18294

News Release
For Immediate Release

SPS Offers Free Credit Monitoring Following Cyber Attack on IT Network

December 3, 2020 - Springfield Public Schools (SPS) is offering two years of free credit monitoring to some current and former employees and a small number of job applicants following a cyberattack that occurred on its computer network this fall.

Superintendent of Schools Daniel Warwick said the move is taken as a cautionary measure to help protect against any breach to the security of personal information that may have occurred because of the cyberattack.

"We sincerely regret that this event would cause concern and we are doing all we can, going above and beyond, to offer services free of charge to help them enhance the protection of their private information and hopefully provide some peace of mind," Warwick said, adding that the district is providing two years of free credit monitoring; two years of monitoring for data appearing on the dark web; assistance with identity recovery if needed; and identity theft insurance for individuals whose personal information may have been compromised.

Today, the district mailed letters to those individuals whose personal information may been compromised. Those who do not receive a letter are not believed to have had their personal information possibly compromised.

The security incident occurred after hackers attacked the district's network on the morning of October 8th. The attack, which caused a cancelation of remote learning for the day, was an attempt to encrypt all SPS network data and extract data with sensitive information. The network was protected to industry-standard; had a fully updated firewall; and was covered with intrusion detection and malware tools. However, the attack relied on a new version of malware that was not detectable by current tools, and which was only identified after assistance from the Federal Bureau of Investigation and a cybersecurity resource endorsed by the Department of Homeland Security.

The SPS Information Technology (IT) department interrupted the attack by shutting down the network, which is what prompted the cancellation of remote education for the day. The IT team then prioritized restoring data and remote learning services. Today, the IT department remains focused on ensuring the security of the network and the continual restoration of data and services from the backup system. Additionally, the team, in partnership with law enforcement, is investigating the source of the attack. That investigation recently determined that the data of some current and former employees may have been compromised, causing the district to notify those whose information the attackers may have accessed via mail this week.

"We'd seen districts throughout the country grapple with cyberattacks, so we were extremely diligent and proactive in implementing layers of defense, but unfortunately, we live in a world where no protective measure is 100 percent effective against cyber threats," said Chief of Information Technology Paul Foster.

Since the attack, the district's network security has been further enhanced, additional security practices and protocols have been put in place, and the district's cybersecurity partners will continue to provide further recommendations to the district. Warwick said the district is poised to devote the necessary resources to help protect its IT system from further attack and to providing as many protective resources as possible in response to the October 8th attack.

If you believe your information may have been compromised in this cyberattack, please call 833-905-3224 to enroll in credit monitoring services. To learn more about your rights under Massachusetts and federal law, please visit the district's website at:
https://www.springfieldpublicschools.com/news/news/free_credit_monitoring_following_cyber-attack

(END)