Ransomware Targeting Educational Institutions

Recently, Federal Student Aid (FSA) has identified multiple ransomware attacks against educational institutions. These attacks deny access to information technology systems and data unless an institution pays a ransom--if then. Ransomware can have a crippling effect on an institution's ability to operate until the attack is remediated.

How could ransomware impact your institution?

Attackers use phishing scams to collect account credentials and then use those credentials to install ransomware across a network. Educational institutions have lost access to critical systems and data, dramatically impacting their operations.

Why are schools frequent targets?

Educational institutions are an attractive target for criminals because they have valuable information, including personal and financial information, research data, and intellectual property.

How to protect your institution

We strongly encourage each institution to strengthen its cybersecurity posture by implementing these best practices:

- ✓ **Establish a process to back up data. Ensure backups are stored offline but are accessible.**
- ✓ **Implement multifactor authentication to mitigate account compromises.**
- ✓ **Continuously monitor your networks to detect unauthorized access and malware.**
- ✓ **Regularly patch hardware and software.**
- ✓ **Create your Incident Response Plan and keep it up-to-date.**
- ✓ **Emphasize phishing during trainings. It is often the entry point for ransomware attacks.**

What if your school falls victim to an attack?

1. Shut off networks and systems to limit spread.
2. Bring systems back online only after they are checked and cleared of infection.
3. Block IP addresses that were related to the attack.
4. Reset credentials for potentially affected accounts.
5. Perform forensic analysis on server, network, and application logs from recent weeks.
6. Restore data from backups.
7. Notify law enforcement of any criminal activity.

Report incidents immediately to cpssaig@ed.gov and FSASchoolCyberSafety@ed.gov and include:

- Institution name
- OPEID (school code)
- Incident date (if known)
- Incident discovery date
- Technical details (if known)
- Extent of impact
- Remediation status
- Institution point(s) of contact

We are committed to working with institutions to combat ransomware attacks and protect student financial aid information. If you have any questions about the information provided here, please contact FSASchoolCyberSafety@ed.gov.

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION