Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • February 2017 • 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!

Can you hear me now?

"Can you hear me now?" These words might be the *last* you hear before you open yourself up to an insidious scam that's plaguing the nation. According to the Better Business Bureau, if you answer "yes" to the crafty query, your recorded answer could be used against you "to sign you up for a product or service and then demand payment." If you refuse to pay up, "the caller may produce your recorded 'yes' response to confirm your purchase agreement." The truly tricky thing about this scam is that most anyone is likely to automatically respond "yes" in an effort to reassure a questioning caller. And sometimes "Can you hear me?" is replaced by another question designed to elicit an affirmative response (for instance, "Are you the homeowner?" or "Are you over 18?"). Recently, scammers have also been "identifying" themselves first—as government employees, cruise line reps or home security agents (seemingly reputable, non-threatening entities). And it's not just your voice that scammers are after; it's also your digits. If you so much as press a button when prompted, you're reassuring robocallers and other crooks that you have an active number. Once you do that, you've signed yourself up for even more phone-stalking (a vicious cycle if we've ever heard of one). So what to do? Don't pick up the phone if you don't recognize the number. If you *do* pick up, don't answer any questions from an unknown source. Make the words of Super Bowl halftime star Lady Gaga your motto when it comes to phone scammers: "Call all you want but there's no one home. And you're not gonna reach my telephone."

Not the beer!

It's bad enough when scammers target for-profit corporations; it's even worse when they begin attacking public schools, tribal organizations, non-profits and, in a blow to beer lovers everywhere, brewhouses. Unfortunately, the W-2 scam we wrote about months ago has spread like wildfire and is now afflicting the aforementioned innocents. According to the Internal Revenue Service (IRS), the W-2 debacle is "one of the most dangerous email phishing scams we've seen in a long time. It can result in the large-scale theft of

sensitive data that criminals can use to commit various crimes, including filing fraudulent tax returns. We need everyone's help to turn the tide against this scheme." So how does it work? The scammers usually contact someone in the organization's payroll or HR department, pretending to be a colleague of consequence (like the executive director or another senior manager). They demand the W-2s for tax purposes and, just like that, the organization has opened up hundreds, perhaps thousands, of its employees to identity theft and tax fraud (the scammers use the employee's personal info to file taxes "on their behalf"—gee, thanks a lot—and to, of course, collect the refund). And if innocent school districts being subjected to such a scam doesn't tug at your heartstrings, then perhaps the risk to a brewhouse will: Let's hope Scotty's Brewhouse (a popular chain in Indiana) won't be brought down by scammers who, according to a tearful Scotty, collected 4,000 of his employee W-2s by sending his payroll manager an email from an address that appeared to be from him. "You just never think it's going to happen to you," Scotty said. "And then it does."

Facebook fakes

Facebook scams are running rampant right now, so we've dedicated this entry to detailing the top ones targeting *you*: the social media addict. It's bad enough that the site has been inundated with fake news; now there are fake friends, fake customer support numbers and even, perhaps, a fake YOU floating around! Let's start with the fake friends: Cloning a Facebook user's account is relatively easy for scammers. If you get a friend request from someone you're already friends with, instead of wondering if they've unfriended you and rushing to accept them back into your online life, question the validity of the account (and search to see if you are still actually friends with the real person). It gets worse: These cloned "friends" might even PM (private message) you asking for money. And here's the creepy part: YOU might be the cloned account. That's right, your family member or bestie could think they're helping you out by sending you cash, only to fall prey to a scammer. (So you should help your pals out by sending them this article first—because friends don't let friends accept cloned friends.) So, what if you want to complain to Facebook's customer service about such doppelgangery? Just know that the number that pops up when you run a Google search for "Facebook customer service" is a fake as well. Instead of reaching Facebook, you'll reach a scammer who instructs you to buy a gift card so that he can drain the funds—thanks for making a bad situation worse, scammer! The only way to reach Facebook (unless you personally know Mark Zuckerberg) is through its online help center. And while you can report your suspicions, don't expect a lot of help. Recently, one staff member reported a fake profile, and Facebook advised her to "Block him." Stay vigilant!

Home UNimprovement

High-pressure tactics. If someone comes to your house, unsolicited, offering to perform home improvement work, don't let them do it without taking the time to research the legitimacy of the business (no matter how much that loose shingle has been driving you crazy). Take it from this woman, who paid a couple of men to pressure wash her house, only to later find out that they were unlicensed and uninsured. (Meaning: If they hurt themselves on her property or damaged it in any way, she wouldn't have been compensated and could even have been subject to legal action.)

Raise the roof. Roofing scams seem to be all the rage these days. Why? Because *you* can't really get up there (unless you've got wings or a very long ladder), so crooked roofers can quote you exorbitant prices

for unnecessary repairs that they claim "need fixing" ASAP. If you're worried about a leaky roof or clogged gutter, be wary of randos who show up at your door offering to ease your anxieties. Learn from this unfortunate couple; they enlisted the "help" of an unlicensed contractor who only made things worse.

It's electric! Brrr…it's cold out there (and downright miserable if you don't have working heat or electricity). But don't be so desperate to stave off an indoor chill that you fall prey to fraudsters calling and threatening to turn off the heat if you don't pay up. And while we know it's expensive to keep your home at a comfortable temperature this time of year, don't give personal or financial info to callers who claim they can lower your utility bills.

Tips!

- **You want me to put that WHERE?!** Actress Gwyneth Paltrow has had some weird ideas about what women should do with their nether regions, but this one has us egg-stremely confused. The celebrity's website is now selling $66 jade "eggs," and, well, we'll let the *Washington Post* tell you where (not) to stick 'em. The *Post* interviewed a gynecologist who strongly advised against using the stones, which Paltrow's site preposterously claims will make you more attractive, balance your hormones, "tighten and tone" and more.

- **Too many phish in the sea.** PayPal, Gmail *and* Netflix are *all* experiencing similar scams right now, in which a fake email and/or website (that closely resembles each company's real one) is employed to "phish" for users' private information. The email/site prompts the user to log in (thereby giving up their password) or to enter account information (thereby giving up their financial or identity info). If you're interacting with what seems like a company's official online presence, pay close attention to the sender and/or the URL (web address) to make sure it's really them.

- **Making scammers great again.** The *New York Times* has written a strong opinion piece about the risks inherent in the new administration's repeal of a law that forbids conflicts of interest in retirement investing. (The common-sense law would, for instance, keep your financial adviser from giving you bad retirement advice just because he or she received kickbacks or other benefits from selling the risky or sketchy investments.) "So, what's motivating the attack on financial regulation?" the *Times* asks. "Well, there's a lot of money at stake—money that the financial industry has been extracting from unwitting, unprotected consumers." Draining the swamp, eh?

- **Bills, bills, bills.** While Destiny's Child was all about someone else paying the bills, the Federal Trade Commission seems to disagree. The watchdog agency is warning you to be wary of triflin' good-for-nothing types of scammers who claim to be with a government program that will pay your bills (for a fee, of course).

- **Wire you helping scammers?** It turns out that money transmitter Western Union knew all along that it was *the* go-to company for wiring funds to scammers. It just admitted that it "allowed criminals to use its global money transfer service to carry out 'hundreds of thousands' of scams" (and had received around 550,000 customer complaints on this very issue over the last decade or so). Transmit this: Western Union has been ordered to pay its victims $586 million.

- **Attention Walmart shoppers!** Walmart recently launched a helpful website that outlines some of the

latest and not-so-greatest scams and frauds. If you've ever wondered what the difference between phishing, vishing and smishing is, then you're going to the right place. The retail giant—and its staff—have been ramping up efforts to protect consumers from evil-doers, with one perceptive New York employee even preventing an elderly couple from falling prey to a $2,500 gift card scam!

Suspicious snail mail. If you owe student loan debt, you may have already seen a letter in your mailbox purporting to be from the U.S. Department of Education (ED). These misleading mailings, however, are actually from for-profit marketers looking to sell you expensive repayment plans—plans that you shouldn't have to pay for in the first place (they're typically free through the ED). The senders may also be looking to steal your identity (particularly if they ask for your Federal Student Aid ID, which you should *never* divulge to anyone other than the education department).

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.
