Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • February 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!

You're dead to me

How low can scammers go? Try this: scammers who try to cash in on the dead. They troll obits to find victims and then open new credit cards in the deceased person's name or use a phishing scheme to pressure a grieving spouse into paying for a bogus benefit. Or say it's a call from an insurance company to reinstate an expired life insurance policy if survivors just make a payment to cover the last few years of unpaid premiums. Or try to rent the deceased's vacant home to unsuspecting victims. What to do? Limit the information you put in your loved one's obituary or post online, including on social media. Notify the Social Security Administration of the death if the funeral home hasn't done so. As soon as you can, alert major credit reporting agencies about the death. Notify financial institutions, insurers and taxing authorities that the accountholder has died. The AARP and the FBI offer tips to survivors.

Like a Virgin?

Just because you're a billionaire doesn't mean scam artists aren't after you too. Sir Richard Branson, founder of Virgin Airways and other enterprises, told Reuters he was targeted by a con artist posing as former British Defense Minister Michael Fallon, who tried to get $5 million in a "secret" ransom payment. Branson said the caller sounded like Fallon and had a rather convincing story that the government was asking "four or five" billionaires to pony up a $5 million ransom to rescue a senior diplomat because the UK government wasn't allowed to pay ransoms. Branson didn't fall for it but a close friend stateside got the same call, this time from "Branson," and he did send money to the scam artists. As to the rest of us, know that "virtual kidnapping" schemes have targeted people in all walks of life. Last fall the FBI warned people to "Beware of Virtual Kidnapping for Ransom Schemes" in a podcast. The FBI said it "wants to prevent you and your loved ones from becoming victims" of this cruel extortion scam.

Hooked on Netflix?

If you get an email that appears to be from the popular streaming video service, it could a "phisherman" reeling you in! You might be asked to click on a link to verify or update payment information, but you're really going to a convincing "lookalike" website aiming to steal your credit card number and password. Now Consumer Action's warning about a Spanish version of the email. (English version.) Don't get hooked! (*¡No te dejes enganchar!*)

Angels in disguise

Some of the most inspiring human interest stories we've heard feature people who helped total strangers avoid fraud. Among them is the quick-thinking Walmart clerk who saved a New Jersey grandfather from wiring money to a scammer. And the people in the USA Today story by a son whose dad suffered from dementia. He said, "Dad had a couple angels looking out for him before we fully realized just how bad it had gotten...There was the drug store clerk that stopped dad from mailing a Green Dot card, and a post office clerk and her manager who stopped him from sending a large check through the mail." Also, the quick-thinking postal employees who stopped a scam and saved an elderly Texas man thousands of dollars. These are the kinds of "busybodies" we like!

Sweeping away our trust!

No prize for you! The Consumer Financial Protection Bureau (CFPB) sent an email from its Office for Older Americans last month warning that office employees are "never going to call you to confirm that you have won a lottery or sweepstakes." Apparently the Bureau learned that the name of employee Stacy Canan had been used in "an elaborate imposter scam." An imposter scam happens when a criminal tricks you by claiming to be someone you trust. Lottery scams make money by asking victims to pay "shipping and handling" to get their winnings, which (of course) don't exist. While we think all SCAM GRAM readers would've spotted this one a mile away, go ahead and spread Stacy's message: "CFPB staff do not collect information about lottery or sweepstakes winnings, nor do we call people to confirm winnings." If you get an email from Stacy, report it!

Congratulations! (Or not.) A SCAM GRAM reader wrote us to ask if we thought her online sweepstakes game "addiction" might have resulted in some email invoices she received for stuff she never ordered. (Well, yes...) What we can say about sweepstakes is that the odds are definitely NOT in your favor. Even most legitimate sweepstakes exist only to collect information about you that can be sold to marketers. Many are outright scams. And, perhaps even worse, people who are obsessed with online sweepstakes may succumb to a gambling addiction. It's a good idea to know the warning signs that sweepstakes and gambling are starting to take over your life.

Hall of shame. Scammers are constantly evolving their tactics to outsmart their victims and stay ahead of law enforcement. Our friends at the National Consumer League's Fraud.org just released the Top Ten Scams of 2017 to warn consumers what to watch out for. Number one is bogus merchandise offers on the internet, which accounted for nearly one-third (29.39%) of complaints received. Consumers didn't just lose chump change—one man lost more than $22,000 when he ordered animal feed from a scammer posing as a legitimate supplier. Other big ones that SCAM GRAM readers are no doubt familiar with: fake check

scams, tech support hustles, sweepstakes fraud and sweetheart swindles. Read 'em and weep.

Tips!

Shut it! The threat of a government shutdown won't shut down scammers determined to use it as a ploy to steal your money. Big news event, like immigration actions, natural disaster or threats to Medicare funding? Shysters see it as an excuse to scare you or pull at your heartstrings. The approach could be a phishing email or a telephone call to get you to "verify" your personal information or make a charitable donation. But, dear SCAM GRAM readers, we know you're too smart for this!

Powerful knowledge. The phone rings, and a caller says she's from your electric company: You haven't paid the bill and your power is about to be cut off. Enough to get anyone all het up. Consumer Action recently warned consumers about scammers who claim to be representatives of the utility company. (Spanish alert.) They even spoof utility company telephone numbers with the company's name. If you get a call like this, stay calm—in all likelihood, it's a scam.

This is taxing. With W-2s and 1040s on our minds, Consumer Action's January Hotline Chronicles discussed how to protect yourself from tax scams and refund fraud.

Crooked by the 'book? Facecrooks [dot] com says its mission is to monitor and chronicle the seedy, unsavory and sinister side of social media. It does so with a Facebook page full of warnings about social media scams and hoaxes. If you "like" the page, you'll learn about all manner of threats to your privacy and online safety. This warrants at least one smiley face emoji, doesn't it?

Got your number. Scammers are using auto-dialers to call cell phone numbers and let the phone ring once—just enough for a missed call message to pop up. They hope you'll call back out of curiosity. If you do, you might be put on hold and slammed with some hefty international rates. The calls are from numbers that look like they're from inside the U.S., but are really international numbers, often based in the Caribbean. These area codes include: 268, 284, 473, 664, 649, 767, 809, 829, 849 and 876.

No safe dosage. Ever fantasize about giving phone scammers a taste of their own medicine, playing a trick on them or stringing them along just for kicks? You can revel in that fantasy all you want, but just don't do it! Pennsylvania's WGAL News reported that an Alabama man decided to purposely waste a phone scammer's time over a few days. The scammer was not amused and exacted a quick revenge by "swatting" the consumer—falsely reporting to police that a shooter was at the man's home, leading a SWAT team to surround the home. The best medicine you can give a scammer is to just hang up.

World Cup feint. Imagine traveling all the way to Moscow this summer, World Cup tickets in hand, and being told to go away because your tickets are fake. Soccer fans shopping for World Cup tickets have a few obstructions to avoid, including fake, invalid and undelivered tickets. Avoid a foul by following a few tips from the Federal Trade Commission, and remember this key fact: FIFA.com is the only official source for World Cup tickets. Hopefully, the only cries you'll hear on match day will be *¡Goooooool!, Toooooor!, Buuuuuut!*, etc.

Tech support scam 'payback'. The Federal Trade Commission is mailing refund checks totaling more than $668,000 to victims of a tech support scam. Big Dog Solutions LLC (aka Help Desk National and Help

Desk Global) lost its bark in the settlement with the FTC and Florida Attorney General: It's been banned from marketing or providing tech support products or services in the future. Consumers who have questions about the refunds can call Rust Consulting at 877-309-1959.

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.