Federal Student Aid

Cybersecurity Updates September 2022

Cyber Attack Advice from Brian Peacher, IT Director at Lincoln College

"It had been a great day and I was enjoying dinner on Sunday evening with my family. Then I got the phone call," recalls Brian Peacher, Sr., who had been confirmed as the new IT Director at Lincoln College, in Lincoln, Illinois, just two days earlier.

The college had been hit by ransomware. Cybercriminals had infiltrated an unpatched 2016 Microsoft Exchange Server vulnerability and encrypted all the school's data. Across campus, printers were spewing out ransom demand notices.

What followed was a hectic scramble to gather manpower and resources to assess the situation and determine next steps. It took several months, but the college was able to get all systems and data fully restored by March 2022.

While no personal identifying information was exposed, the attack caused major disruption to the university. The hardest hit was recruitment, retention, and fundraising. After systems were restored, the college uncovered further projected enrollment shortfalls due to COVID-19, leading to the decision to close the university.

Peacher wants his first-hand experience with a cyber-attack to help fellow institutions prepare for a potential breach. His top advice includes:

- Have a process for identifying and patching vulnerabilities on a regular basis.
- Assume you're going to be attacked and have a response plan ready.
- Confirm you have cyber insurance and know who the carrier is. (Keep their contact information at home in case your work

systems are unavailable.)
- Don't build all your business processes around one platform (i.e. one Exchange Server, single email addresses).

Hear more experiences and lessons learned from university IT leaders at the 2022 FSA Training Conference.

50%

That is the percentage of all breaches caused by stolen credentials, the top cause in the education sector. Cyber attackers are exploiting a common practice at IHEs: the use of single-factor authentication to access institutional systems. FSA strongly recommends implementing multi-factor authentication (MFA) across your educational institution to dramatically improve resilience against common cybersecurity threats such as compromised credentials.

Additionally, FSA is now requiring MFA enrollment for all new FSA ID users and will require all existing users to enroll by the end of the year.

Learn more about implementing strong authentication methods at the link below.

Learn More

How to Protect Your Systems from Exploitation

Malicious cyber actors often aggressively target newly disclosed critical software vulnerabilities. One way to protect your institution's systems and data is by

implementing a centralized patch management system and by immediately patching known exploited vulnerabilities.

Read more about top routinely exploited vulnerabilities and recommended mitigations at the link below.

Read More

New Cybersecurity Resources Available

New FSA documents, including ransomware and data sanitization best practices, are now available on FSA's Partner Connect cybersecurity page.

Cybersecurity Resources

Did You Know?

The Cybersecurity and Infrastructure Security Agency (CISA) offers free scanning and testing services, including vulnerability scanning and phishing campaign assessments, to help organizations mitigate cybersecurity threats.

Free Cyber Hygiene Resources

Report a Breach

Report breaches immediately by emailing **CPSSAIG@ed.gov**

Upcoming Events

- **October is Cybersecurity Awareness Month**
  Promote cybersecurity best practices at your institution throughout October.

- **2022 FSA Training Conference for Financial Aid Professionals** The FSA Conference will be held virtually November 29 – December 2, 2022. The conference will feature dynamic keynote addresses, engaging general forums, and informative breakout sessions.

Critical Vulnerabilities

- **Confluence Server and Data Center (CVE-2022-26134)**

- **CISA Alert: Weak Security Controls and Practices Routinely Exploited for Initial Access**

- **2021 Top Routinely Exploited Vulnerabilities**

Subscribe to the Department's Monthly Student Privacy Newsletter

The U.S. Department of Education's Student Privacy Policy Office (SPPO) administers and enforces Federal student privacy laws and

provides technical assistance to help safeguard information about students. SPPO publishes a monthly Student Privacy Newsletter highlighting resources, public engagements, and SPPO and Privacy Technical Assistance Center support. Subscribe to the Student Privacy Newsletter here.

Feedback or Suggestions?

Email **FSASchoolCyberSafety@ed.gov** your recommendations for what to include in upcoming newsletters.

This email was sent by: Office of Federal Student Aid
U.S. Department of Education
400 Maryland Ave. SW,
Washington, DC, 20002, US