Ransomware Attacks in the Education Industry

According to the 2022 Global Risks Report, 82% of malware attacks target the education sector. In the US alone, cybersecurity incidents affecting schools have increased almost 900% since 2019. Similarly in the UK, authorities report that ransomware attacks went up by more than 140% in the last two years.

Understanding the risks of vulnerabilities and cyberattacks is the best way to defend schools and students against threats.

Vulnerabilities That Lead to Ransomware Attacks

Phishing

A social engineering attack that attempts to collect information from victims.

Lack of security awareness

82% of breaches in 2022 involved human error, including incidents targeting happy clickers.

Use of outdated or EOL software

Continued use of end-of-life (EOL) software poses a consequential risk and leads to security vulnerabilities.

Trojan Malware Leads Cyberattacks Targeting Schools

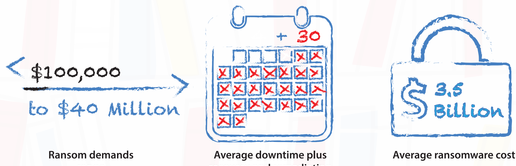
ZeuS

A trojan with several variants that targets Microsoft Windows operating systems. Hackers target machines and send stolen information to command-and-control servers.

Shlaye

A trojan downloader and dropper for macOS malware that is primarily distributed through malicious websites, hijacked domains, and malicious advertising posing as a fake Adobe Flash updater

The Cost of Ransomware in Schools and Colleges



Ransom demands range

Average downtime plus recovery and remediation

Average ransomware cost

Ransomware Attacks Targeting Education That Made Headlines

2020 | U.S. | Clark County School District
Affected Population: 320,000 students, staff, and faculty
Impact: Credential theft, leaked personal data, dark web exposure risk
This is largest ransomware attack against an educational institution since the COVID-19 pandemic started. Hackers published about 25GBs of personal data, including social security numbers.

2020 | Canada; US; UK | 8 Universities
Affected Population: 300,000+ students, staff, and faculty
Impact: Stolen data
Blackbaud, a Cloud computing provider was targeted by hackers to extort funds. Some of the stolen data included phone numbers and donations/events history.

2021 | UK | The Isle of Wight Education Federation (IWEF)
Affected Population: 2,000+ primary and secondary school (K-12)
Impact: Encrypted data including children and staff records, access to learning and admin systems
IWEF was asked to pay a ransom of $1M. Reportedly, they did not pay the ransom and instead had to spend thousands of dollars in recovery and remediation.

2022 | US | Finalsite
Affected Population: 5,000+ boarding schools, high schools, colleges
Impact: Interrupted communications, system outages
Finalsite, the online learning and communications platform that hosts thousands of K-12 and higher ed websites, shut down its systems after identifying the presence of ransomware.

Best Practices for Schools, Colleges, and Universities

1. Protect happy clickers: Think before you click. Breaches are relevant to our everyday duties
2. Run consistent software updates: Embrace the culture of patching and enable automated software updates
3. Promote security awareness: Empower students and faculty with security education
4. Seek additional funding opportunities to optimize security: Get extra financial support to optimize security through fundraising or subsidized programs sponsored by local or federal entities
5. Consider outsourcing security: Sometimes, partnering with a managed service provider is the most effective way to access advanced security solutions

Key Security Solutions

Learn More at watchguard.com/education

https://www.comparitech.com/blog/information-security/school-ransomware-attacks/
https://www.codastory.com/disinformation/ransomware-schools/
https://www.ncsc.gov.uk/news/support-for-uk-education-sector-after-growth-in-cyber-attacks
https://www.cisa.gov/uscert/ncas/alerts/aa20-345a
https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector