# Frequently Asked Questions

**Q: Was the Rockville Centre School District a victim of a cyber attack?**

**A:** Yes. On the night of Thursday, July 25, 2019, the School District was attacked by the Ryuk virus, which was designed to encrypt all operating systems and data. While the District maintains firewalls and anti-virus software that identifies and blocks thousands of viruses and malicious software every day, this particular virus was able to evade detection.

**Q: How did the District detect and respond to this cyber attack?**

**A:** On Friday morning, July 26, 2019, the Director of Technology recognized that there was a problem with email and shut down the entire system immediately. By acting as quickly and thoroughly as he did, he was able to limit the damage to our data files and emails.

**Q: What is the recovery process and how is the District managing its recovery?**

**A:** Immediately following the shutdown, the recovery process began. In the hours that followed, the District contacted the local police, Homeland Security and the FBI. In addition, we contacted our insurance carrier to investigate their protocols for cyber attacks. Our staff mapped out a plan that would allow the School District to continue its operations without interruption by Monday, July 29, 2019. All communications were reestablished and fully operational by Monday. Our student management system had been untouched and not encrypted by this cyber attack. Our financial management system had been encrypted, but we were able to restore our data from a backup. A team of technology specialists worked to clean and reimage every desktop and laptop in classrooms and offices throughout the District. Since that time, our other systems such as transportation, security and food service have been restored, enabling

the District to continue its operation without interruption.

The encryption affected our file servers, which include our historical data and our email. Recovery of these files and emails requires an extensive cleansing process that ensures that no file or email has a virus attached to it. While this is a slow process, we expect to have our files by the opening of school and most of our emails soon after that.

**Q: How has law enforcement been involved?**

**A:** At the outset, our first calls were to the Rockville Centre and Nassau Police Departments who took statements and recorded the extent of the damage. We contacted both Homeland Security and the FBI, and each agency sent teams of experts to the District. They were instrumental in helping us identify the virus which may have entered this system as early as March, 2019 and lay dormant in the system until July 25, 2019. Neither agency, however, had a decryption tool that would effectively enable us to restore our data and emails and no other aid was offered to us.

**Q: Did the School District have virus protection software, backups and insurance?**

**A:** The School District had the latest version of virus protection software which successfully shielded us from daily attempts at invading our systems until the Ryuk Virus penetrated our system. Research tells us that Ryuk uses sophisticated technology to bypass all protections and firewalls world-wide that municipalities, school districts and businesses have put in place.

Our priority now is to learn from this experience and use this knowledge to find, if available, a more robust backup system that can avoid intrusion by outside viruses. We will work with our Board and cyber security experts, including Homeland Security and the FBI, over the next few months to determine ways of securing more effective antiviral and backup systems for the District.

The School District has an insurance plan that covers the cost of recovery related to cyber attacks. This insurance plan, after a $10,000 deductible, will pay for the recovery.

**Q: Was there a breach of student or staff data?**

**A:** After careful review Homeland Security and the FBI informed us that to the best of their knowledge, no staff or student information left the school district. These agencies emphasized to us that the goal of these attacks is to encrypt and hold data for ransom, not breach or steal the information from the District.

**Q: Were iPads affected by the cyber attack?**

**A:** Because of the nature of the technology associated with iPads, they were not affected by the virus.

**Q: Was there a ransom paid? If so, how much was paid and did it have an impact on the local taxpayer?**

**A:** After exhausting all of our own efforts to recover and restore our data, we found ourselves evaluating what data would be lost if no decryption tool was available. After an extensive and detailed analysis of the cost, time, and overall effectiveness of recovery without paying the ransom and its impact on students who had projects stored in files on the system, the District decided to pay the ransom to make the District whole.

Because we were able to shut down the cyber attack early in the encryption process, the ransom demand was lower than typical. By finding ways to restore some of our data, the ransom demand went from approximately $176,000 to $88,000. As part of the recovery, the District paid only the $10,000 deductible and the Insurance policy paid the rest. Since our insurance deductibles are budgeted, there will be no impact on the local taxpayer.

**Q: Did the District consider not paying the ransom?**

**A:** Yes. However, while it was certainly a difficult decision, the District was made aware that many of its files would not have been recovered without paying the ransom. That was particularly true of files involving student work and projects. In addition, there was no guarantee that email records could be recovered in a timely manner, but it would take months of extensive work and considerable expense to restore them. The cost-benefit comparison clearly showed that the least expensive and most time-effective restorative process was to pay the ransom.

Once the ransom was paid, the decryption tool was provided within the hour of payment and has effectively enabled the School District to access all of its data and emails. Recovery, however, still involves cleansing which takes time.

**Q: Why was one district able to avoid paying ransom?**

**A:** It's important to acknowledge that every cyber attack is somewhat unique. For example, a district mentioned in a Newsday article, which had also suffered a similar attack, had made the decision over the summer to take its backup offline in order to work on it. Since it was disconnected from its system at the time of the cyber attack, they were fortunate not to be faced with the same exact issues as our district. However, since the strategy of the cyber attack is to go after backups, in many cases, districts are finding themselves in a similar position as Rockville Centre.

**Q: What can parents and students expect on the first day of school?**

**A:** We are pleased to report that we expect a seamless start of school for our students, teachers and staff. All student placements and schedules have been completed. Schedules have been mailed to Middle School and High School families. As planned, the Elementary parent portal will be opened on Wednesday, August 28th for student placements. The District is continually working on upgrading programs and apps available to our students and staff. Those changes, such as the movement from eBackpack to Google classroom, were planned and will be put into place for the upcoming school year.

**Q: Will the District provide the community an opportunity to discuss this in public?**

**A:** On September 5th, the first Regular meeting since this cyber attack, the Board of Education agenda will include an Item for Discussion on this subject. The Board intends to have a full and open discussion of this topic and will provide members of the public an opportunity to raise questions and concerns. The Board welcomes your attendance at this meeting.