Privacy Technical Assistance Center
U.S. Department of Education
(855) 249-3072
privacyTA@ed.gov
https://studentprivacy.ed.gov

Cyber Advisory - New Type of Cyber Extortion / Threat Attack

Summary

Schools have long been targets for cyber thieves and criminals. We are writing to let you know of a new threat, where the criminals are seeking to extort money from school districts and other educational institutions on the threat of releasing sensitive data from student records. In some cases, this has included threats of violence, shaming, or bullying the children unless payment is received.

These attacks are being actively investigated by the FBI, and it is important to note that none of the threats of violence have thus far been judged to be credible. At least three states have been affected.

How to Protect Yourself

The attackers are likely targeting districts with weak data security, or well-known vulnerabilities that enable the attackers to gain access to sensitive data. This may be in the form of electronic attacks against school/district computers or applications, malicious software, or even through phishing attacks against staff or employees.

IT Staff at Schools / Districts are encouraged to protect your organizations by

- **conducting security audits to identify weaknesses and update/patch vulnerable systems;**
- **ensuring proper audit logs are created and reviewed routinely for suspicious activity;**
- **training staff and students on data security best practices and phishing/social engineering awareness; and**
- **reviewing all sensitive data to verify that outside access is appropriately limited.**

What to Do if This Happens to You

If your organization is affected by this type of attack, it is important to contact local law enforcement immediately. It's not mandatory, but if you are an affected K12 school, please contact us at privacyTA@ed.gov so that we can monitor the spread of this threat. Additionally, the PTAC website contains a wealth of information that may be helpful in responding to and recovering from cyber attacks.

While this new threat has thus far been directed only to K12, institutions of higher education should know that they are required to notify the Office of Federal Student Aid (FSA) of data breaches via email pursuant to the GLBA Act, and your Title IV participation and SAIG agreements. Additional proactive tools for institutions of higher education are available at our Cybersecurity page on ifap.ed.gov.