unfortunately, recipients have been paying up. Knowing is half the battle though, and now you know: If one of these "sextortion" attempts crosses your desk, you can proudly declare "Ain't no shame in my game!" and report it to the FBI's Internet Crime Complaint Center.

Leaving destruction in their wake. It's hurricane season, and the news media are already warning about the predictable but devastating impact of scams post-Dorian. Every time a natural disaster strikes, scammers (opportunists that they are) are on the ground ready to

offer their "services," including home repair, food and water, housing and, of course, charity work (they just need donations). Callers may claim to be with your insurance company or a government office offering aid. Sometimes they'll even pretend to be a natural disaster victim, taking to social media with a bogus sob story. While no one can be as prepared as this guy, you *can* click here for more info or to report any suspicious post-disaster frauds.

Nothing's certain but death and taxes (and tax scams). Tax-related funny business has been occurring for millennia, and although it's not currently tax season, as an IRS official pointed out, "tax scams are a year-round business for thieves." So, what is it *this* time? If you see an email with the phrases "Automatic Income Tax Reminder" or "Electronic Tax Return Reminder" in the headline, report it immediately to the IRS; it contains links that direct those naive enough to click to imposter IRS.gov websites. Attempting to input a temporary password into the website will lead to malicious files downloaded to your computer, and that malware could steal your information and/or take control of your machine. While the common tax scam evolves each year, one thing remains the same: The IRS will never send you emails about tax refunds.

Tips!

- **Pretty sneaky, sis.** Scammers are connecting directly to the digital calendars of computer, tablet and smartphone users, knowing that many have their email accounts set to automatically add calendar invites. They're not syncing up because they want to meet up; they want you to click on the links they've added to the events they've created (and they know that when you're confused about an event, you are more likely to click). Unfortunately, there's no additional info to be had by clicking, only malware that automatically downloads to your computer, or a visit to a bogus website looking to obtain your personal/financial info. Fortunately, KrebsOnSecurity has detailed instructions on how to stop the events from auto-adding via Outlook and Apple's calendar settings. (This can also be done directly through email services like Gmail.)

- **All your base are belong to us.** Not only are our smart-home devices eavesdropping, they're also sending us straight into the carefully laid traps of tricksters, who have taken over the internet by substituting their own phone numbers for those of legitimate businesses (or just making up nonsense businesses that they can push to the top of search engine results). This has been a problem for some time, when people have performed Google searches for tech support, customer service, home repair companies, locksmiths and the like (and gotten fake results). But now, even an innocuous "Alexa, call Verizon tech support" could dial out to one of these fake numbers (and a clever criminal "representative" on the line, looking to coax out your credit card number). Unfortunately, for now, the only way to handle the hoax is to do your homework (instead of delegating it to a digital assistant that's simply dialing the first number in a search algorithm).

They want to do WHAT?! We were shocked to hear that, under Trump administration-appointed leadership, the Consumer Financial Protection Bureau (the CFPB, which was created to *protect* consumers like you) has proposed to not only allow debt collectors (even scam "collectors") to call and text you relentlessly, but *also* to allow them to send emails and texts with links to webpages. Anyone who's been paying attention knows why this is a horrible idea: It's giving criminals the green light to imitate debt collectors and embed malware in the links, send recipients off to imposter websites, etc. If the CFPB's proposal goes through, you'll have no way of knowing if a link *does* happen to be legit (which means you won't click for info about debts you owe, or to request that, under the law, collectors stop harassing you, etc.). You only have a few days (through Sept. 18) to tell the CFPB that its proposal is the *worst idea ever*. The good news? We've made it super convenient to give the agency an earful!

#TimesUp. TikTok, a video-streaming app that allows its approximately 1 billion users (mainly children to teens) to upload their own content, is becoming inundated with scams, including fraudsters posting videos of attractive young women or impersonating internet famous "TikTokers" who then redirect targets to Snapchat, Instagram or adult "dating" sites, where it's easier to part them from their digital dollars. Scammers get paid $1-$3 for every "lead" they send to the sites, and around 60¢ for every useless "app" they convince victims to download. While video aficionados can click the three little dots in the top right of the TikTok app to report scams, Common Sense Media recommends that parents restrict children under 16 from downloading TikTok in the first place. Time to start monitoring your kid's in-app activities? You may want to install a "parental control" app of your own (but first, do your research to make sure the one you're considering monitors the apps you're worried about, on the device your child uses).

Glorifying grift. Pop culture's fascination with fraud continues. Showtime is featuring Kirsten Dunst and a—spoiler alert—quickly disposed-of Alexander Skarsgård in *On Becoming a God in Central Florida*, a wild, all-American dark comedy that makes you really hate pyramid schemes (and those at the top of them). Dunst plays Krystal, a desperate woman who "inherits" a multi-level marketing "empire" that her husband (played by Skarsgård, in an uncharacteristically *un*attractive role) mismanaged before his untimely death (a death that warrants watching the first episode alone). Then there's music: In the last month, blogs like Stereogum and Pitchfork have highlighted "scam-rap," with Stereogum going so far as to call it "the future" of music. There's one problem, however: The performers could end up behind bars due to the very specific admissions contained in their raps (assuming what they're saying is legit). Some already have (like JT, from the popular City Girls group, who went to prison for credit card fraud), and some may be, like Detroit teen TeeJayX6, who advises listeners to use fake credit cards to purchase electronics at Walmart (like he claims to have done), download the Tor browser to conduct illegal activity on the Dark Web, and use money-transfer apps like Zelle and Venmo to con victims.

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.