Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • June 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!

Waste of a router

If you thought President Trump was the only one having trouble with the Russians, think again! Several weeks ago, the FBI warned Americans that Russian hackers had infiltrated their home and office routers with a sophisticated type of malware (malicious software) called VPNFilter. That this type of malware can collect personal and financial information passing through your router is no surprise. So what's the big deal? Apparently, VPNFilter can even modify the content of websites you access. (For instance, the hackers could siphon money from your bank account and make it appear on the screen like your online balance remained as high as it was prior to them stealing the funds.) But, according to one software analyst, the *really* big deal is that the code found in VPNFilter has "overlapped with some other threats that were used a couple of years ago in Ukraine with the cyberattack that took down [that country's] power grid." Fortunately, the power outages in Ukraine only lasted an hour, but any sort of attack on critical U.S. infrastructure could lead to widespread chaos (imagine how you feel when your internet goes out for even a minute!). The FBI tells the public to simply reboot their routers, but experts are saying this isn't enough to destroy the virus. Meanwhile, it's proliferating. Installing the latest firmware, performing a factory reset (which you can Google how to do based on your brand of router) and creating a new password is more likely to work, but you're still playing Russian roulette with your router. The one thing that will *definitely* work? Trashing your router and getting a new one.

No one wins

The Better Business Bureau (BBB) just released a study relevant to all who wanna get rich quick (in other words, all of us). While anyone who believes it's "their turn to win" can fall prey, *Sweepstakes, Lottery and*

Prize Scams reveals how older people (aged 65-74) constitute the majority of victims (particularly if they are suffering from dementia or Alzheimer's). The report analyzed the more than 2,800 scams reported to the BBB's Scam Tracker tool in 2017 and determined that victims suffered median losses of $500 (mostly through wire transfers). And lest you lack sympathy, the report states that: "Interviews with victims show that they are not overcome with greed. Rather, scammers encourage them to think about the nice things they can do for their families or communities with the money." Aw, shucks. And it's easy to become prey when, "The crooks are professionals… They have scripted answers for any question posed to them." You've been warned. According to the study, a whopping one-third of the targets are contacted through social media (often Facebook) to "claim their prize." Interestingly, a lot of the actual *phone* calls from scammers are originating from Jamaica, where actual gang wars (!!) have erupted over the boatloads of dirty money flowing in to the Caribbean island (and here we thought sunscreen-slathered tourists pouring off mega-ships were the worst *en masse* arrivals). Fear not, though, AARP goes into detail on how to avoid prize scams, with an emphasis on the motto: If you have to pay to receive it, don't believe it!

Home invasions!

Alexa, butt out. From smart TVs to children's toys, by now you've probably heard about consumer products "spying" on your family and doing bad things with the collected data. (And if you haven't, check out what Amazon's Alexa did after eavesdropping on this couple.) Consumer groups are pushing for legislation that would require these types of products to come with privacy protections. In particular, a California law (which could, with any luck, become a model for national laws) would require products to A) warn users (at the point of sale) that the products can collect sensitive user data, B) obtain consent from users to gather said data and C) notify users when the devices are in the act of gathering it. Contact your members of Congress and ask them to introduce similar legislation!

Some pal! As Fraud.org points out, those of us looking to "declutter our homes and earn some extra cash" by listing our stuff online should watch out for the PayPal "check is in the mail" scam. This con occurs when a bogus buyer creates a fake PayPal email "confirming" that money for the listed item has ended up in the seller's PayPal account. Sometimes the emails say that the item must be shipped *prior* to the payment hitting the account. And sometimes fraudsters will simply send an email saying that they overpaid for an item (that they never actually paid for) and you owe them "money back." Beware spoofed emails and always log into your PayPal account to see what's up.

Processor pot o' gold! All you Bitcoin aficionados, watch out! Cryptojacking is a "thing" now, and it occurs when a scammer gains access to all the pot of cryptocurrency you've been hoarding on your computer like a digital leprechaun. The Federal Trade Commission (FTC) describes how it goes down: "Scammers can use malicious code embedded in a website or an ad to infect your device. Then they can help themselves to your device's processor without you even knowing." This code "mines" your computer for the digital dollars, which the scammers then steal and convert into real dollars. According to the FTC, one of the signs that you may have mining software running in the background is slow device performance. Keep your coins safe by following the FTC's advice!

Tips!

- **Clean up your act.** We'd like to believe that ActBlue, the online fundraising platform that helps leftist political candidates and non-profits raise money from small-dollar donors, hasn't been bilking cash from its base. Unfortunately, one reader wrote in to say, "They ask for a 10 percent or so one-time donation, then they switch it to recurring monthly donations without your consent….Even after complaining, they keep charging your credit card!" We looked into the phenomenon and determined that this reader is far from the only one experiencing it. Whether intentional or not, as one TruthOut author wrote, "the result of ActBlue's [ongoing] operational failures may lead to cynicism and anger—causing serious damage to the grassroots fundraising activities of Democratic candidates." This author felt better when she was able to sign in to her ActBlue account and see that stopping recurring donations *is* an option, as is deleting stored credit card info. We advise you to do the same!

- **A date with disaster.** Facebook is joining the fray of online dating services, promising to help would-be soulmates find each other. Facebook Dating, as it will be called (zero points for creativity), relies heavily on not only your existing Facebook data, but also on your answers to questions that will likely range from silly to seriously invasive. And since we all know how great Facebook's been about guarding our personal data [sarcasm], many are pointing out that this is a date with disaster—the *Washington Post* called the service "the chance to meet the catfisher, advertiser or scammer of your dreams." Romance scams leading to financial fraud are already a huge problem for Facebook, so we'll take it slow and see where this new relationship goes…

- **Record robocalls!** If you're like us, you've been absolutely inundated with automated calls that appear to be local. You might even pick up, thinking it's the doctor's office or that awesome job you applied for last week. Unfortunately, it's a scammer on the other end of the line. Why does it seem like it's happening more and more (with more than half of these robocalls now coming from what appears to be a neighboring number)? As MarketWatch points out, "The more people that pick up these calls, the more lucrative it becomes for the scammers." The number of robocalls reached a record 3.36 billion in April. So what is an exasperated consumer to do? Contact the Federal Communications Commission (FCC) and tell it to preserve a strong Telephone Consumer Protection Act (so that it protects you from these types of scam calls and keeps scammers from leaving more obnoxious voicemails). And even though so many people dislike voicemails (leave a text!), just let it go to voicemail. If you do pick up the phone and hear someone you don't know speaking in Chinese or asking "Can you hear me?," you definitely want to hang up right away: These are two huge scams.

- **Don't be a Target.** If someone sends you a text or a social media message (even if they appear to be a "friend") telling you to text the word "TARGET" to get a free gift card to the big red retailer, don't do it. No amount of dish soap, inexpensive (and really cute, actually) summer clothes, cat food and cheap wine is worth becoming a target for even more scammers, compromising your social media account or entering your credit card or personal info into whatever website the text you receive back prompts you to visit. These types of coupon scams are becoming increasingly popular. One minute it's $100 for Walmart; the next, it's $50 for Home Depot. But the only thing you'll be buying is misery!

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.