Washington, D.C., Officials Block 'Widespread' Attempt to Breach Cyberdefenses

Theo Douglas | July 30, 2018

The nation's capital city successfully fended off a large-scale, multinational attempt to breach its cyberdefenses on July 24, a technology official confirmed via email.

The Office of the Chief Technology Officer's Security Operations Center was made aware through "prompt reporting by D.C. government employees" that they were receiving phishing emails requesting sensitive information including passwords, interim Chief Technology Officer Barney Krucoff said via email. Asked how many departments and attempts were received, Krucoff described the incident as a "widespread, non-targeted attempt that did not single out any one person or department."

"We received multiple and perhaps coordinated email phishing attacks from both overseas and domestic sources," said Krucoff, who was elevated to the interim role in January. On the topic of whether the event, if successful, might have delivered a virus or resulted in a ransomware cyberattack, he said the evolving nature of security risks is one of cybersecurity's "most challenging aspects" and why OCTO is continually engaged in hardening its cybersecurity systems against such threats.

District officials told *The Washington Post* they weren't aware that any information had been compromised as a result of the incident and took "multiple actions" against

it. The Post reported the emails were sent to 30,000 employees; and in its article, Krucoff cautioned the “frequency and sophistication” of such attacks will increase, so city employees should “exercise caution.”

Staffers’ alert posture enabled OCTO’s security and messaging teams to block the attacks, the interim CTO said, noting that the agency continually monitors against bad actors. Typically, when the agency verifies a phishing email, it moves to protect the user from visiting a malicious link and keeps the email from being further distributed, the interim CTO said, noting that OCTO reports cyberincidents to various state, regional and national partners. In this case it referred the matter to federal law enforcement.

“Phishing attempts like this one are common attacks most government agencies experience, and being in Washington, D.C., we are a high-profile target. Each year, we see more than 1 billion malicious intrusion attempts, including ransomware, denial-of-service and phishing attacks,” Krucoff said.

http://www.govtech.com/security/Washington-DC-Officials-Block-Widespread-Attempt-to-Breach-Cyberdefenses-.html