



**SECURITY**  
INFOWATCH.COM®



# CAMPUS SECURITY

Cover image credit: ©Christopher Boswell

# EVERY ENTRANCE. EVERY HALLWAY. *ALWAYS PROTECTED.*

From K-12 schools to sprawling university campuses, safety teams protect more ground with fewer people, and less time to act when seconds count. The Ambient platform delivers Agentic Physical Security across every building and entrance, autonomously detecting weapons, unauthorized access, and perimeter threats the moment they emerge. It sees the threat, reasons about the context, and triggers response in seconds, across the cameras, VMS, and access control you already have.

## 01 / SEE

### AMBIENT FOUNDATION

AI-native VMS. Unifies every camera across every building and campus into one intelligent system, built on reasoning AI from the ground up.

## 02 / DETECT

### AMBIENT THREAT DETECTION

Real-time detection of weapons, fights, intrusion, and pre-incident behaviors across entrances, hallways, and grounds.

## 03 / CONTROL

### AMBIENT ACCESS INTELLIGENCE

Correlates access events with live video to catch tailgating, propped doors, and after-hours entry across dorms, labs, and facilities.

## 04 / RESOLVE

### AMBIENT ADVANCED FORENSICS

Natural language search across recorded video. Safety reviews and investigations resolved in minutes, not hours.

## OUTCOMES SCHOOL & CAMPUS SAFETY TEAMS MEASURE

# 24/7

autonomous detection across every camera

# < 1 MIN

to resolve 90%+ of alerts, from detection to action

# 10x

faster response through automated escalation

See what Agentic Physical Security looks like across your campus.

[AMBIENT.AI/DEMO](https://ambient.ai/demo)

[BOOK A DEMO →](#)



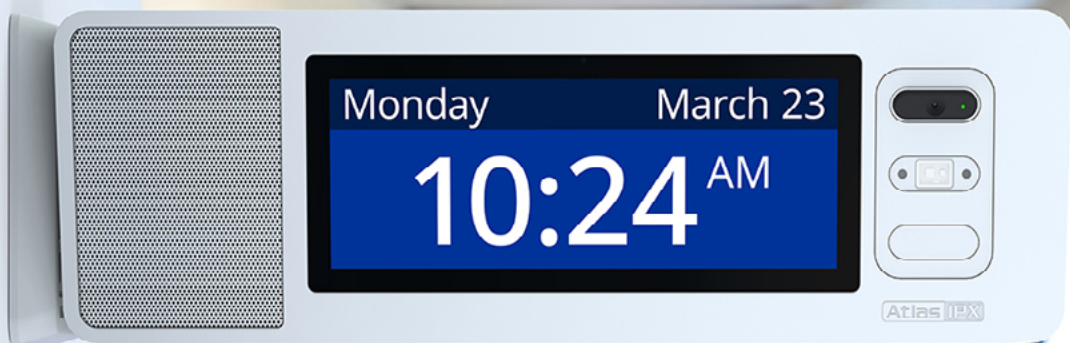
# CONTENTS

## ARTICLES

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| Can AI Technology Really Stop School Violence Before It Happens? .....             | 5  |
| Beyond Locks and Keys: Why Access Control Is the Foundation of School Safety ..... | 12 |
| Before Technology: Why School Security Must Start with the Fundamentals.....       | 16 |
| When AI Learns to Lie: The New Era of Campus Phishing.....                         | 21 |
| Safer Schools, Stronger Societies: Rethinking Student Security for 2026.....       | 29 |

## ADVERTISEMENTS

|                                  |    |
|----------------------------------|----|
| Ambient.ai .....                 | 2  |
| AtlasIED .....                   | 4  |
| NAPCO Security Technologies..... | 11 |



# Meet the AIX Series

An extensive safety system - mass notification, gunshot detection, AI-enabled gun identification, environmental oversight, visual notification, intercom - with one network drop.



**MORE CAPABLE. MORE ACCURATE. MORE INTELLIGIBLE. MORE SECURE.**



**RAPID  
ALERT**

**WEARABLE  
SECURITY BADGE**

**Alyssa's Law Compliant**

**Atlas IPX**

An AtlasIED Brand



Tell me more



Check us out at [AtlasIED.com](https://atlasied.com)  
or engage with us on your  
favorite social media platform

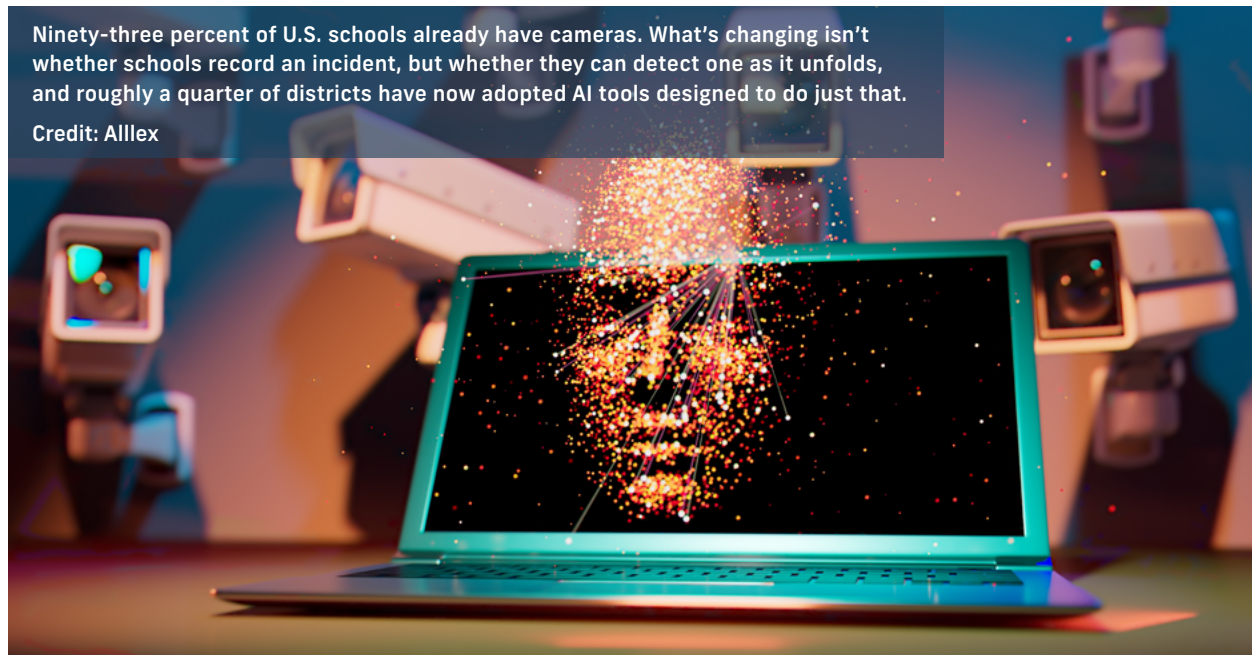
# Can AI Technology Really Stop School Violence Before It Happens?

An AI detection system in one district identified six real firearms, while a similar system in another district mistook a bag of chips for a weapon and brought police in with guns drawn. As AI threat detection spreads through K-12 security faster than anyone can evaluate it, the answer from the people building and deploying the technology is more layered than any single case would suggest.

BY HOWARD CARDER

Ninety-three percent of U.S. schools already have cameras. What's changing isn't whether schools record an incident, but whether they can detect one as it unfolds, and roughly a quarter of districts have now adopted AI tools designed to do just that.

Credit: Alllex



Montgomery County, Maryland's chief safety officer wrote to families at three pilot high schools, Seneca Valley, Bethesda-Chevy Chase and Magruder, on Feb. 8, 2026, describing a short trial period of an AI-powered weapons detection system. The next day, a 16-year-old brought a gun into [Thomas S. Wootton High School](#), a fourth school in the same district that wasn't part of the pilot and shot a classmate. The timing was coincidental, but the questions it raises are not.

Within just a few years, AI threat detection has moved from a novelty discussed at trade shows to something districts feel they can no longer ignore. Ask the people who build and sell these systems and live with the consequences when they succeed or fail, and the answer to whether AI tools actually work is far more layered than any single case makes it look.

This isn't a story about whether AI belongs in school security, since it's already there and

expanding faster than most districts can evaluate it; it's a story about what the technology can and cannot currently do, and why the security professionals closest to it keep arriving at the same conclusion from different directions: that the technology was never the variable that mattered most.

### Ninety-Three Percent of Schools Already Watch

Ninety-three percent of U.S. schools already have security cameras, according to [National Center for Education Statistics](#) data, a number that has held steady for years and suggests cameras were never really the problem; camera use is widely accepted. The gap security leaders are working to reduce now is the distance between recording an incident for forensic use and proactively detecting an event as it unfolds, and that's where AI has potential. A May 2026 [EdWeek Research Center](#) survey found roughly a quarter of districts now use AI-enabled camera monitoring to flag weapons or physical altercations, a sharp jump from a few years ago.

Daniel Young, founder and chief innovation officer at [Circadian Risk](#), frames AI's value through what he calls the three Ds and three Rs: deter, detect, delay, then respond, report, recover. In his view, AI's most defensible role sits early in that sequence, since proactive security doesn't start inside the building.



*Daniel Young, founder and chief innovation officer at [Circadian Risk](#)*

"You can't start within the building," Young said. "These individuals have to get to the door. If you're using AI, it needs to be on analytics cameras, on devices where we can actually

see these things happening quickly. Catching potential problems from the perimeter inward is key, because the average response time to an active shooter event is under three minutes, so the quicker the detection and response, the less severe the outcome tends to be."

Ron Self, director of strategic initiatives at [CENTEGIX](#) and a former district end user of the company's alert platform, measures smart tool use and success from his company's own data. Drawn from more than 346,000 alerts across 18,000-plus locations in the 2025-2026 school year, CENTEGIX found that 99% of events were everyday emergencies rather than campus-wide threats. Medical events, behavioral incidents, and student elopement were the top concerns.



*Ron Self, director of strategic initiatives at CENTEGIX*

"The real question districts should be asking isn't just, will this work during an active threat," Self said. "The question is, will our staff actually use this technology

every single day, and will it also work when the worst day comes?"

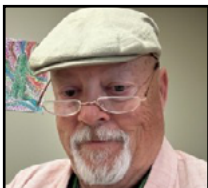
Another dimension to this issue is that in the face of rapid deployment and constant innovation, governance hasn't kept pace with the topic. ASIS International, for example, published its first [School Security Standard](#) within the past year and is already revising it, while the Security Industry Association's [2026 K-12 School Security Symposium](#) brought vendors, administrators and law enforcement together to work through how the standard fits alongside other frameworks, a sign that deployment is outpacing any shared understanding of how to deploy AI-powered tools effectively and responsibly.

### When It Works, and When It Doesn't

The clearest way to understand where these systems succeed and fail is through the incidents themselves, which are mixed enough to unsettle anyone looking for a simple verdict.

A 17-year-old shot and killed a 16-year-old student at [Antioch High School](#) in Nashville in January 2025, after the district's system failed to identify the weapon. Investigators attributed the failure to the camera's positioning relative to the shooter, rather than a flaw in the underlying model. [Nashville Public Schools](#) responded by installing a similar system districtwide, and by March 2026, those systems had detected at least six guns, evidence supporting that the technology can work when positioning and coverage are optimal.

The news cuts the other way in Baltimore County, where a system flagged a [Kenwood High School](#) student's hand movement while he held a bag of chips as a possible weapon and police responded with guns drawn. A subsequent [inspector general review](#) cleared the system of bias but recommended additional staff training before alerts reach a response team, and in the same report, a security official in a neighboring district running the same system said his program has recorded zero false positives of that severity, crediting the difference to routing alerts to trained security staff rather than building principals.



*Guy Bliesner, a school safety and security analyst for the state of Idaho and a founding board member of the [National Council of School Safety Directors](#).*

Even so, the security professionals interviewed for this article don't see these incidents as evidence that AI doesn't belong in schools. Guy Bliesner, a school safety and security analyst for

the state of Idaho and a founding board member of the [National Council of School Safety Directors](#), arrived at the same conclusion as Young and Self: detection without human verification and follow-through is where these systems break down, not the underlying pattern recognition itself.

"We [schools] do not have an eye in the sky. We don't have a bunch of people sitting in a room looking at monitors with a radio ready to call out a response team," Bliesner said. "With many of these false positives, the data may not have been reviewed properly before they decided to call out the cavalry. If we rely solely on AI, it's like relying solely on a fire alarm system. We get spurious fire alarms fairly regularly. It doesn't mean that the system necessarily failed."

### The Other AI

Despite covering different corners of school security, all those interviewed for this article arrive at the same conclusion: the technology is meant to amplify people, not replace them. Bliesner has made that case publicly for years, including to a room full of vendors at the ISC West trade show, where he argued that most of what they sell isn't a solution at all.

"Security integrators do not provide solutions," Bliesner said. "They provide tools that, when effectively used to address an identified threat, may be a solution. Most school security failures are human, not equipment, failures. Stuff doesn't keep schools safe. People keep schools safe."

That thesis has a name Bliesner has written about under his own byline: the other AI, or "active involvement," a phrase he uses because the human element mattered in school security long before artificial intelligence did.

Daniel Young makes the same point from the risk-management side of the business. In his experience, the schools with the most impressive countermeasures on paper aren't necessarily the safest ones.

"The countermeasures, the ones with the best countermeasures, aren't going to be the winning culture or the winning organization," Young said. "It's going to be the organization that understands its risk the best. We look at schools, even the most recent events, and they have countermeasures in place already, and we're still seeing school shootings. It's not necessarily a technology issue; it's a culture issue; the recognition that these tools are there for a reason."

AI's real value, in his view, is filling that gap for people who were never trained to spot threats, much like how an untrained observer might walk right past a health emergency that a doctor would recognize instantly.

"Individuals who are not trained to see that type of thing, and the expectation that they should be aware of it, are two entirely different things," he said. "That's where AI can help, amplifying our thought process to an individual who doesn't have that insight and training."

Ron Self sees the same balance play out at the product level. The systems he works with were built around a badge a staff member presses to summon help, with AI-triggered detection layered on top of that human step rather than replacing it.

"In a crisis, the person closest to the incident is still the fastest and most reliable sensor in the building," Self said. "Human intuition and AI technology are not competing philosophies. They are complementary layers. The AI never gets tired

and it never hesitates. A human operator never gets fooled by context. By bringing them together, we close the safety gaps that either one would have if left completely alone."

Geva Barash, whose firm [Secure Our City](#) designs low-voltage security systems for schools and public safety facilities, pushes the same idea further still, arguing that most people think of school AI as cameras and little else.

"AI is not just for security cameras," Barash said. "Take a look at the IT racks. You're using smart tools that leverage analytics to secure your data, and they learn your data usage patterns so they can notify you of any irregular activity or breaches. AI is used in data protection, device protection, and so forth. We now use vape sensors in many of the schools we work with, and they provide about 30 different readings on air quality, temperature, and the presence of smoke or vaping. There's definitely a lot of opportunity in schools for the use of AI."

### The Line Districts Are Reluctant to Cross

Barash's most counterintuitive finding from his work with districts is that privacy, in the broad sense, is rarely the sticking point.



*Geva Barash, is the CEO of [Secure Our City](#) designs low-voltage security systems for schools and public safety facilities.*

"Privacy is not a major issue," he said. "All the schools have cameras. It's more of a question of whether they're willing to do facial recognition, and how deep they want to use the information they have."

He's taken that same distinction directly to lawmakers, testifying before the Connecticut General Assembly

on a proposal to use facial-recognition technology in a public-safety building. He told the room there were no photographs involved, no images stored anywhere, then turned the question back on the assembly members themselves by asking how many of them had a campaign photo on their website, or their own face on a yard sign at election time? Every hand went up.

"So, you're okay with your face being everywhere," Barash told them, "but the one place that doesn't have your face, and lets me recognize you coming in and open the door for you automatically, that's not okay?"

That same split in perception shows up nationally in a patchwork of conflicting laws: New York has moved toward a moratorium on biometric surveillance in schools, while Georgia's HB 268 goes in the opposite direction, mandating panic-alert systems and formal threat-assessment teams. Districts operating across state lines are left to navigate that patchwork with no consistent guidelines, and even when a state does weigh in, the law doesn't settle the harder, day-to-day questions for them.

Self, who has helped hundreds of districts work through their own data retention and privacy decisions, said the variation runs deeper than state lines. No two districts land in the same place, he said, even within the same state.

"If you've seen one school, you've truly only seen one school," he said. "They each function as their own unique ecosystem." His advice is to start with the people who will actually respond, not a compliance checklist: "There's no need to reinvent the wheel here. There are plenty of ready-to-use resources and blueprints districts can customize for their exact workflow."

### What Comes Next

The standards effort that began with ASIS's first School Security Standard is already moving into a revision cycle less than a year after publication, and Young has floated the idea of a national compliance index to track how many districts actually meet the standard's baseline requirements, rather than simply buying technology and assuming compliance follows.

"We need to know how many schools are actually complying with the must-have standards," Young said. "It would give us a good sense of where we need to improve."

The [Partner Alliance for Safer Schools](#) is a third major framework districts and security professionals can lean on, alongside ASIS and SIA. PASS released the seventh edition of its free Safety and Security Guidelines this spring, and its July Summer Summit is running a session specifically designed to show districts how to use the two frameworks together: ASIS for overall risk management, PASS for hands-on steps at the campus level, evidence of how much coordination this space still needs.

Bliesner brings a facilities-and-funding lens to the same question, tracking where state and federal security dollars are landing relative to what the incident record suggests should be prioritized, and he's blunt about the mismatch.

"In many cases, we're giving people the security house, or the roof to their security house, when they have no foundation," he said, pointing to schools where duress panic systems have been mandated even as basic classroom door locks remain unreliable.

### The Question That Matters

Three threads run through this story, and none cancel the others out. The modest, defensible take is that AI threat detection hasn't yet proven itself either way. It's a tool, and its value depends entirely on the discipline of the humans running it. Technology itself will keep improving, but likely faster than the training, verification protocols, and the use standards built around it.

The sharper take, echoed independently by more than one source in this piece, is that the real story was never AI versus no AI but culture versus countermeasures. A district that buys detection technology without investing in the human systems around it is buying a false sense of security.

And the forward-looking take is that the standard-setting happening right now through

ASIS, SIA, PASS, and a growing patchwork of state legislation is racing to catch up with deployment that has already outpaced it. The next few years are likely to determine whether AI threat detection becomes a mature, governed practice or a cautionary case study.

### About the Author

**Howard Carder** is a seasoned freelance writer specializing in the physical security and professional audio/video industries. With over 30 years of experience, including a long tenure at a large, global video security company, Howard has crafted compelling content for leading brands and publications across the industry. His expertise spans video security and Pro AV technologies, allowing him to distill complex topics into engaging narratives. Howard's work includes hundreds of case studies, white papers, and thought leadership articles. When not writing, he enjoys playing music and exploring healthy cooking. Learn more at [www.hcwriter.com](http://www.hcwriter.com).

# MVP Cloud Access Control



Ask About  
**NAPCO**  
Proven School  
Solutions

## Most Valuable Platform For Long Term Security



### Smarter Security for Every Door

The NAPCO MVP Cloud Access Platform provides secure, easy-to-manage access control for organizations of any size — from small offices to multi-building campuses.



Control doors, users, and credentials across your facilities from a smartphone or web browser while maintaining strong security & operational flexibility. Integrate with security & video, too.



### Why Choose MVP Stronger Security

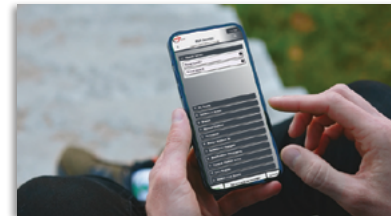
- Custom Access Control for all applications
- Instantly add or remove user access
- Monitor entry activity and door events
- Lockdown or unlock doors remotely – send alerts
- Control access schedules & permissions

### Simpler Management

- Easy App or App/Web-Browser
- No more onsite PCs, servers, hardware upkeep or IT issues
- Manage doors from anywhere
- Easily enroll users and credentials
- Automatic system updates

### Built to Grow With You

- Expand from a few doors to thousands
- Add buildings, users & credentials anytime
- Supports multiple facilities and locations
- Scalable Architecture- No hardware or software to change (*No rip out & replace*)



### One Integrated Security Platform

**MVP integrates multiple security technologies into a unified system:**

- Cloud access control
- Intelligent access panels
- Intrusion system integration
- Wireless access locks
- Multiple credentials
- Video VMS integration

#### MVP EZ

Simple smartphone-managed access control ideal for small & mid-sized facilities

##### Perfect for:

- Offices
- Retail stores
- Medical practices
- Professional businesses
- Restaurants
- Multi-tenant & STR properties



App-Only

#### MVP Access

Easy Auto-Migration to Advanced Hybrid App/Browser-Based Enterprise Version- Advanced centralized access control designed for larger organizations & multi-site operations.

##### Ideal for:

- Corporate facilities
- School campuses
- Healthcare organizations
- Industrial facilities
- Transportation.
- Enterprise operations

Web Browser  
& App



1.800.645.9445 • MVPAccess.com

MVP Access/EZ are trademarks of NAPCO Security Technologies, Inc.  
Other marks remain intellectual property of respective cos.

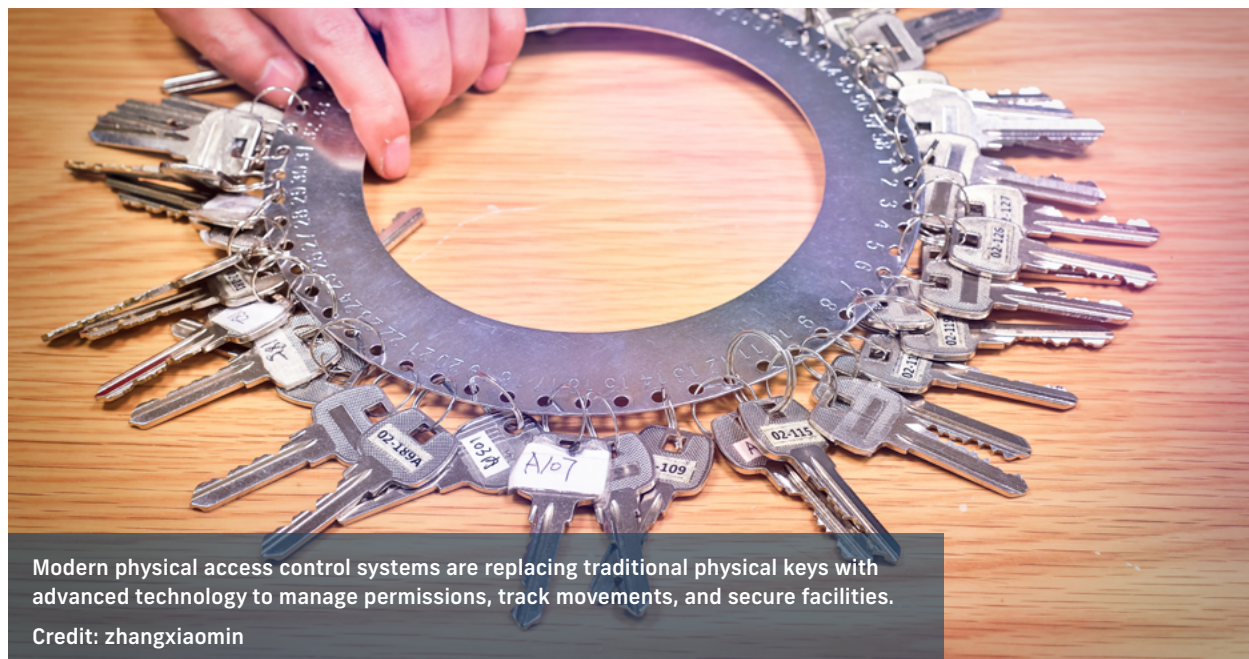
Meet Up or  
Request Demo  
(Scan QR Code)



# Beyond Locks and Keys: Why Access Control Is the Foundation of School Safety

Modern access control is no longer just about replacing metal keys with electronic credentials. It gives school leaders the visibility, accountability, and real-time control they need to protect students, reduce risk, and respond confidently to emergencies.

BY SHARON HONG



Modern physical access control systems are replacing traditional physical keys with advanced technology to manage permissions, track movements, and secure facilities.

Credit: zhangxiaomin

"What keeps me up at night is not knowing how many doors I have and who has the ability to go through those doors." And then she paused thoughtfully to reflect. For that brief moment, everyone in the room could feel the gravity of her words.

I was a technologist at the time, responsible for working with customers on integrating their security technologies: video surveillance, access

control, voice communications, and incident management. On that day, I was in a meeting at a well-known local private school with the principal, the assistant principal, and their school resource officer. I was joined by a team representing physical security, communications, and software solutions, and my role was to help connect the pieces into a broader school safety strategy.

We presented a high-level overview to help shape the discussions, then opened the floor for questions to learn more about their operations and their needs for school safety. What did they use for cameras, radios, software, and system integrations?

When I asked what they used for access control, the principal asked, "What's access control?"

We explained that modern physical access control systems are replacing traditional physical keys with advanced technology to manage permissions, track movements, and secure facilities.

And then she told us how that was what kept her up at night. They had analog locks and keys. She didn't know exactly how many doors they had, if or when they were locked, and who had keys that shouldn't have them.

Against the backdrop of a discussion about integrations, software, and advanced security technologies, we collectively realized that none of it mattered to her. The real need for this school wasn't a more sophisticated security ecosystem. It was access control.

She wasn't alone. Many of the principals, security directors, and superintendents I met while in the role were similarly situated. Managing and controlling who had access to the interiors of their schools was no doubt a challenge.

"There's a joke we used to have at one of the schools I worked at years ago," says A.J. Stich, founding principal of The Greater Dayton School in Ohio, "When you became a principal, one of your welcome gifts was a basket of keys."

### The "Key" Challenges

With a basket of keys comes a number of challenges. "Managing those keys was a nightmare," says Stich.

The first challenge is that traditional metal keys are easy to duplicate, making it difficult to track who has access to school doors. While duplicating keys to government facilities, schools, or high-security infrastructure without authorization is illegal and can result in criminal charges, individuals possessing the tools to do this can still easily cut duplicate keys. "We used to have a local guy who made keys for a living," says Dr. William Long, Superintendent of the Center Grove Community Schools Corporation in Indiana. "We used to tell him all the time to stop making copies of our keys, but he'd keep doing it even though the key clearly said, 'Do Not Copy.'"

Restricted, patented, and high-security mechanical keys can help with this problem but are also two to four times as expensive as traditional keys. Additionally, while master keys allow critical operational leaders to open doors across the school or district, losing one can be very expensive. The result is the replacement of all locks accessible with the master key and the reissuing of the master keys. Depending on the size of the school district, this could be a six- or seven-figure problem to solve.

Another challenge is that for every locked door a teacher or staff member needs to enter, there is another key they have to carry and fumble with.

When a key is required to enter and exit a high-traffic door, it leads to a third, critical challenge: the propped door. Propping a door open is a simple

solution for school faculty who make multiple trips to and from the school parking lot, rather than fumbling with keys each time. It is also common for gym doors to become unlocked by staff to accommodate school teams coming to and from practice. Unfortunately, they forget to lock them again.

Many times, when a door is unlocked or “propped open,” it can be cracked open just enough that it does not latch and goes undetected by the human eye. This is one of the most significant physical security vulnerabilities in school safety. Every school leader believes their exterior doors are secured. Unfortunately, an undetected propped door can defeat even the most carefully designed security procedures without anyone noticing.

### The Difference Between Managing Keys and Managing Access

Often, when people use the term “access control” in physical security, they think of the physical elements of these solutions: doors with electronic or wireless locks, key cards and readers, and access management software. But the issue isn’t really about replacing traditional keys and locks with new technology.

The real issue is that administrators lack visibility and control over who can enter the building and when. “Access control” is exactly as it is named. It gives administrators control over who can enter their buildings, where they can go, and when that access changes.

Access control enables schools to not only increase their safety measures but also create a more efficient working environment:

- A teacher’s card credential doubles as their ID and allows them to easily move through every

door they need access to, saving them the effort of carrying separate keys and searching for the right ones to open specific doors.

- The credentials of a school district employee can be instantly deactivated when they leave or are dismissed, preventing them from accessing unauthorized entries into the school.
- School leaders no longer need to manage a set of traditional keys, make copies, keep track of who has which keys, and prevent unauthorized copies. They can now manage all of that with a single software interface.
- A lost access card does not lead to the replacement of existing locks, and can be deactivated remotely, with a new one issued within minutes.
- School security teams know exactly who has entered the school premises and are alerted when specific doors are opened when they shouldn’t be or if one is propped open. They can also remotely lock a door or doors as needed.

The goal is no longer just to secure doors, but to eliminate uncertainty about who has access and to enable administrators to respond quickly during emergencies.

### Overcoming the Challenges of Funding, Deploying, and Managing Access Control

From a funding standpoint, the lowest barrier to entry for procuring access control systems is during the construction of new school buildings. “We built [The Greater Dayton School] with access control in mind,” says Stich. Over the last several years, the need to add access control to other parts of the building emerged. To fund this expansion, Stich and his team learned about a grant opportunity through the Ohio Department of Administrative Services’ InnovateOhio Platform, OHID.

At Center Grove Community Schools, Dr. Long took a pragmatic approach. Access control was incorporated into the design and construction of new schools, while existing buildings were upgraded over time through a phased retrofit strategy. One of the biggest considerations for older facilities is that each controlled door typically requires an electric strike: an electronically operated latch that allows authorized users to gain entry with a credential. Since electric strikes also require power at the door, districts should factor both installation and electrical work into their budgets and project plans.

Schools with existing access control systems need to ensure their technology stays current. “We had an older access control system when I came into the job,” says Lou Cammisio, Director of Safety and Security at Naperville Community Unit School District 203 in Illinois. “After we discovered a security vulnerability with the old system, we prioritized the funding to upgrade our access control to an encrypted solution to prevent hacking into the system.”

K-12 schools considering investing in access control systems but feeling overwhelmed about where to start can begin with the exterior doors that see the most traffic. A small investment can make a significant operational impact. “At one of the schools I worked at, there were six

exterior doors, two of which were the primary and secondary entrances,” Stich says, “By implementing access control at those two doors, we could have eliminated keys that we issued and managed across 80% of teachers and staff.”

### Investing in Certainty

“To thrive in school you need to feel safe,” says Cammisio. When I think back to the principal who asked about access control, I realize her concern wasn’t really about doors. It was about uncertainty.

Access control provides the foundational peace of mind required for that environment of safety to exist. By replacing the heavy, uncertain basket of metal keys with digital visibility, school leaders can stop guessing who has access to their buildings. When educators don’t need to worry about safety, they can focus on what matters most: teaching.

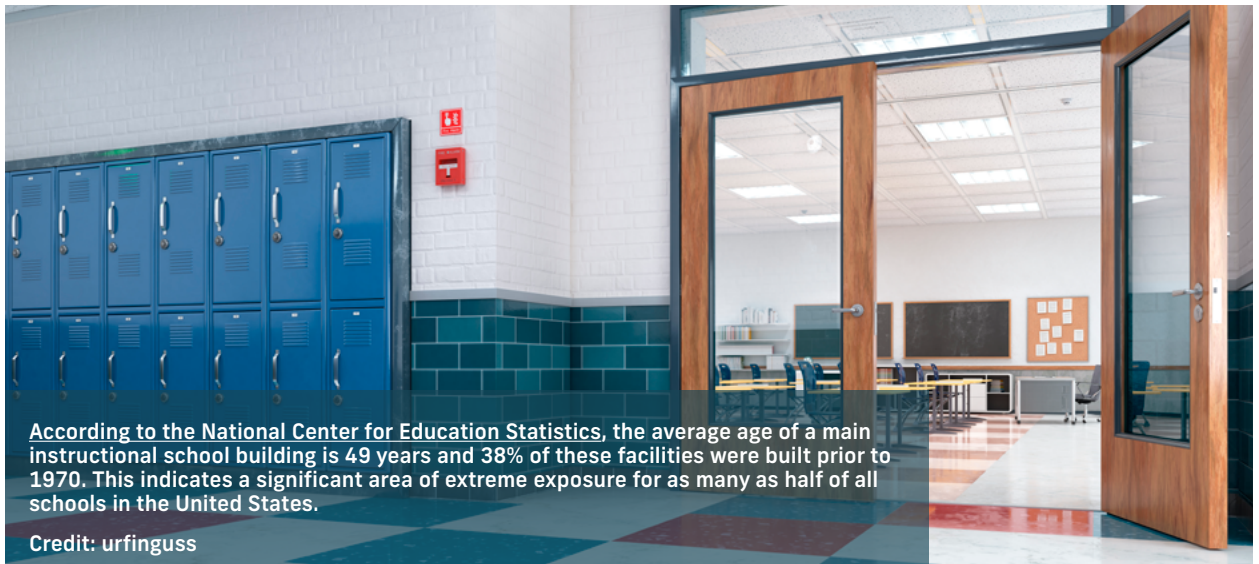
### About the Author

**Sharon Hong** is a seasoned executive with over 20 years of experience in the safety and security industry. She previously served as Vice President of Ecosystem Solutions and Sales Engineering at Motorola Solutions. Throughout her career, she has led across engineering, product management, presales, channel sales, sales operations, and service offers. She holds a B.S. in Electrical Engineering from UCLA and an M.S. in Engineering Management from USC.

# Before Technology: Why School Security Must Start with the Fundamentals

As lawmakers race to mandate the latest school security technologies, many K-12 campuses still lack the most fundamental layer of protection: classroom doors that can be secured quickly and safely. Lasting school safety begins with risk-based planning—not one-size-fits-all mandates.

BY GUY BLIESNER



According to the National Center for Education Statistics, the average age of a main instructional school building is 49 years and 38% of these facilities were built prior to 1970. This indicates a significant area of extreme exposure for as many as half of all schools in the United States.

Credit: urfinguss

Violence, and in particular gun violence, in our K-12 schools has altered both the perception and reality of the safety of the K-12 school environment. No one would argue that the human cost has not been tragically high; there have been far too many victims. But there is a forgotten victim in all this.

The entire K-12 school system of the United States has been, to an extent, victimized by the

incidents at Columbine, Sandy Hook, Parkland, Uvalde and all the rest. This is not hyperbole. It is a simple acknowledgment of the fundamental alteration in both perception and reality for K-12 schools. The entire K-12 school system of the United States has been victimized. Issues of school operations for students, parents, teachers, administrators, and policymakers have been fundamentally altered.

### Every School Is Different, So Is Every Security Risk

School safety is always a thorny topic, particularly following an incident of violence in a school. As we grapple with the fallout, policymakers at both the state and federal levels are under intense pressure to act and be seen as doing “something” to make schools safer. Couple this with an incredible amount of noise and chaos in the school security space, with manufacturers, vendors, and school safety advocacy organizations pressuring for the immediate purchase and deployment of the things they make, sell, or advocate for. This creates a “perfect storm” situation, ripe for poor decision-making.

In most cases, I do not ascribe ill intent to any of the parties involved, but I am fond of a quote from Vikram Seth: “God save us from people who mean well”. This quote applies here. Far too often recently, the answer has been a one-size-fits-all statutory mandate to deploy a specific technology or process universally at all the schools under their jurisdiction.

Unfortunately, there are no easy answers. No “one size fits all” solution. No “buy this one thing” school safety remedy. No “just do this, and your school will be safe” process. The radical differences in exposure, security posture, school community demographics, location, building design and condition, and a dozen other factors preclude a universal “best” answer to security improvement at any individual school.

Monies are being allocated and mandates developed. With well north of three billion dollars annually from a variety of sources directed at school security issues in the United States, the issue is less a lack of funding and more a lack of understanding to address the foundational needs. These well-intentioned mandates fail to account

for the unique conditions that exist in every school and district in the United States.

### The Forgotten Foundation of School Security

Recent research from the [ALERT Center at Texas State University](#) reaffirms that a classroom door with proper locking hardware is a leading practice in school security. This aligns with recommendations in ASIS International’s School Security Standard, P.A.S.S. K-12 School Safety and Security guidelines, and the “Foundational School Physical Security” position paper. There is consensus that a classroom door that meets the guidance’s requirements is an effective protective factor against an active shooter incident.

Current recommendations are that all classroom doors in a K-12 school should be fire-rated, solid-core types installed in welded metal frames with appropriate hardware and a lockset that can be secured from the interior of the classroom without a key. Door hardware should be ASTM and UL listed and meet IFC, NFPA, and ADA requirements. Secondary locking, barricade, and blockade-type devices not listed and not meeting applicable code should not be used.

[According to the National Center for Education Statistics](#), the average age of a main instructional school building is 49 years, and 38% of these facilities were built before 1970. This indicates a significant area of extreme exposure for as many as half of all schools in the United States.

So how did we get to the current condition? Design planning assumptions were different. Well into the 1990’s, classroom door hardware was designed to preclude a student from locking the

door while a teacher was outside the classroom. In some cases, this meant that there was no locking mechanism on the interior side of classroom doors. In others, it meant a keyway requiring a metal key was installed. In either case, there are significant operational impediments to quickly locking the classroom door, particularly in a high-stress incident. This creates a significant vulnerability for as much as half of all classrooms in the U.S.

This has also created a whole segment of the school security industry, manufacturing and aggressively marketing classroom door secondary locking and blockade devices that, in most cases, fail to meet classroom egress code requirements.

In any school constructed before 1970, the door itself and the frame it is installed in could pose a vulnerability, as well. Lightweight interior-grade doors in wooden frames were the rule rather than the exception. Here, the design planning assumption was much more concerned with cost efficiency than with a classroom environment that could be quickly and effectively secured.

Understanding the research, it would seem to make sense to address this issue of classroom doors. And that begs the question, "How many classroom doors in the United States fail to meet the standard?" While specific data is unavailable, inferences can be drawn from the school's age and the building code in effect at the time of construction.

### Technology Can't Replace Physical Readiness

The current focus of legislative policymakers across the nation seems to ignore one of the most foundational needs: the ability to quickly and effectively lock the classroom door in favor of technology-based enhancements.

Many mandates focus on a silent panic alarm system directly connected to law enforcement. Often included is mandated GIS mapping of the school grounds and building. The intent is to provide both a faster response time and enhanced wayfinding for law enforcement during an active shooter event. I don't disagree with the statement that this may benefit some schools in such an event. A 30-second reduction in response time from 4 minutes is significant and will likely save lives.

However, a school without the ability to effectively lock classroom doors will still be more exposed during that faster response. Don't overlook that rural and remote schools (more than 50% of U.S. schools) with protracted response times will benefit significantly less from such a system. In both cases, a classroom door that can be quickly and effectively locked is a required school response.

Another area where we see emerging legislative mandates is weapons detection. Both walk-through and handheld systems are the subject of this effort. There is an increasing focus on AI-based visual weapons detection systems. These systems may well serve a viable prevention purpose. However, once detected, the foundational ability to quickly and effectively lock classroom doors in response will be an absolute requirement.

The recent news coverage on the deployment of attack drones in schools in both Georgia and Florida is equally concerning. While I cannot prove it, I strongly suspect that there are classroom doors at schools in both states that do not meet the currently recommended standard. If I were a parent, student, or educator in a school lacking adequate classroom doors, the reported \$ 550,000 allocated to the drone project in Georgia would be a matter of deep concern to me.

Last is a mandate for integrated emergency response technology. A noted practitioner, Guy Grace, calls this a unified life safety system. This is simply common sense: build a security program with systems that work together to achieve a defined goal. Still, a foundational element of this process must include consideration of the securable classroom door.

Please do not misunderstand me. I am not a Luddite, simply opposed to security technologies. Certainly, security technologies and, as they mature, AI-enhanced school security systems in particular will play an increasingly important role in a school's overall security posture. Equally, I'm not opposed to a stronger focus on school safety and security by our policymakers. And I am not opposed to more money directed to improve school safety and security. I am deeply opposed to that limited money being poorly spent and failing to address a school's foundational physical security needs.

The likely outcome here will be akin to mandating that a school must have a roof for its security house when it lacks a foundation. The real risk is that limited funding will be misspent and fail to address the most pressing needs in any given school. A school that lacks appropriate classroom doors that can be locked from inside the classroom needs to be provided with this capability. The resources to address that vulnerability should be provided before legislating and statutorily requiring the deployment of any mandated technological system. The mandated system may well be effective, but it simply does not address the most pressing need in that particular school.

### Policy Must Follow Risk, Not Headlines

As security professionals work with schools, and more importantly, with our policymakers, we need to dispel the idea that a universally

mandated solution applied to every school will make all schools safer. Equally, we need to help our policymakers understand the wide variance in security profiles between schools and districts. More heavily resourced school districts likely have many of the foundational elements of school security in place. Smaller, more rural districts and/or those with aging facilities are likely to lack some of the foundational components of effective school security. This is a case where one size will not fit all.

The failure to focus on classroom doors is understandable. From the general perspective, a door is a door, and a lock is a lock. Doors have been in use forever. The general public and many of our policymakers lack understanding of the foundational function of the classroom door in school security. Additionally, doors and door hardware lack the appeal of the flashier technology-based solutions. And last, we are fighting the perception that if you simply make the right purchase, that one act will make your school secure.

Our policymakers would do well to remember the old educational maxim "access before you treat," and I would add "access before you spend." The recommendation to conduct a comprehensive risk, threat, and vulnerability assessment at any school prior to purchasing and deploying security equipment or technology is an industry standard. This is so common that many federal security grant applications require the assessment component as part of the grant process.

### A Secure School Is a Process, Not a Product

I hope that this will foster a frank and open national discussion asking the simple question,

“What are the foundational elements for a safe and secure school that should be available at every K-12 school and in place protecting every K-12 student in the country?”.

Such a conversation will not be comfortable. There will be an acknowledgment that not all schools are equally secure, and not all students are equally safe. There will be financial implications. Hopefully, the outcome will be a better understanding of the foundational requirements for a secure school by both policymakers and the general public. And the potential for a mechanism to provide resources to schools lacking those foundational elements. One size will never fit all.

There is one factor to be mindful of: regardless of the available resources, at its core, a secure school is not a purchase a school can make; it is a process the school must engage in. It will always be the people of a school community, effectively using the tools available to them to address their identified vulnerabilities and following their security processes with fidelity, who will create a more secure educational environment.

### About the Author

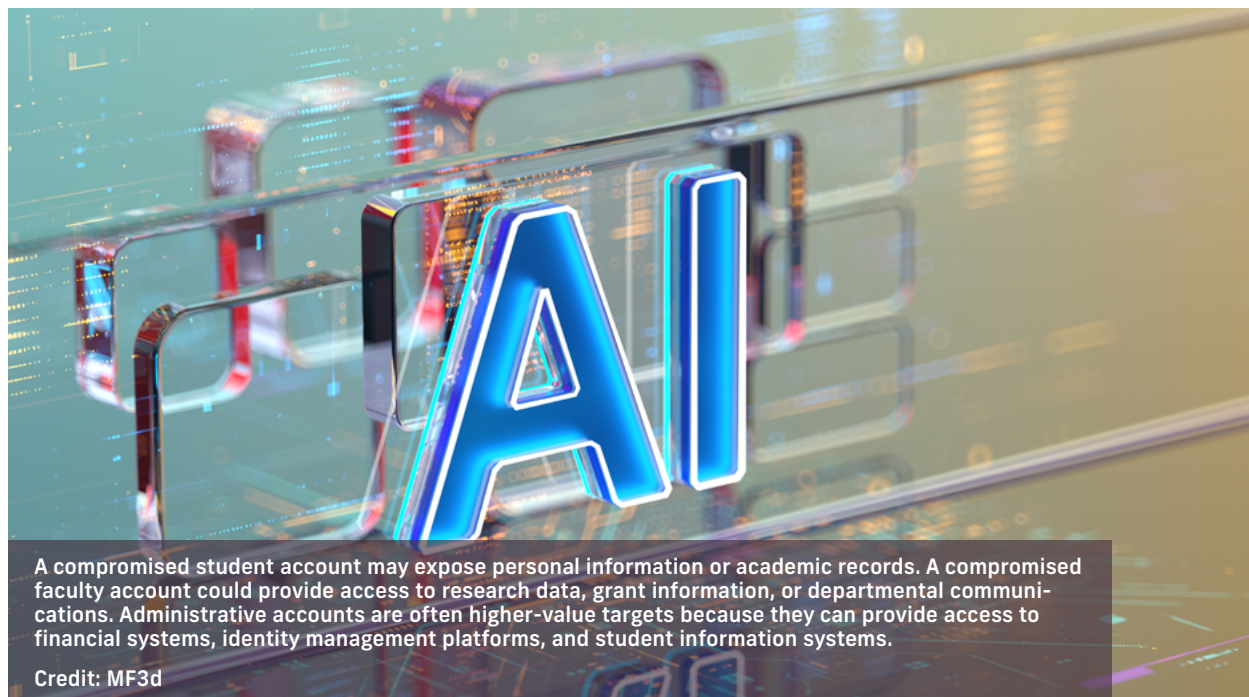
*Guy Bliesner is a School Safety & Security Analyst with the Idaho BOE. President, National Council on School Facilities. Founding Board Member: National Council of School Security Directors. Sub-committee chair for ASIS school safety standards.*



# When AI Learns to Lie: The New Era of Campus Phishing

Artificial intelligence has transformed phishing from mass email scams into highly personalized social engineering attacks that exploit institutional trust. Here's why schools and universities must rethink identity security, authentication, and cyber awareness before the next attack succeeds.

BY ANTOINETTE KING, PSP, DPPS, SICC, CMMC-RP



A compromised student account may expose personal information or academic records. A compromised faculty account could provide access to research data, grant information, or departmental communications. Administrative accounts are often higher-value targets because they can provide access to financial systems, identity management platforms, and student information systems.

Credit: MF3d

At 8:17 a.m. on a Tuesday morning, a university employee receives what appears to be a routine email from the financial aid office. The message references a new federal aid verification requirement, contains institutional branding, and arrives during the busiest period of the FAFSA processing season. Nothing about it seems unusual. The language matches previous campus communications, the request appears

legitimate, and the timing makes sense. The employee clicks the link, signs in, completes the requested authentication step, and returns to work.

Within hours, cybercriminals have access to the employee's account. The message was not sent by the financial aid office, nor was it written by a human scammer. It was generated by artificial intelligence.

While this scenario is hypothetical, it reflects a growing reality facing educational institutions across the United States. Artificial intelligence has fundamentally altered the economics of phishing, enabling cybercriminals to create convincing, personalized social engineering attacks at a scale that was previously impossible. The same generative AI technologies that help students write papers, assist researchers with data analysis, and improve administrative efficiency are also empowering attackers to produce highly targeted phishing campaigns that can mimic trusted voices with remarkable accuracy, at scale.<sup>[1]</sup>

For educational institutions, the threat is particularly acute. Schools and universities depend on trust, collaboration, and open communication. Students, faculty, staff, parents, contractors, researchers, and vendors exchange information constantly, often under tight deadlines and with little reason to question the legitimacy of routine requests. Those characteristics are essential to the educational mission, but they also create ideal conditions for social engineering attacks. As AI-generated phishing becomes more sophisticated, educational institutions are discovering that the very openness that makes learning possible can also enable deception.

### Why Education Has Become a Prime Target

Cybercriminals have long viewed educational institutions as attractive targets due to their limited cybersecurity resources, open culture, and expansive technology stack, but AI has dramatically increased opportunities for exploitation. Unlike many corporate environments, schools and universities operate within complex ecosystems that prioritize accessibility over restriction. Students expect

to communicate with faculty. Parents expect updates from administrators. Researchers collaborate with external partners. Vendors interact regularly with departments across campus. Every one of these interactions creates a potential opportunity for impersonation.

Higher education institutions face an especially challenging environment because of their decentralized technology structures. Individual colleges, departments, and research centers often maintain independent systems, applications, and workflows.<sup>[8]</sup> Faculty members may enjoy significant autonomy in their technology choices, while students routinely connect personal devices to institutional networks. This decentralization supports academic freedom and innovation, but it can also create inconsistencies in security controls and increase the attack surface available to adversaries.

The volume of communications further compounds the problem. During enrollment periods, students may receive dozens of messages related to registration, financial aid, housing, tuition payments, and academic advising. Faculty members juggle communications from students, colleagues, grant organizations, and external partners. Administrative staff process requests from multiple constituencies simultaneously. It becomes increasingly difficult to distinguish legitimate communications from fraudulent ones, particularly when attackers can use AI to craft messages that appear authentic.

Researchers at Google Threat Intelligence have observed that higher education institutions remain frequent targets of credential theft and phishing campaigns because they contain large amounts of personally identifiable information, financial data, and valuable research assets.<sup>[2]</sup> Educational

institutions are also attractive because their users span a range of cybersecurity awareness, from young students navigating institutional systems for the first time to faculty members whose primary focus lies outside information security.

### How AI Has Changed the Phishing Landscape

The stereotype of a phishing email, a poorly written message riddled with spelling errors and awkward grammar, is now obsolete. Generative AI, the type of artificial intelligence that creates new content by learning patterns from existing data, has enabled attackers to produce professional-quality communications that are often indistinguishable from legitimate correspondence, making them difficult to catch with spam filters and even more difficult for humans to spot.

Large language models can generate emails that mimic organizational writing styles, replicate formal administrative language, and incorporate contextual information that makes a message appear credible.<sup>[1]</sup> An attacker targeting a university can reference actual campus events, enrollment deadlines, athletic schedules, research projects, or administrative initiatives. Publicly available information from institutional websites, social media platforms, and faculty directories provides abundant material for personalization.

The implications are significant. In the past, attackers often relied on volume, sending generic phishing emails to thousands of recipients in the hope that a small percentage would respond. AI enables a different strategy. Instead of sending identical messages, attackers can generate thousands of unique communications tailored to specific institutions, departments, or

individuals within minutes. The result is a level of personalization and scale that dramatically increases the likelihood of success.

Federal investigators have warned that artificial intelligence is accelerating the growth of cybercrime by lowering barriers to entry and increasing the sophistication of attacks.<sup>[1]</sup> Security professionals increasingly describe this trend as the industrialization of social engineering. Tasks that once required substantial effort, such as researching targets, writing persuasive messages, and adapting communications to different audiences, can now be automated.

This shift is particularly concerning for educational institutions because trust is embedded into their daily operations. When a student receives a message that appears to come from a financial aid counselor, or a teacher receives a request that appears to originate from district leadership, there is often little reason to assume malicious intent. AI-powered phishing exploits trust by making fraudulent communications look increasingly legitimate.

### Financial Aid Fraud Signals a New Phase of the Threat

One of the clearest examples of how attackers target educational processes comes from recent federal investigations into student financial aid.

In February 2026, the U.S. Department of Education Office of Inspector General issued a fraud advisory identifying 12,026 dependent student identities associated with 1,991 parent identities, for which investigators determined that the students and parents were unlikely to be related or connected.

<sup>[13]</sup> The OIG concluded that these FAFSA submis-

sions demonstrated a high likelihood of fraud and represented a potential loss of nearly \$3.5 million in federal student aid funds.<sup>[13]</sup>

The findings underscore a critical shift in the threat landscape. Attackers are no longer focused solely on stealing usernames and passwords. Increasingly, they are exploiting the trust built into educational systems themselves.

Financial aid offices have become particularly attractive targets because they serve as gateways to both sensitive information and financial resources. Attackers routinely impersonate financial aid personnel, enrollment administrators, bursars, and student services representatives to trick students into disclosing credentials or responding to fraudulent requests.<sup>[6]</sup> The timing of these attacks often coincides with registration periods, tuition deadlines, and aid disbursement cycles, when recipients are already expecting communications from institutional offices.

Artificial intelligence amplifies these efforts by allowing attackers to create realistic messages tailored to specific students and circumstances. The more relevant and personalized a message appears, the more likely recipients are to trust it. For institutions, the consequences can include financial losses, administrative disruption, reputational damage, and diminished confidence in critical student services.

### The MFA Problem: When Authentication Isn't Enough

For years, cybersecurity professionals have promoted multifactor authentication (MFA) as one of the most effective defenses against phishing. The advice was sound. Requiring users to provide

a second factor beyond a password significantly reduced the effectiveness of traditional credential theft campaigns.

Unfortunately, attackers adapted.

Today, many sophisticated phishing campaigns no longer stop at stealing usernames and passwords. Instead, they employ techniques designed to capture authentication tokens after users successfully complete MFA. Known as adversary-in-the-middle (AiTM) attacks, these methods allow criminals to intercept authenticated sessions and effectively bypass many conventional MFA protections.<sup>[10]</sup>

The attack sequence is deceptively simple. A victim receives what appears to be a legitimate email directing them to sign in to a familiar service. The login page looks authentic because it has been carefully designed to mimic the real website. The user enters their credentials, completes MFA, and believes they have successfully authenticated. In reality, the attacker captures the session token generated during the process and uses it to gain access to the account.

For educational institutions, the implications are significant. A compromised student account may expose personal information or academic records. A compromised faculty account could provide access to research data, grant information, or departmental communications. Administrative accounts are often higher-value targets because they can provide access to financial systems, identity management platforms, and student information systems.

The challenge is compounded by the collaborative nature of educational environments. Once an attacker gains access to a legitimate account,

they can send messages from a trusted source. Colleagues, students, and external partners are far more likely to trust communications originating from a genuine institutional account than from an unknown sender. In many cases, the initial compromise becomes the starting point for a broader campaign.

This evolution underscores a critical reality: the phishing problem can no longer be viewed solely as a user awareness issue. It is increasingly an identity security challenge that requires stronger authentication mechanisms and a more comprehensive approach to account protection.

### Why Traditional Awareness Training Is No Longer Enough

For decades, cybersecurity awareness programs focused on teaching users how to identify suspicious emails. Employees were instructed to watch for misspellings, grammatical errors, unusual sender addresses, and requests that seemed out of character.

Those indicators still matter, but they are becoming less reliable.

Generative AI has enabled attackers to produce polished communications that often exceed the quality of legitimate institutional messaging. Messages can be personalized, professionally written, and tailored to current events or organizational activities. In some cases, they may reference ongoing projects, upcoming deadlines, or actual conversations gleaned from publicly available information.

The result is that users are being asked to identify threats that increasingly resemble

legitimate communications. This does not mean awareness training is obsolete. On the contrary, user education remains one of the most important components of a cybersecurity program. However, the focus must evolve. Rather than teaching users to spot obvious red flags, institutions should emphasize verification behaviors and decision-making processes.

Many organizations are moving toward continuous awareness programs that include regular phishing simulations, role-based micro-learning modules, and scenario-based exercises.<sup>[6]</sup> These programs expose users to emerging attack techniques and reinforce security habits throughout the year rather than relying on a single annual training session.

The objective is not to create a workforce that never clicks on a malicious link. Such a goal is unrealistic. The objective is to create a community that recognizes when something warrants additional scrutiny and knows how to respond appropriately.

### Building Phishing-Resistant Defenses

If attackers are using AI to improve phishing, defenders must rethink how they protect identities.

One of the most important recommendations from cybersecurity agencies and industry experts is adopting phishing-resistant MFA. The Cybersecurity and Infrastructure Security Agency (CISA) has repeatedly emphasized the importance of authentication methods that cannot be easily intercepted through phishing attacks.<sup>[3]</sup>

Technologies based on the FIDO2 standard, including hardware security keys and passkeys, represent the current gold standard.<sup>[4][11]</sup> Unlike traditional MFA methods that rely on text messages,

email codes, or push notifications, FIDO2 authentication uses cryptographic credentials tied to a specific device and domain. This makes it extraordinarily difficult for attackers to capture and reuse authentication data through phishing sites.

Even if a user is tricked into visiting a fraudulent website, the authentication process will fail because the credentials are bound to the legitimate service.<sup>[4][11]</sup>

For educational institutions, implementation often begins with high-risk groups. Financial aid personnel, IT administrators, payroll staff, senior leadership, and system administrators are particularly attractive targets due to the sensitive information and privileges associated with their accounts. Extending phishing-resistant authentication to these users can significantly reduce institutional risk.

The transition may require planning, investment, and user education, but the long-term benefits are increasingly difficult to ignore. As phishing techniques become more sophisticated, relying on legacy authentication methods becomes increasingly risky.

### Fighting AI with AI

Artificial intelligence is not only transforming the offensive side of cybersecurity. It is also reshaping defense.

Modern email security platforms increasingly rely on machine learning, behavioral analytics, and anomaly detection to identify suspicious communications before they reach users.<sup>[6]</sup> Rather than relying solely on known indicators of compromise, these systems evaluate patterns, context, and behavior to identify potential threats.

For example, an AI-powered security platform may recognize that an email claiming to come from a school administrator uses language patterns inconsistent with previous communications. It may detect subtle indicators of impersonation, unusual sending behavior, or requests that deviate from established workflows.

These capabilities are particularly valuable against business email compromise attacks, which often involve no malicious attachments or obvious technical indicators. Instead, they rely entirely on social engineering and trust manipulation.

While no technology provides perfect protection, AI-enhanced security tools offer institutions a better chance of identifying sophisticated threats before they reach students and staff.

The reality is that defenders cannot rely solely on human judgment to counter attacks generated by machines. Effective protection increasingly requires a combination of human awareness and intelligent automation, also known as human-in-the-loop decision-making.

### Creating a Culture of Verification

Technology plays an essential role in defending against phishing, but organizational culture remains equally important. The most resilient institutions cultivate environments in which verification is viewed as a normal part of business operations rather than an inconvenience. Staff members should feel comfortable questioning unusual requests, confirming instructions through secondary channels, and reporting suspicious communications without fear of criticism.

This is especially important for requests involving financial aid, payroll changes, direct-

deposit modifications, password resets, grade changes, wire transfers, or access to sensitive student information. These activities are common targets for social engineering because they involve valuable assets and often require rapid action.

Verification procedures should be simple, clearly documented, and consistently enforced. A phone call to a known number, confirmation through an official portal, or direct communication with a trusted contact can prevent a costly compromise.

Institutions should also make it easy to report suspicious messages. Quick-reporting mechanisms allow security teams to investigate potential threats, identify trends, and remove malicious emails before additional users are affected.<sup>[6]</sup> The faster a suspicious message is reported, the faster defenders can respond.

In many cases, the difference between a minor incident and a major breach comes down to how quickly an organization recognizes that an attack is underway.

### Looking Ahead

Educational institutions have always relied on trust. Students trust advisors. Parents trust administrators. Faculty trust colleagues. Researchers trust collaborators. These relationships are essential to learning, discovery, and institutional success.

Artificial intelligence is changing how attackers exploit that trust.

What makes AI-powered phishing particularly dangerous is not merely the technology itself.

It is the way technology amplifies the most effective elements of social engineering: credibility, personalization, and scale. Attackers can now create communications that are more convincing, more relevant, and harder to detect than those seen in previous generations of phishing campaigns.

For K-12 districts and higher education institutions, the challenge extends beyond cybersecurity. It touches governance, risk management, identity protection, and organizational culture. The question is no longer whether phishing emails will become more convincing. That transformation is already underway.

The best-positioned institutions to succeed will be those that recognize phishing as more than a technical problem. They will invest in phishing-resistant authentication, deploy intelligent detection technologies, strengthen verification processes, and foster cultures in which security becomes a shared responsibility.

The age of obvious phishing emails is over. In an era where artificial intelligence can convincingly imitate trusted voices, the most important security control may no longer be the ability to recognize deception. It may be the discipline to verify trust before acting on it.

### References

<sup>[1]</sup> Federal Bureau of Investigation (FBI). "FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence."

<sup>[2]</sup> Google Cloud Threat Intelligence. "Phishing Campaigns Targeting Higher Education Institutions."

<sup>[3]</sup> Cybersecurity and Infrastructure Security Agency (CISA). "CISA Releases Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication."

<sup>[4]</sup> U.S. General Services Administration. "Phishing-Resistant Authenticator Adoption Playbook."

- [5] National Cybersecurity Alliance. "What Is Phishing?"
- [6] CampusGuard. "Campus Phishing Scams Target Financial Aid."
- [7] EdTech Magazine. "How AI-Driven Phishing Is Putting Schools at Risk."
- [8] Campus Technology. "Cybersecurity Trends to Watch in Higher Education."
- [9] Verizon Business. 2025 Data Breach Investigations Report.
- [10] Microsoft Threat Intelligence. "The Evolution of Phishing and Credential Theft Attacks."
- [11] FIDO Alliance. "FIDO Authentication and Phishing Resistance."
- [12] EDUCAUSE. "Top Cybersecurity Issues Facing Higher Education."
- [13] U.S. Department of Education Office of Inspector General. "Fraud Advisory: Potential Fraud Involving FAFSA from Dependent Students with Unusual Parent Data." February 12, 2026.

### About the Author

Antoinette King has over two decades of experience in the security industry, with a focus on integration, manufacturing, and consulting. Antoinette founded Credo Cyber Consulting in 2020, with the intention of providing her clients with a holistic perspective on security, bridging the gap between the physical and cybersecurity domains, and focusing on data privacy and protection. Her first book, *The Digital Citizen's Guide to Cybersecurity: How to Stay Safe and Empowered Online*, hit the Amazon Best Sellers list for all its categories in the first 48 hours of release. Her latest book, co-authored with Michelle Kreiger and released in October 2025, is *From Chalk Dust to Digital Trust: A guide in Data Privacy and Security for K-12 Leaders* was #1 in Cloud-Based Computing books in the first week of release.

### 7 Ways Schools Can Reduce AI-Powered Phishing Risk

Artificial intelligence has changed phishing—but educational institutions can dramatically reduce their exposure by adopting these best practices.

1. Deploy phishing-resistant MFA Move beyond SMS codes and push notifications by implementing FIDO2 security keys or passkeys for high-risk users.
2. Prioritize your highest-risk accounts Begin with financial aid, payroll, IT administrators, registrars, HR, executive leadership, and system administrators.
3. Modernize security awareness training Teach employees to verify requests rather than simply spotting spelling mistakes or suspicious grammar.
4. Establish verification procedures Require secondary confirmation for requests involving financial aid, payroll, banking information, password resets, grades, or sensitive student records.
5. Use AI-powered email security Behavioral analytics and machine learning can identify sophisticated phishing attempts before they reach inboxes.
6. Make reporting easy Provide one-click reporting tools so security teams can quickly investigate suspicious emails and warn others.
7. Build a culture of healthy skepticism Encourage faculty and staff to verify unusual requests without fear of criticism. Security should be everyone's responsibility.

# Safer Schools, Stronger Societies: Rethinking Student Security for 2026

From non-metallic weapons and bio-agents to cyber intrusions and AI-enabled threats, the next era of school security demands technologies and policies that safeguard lives while preserving trust and learning environments.

BY BRYAN CUNNINGHAM



Cliches like “the children are our future” become so because they’re true. In addition to being a moral imperative, protecting our students from physical and other threats will be a linchpin in the coming global struggle between free societies and authoritarian ones. Ensuring children and young adults feel safe and secure while they learn will make us more competitive with our adversaries for the foreseeable future. The stakes could not be higher.

Multiple empirical studies validate the commonsense notion that students learn better when they feel safe. But the accelerating threats to students’ lives and safety in the United States will

continue to grow and evolve with new technologies and the ingenuity of bad actors. Physical threats, of course, remain the most concerning for students, parents, teachers, and administrators. School shootings have claimed at least 47 lives in 2025, with non-metallic weapons like ceramic knives and ghost guns slipping through metal detectors. Insider threats, including disgruntled students, staff, or visitors, will likely also continue to rise, fueled by mental health crises and online radicalization. Even bio-agents, such as fentanyl-laced narcotics and smuggled pathogens, pose alarming new risks, with CDC reports noting more than a dozen school incidents involving concealed substances last year. The arrest of two alleged

Chinese agents attempting to smuggle deadly *Fusarium* into Michigan earlier this year illustrates that such threats, perhaps once the stuff of science fiction, are becoming all too real.

Beyond physical threats, cyberattacks, and other virtually enabled but very real dangers are emerging. So far in 2025, schools have reported at least 1,800 cyber intrusions. Beyond personal and other data, attacks against physical infrastructure, for example, through IoT vulnerabilities in smart locks and cameras, may also be expected to continue and become more sophisticated. Meanwhile, ransomware attacks, often backed by nation-states such as Russia or China, will likely continue to disrupt learning and exact millions in ransom payments, as seen in the Los Angeles Unified School District's \$10 million payout in 2024. And this is before we even get to Artificial Intelligence (AI), which can not only enable cheating but also, more significantly, create deepfakes to impersonate administrators for social engineering attacks or generate blueprints for 3D-printed weapons that evade traditional metal detectors.

Perhaps most troubling, the last few years have seen multiple examples of teenagers attempting to bring metal-detector-evading 3D weapons into schools. While, thankfully, no actual shootings with such weapons in the US have been reported yet, the fact that such weapons have evaded metal detectors is alarming.

### How Do Schools “Future Proof” Against These Threats?

Schools must plan and equip to protect against not only current threats but also emerging ones. To future-proof schools most cost-effectively, schools and school districts should prioritize

integrated systems that blend cyber resilience with physical threat detection and barriers. In the cyber realm, zero-trust networks are becoming standard, enabling the verification of each user and device and to better detect incoming threats. Schools may also consider AI-driven predictive analytics to flag behavioral anomalies, such as unusual access patterns. Still, they must take reasonable steps to guard against unwarranted privacy invasions and the tendency of even the best AI technologies to “hallucinate” at times.

### Cyber Protections Are Not Enough

Preventing deadly weapons from being brought into schools is paramount, but students should not only be safe but also feel safe. Fortunately, emerging security screening technologies can detect metallic and non-metallic threats before they are brought into a school. Among these new technologies, millimeter-wave screening portals offer a significant advance. These contactless systems use AI and 3D imaging to detect a broad spectrum of threats, including metallic and non-metallic weapons, liquids, powders, plastics, 3D-printed guns, bio-agents, explosives, and narcotics. They can detect in seconds and process up to 1,000 people per hour with minimal staff. Equally important, such systems enable walk-through screening without requiring students to stop, minimizing additional anxiety while protecting them and deterring attempts to bring deadly threats into our schools.

Wherever feasible, threat screening and other new technologies should be “future-proofed,” for example, by using AI to adapt to emerging threats over the coming years without replacing previously purchased hardware. Furthermore, such systems should be portable, allowing schools to move units

from one entry point to another. Fortunately, some such screening systems can now be relocated by one or two people in under 30 minutes, making these solutions both flexible and cost-effective. 2026 will likely see such protective technology enhancements for student safety, supported by federal and state funding and, in some states, potentially legally mandated.

Schools shouldn't be fortresses, but they must be sanctuaries. As both a father and a security

professional, I know it is possible to strike the right balance here. And we must.

### About the Author

*Bryan Cunningham is President of Liberty Defense. He is a lawyer, security expert, former CIA officer, and tech executive. He is a senior counsel and Executive Director of Palantir's outside advisory group on privacy and civil liberties. A key figure in multiple tech startups, he previously served as Deputy Legal Adviser to Condoleezza Rice, worked with the 9/11 Commission, and advised the Chertoff Group.*

