SEPTEMBER 2024 ISSUE • VOL 14

IKON INSIGHTS

TECHNOLOGY NEWS FOR K-12 SCHOOLS

Brought to you by IKON EduTech Group, Inc.

IN THIS ISSUE

This monthly publication provided courtesy of IKON EduTech Group.

IKON is a premium IT consulting company focused on providing K-12 schools with customized technology solutions and personalized support.

Get More Free Tips, Tools and Services on Our Website:
www.ikonbusinessgroup.com
(212)334.6481

MAXIMIZING RESOURCES

HOW K–12 SCHOOLS CAN ADAPT TO LESS FUNDING

The substantial federal support K–12 schools received through the Elementary and Secondary School Emergency Relief Fund (ESSER) has officially come to an end. This shift presents challenges for school districts that have relied on these funds to advance educational technology, professional development, and classroom resources. As the 2024–2025 school year approaches, schools will need to adjust to a leaner funding environment, making it essential to reassess and prepare for budget constraints.

FEDERAL FUNDING: WHAT'S ON THE HORIZON?

While there are no new relief funds for technology devices, professional development, or other critical areas, schools can still leverage some ongoing federal programs. The federal government has earmarked funds for school safety, mental health services, cybersecurity, and Wi-Fi initiatives, which could provide partial relief in some areas.

The loss of substantial federal funding will force schools to make strategic decisions, especially around deadlines for programs like E-Rate. Now, more than ever, districts must be vigilant in taking advantage of available resources, particularly when planning for the year ahead.

continued on page 2

HOW K–12 SCHOOLS CAN ADAPT TO LESS FUNDING

LEVERAGING E-RATE FOR CONNECTIVITY & CYBERSECURITY

Alyssa's Law is a pivotal piece of legislation mandating that public schools install silent panic alarms to notify law enforcement directly in emergencies. Named after Alyssa Alhadeff, a victim of the 2018 Marjory Stoneman Douglas High School shooting in Parkland, Florida, this law honors her memory and aims to prevent future tragedies. The Parkland shooting resulted in the loss of 17 lives and critically injured 17 others, underscoring the urgent need for faster emergency response in schools.

One of the largest and most dependable funding sources for schools remains the E-Rate program. With the deadline to use 2023 commitments approaching on Sept. 30, 2024, it's crucial that schools properly allocate these funds. For the 2024–2025 school year, schools should begin preparing now, ensuring they submit the necessary paperwork, such as Form 470, by mid-February to meet upcoming deadlines.

The updated E-Rate program includes funding for off-campus services like bus Wi-Fi and hotspots under Category One. This presents an opportunity for districts to maintain student connectivity beyond the classroom, particularly for those in underserved areas. Additionally, the FCC's new cybersecurity pilot program opens to applicants in September, giving schools the chance to secure additional funding for network security.

STATE-LEVEL FUNDING: A KEY TO CLOSING GAPS

As federal funds decline, many states are stepping up to fill the gap. For instance, Michigan's education budget for 2024 is the largest in the state's history, while Ohio is preparing a significant investment for the upcoming fiscal year. School administrators should prioritize researching available state-level grants and other funding initiatives. Planning ahead and building relationships with local and state officials will increase the likelihood of securing these funds.

OTHER FEDERAL PROGRAMS TO WATCH

Despite reductions in federal funding, several programs remain available for schools to support specific needs:

Despite reductions in federal funding, several programs remain available for schools to support specific needs:

- **Title I and Title II:** Although these programs face potential cuts, they remain vital sources for at-risk student funding and professional development. Schools should monitor these funds and plan accordingly, given the uncertainty of future budget allocations.
- **Distance Learning & Telemedicine Grants:** Ideal for rural schools, these grants can be used for student laptops and Wi-Fi. Schools should prepare applications in advance of the expected December opening.
- **School Violence Prevention Program:** This grant supports school safety initiatives and typically opens in late March. Schools should start now by updating safety plans and coordinating with local law enforcement to strengthen applications.

THE ROAD AHEAD: WHY SCHOOLS MUST PLAN NOW

As federal funding recedes, K–12 schools need to make proactive adjustments to maintain essential educational services. The key is forward-thinking preparation and strategic use of the remaining federal and state resources.

KEY FUNDING SOURCES AT-A-GLANCE

ACTION	DEADLINE	DESCRIPTION
E-RATE FORM 470 SUBMISSION	Mid-February 2025	Begin planning for technology partnerships by submitting Form 470 early. Schools must wait 28 days after submission before selecting vendors.
MAXIMIZE USE OF 2023 E-RATE FUNDING	September 30, 2024	Ensure all 2023 funding commitments are used by this date to avoid losing critical funds.
FCC CYBERSECURITY PILOT PROGRAM	November 1, 2024	Apply for this FCC pilot program to secure additional cybersecurity funding.
STATE-LEVEL GRANT RESEARCH	Ongoing	Research available state funding opportunities, such as Michigan's record education budget and Ohio's substantial investment.
DISTANCE LEARNING & TELEMEDICINE GRANT	December 2024 (expected)	For rural schools, prepare applications early to qualify for funding for student laptops and Wi-Fi access.
SCHOOL VIOLENCE PREVENTION PROGRAM	March/April 2025 (expected)	Update safety plans and consult with local law enforcement to apply for this safety grant in spring 2025.

NEW CYBER THREAT TO K-12 SCHOOLS: AI FAKE DATA BREACHES EXPLAINED

As cybercriminals become more sophisticated, they are using AI to create elaborate scams targeting organizations, including K-12 schools. One of the latest threats is the rise of fake data breaches, where hackers use AI to generate convincing but fraudulent data sets to trick school districts into believing they've been compromised.

Even though the data breach may be fake, the consequences are real and costly. Understanding how these scams work and how to protect your school is more important than ever.

HOW ARE CYBERCRIMINALS CREATING FAKE DATA BREACHES?

AI-powered tools like ChatGPT enable cybercriminals to generate realistic-looking data sets with minimal effort. With enough research, they can fabricate fake student and staff data that appears credible—complete with names, addresses, phone numbers, and email addresses. They may also use automated data generators designed for testing purposes to create these large data sets.

Hackers then claim to have stolen this data from a school district and post it on the dark web. The threat of a supposed data breach creates fear and uncertainty, even though the data is entirely fabricated.

WHY ARE K-12 SCHOOLS BEING TARGETED?

K-12 schools are attractive targets for cybercriminals for several reasons:

1. **Creating Distractions** - Schools already have limited IT resources, making them particularly vulnerable to distraction techniques. When a school district scrambles to investigate a fake data breach, it often takes attention away from real vulnerabilities, potentially opening the door to other cyberattacks.
2. **Reputation Building for Hackers** - Cybercriminals gain credibility within hacker communities by publicly claiming responsibility for breaching school systems, even if the breach is fake.
3. **Manipulating School Funding** - Fake data breaches can create panic that impacts the financial stability of a school district. Widespread fear over a breach can cause parents, staff, and even state or federal agencies to question the district's ability to manage its funds and keep sensitive information secure.
4. **Learning About Security Systems** - By faking a data breach, cybercriminals can observe how your district responds, gaining valuable insights into your security protocols, response times, and vulnerabilities. This knowledge can be used to launch more sophisticated attacks later.

HOW CAN K-12 SCHOOLS PROTECT THEMSELVES FROM FAKE DATA BREACHES?

While it's impossible to completely prevent cybercriminals from attempting these scams, there are steps K-12 schools can take to reduce the risks and minimize the impact:

1. **Monitor the Dark Web for School Data** - Proactively monitoring the dark web can help your IT team or cybersecurity partner detect any suspicious activity. If fake data sets claiming to belong to your district are posted, you can respond quickly to investigate and debunk the claims before they spread.
2. **Create a Crisis Response Plan** - Develop a disaster recovery plan that includes a communication strategy for handling both real and fake breaches. Knowing how to respond and who should communicate with parents, staff, and the media is critical to maintaining control of the situation and protecting your school's reputation.
3. **Partner with Cybersecurity Experts** - Most K-12 schools don't have the resources to keep up with the constantly evolving world of cyber threats. By working with a cybersecurity expert, your school can benefit from proactive monitoring, real-time threat detection, and strategic response planning. This partnership ensures that your district is prepared for both real and fabricated threats.

STAY ONE STEP AHEAD OF CYBERCRIMINALS

As the threat landscape evolves, K-12 schools must stay vigilant in protecting sensitive student and staff data. Fake data breaches, fueled by AI technology, are an unfortunate new reality, but with proactive measures, you can minimize their impact on your district.

IKON's team of cybersecurity experts is ready to provide your district with a FREE Security Risk Assessment, ensuring your systems are secure and prepared for any cyber event.

TOP 10 CYBERSECURITY TIPS FOR TEACHERS

In today's digital world, teachers play a vital role in protecting student data. With cyberattacks on the rise in schools, it's crucial for educators to adopt strong cybersecurity practices. Here are ten essential tips every teacher should follow to safeguard sensitive information and maintain a secure learning environment.

1. BE AWARE OF SOCIAL ENGINEERING TECHNIQUES

Cybercriminals often use social engineering tactics like phishing to gain access to sensitive data. Stay vigilant when receiving unexpected emails or messages, especially those that request personal information or login credentials. Always verify the source before clicking on links or downloading attachments.

2. USE STRONG AUTHENTICATION PRACTICES

Use multi-factor authentication (MFA) whenever possible, and create complex passwords for your accounts. Avoid using the same password across multiple platforms. Using MFA significantly reduces the risk of unauthorized access to school systems and personal data.

3. KEEP DEVICES UPDATED

Regularly update your devices with the latest software and security patches. Hackers exploit outdated software to access systems. Ensuring your devices are up-to-date is one of the simplest ways to protect against vulnerabilities.

4. USE ANTI-VIRUS SOFTWARE AND SCAN DEVICES OFTEN

Install reputable anti-virus software and perform regular scans on your devices. This helps detect and remove malware, keeping your computer and personal information secure. Schedule routine scans to ensure you catch potential threats early.

5. ENCRYPT SENSITIVE INFORMATION

Encryption is crucial when handling sensitive student data. By encrypting files and emails containing personal information, you add an extra layer of protection that prevents unauthorized access, even if data is intercepted.

6. USE ONLY APPROVED SOFTWARE

Always use school-approved software and applications to avoid inadvertently introducing security risks. Unapproved programs can pose a threat to the school network and compromise data privacy. IKON can help K-12 schools identify and implement secure, approved software solutions to ensure student data is protected.

7. USE SAFE BROWSING STRATEGIES

Be cautious while browsing the internet. Avoid clicking on suspicious links or visiting unverified websites. Using a secure web browser and enabling security settings helps reduce the risk of downloading malicious content.

8. BACKUP YOUR DATA

Regularly back up your data to an external device or cloud service. In case of a ransomware attack or data loss, having a backup ensures you can quickly restore important information without paying hackers.

9. NEVER LEAVE DEVICES UNLOCKED OR UNATTENDED

Always lock your devices when not in use, even if you're stepping away for just a moment. Unattended, unlocked devices are vulnerable to unauthorized access. Develop the habit of locking screens to safeguard student information.

10. AVOID PUBLIC WI-FI

Public Wi-Fi networks are often insecure and can be easily exploited by hackers to intercept data. Avoid accessing sensitive information or logging into school accounts when connected to public Wi-Fi. Use a virtual private network (VPN) for a more secure connection if you need to access school systems remotely.

Cybersecurity is a shared responsibility. While these tips are essential, teachers need ongoing support and training to keep up with the ever-evolving digital landscape.

ON-DEMAND WEBINAR: HOW TO SUCCESSFULLY APPLY TO THE FCC'S CYBERSECURITY PILOT PROGRAM

Watch Now

Cybersecurity attacks on schools and libraries are escalating, putting sensitive data and critical networks at risk. In response, the FCC has launched a $200 million Cybersecurity Pilot Program to help eligible schools and libraries fortify their defenses against these growing threats.

This exclusive three-year program offers funding for essential cybersecurity services and equipment to protect broadband networks and data. The application window is now open—don't miss your chance to secure funding for your institution.