Issued 9/28/18

Social Engineering Attacks Skyrocket More than 500 Percent

Attempts to trick users into giving personal information spiked more than 500 percent from the first to second quarter of 2018, researchers at Proofpoint said. “Social engineering is increasingly the most popular way to launch email attacks,” the cybersecurity firm said in their second quarter threat report. “Criminals continue to find new ways to exploit the human factor.” The use of cryptocurrency, fake antivirus and browser plugins were responsible for the jump in attempts to manipulate users via email, according to the report. Overall, the volume of email fraud that organizations receive has increased 87 percent year-over-year, the report said. Proofpoint said that agencies and companies should assume that users will click on malware and have security systems as a backup to stop hacking attempts. The Department of Homeland Security received more than 30 million emails from December 2017 to May 2018, the top IT official at the agency, John Zangardi said Sept. 7. Roughly 21 percent of those emails were malicious, he said during the Billington Cybersecurity summit. Even though 10 employees clicked on the link, the department’s network was not infected.