Industry Brief

mimecast

Ransomware in Education

The Detrimental Effects and How Mimecast Can Help Safeguard Your Educational Institution

What is Ransomware?

Ransomware is a form of malicious software (or malware) that, once it has taken over your computer, threatens you with harm, usually by denying you access to your data. The attacker demands a ransom from the victim, promising—although not always truthfully—to restore access to the data upon payment.

Why is Ransomware So Detrimental?

Disruption to due ransomware compromises:

- Student education
- Sensitive staff and student data including PII, payroll info and medical records
- Online services including email, school websites, grading systems and lunch payments

Even if an organization decides to pay the ransom, there is no guarantee that:

- Compromised files will be unencrypted or fully accessible
- Criminals won't sell or exploit the stolen data

How Mimecast Can Help

- **Email Security:** comprehensive protection against email-borne cyberthreats including ransomware, phishing, impersonation attacks, malicious URLs and weaponized attachments
- **Web Security:** integrated web security services boost defenses by preventing infiltration and spread of attacks
- **Security Awareness Training:** delivers comprehensive cloud-based education modules, risk scoring and phish testing to improve the security awareness of staff and reduce security risks resulting from human error
- **Sync & Recover:** enables point-in-time archive retrieval of mailboxes, calendars and contacts—an especially effective way of recovering from a ransomware attack

2019-2020 STATE CERTIFIED ★ CYBERSECURITY TRAINING PROGRAM ★ DIR

Why Are Schools So Highly Targeted by Ransomware?

- Insufficient security budgets and limited IT resources make educational institutions soft targets for ransomware
- Schools have valuable student information; hackers capitalize on this by targeting schools and hoping they will pay large ransoms if access to this critical data is compromised
- Often, schools don't have strong data backup and recovery processes in place to circumvent a ransomware attack

It's No Longer a Matter of IF an Attack Will Occur, but WHEN.

- Cyberattacks are becoming more common
- Email is the #1 attack vector used to launch a cyberattack
- Educational Institutions need to be proactive
  - » Protect yourself before, during and after an attack
  - » Key is to have a cyber responses plan in place and know what to do if you need to execute on it
  - » Need a contingency plan in case your institution loses access to its critical data

In the News: Recent Victims of Ransomware

1. **K-12 Has Become the Most Targeted Segment For Ransomware:** According to an FBI report, nearly 60% of all reported ransomware attacks in August and September 2020 were targeted at K–12. That's a 28% increase from the previous six months.
2. **Baltimore County School District Hit with Ransomware Attack:** The attack took nearly a week to get under control and cancelled two school days for 115,000 students learning remotely.
3. **University of California San Francisco Pays $1.14 Million Ransom:** The university was forced to pay the ransom to regain access to academic data.
4. **Hackers Demand $50,000 from Texas School District in Ransomware Attack:** The Texas school district was attacked by hackers demanding $50,000 in ransom. They voted to pay it.
5. **More Than 1,600 Schools Were Targeted By Ransomware in 2020 Alone:** This is largely due to a lack of security awareness training, shrinking budget and an increased attack surface due to COVID-related remote learning.