Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert | September 2015 | www.consumer-action.org

SCAM GRAM is Consumer Action's new 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, cheat and crooks—wise up with SCAM GRAM!

View this newsletter in a browser.

If you no longer wish to receive email from Consumer Action, go to the end of this message and click the link to opt-out.

Sign the petition and end robocalls

"Hi, it's Rachel from cardholder services." Too many of you have picked up the phone to hear Rachel the robocaller's annoying voice. Robocalls—automated telephone calls, frequently used by telemarketers and scammers—not only invade your home and privacy, they may illegally circumvent the federal Do Not Call list. And they can cost you real money. An estimated $350 million a year is lost to phone scams. Phone companies can block the calls before they reach you—yet they aren't doing it. That's why Consumers Union launched the ***End Robocalls*** campaign, which calls on the big phone companies to give their paying customers free tools to stop these calls. You can end robocalls. Sign the petition and join the more than 400,000 consumers who have sent a wake-up call to the big phone carriers. *Demand tools to end the robocall madness now!*

Ashley Madison and the shame-based scam

According to the *New York Times*, scammers have wasted no time exploiting philanderers in the Ashley Madison database after a hack exposed their personal information to the world. And it gets even darker: This online adultery service boasting the slogan "Life is short. Have an affair" is itself largely a scam, evident as reports pile up that few to no women were actually using the sordid site. Male users were fooled into making plans to "cheat" with automated fembots (R2-D2 with lipstick?) and charged money by the site to cancel their accounts. The *Times* writes that many men have reported extortion attempts, and users remain vulnerable to deceptive offers of help. Scammers could use data from the breach to trick victims into giving up more information, or even to hack into their computers to wreak further havoc. Such attacks are likely to continue for weeks and months. What's more, those curious to find out if a spouse, employee or acquaintance was registered on the site are feeling the fallout, too, as they're baited into clicking malicious links claiming to list the identities of users. Our advice: Avoid all things Ashley Madison!

Housing Horror

Mortgage scams come in all sorts of packages. Take, for instance, the New Jersey father-son duo who were busted for bank fraud earlier this month after stealing millions from home buyers; the senior loan officer indicted for using fake documents to defraud lenders into issuing loans to consumers; and the Peruvian fugitive who set up shop in the U.S. to take advantage of limited-English-speaking clients in order to receive higher commissions after selling them homes that they couldn't afford. Mortgage scams don't just occur when you're signing a deed—they can happen when modifying an existing loan, refinancing your home, getting a reverse mortgage, transferring a deed or selling the home (particularly when you're dealing with foreclosure). Knowledge is power; educate yourself to avoid falling victim to these devastating scams.

Medicare malfeasance

Did you know that $60-$90 billion is lost each year to Medicare fraud and abuse? This type of fraud is a booming "business" targeting seniors across the country. The *Los Angeles Times* published a great article on the real-life impact to consumers. The piece offers a number of tips to avoid becoming a victim, such as protecting your Medicare number; avoiding speaking with anyone who cold-calls you or shows up at your door claiming to be with the government/Medicare; declining offers of medical equipment without a medical exam; and regularly reviewing your Medicare records to monitor unrecognized charges or other changes to your account.

It's easy not to fall for the E-ZPass scam

"Transponder" devices placed inside car windshields that allow drivers to pay tolls electronically are popular with commuters in many states. Unfortunately, scammers are sending "phishing" emails to E-ZPass/FasTrak customers saying that they have "missed" or "unpaid" toll fees. (Phishing emails appear to be from a company the recipient does business with but they are designed to steal personal information.) If you click the link embedded in the email, you give the scammers a fast track to personal and financial information stored in your computer or mobile device. For more info and a screenshot of a bogus email, check out this news report.

A sweet talkin' scammer ensnares investors

In news of the weird, a shady-looking, smooth-talking scammer convinced more than 50 people to invest millions for land he claimed is located near a soon-to-be-built Disney theme park in, of all places, North Texas. A picture is worth a thousand words, so click on this link to take a look at the man, who's been sentenced to 17-and-a-half years in prison for wire fraud and making false statements to the FBI. The Walt Disney Company denies rumors of a North Texas theme park. So one has to wonder how so many seemingly intelligent investors were duped? According to one of the men, the scammer had a way with words.

It's a Brave New World out there!

A Taylor-made scam opportunity. Taylor Swift's 1989 tour is the event of 2015! Unfortunately, counterfeit tickets could keep you from experiencing it. Ticketmaster offers a guide to help festival and show-goers avoid the fake stuff.

Avoid burns on Tinder. If you're using the dating website Tinder, watch out for "catfishers" who hide their real identities to entrap the lovelorn. The Better Business Bureau (BBB) released an alert advising users to swipe left on scammers, who have begun targeting the online dating site.

Don't bite this Apple. Heads up! Watch out for scams surrounding the newly announced iPhone 6S. One attempt to defraud involves a pop-up offering a chance to test the new device. Do not click strange links: You might install malware that could ruin your computer.

Tips to keep you safe

Be wary of offers for an **extended automobile warranty**, especially if the offer comes from a third party. Consumer Action offers some handy advice for avoiding vehicle warranty scams.

The Better Business Bureau's been busy lately developing a new **scam tracker**. If you think you're being targeted, you can use the online tool to search for similar incidents and report your experience.

Check out Consumer Action's new guide to **electronic chip cards**, which are arguably more secure then non-chip cards (you know, the standard ones that only use magnetic stripes).

Thanks for reading SCAM GRAM. (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.