CYBERSECURITY:

Ransomware Protection for Schools

JA | JAMES ALLEN INSURANCE

What is Ransomware?

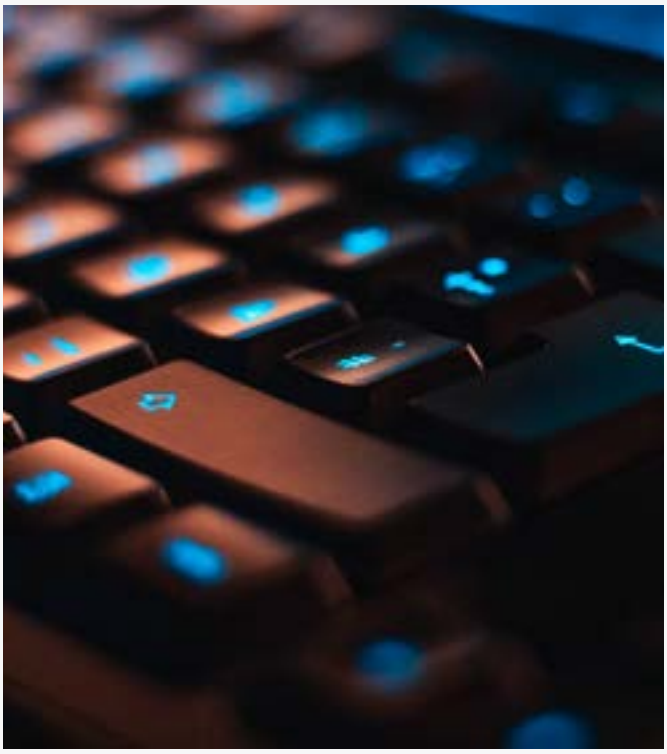
YOUR SCHOOLS' COMPUTERS HOLD VALUABLE INFORMATION. ARE YOU SURE YOUR FILES ARE SECURE?

Ransomware is a form of malware. It encrypts files, making them unusable and unreadable. Hackers then ask for a ransom in exchange for the decryption key that will restore your files.

Ransomware enters your network through anything from an email attachment to a USB drive. Typically, the malicious software starts encrypting files on local computers and networks before the victim knows it is happening. It is downloaded and installed without the user's knowledge, hidden among the computer's ordinary files and operations. Once files are encrypted, a ransom note will then pop up on the user's screen, threatening destruction if a payment is not made.

Hackers don't always go after the average Joe. They like to target government entities—schools, cities, police stations, etc. Hackers have proven these are easy targets with large pocketbooks and a lot to lose.

The FBI reports more than $1 billion was paid to ransomware hackers in 2016.



The Cost of a Ransomware Attack

Ransomware attacks can be very expensive. Ransoms can range anywhere from a few hundred dollars—if you're lucky—up to hundreds of thousands of dollars. The FBI reports more than $1 billion was paid to ransomware hackers in 2016. The Department of Justice reports an average of 4,000 attacks per day in the U.S. that same year.

And demands are getting higher. Recently, Crowder College was hit with a $1.6 million ransom, and Monroe College in New York received a $2 million ransom. Schools that choose not to pay may have to rebuild total infrastructures after data recovery is attempted. This can also carry a price tag into the millions. Is that a price your institution is willing to pay?

Attacks on the Rise

In 2019, ransomware attacks have hit over 500 U.S. schools and infected 54 educational organizations such as school districts and colleges. And that number is quickly rising. According to McAfee, ransomware attacks have more than doubled in 2019. Private and critical information is being held hostage and stolen nationwide at an alarming rate. At the start of the 2019-20 school year, 15 school districts accounting for more than 100 K-12 schools were hit.

SCHOOLS THAT HAVE BEEN UNDER ATTACK:

Ava R-I School District Ava, MO

Wallenpaupack Area School District Hawley, PA

Mad River Local Schools Riverside, OH

Papillion-La Vista Comm. Schools Papillion, NE

Rockford Public Schools Rockford, IL

Souderton Area School District Lansdale, PA

Wakulla County School District Crawfordville, FL

Jackson County School District Marianna, FL

Wyoming Area School District Exeter, PA

Mobile County School District Mobile, AL

Houston County Board of Education Perry, GA

Guthrie Public Schools Guthrie, OK

Smyth County Public Schools Saint Marion, VA

Northshore School District Bothell, WA

According to McAfee, ransomware attacks have more than doubled in 2019.

Education is Crucial

It is imperative to educate your network users of the risks and precautionary measures to take against ransomware attacks. This includes students, faculty and staff. Regularly remind them of best practices, such as:

- Do not to open email attachments from an unknown source
- Change your password often, and make sure it is unique from other passwords you may have
- Keep your antivirus software up to date
- Report any suspicious emails to the designated IT supervisor or staff member

How Schools are Affected

Schools are an easy target due to their vulnerability, wealth of data, and a limited budget for cybersecurity staffing. When schools are under a ransomware attack, every second counts. While negotiations are underway and heart rates rise, the school, students and families are compromised. Email systems and entire computer networks are held hostage. A successful attack can do anything from disrupt a lesson plan to delay the start of the academic year.

Does School Size Matter?

According to the FBI's cyber division, both large and small school districts have the same possibility of being hit. Whether it's public or private, grade school or secondary education, criminals hit all types of organizations.

SMALL SCHOOLS

Smaller schools usually have less money in their budget set aside for cybersecurity, making them more vulnerable to ransomware attacks. Some attackers experience greater success hitting a lot of smaller schools and demanding relatively smaller ransoms to be paid, rather than trying to carry out a larger attack on a bigger school.

LARGE SCHOOLS

Universities tend to have larger networks than K-12 systems. They also have more financial resources to pay out larger ransoms, making them more tempting. Hackers are usually more successful sending out a dangerous email to a larger number of people, because there is a higher chance of someone opening a file or clicking a link that will lead to an attack.

By Marc Graber

Marc Graber has been in the insurance industry for 34 years, and currently serves as Director of Asset Management & Retail for James Allen Insurance. In that role, he oversees the agency's cybersecurity service line where he helps organizations achieve peace of mind that they will be covered in the event of a cyber attack.

How to Prepare

INVEST IN CYBERSECURITY INSURANCE

Select an insurance policy that takes a comprehensive approach to cybersecurity and supports your institution's compliance requirements and risk management systems.

LOCK ADMINISTRATIVE RIGHTS

Limit the number of users with permissions on your server. This can limit the spread of a ransomware attack throughout the network.

STAY UP TO DATE

Keep your system up to date with the latest patches and security measures. Reducing vulnerability in applications and operating systems in turn reduces the likelihood of an attack.

BACK UP DATA

Back up your data daily to a local storage device or server that is offline. This prevents the ransomware from being able to reach it. And be sure to continuously test your backup system to ensure it's always working properly.

DON'T OPEN ATTACHMENTS

If an email seems suspicious, it probably is. When you don't recognize a sender or the message asking you to open an attachment seems unusual, do not open it. This also goes for online ads. Being cautious also protects your computers from malware. A new tactic includes "malvertising," where ads are embedded with malware and then sent out to sites you know and trust.

MONITOR YOUR SERVER AND NETWORK

Monitoring tools can detect any unusual files that might otherwise be overlooked. This prevents malware from starting an attack.