LUMU

# CYBERSECURITY IN EDUCATION 2025

# Executive Summary

Lumu's threat data from the first half of 2025 showed that the education sector is the top target for cyberattacks in the Unites States. Lumu is determined to help schools build effective defenses against cybercriminals. To help with this, we gathered together the essential takeaways for cybersecurity in education from our in-depth compromise report.

From the data that Lumu gathered, the education sector faced more attacks than any other industry, including over:

**43.5%** of **anonymizers** (tools used to hide an attacker's identity)

**36.5%** of **droppers** (malware designed to install other viruses)

**38.5%** of **ransomware incidents**

We wanted to help schools answer: What are the evolving dangers we face? And how can we best defend our students?

Protecting student cybersecurity is not just about avoiding classroom disruption. Student data is valuable and can be used for criminal purposes such as credit fraud. Ransomware and other financially motivated attacks can bring establishments to their knees.

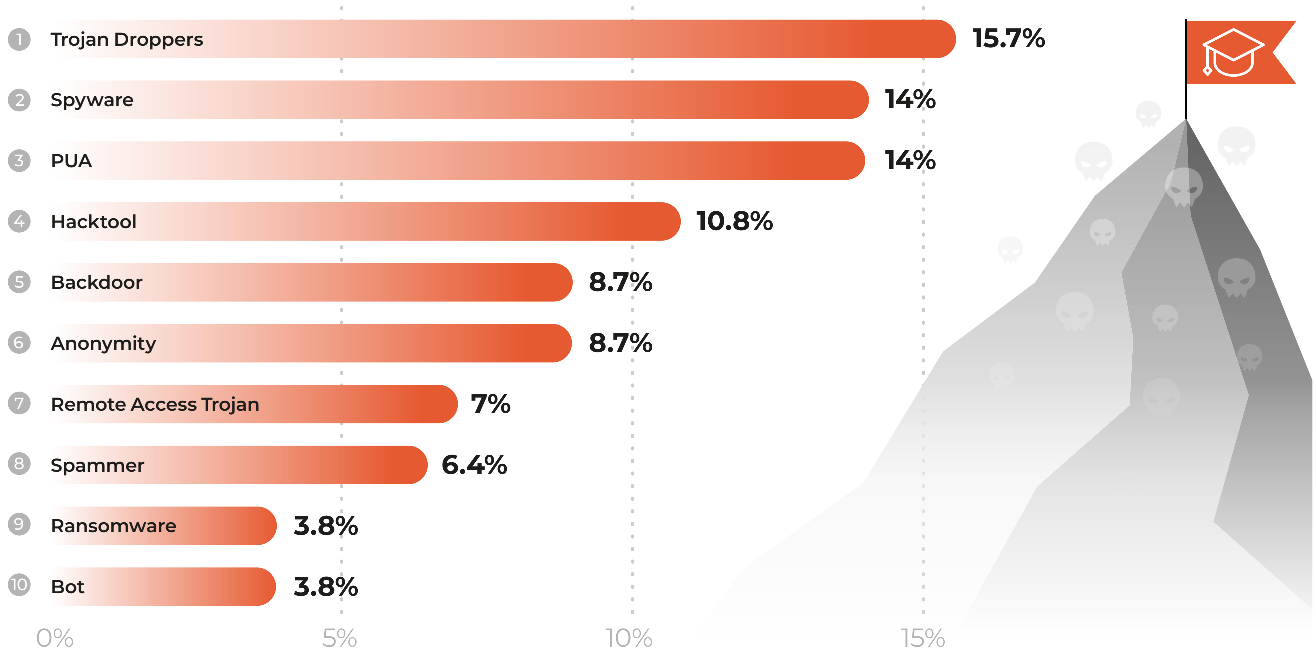
Since school IT teams are often small, they must leverage threat intelligence effectively and design a security stack tailored to the threats targeting education. This report aims to help you do that.

# Index

## How Malware Impacts Education

When targeting schools, cybercriminals play the long game, prioritizing stealthy infiltration over noisy, immediate attacks. Attackers have a clear goal: gain initial access, gather intelligence, and then launch a final attack.

### Top 10 Threat Types Affecting the Education Sector in the USA



**Droppers** are the most recorded malware threat in education. These are used to gain initial access and deliver further malware. We look in more detail at these below.

The second most common malware type we recorded was **spyware** — a malware that secretly gathers information from a user's device and sends it to a third party. This includes browsing history, keystrokes, login credentials, and even financial details. The most prominent type of spyware used is called **infostealers**. Again, we are going to look in more detail at infostealers.

**Potentially Unwanted Applications (PUAs)** and **hacktools** are also prevalent. Hacktools is a general term for threats such as tools used for password cracking, network scanning, or malware deployment. They are often parts of bigger cyberattacks. This suggests that attackers try to take advantage of user mistakes and weak systems to gain unauthorized access.

Once attackers get in, they try to move laterally (spreading from one computer to another) and escalate their privileges (gaining higher levels of administrative control). The common use of **anonymity tools** and **backdoors** shows attackers work to keep access and avoid being found. Anonymizers will also be discussed in more detail below.

While **ransomware** appears less frequently than initial-access tools, this isn't surprising. Ransomware is usually a later-stage attack that can only be deployed if or when an attacker gains access to your network. We will look in more detail at ransomware, below.

## Taking Advantage of Trust: Phishing

While a cyber attack might end in ransomware, the most common starting point is phishing. Attackers use phishing for two main purposes:

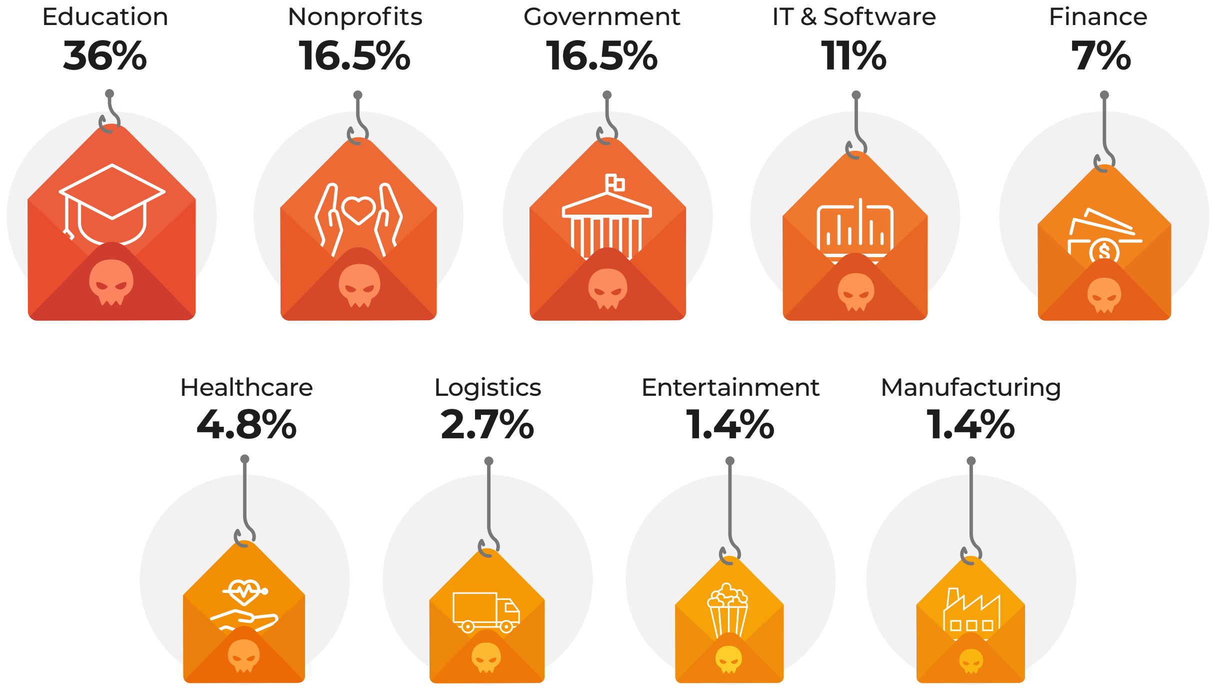
- Manipulating individuals into giving away sensitive information. This might be usernames, passwords, and financial details.
- Tricking people into downloading and executing a malicious file, such as a dropper or infostealer.

Bad actors often use fake emails that look like they come from real, trusted sources. This can be well-known companies, government agencies, or even personal contacts. To make these attacks even more effective, nearly 58% of phishing emails are sent from legitimate, hacked accounts. An email sent from a real, trusted account is far more likely to be opened and acted upon.

### Phishing by Sector

Phishing, as most other malicious activities, targets a wide range of victims. Everybody must be alert for these attacks — however education was the victim of more than double any other sector in our data set.

Phishing by Sector in the USA



Why is education particularly targeted? Essential services such as education, government, and healthcare were all high on attackers' lists. It seems that causing disruption and social impact can be a motivation.

Educational institutions now regularly have large networks that include remote devices and cloud computing. They also have numerous end users who access the network, with varying technical abilities. This greatly increases the attack surface available to criminals.

### Phishing Techniques

There are several novel techniques that are being used. Schools need to keep up to date with these and train staff. These are some that are growing in popularity:

- **Fake-CAPTCHA**
  Copying a CAPTCHA check, like those used to access websites to trick users into copying and pasting malicious scripts.
- **AI-Powered Polymorphic Phishing**
  Phishing emails can be generated at a large scale, using Artificial Intelligence. Each email has small differences to avoid normal detection.
- **MFA Fatigue Exploitation**
  Bombarding users with authentication requests until one is approved out of sheer frustration.
- **Quishing (QR Code Phishing)**
  Malicious links in QR codes distributed through emails, attachments, or even business cards.

## Evading Your Defenses: Droppers & Downloaders

A teacher downloads a file from a phishing email. It seems completely innocent at first — and the antivirus on the computer doesn't notice a thing. But it contains a ticking timebomb inside.

Cyberattackers often use dropper malware as the first stage in more complex campaigns. Droppers aim to get past security and gain a foothold on a compromised system.

A dropper will be a small file that looks harmless, like a normal document, image, or update. Because it seems safe at first, it slips past defenses. Then, it installs the main malware that carries out the attack.

This two-step process is effective because many security tools focus on scanning for known, dangerous malware. The dropper itself is often new and unknown, allowing it to evade these initial checks.

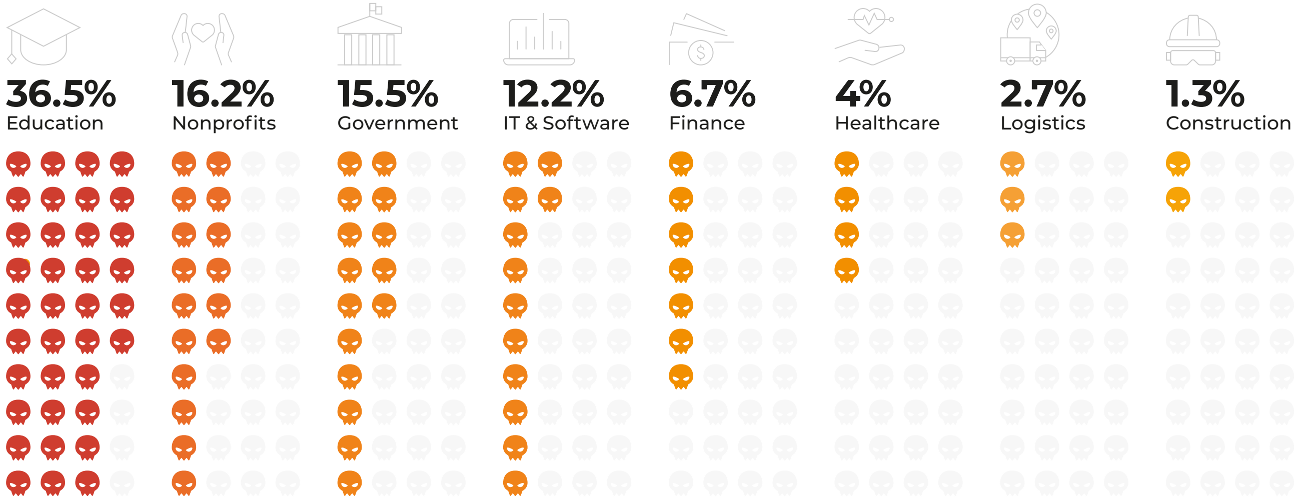
This harmful payload can be many types of malware. These include ransomware, infostealers, or Remote Access Trojans (RATs). Since droppers lead to many threats, strong defenses against them are vital.

Downloaders are similar to droppers and often grouped with them. What is the difference? A dropper carries the harmful software inside itself. A downloader fetches the harmful software from elsewhere using the internet. The definition doesn't always stand true, however, as some droppers can also download.

### Droppers in the USA by Sector

All sectors experienced attacks involving droppers and downloaders — however, education again tops our list.

Droppers in the USA by Sector



The social importance of the top three sectors may suggest that disruption and ransoms are motivations. Attackers also know that schools are often under-resourced, manage sensitive data, and cannot tolerate downtime, making them more likely to pay a ransom.

## Getting Your Sensitive Data: Infostealers

Infostealers are spyware designed to steal sensitive information. This includes logins, bank details, and personal data, which is then often sold on the dark web. Attackers buy that data to speed to break into a network and proceed directly to their main objective.

The information that infostealers gather is used in many attacks, such as ransomware and stealing from cryptocurrency wallets. It can also increase the impact of attacks, as it gives defenders less time to respond.

Infostealers work quietly and often avoid Endpoint Detection and Response (EDR) by running only in the computer's memory, as well as other techniques.

By avoiding initial detection, infostealers can explore a system more deeply. They can gather things like detailed system info, private user data, and internal network details. This provides a strong foothold for further attacks.

## Sectors Targeted by Infostealers

The following statistics show the volume of infostealer attacks Lumu recorded by sector.

### Infostealers by Sector

| | |
|---|---|
| Government | 19.2% |
| Finance | 18.6% |
| Education | 12.1% |
| IT & Software | 9.6% |
| Healthcare | 6.6% |
| Nonprofits | 4.7% |
| Telecommunications | 3.3% |

Lumu's data shows education in the top three. This cements its place as one of the most preyed upon sectors.

The stolen credentials from school networks are uniquely valuable. They may provide access not only to the institution's financial data but also to the sensitive personal data of students and faculty, which can be used for identity theft for years to come.

## Case Study: Lumma Stealer

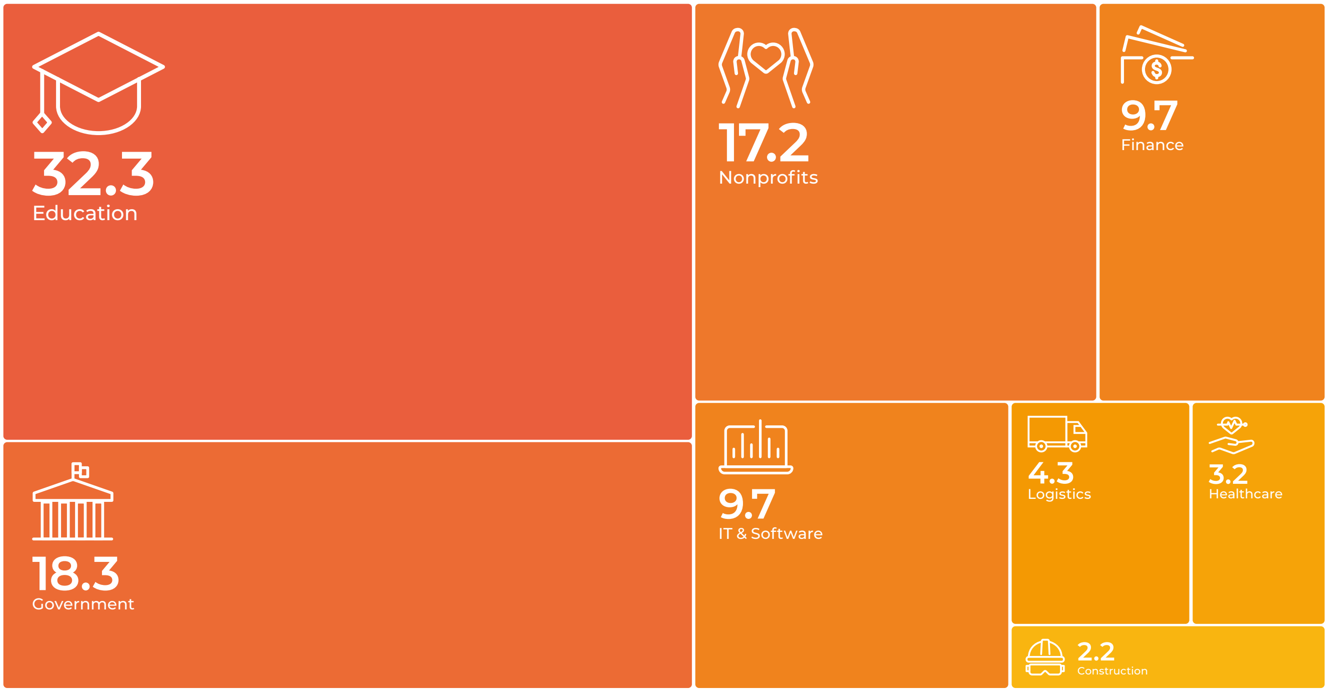
Lumma Stealer became the top infostealer threat in 2025, largely because it's sold like a subscription service on the dark web. This Malware-as-a-Service model makes it easy for many criminals to use. The threat is so significant that law enforcement recently dismantled its network, but it rebounded almost immediately.

Lumma Stealer focuses on the exfiltration of sensitive user data. Its primary targets include login credentials, such as:

- Usernames and passwords
- Browser cookies, history, and saved form data (autofill)
- Data from two-factor authentication (2FA) browser extensions

Unlike the general infostealer stats, the education sector is the top target for Lumma malware.

Lumma Stealer in the USA by Sector



Criminals using this tool have identified school networks as a target-rich environment. While schools depend heavily on technology, there are likely to be many users (students and faculty) and relaxed security practices — opening the door to valuable personal data, access to financial accounts, and ransom demands.

## Hiding Their Identity: Anonymizers

Many people use anonymizers for positive motives, for example, to protect privacy and bypass censorship. Attackers, however, can use them to hide their harmful actions.

Criminals often use something called the Tor network. Tor sends internet traffic through many layers of scrambling and relays, which makes the source very hard to find. Tor was first developed to protect privacy and secure messages — but attackers use it to make it harder to spot and stop them.

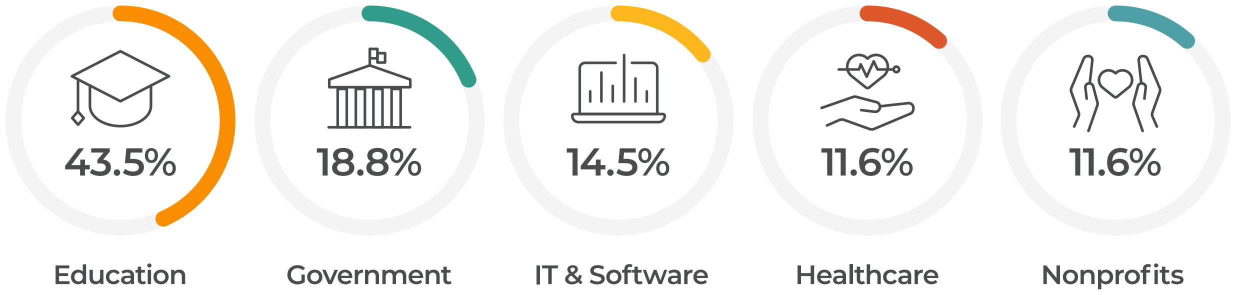
### Why Is Anonymization Dangerous?

Anonymizers change locations or hide IP addresses. This makes traffic look authentic so that it can avoid security controls. Malware can use Tor to hide the location of its command and control servers, making it harder for defenders to find and stop the attackers' systems.

Bad actors also utilize Tor for data exfiltration. Tor's anonymity lets malware sneak sensitive information out of hacked systems. It also makes it difficult to trace the destination of the stolen data.

### Anonymizers in the USA by Sector

The use of anonymizers for attacks has greatly increased in all sectors in the USA. Our data shows that schools and education, however, have experienced the highest number of these incidents by a significant margin.



Attackers are taking deliberate steps to hide their identities, fully aware that they are targeting critical infrastructure and sensitive data related to children.

Attackers use anonymizers to get around security by looking like normal activity. This can help infostealers and ransomware steal data, which is often the main goal of school attacks. Anonymizing the attack source also makes it much harder to trace ransom payments.

This widespread use of anonymizers highlights a critical security gap. When attackers can hide their origin, perimeter defenses are no longer sufficient — telltale signs like IP Addresses cannot be seen. This necessitates a shift towards network visibility — the ability to monitor internal traffic, analyze its behavior, and expose malicious actions, even when the source is anonymous.

## Going For The Money: Ransomware

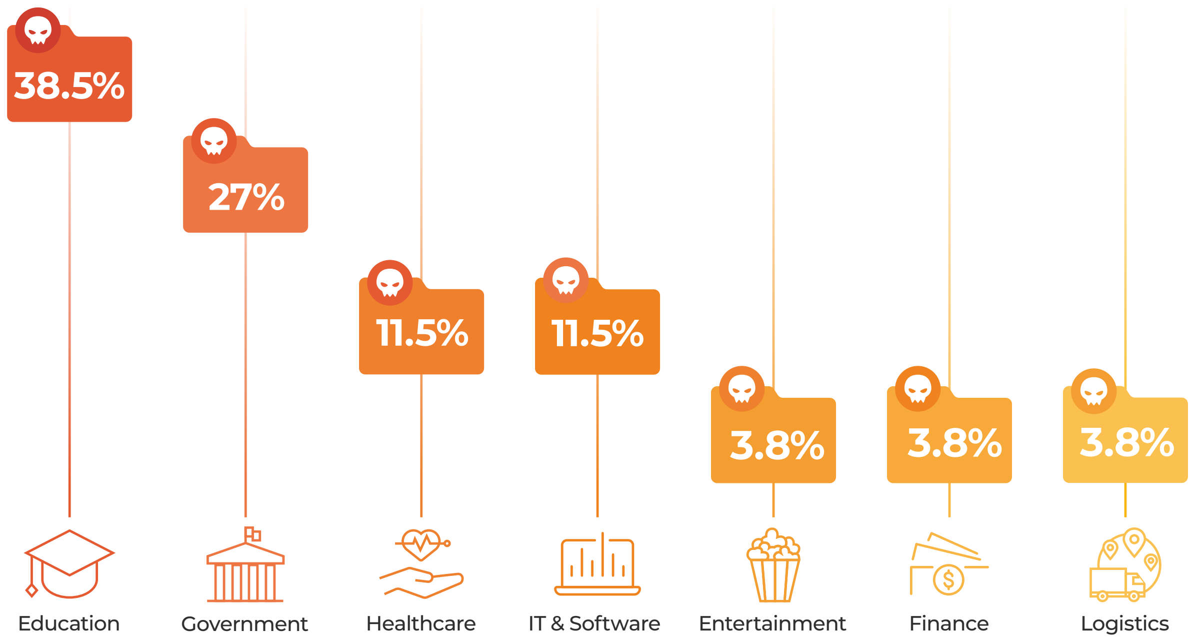
Over the time period of this report, ransomware was the cause of nearly one out of every six incidents detected by Lumu. Given the havoc that can be caused by a ransomware attack, this is a statistic that will set alarms ringing.

A successful ransomware attack goes beyond just locking data. It cripples daily operations, cancels classes, exposes schools to regulatory fines, and incurs massive recovery costs, whether the ransom is paid or not.

### Sectors Most Affected by Ransomware

Lumu has consistently observed that Education is the top sector hit by ransomware. Ransomware gangs tend to target sectors where they can cause maximum disruption. The impact on students' education and a schools' reputation increases the probability of a ransom payment and often allows attackers to demand higher amounts.

Sectors Most Affected by Ransomware in USA



An attack may start with a single deceptive email. The user downloads a dropper that delivers an infostealer. The data that is extracted from your network is sold on the dark web. A criminal buys the access credentials and delivers ransomware. The successful attack locks you out of your system and demands a ransom be paid or the data will be deleted or released.

This shows how easily criminals can get past defenses and start moving around your network. So what can be done?

## Securing Education in an Evolving Threat Landscape

As we have seen in this report, from the initial phishing email to the final, devastating ransomware payload, attackers leverage a full suite of tools to achieve their goals. Protecting schools requires moving beyond traditional perimeter defenses, which often miss the subtle internal activity that signals a breach.

This is where Lumu Defender's Network Detection and Response (NDR) provides a critical advantage. By continuously monitoring all network traffic, Lumu can see the threats other tools miss: the dropper communicating with its server, the infostealer exfiltrating data through an anonymizer, or the lateral movement that precedes a ransomware attack.

For often under-resourced IT teams, Lumu NDR acts as a force multiplier. It continually assesses the network 24/7 to immediately spot unusual activity and respond in real time, ensuring that students' education isn't disrupted. It provides clear, actionable insights to your IT team. You don't have to fight this battle alone.

Lumu is committed to protecting our schools. Contact us today to discuss how we can secure your institution and learn about special pricing programs available for the education sector.

www.lumu.io

**Lumu Technologies** | 8600 NW 36th Street, Suite 150 Doral, FL 33166 | info@lumu.io | +1 (877) 909-5868