IDENTITY AUTOMATION

The average total cost to rectify a ransomware attack in the education sector is $2.73 million, when considering downtime, people time, device cost, network cost, lost opportunity, and ransom paid— the highest across all sectors surveyed.[1]

Preventing Ransomware with Digital Identities

Increasingly, malicious actors are targeting education users as a means to initiate ransomware attacks. Education is by far the most targeted industry with over 5.8 million reported malware encounters in the last thirty days.[2]

In K-12 alone, 54% of school districts have endured a malware or ransomware attack since the onset of COVID-19.[3] Likewise, colleges and universities have seen ransomware attacks double between 2019 and 2020.[4]

So, why is education the number one target for malicious actors? For starters, education is known for having limited funding and resources. In fact, 77% of school districts do not have a dedicated full-time staff member for network security.[5]

Furthermore, users recycle the passwords across multiple platforms in their personal lives. Unfortunately, when these credentials are compromised in a data breach outside of your organization, your users can inadvertently become a threat vector, allowing malicious actors to perpetrate an account takeover and hold your institution hostage.

RapidIdentity Compromised Credential Monitoring

With RapidIdentity, your digital identities' credentials are continuously monitored and evaluated for passwords that are known to be compromised from previous breaches. Even better, RapidIdentity automatically sends an alert if an account's credentials become a risk. Users with compromised credentials can then be enrolled in a multi-factor authentication (MFA) policy until their password is safely changed and the threat is removed.

Password complexity rules simply aren't enough, and breaches are continuing to happen every day. Ransomware attacks not only put your users' digital identity data at risk, but can cause your school to temporarily close and cost millions in taxpayer dollars. Now is the time to ensure your institution is protected with RapidIdentity Cloud's compromised credential monitoring.

To learn more about how RapidIdentity Cloud secures identity data, request a demo.

Contact Us | sales@identityautomation.com | 877.221.8401 | www.identityautomation.com

1 https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-education-2021-wp.pdf.
2 Microsoft Security Intelligence, Global Threat Activity Map by Industry, Microsoft (website), accessed July 14, 2021.
3 "New Research: K-12 Districts Must Face the Mounting Cybersecurity Challenges." Identity Automation, 7 Apr. 2021, https://blog.identityautomation.com/new-research-k-12-districts-must-face-the-mounting-cybersecurity-challenges.
4 Klavon, Ken. "BlueVoyant Report Reveals Ransomware Is the Number 1 Cyber Threat Facing Higher Education." BlueVoyant, 23 Feb. 2021, https://www.bluevoyant.com/news/bluevoyant-report-reveals-ransomware-is-the-number-1-cyber-threat-facing-higher-education/.
5 Torchia, Rebecca. "Cybersecurity Tops CoSN's Annual Ed Tech Leadership Report." Technology Solutions That Drive Education, EdTech: Focus on K–12, 9 July 2021, https://edtechmagazine.com/k12/article/2021/07/cybersecurity-tops-cosns-annual-ed-tech-leadership-report.