Issued 9/20/18

US Senate, Staff Targeted by State-Backed Hackers

Foreign government hackers continue to target the personal email accounts of U.S. senators and their aides — and the Senate's security office has refused to defend them, a lawmaker says. Sen. Ron Wyden, an Oregon Democrat, said in a Wednesday letter to Senate leaders that his office discovered that "at least one major technology company" has warned an unspecified number of senators and aides that their personal email accounts were "targeted by foreign government hackers." Similar methods were employed by Russian military agents who leaked the contents of private email inboxes to influence the 2016 elections. Wyden did not specify the timing of the notifications, but a Senate staffer said they occurred "in the last few weeks or months." The aide spoke on condition of anonymity because he was not authorized to discuss the issue publicly. Wyden has proposed legislation that would allow the security office to offer digital protection for personal accounts and devices, the same way it does with official ones. His letter did not provide additional details of the attempts to pry into the lawmakers' digital lives, including whether lawmakers of both parties are still being targeted. The Wyden letter cites previous Associated Press reporting on the Russian hacking group known as Fancy Bear and how it targeted the personal accounts of congressional aides between 2015 and 2016. The group's prolific cyberspying targeted the Gmail accounts of current and former Senate staffers, including Robert Zarate, now national security adviser to Florida Sen. Marco Rubio, and Jason Thielman, chief of staff to Montana Sen. Steve Daines, the AP found. The same group also spent thev second half of 2017 laying digital traps intended to look like portals where Senate officials enter their work email credentials, the Tokyo-based cybersecurity firm TrendMicro has reported. Microsoft seized some of those traps, and in September 2017 apparently

thwarted an attempt to steal login credentials of a policy aide to Missouri Sen. Claire McCaskill , the Daily Beast discovered in July. Last month, Microsoft made news again when it seized several Washington. Such incidents "only scratch the surface" of advanced cyberthreats faced by U.S. officials in the administration and Congress, according to Thomas Rid, a cybersecurity expert at Johns Hopkins University. Rid made the statement in a letter to Wyden last week . "The personal accounts of senators and their staff are high-value, low-hanging targets," Rid wrote. "No rules, no regulations, no funding streams, no mandatory training, no systematic security support is available to secure these resources."