From: CyberScoop <news@cyberscoop.com>
Sent: Tuesday, December 6, 2016 12:06 PM
To: Haley, Nikki
Subject: IoT security rules won't be coming from the FCC

Not rendering correctly? View this email as a web page here.

Right-click here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.
CyberScoop

TUESDAY

December 6, 2016

The FCC was working on cybersecurity rules for IoT devices, but, welp, not so much now. We have more details on how law enforcement brought down the Avalanche network. And in the easiest tease we've written this month: the grades for the education sector's cybersecurity practices aren't good. This is CyberScoop for Tuesday, December 6.

ON HOLD: FCC Chairman Tom Wheeler says he's newly disclosed plans for the agency to regulate cybersecurity for the Internet of Things have been paused. In a letter to Sen. Mark Warner, Wheeler disclosed an agency plan for IoT "risk reduction" that called for the FCC to use its power to certify wireless devices as the basis for minimum security standards and mandatory consumer disclosures for device manufacturers. As Shaun Waterman reports, Warner is urging the Trump administration to take up where the outgoing government has left off.

MORE ON AVALANCHE: Unidentified private-sector technology companies played a critical role in helping law enforcement dismantle a multinational cybercrime network known as Avalanche, according to Robert Johnson, special agent in charge of the FBI's Pittsburgh Division. Avalanche was an internet hosting and management system — comprised of more than 20 staging servers — used to deploy botnets, malware and ransomware. The effort to shut down Avalanche included help from prosecutors and other law enforcement officials in 40 countries. The FBI is encouraging internet service providers and a cohort of private sector partners to assist in removing related computer viruses from known systems.

ANOTHER DAY, ANOTHER GRANT: Human-centric security for the Internet of Things and computer chips that verifiably vouch for their own integrity are two of the research programs that the National Science Foundation is supporting under its $76 million Secure and Trustworthy Cyberspace program. As Shaun reports, it's part of the $160 million invested in cybersecurity research by the agency this year.

ALWAYS BE RECRUITING: When the government released its cybersecurity workforce strategy in July, one piece of low-hanging fruit it identified was guidance from the Office of Personnel Management, putting together all the already-existing exceptions, bonuses and other flexibilities in the federal salary rules that managers could use to sweeten the pot for potential cyber hires. As Shaun reports, four months later, OPM is out with the guide.

ALONG PARTY LINES: Confidence in the legitimacy of the recent U.S. election results differs depending on a person's preferred political party, according to a 1,500-person online survey conducted by the bipartisan Democracy Fund. Nearly half of participating Democrats said they believe an "electronic security breach or hack impacted the vote" count. In contrast, just 31 percent of republican-leaning respondents said they believe hackers were able to influence U.S. presidential election results. Though there has been virtually no evidence of voter fraud occurring at scale in a way which could sway electoral outcomes, confidence in election systems continues to decrease year-over-year. Chris Bing has more.

BAD GRADES: The education industry scored a dismal grade of D in overall security posture, according to a new cybersecurity report released on Monday. The sector, especially higher education, reported the lowest 2017 Security Assurance score of any industry at 63 percent, according to the 2017 Global Cybersecurity Assurance Report Card, which is put out by Tenable Network Security, a private firm. The report attributes the poor score to the multitudes of personally identifiable information stored at colleges and universities that provide fodder for hackers. EdScoop has more on the report.

READ THIS

Noted infosec hivemind leader @krypt3ia is out with his version of Festivus' airing of grievances, and not a group, org or person gets by unscathed. Read for laughs, but be warned, the language is, uh, festive.

In the meantime, how about tossing your favorite new website a follow on Twitter and a like on Facebook? Click those shiny social buttons below to get the best we have to offer across the social web.

This newsletter is produced by Scoop News Group.
Visit cyberscoop.com to read this newsletter on the web.

CyberScoop News 1150 18th Street NW Suite 850 Washington District of Columbia 20036 United States