Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • March 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!

'Dirty Dozen' tax scams

Tax time is bad enough without having to worry about scams too, but, unfortunately, the IRS says they peak during tax-filing season. Crooks are out to steal your personal information, scam you out of money or talk you into engaging in questionable tax behavior. From fake charities to phishing to phone fraud, taxpayers need to stay on their toes. This year, many of the scammers are leading with "tax reform"-related information to make their incursions more legit. The IRS has added some new scams to its 2017 list.

Here's your refund!

Thieves are using phishing and social engineering schemes to steal clients' information from tax preparers, then filing fraudulent tax returns and having the refunds sent to the taxpayers' real bank accounts. Then the scammers, posing as IRS agents, call the taxpayer to say the refund was in error and give instructions on how to "return" the money—by delivering it right into the scammers' hands. If this happens to you, this Forbes story explains what to do and how to return the funds.

Phantom taxpayers

The IRS urges people to file their returns as soon as possible to avoid having someone else file in your name and steal your refund. But some taxpayers have to wait until mid-March or later for tax paperwork such as K-1s. One way to monitor what's going on in the meantime is to sign up for an online IRS account. Washington Post "Color of Money" guru Michelle Singletary explains the ins and outs of doing so (and there are several very important things to be aware of before you start, such as temporarily lifting an Experian credit freeze if you have one). Once the account is established, you can log in to check that a phantom taxpayer hasn't filed your return.

Wolf in sheep's clothing

TurboTax warns of a number of tax scams. One that caught our eye (and we hope doesn't catch yours!) is scammers who pose as legitimate tax preparers or professionals, but actually intend to steal your money. Victims are often people who don't speak English well or don't understand the U.S. tax system. These nefarious individuals take a large fee for their "services" and often inflate deductions with phony benefits or tax credits, and then have the refund forwarded to accounts they control. Anyone with a Preparer Tax Identification Number (PTIN) can prepare a tax return, so we suggest taking some steps to find a good tax preparer. The Washington Post and the Better Business Bureau have some tips. And the IRS has a public directory allowing you to validate credentials for certain (but not all) tax professionals. California, Maryland, Nevada, New York and Oregon have standards for certain tax preparers.

Sharing our secrets

Don't keep this a secret! Phony modeling agency scouts are pretending to look for Victoria's Secret models and, according to the AP, recently targeted University of Nevada students on Instagram. No matter how good you look in your tighty-whities, we suggest you heed the advice offered by Model Scouts (a modeling agency impersonated by scammers in the past): Be aware that modeling agents will rarely, if ever, use social media to search for models; contact the modeling agency directly to verify any communications; and don't respond to requests for photos in your underwear or—this should go without saying—your birthday suit! Police also recommend reporting the matter to law enforcement and to the company that purportedly needs models.

Shhh, shop—till the shoe drops. File this under "too good to be true": an offer to be a "secret shopper" and get paid for trolling retailers and purchasing products. Strange how if such jobs are available, why everyone doesn't have such a lucrative gig! While a rare few real "mystery shopper" opportunities might exist, we feel safe to say that the vast majority of such ads, emails, letters and online posts are bogus. (Even the Mystery Shopping Professionals Association (MSPA) industry group warns of rampant scams.) Often, victims are reeled in with "fake checks" they are asked to cash at their bank, wire a large portion of the money to someone and keep the rest. The check bounces and you're on the hook with your bank for the cash you got plus any non-sufficient funds fees. Or, you may be solicited by a company that says it can get you a secret shopper job (for a fee), "certify" you as a mystery shopper or give you access to a directory of mystery shopping companies. Say goodbye to your money. Run—to the mall if you want—but make sure you leave secret shopper offers in the dust.

I know what you did last summer (and last night!). Whether you've been good or bad, faithful or not, extortionists are sending out letters that threaten to reveal your deepest secrets, some of which may be a mystery even to you! These oh-so-kind-hearted scammers will spare you the embarrassment and other consequences of exposing your secrets, but only if you pay a "confidentiality fee." One such threat was directed to a happily married Oregon man demanding hush money of $3,600 in Bitcoin cryptocurrency. Fortunately, he didn't take the bait. The FBI recommends that internet users avoid sharing personal details online since they can be used to make tall tales sound more convincing. Complaints about these letters should be directed to the Internet Crime Complaint Center at www.ic3.gov.

Tips!

Share the wealth. We've heard of scammers who call to say we've won a lottery we never entered. A dishonest liquor store clerk in Florida played a different kind of lottery scam on a customer with a $600 winning ticket. The clerk told him he'd won $5 and pocketed $595. Only problem: The customer was an undercover agent with the Florida Lottery Commission. AARP advises you sign the back of your ticket as soon as you buy it because most state laws require payment to the person named on the winning ticket. Another tip from the Miami Herald: Use the electronic checkers near the lottery machine (if available in your state) to learn how much you won.

Not the right guy—definitely not the right guy! This scammer should have checked his mark beforehand. Instead he sent a bogus collection notice to consumer advocate Chris Elliott of Elliott.org. We bet the scammer's sorry he did. Elliott (or "Elliott Long") got a threatening email from Esper Law Firm saying he owed money for an online payday loan he never paid back. Starting off politely, Elliott replied they'd gotten the wrong guy. "Back at 'cha," came the scammer, threatening Elliott with a lawsuit and letting him know "Quick Payday is having 17 valid proof and three scientific proofs" the debt is valid. (Ooooh, scary! Gonna get me with your bad grammar?) "I'm not that guy," said Elliott, prompting a request from Esper to "Kindly send us your Photo ID to verify you." *Yeah, right!* More of this amusing back-and-forth can be found on Elliott's blog, along with all the red flags of a debt collection scam.

Can I get your number? Fraudsters are stealing cell phone numbers by "porting" them to a new device they control, warns Fraud.org. Crooks use your phone number and personal details—such as date of birth, Social Security number and address—to pretend to be you and port (transfer) your number. Once the number is ported, the crooks can access your accounts (such as banking, social media, email, etc.) using, ironically, security verification codes texted to the new device (as part of two-factor authentication). Set up security questions or PINs to prevent unauthorized porting. If your phone unexpectedly goes to "emergency calls only" mode, don't take that as an otherworldly sign to report a scam to 911. Instead, as the BBB explains, recognize that it can be a sign your number has been stolen.

Home sweet scam. The dream of homeownership can be snatched from homebuyers who inadvertently wire their downpayment and closing costs to crooks. After hacking into title company accounts, crooks find buyers about to close on a new home and send them timely emails on where to wire funds. The scam, while not new, has recently resurfaced in Ohio and Nevada. The American Land Title Association recommends that homebuyers confirm all wiring instructions by phone directly with their title company—and not use phone numbers in the last-minute emails. The FTC and CFPB offer more tips for avoiding a mortgage closing scam.

Brush off these recommendations. Consumers around the country—from the East Coast to California—have received unordered merchandise from Amazon. It's been tied to an international scam known as "brushing," wherein vendors purchase their own products and have them delivered to unsuspecting consumers. The vendors then write glowing online reviews to generate more sales. While consumers receiving unwanted "gifts" can donate them or re-gift them (before they get invited to appear on a hoarding reality show), the rest of us are duped by fake reviews for unworthy products. Amazon is investigating the unsolicited packages and blocking sellers who violate their policies.

Wet behind the ears? For years we've heard that seniors are more vulnerable to scams. But new data says millennials (ages 20 to 29) lost money to fraud more often than seniors. The Federal Trade Commission's 2017 Consumer Sentinel Network Data Book, which breaks out losses by age for the first time, says 40 percent of millennials lost money, compared with 18 percent of people 70-plus. But victims

aged 80-plus were the biggest losers (suffering a median loss of $1,092 compared to $400 for millennials). Listen to what grandma tells you, dude!

The great equalizer? Two counties just outside Washington, DC, offer Korean-speakers to help residents get help and avoid scams. Howard and Montgomery County are the only counties in Maryland with their own consumer protection offices. Montgomery Office of Consumer Protection Director Eric Friedman said Montgomery already offers services in French, Russian, Spanish and three dialects of Chinese, as well as Korean, and hopes to add Vietnamese. Howard County is looking to add Spanish speakers next. “Scams are the great equalizer,” Friedman said. “Crooks don’t care where you’re from.”

Under his spell. A swindler who stole hundreds of thousands of dollars (and identities) from victims of his online schemes was sentenced to four years in prison. John Edward Taylor targeted victims on matchmaking and networking websites pitching romantic relationships, personal relationships and even employment opportunities. Taylor, who posed as a millionaire oil tycoon, also coerced sexually explicit photos from victims and threatened to make them public. (Note to self: Keep smartphones out of the bedroom.) Check out the FTC's tips for protecting your heart and money.

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.