



IT SECURITY REPORT OCTOBER 2025



MATC (ALMOST) HACKED

November 25th 2024 - An employee Maysville PS was hacked and their email was used in a phishing attack. Caught by manual filtering.

November 26th 2024 - An employee at Paoli PS was hacked and their email was used in a phishing attack. Caught by manual filtering.

December 12th 2024 - A former student of Wynnewood PS was hacked and their email was used in a phishing attack. Caught by manual filtering.

February 5th - An employee at Mesquite ISD was hacked, and their email was used in a phishing attack. Chris Daniel noticed it was suspicious and reported it to IT. He was the only recipient, so he was instructed to delete it.

February 25th - An employee at Waggoners Home Services was hacked and their email was used in a phishing attack. Parker Murphy noticed it was suspicious and reported it to IT. He was the only recipient, so he was instructed to delete it.

April 11th - An email impersonating a school employee went to several employees. Most of them were caught by our email filter, but one made it through to an instructor and they responded to it. IT blocked the email address, talked to the employee about email safety and monitored their account for a week.



IT SECURITY REPORT OCTOBER 2025



MATC (ALMOST) HACKED PART 2

June 11th - An employee at Lindsay PS was hacked and their email was used in a phishing attack. Marci Burkhardt and Dallas Krout reported it. Used Mimecast Threat Remediation to remove the emails.

September 18th - An employee at Lexington PS was hacked and their email was used in a phishing attack. Mimecast AI caught most of them. Used it's Threat Remediation tool to remove any that made it through.



IT SECURITY REPORT OCTOBER 2025



MATC? (POWERSCHOOL) HACKED

December 2024

PowerSchool Account Compromised - PowerSchool had one of their technician accounts comprised that wasn't properly secured and had more access than it should have.

70 million records exfiltrated - World wide the estimate is around 62 million student records and 10 million teacher records.

Denny Prince saw a news story about it - We discovered that we were notified, but went to junk mail.

MATC Notice - We put a notice out on our website and notified current employees and students. We also notified the school's law firm and insurance company.

McDonald Hopkins - Insurance referred us to McDonald Hopkins for the incident. We worked with them to notify the correct entities and what notices we had to put out.

7/16/2025 - Incident is closed and all reporting is done. Removed notice from school website.

Costs - \$4,757.50 to McDonald Hopkins. \$31.39 in postage (to out of state students)



IT SECURITY REPORT OCTOBER 2025



{REDACTED} TECH CENTER HACKED

July 4th 2025

Almost of their systems were encrypted

Took around a week to recover, but they got everything back - All of their important data was in the cloud.

VPN - The attackers gained access through remote VPN

Zero Day vulnerability - There was an unknown flaw in their VPN that hackers were able to use to get in.



IT SECURITY REPORT OCTOBER 2025 LESSONS LEARNED & MOVING FORWARD



Cyber Education is working - We only had one close call this year.

And so is AI - The AI upgrade to Mimecast has allowed me to stop manual filtering and catches most attacks (I just forgot to record them all)

We need data lifecycle management - There is data that we have that we don't need to keep.

VPN = Bad - 2nd year in a row that a Tech Center was hacked through VPN. (But we might need an encrypted connection for off-site computers, just not for accessing on-site resources)

Grants - Waiting on FEMA approval

CT Accreditation - Just did MNTC, and there is paperwork I need to get ready for it.

New Password Policy on campus - 15 characters, emphasis on uniqueness over complexity, scanning employee accounts for breaches