Hot Clicks: GSA Starts Bug Bounty Program with HackerOne

It was the first civilian federal agency to get involved with hacker-powered security in 2017.

Amanda Ziadeh

Mon, 09/24/2018 - 16:37

Photo Credit: Artystarty/iStock

The General Service Administration's Technology Transformation Service awarded HackerOne with a multi-year contract to run a bug bounty program. The hacker-powered security platform has led a number of bug bounties with the Defense Department already, including Hack the Pentagon, Hack the Air Force, Hack the Army, and most recently, Hack the Marine Corps. But GSA was the first federal civilian agency to get involved with a bug bounty program: 18F executed a bug bounty and vulnerability disclosure program with HackerOne in 2017, awarding

bounties to hackers for reporting security vulnerabilities in public-facing digital systems and websites. This contract extends GSA’s momentum with bug bounties, and its period of performance will extend for up to five years. When the program starts, TTS will financially reward hackers for reporting security issues directly to the system owner. BusinessWire

Twitter May Have Slid Into Your DMs Without Your Knowledge

The social media company said it was a mistake — but on September 21 Twitter began notifying users about an API bug that accidentally shared users’ direct messages or protected tweets with Twitter app developers. The bug was found in the Account Activity API, which lets Twitter business accounts grant access to an account’s data to multiple developers at the same time. So, when users contacted business accounts on Twitter that used that AAAPI, the bug sent DMs to unauthorized developers. According to Twitter, the bug was active from May 2017 to September 2018, and hit one percent of users. It was discovered and fixed on Sept. 10. ZDNet

Humans are Causing Earth to Wobble

The Earth’s axis of spin has shifted 34 feet since 1899. Scientists found a third of that wobble is attributed to melting ice and rising sea levels, stemming from human-caused climate change. Another third is due to land masses expanding upwards as glaciers retreat, and the final third has to do with the Earth's mantle, or its middle layer. The team at NASA's Jet Propulsion Laboratory built a computer model of the physics of the Earth’s spin using real data to find the last piece of the wobble was coming from the mantle, which moves as hotter material from closer to the core rises, and cooler material sinks. This wobble isn’t anything to worry about, and any impact it has on navigational equipment is easy to correct for, but it gives scientists a way to figure out where the Earth's mass is, and where it’s going. Space.com

Alexa Will Soon Hear Your Whispers and Emotions

Amazon announced new features and upgrades for its virtual assistant. For starters, Alexa will soon be able to hear you whisper and whisper back to you, which apparently makes it easier if someone is sleeping nearby and you can't shout a demand. Alexa will also be able to listen for warning signs in a home when the user says "Alexa, I'm leaving," such as breaking glass or a fire alarm. This feature is called Alexa Guard, and it'll even send the user a notification to his or her phone with a link to the recording of the sound that triggered the warning. And, if that's not enough, Amazon's labs are working to give Alexa a form of emotional awareness to be able to detect frustration in a person's voice, which is intended to show the tension between using AI to improve functionality. Wired

California Wants to Protect Connected Devices from Hackers

California lawmakers sent the governor draft legislation that strengthens the security of web-connected devices and online gadgets, and if it passes, the state will be the first in the U.S. with a law specifically designed for IoT. The legislation requires connected devices to have a "reasonable" security feature that fits the nature and function of the device, and requires manufacturers to create a different default password for each one they sell, or prompt users to change a common default password before they use the device. There are new types of connected devices entering the market every day, and these lawmakers are hoping new legislation can start protecting them from hackers. Considering the range of connected devices, like vehicles and wearable and embedded health tech, some people are concerned hackers can comprise these devices to seriously injure or kill people. If passed, the legislation would go into effect in January 2020. MIT Technology Review

View printer friendly version
Amazon
GSA
HackerOne
space
NASA
internet of things
Alexa

social media