Safeguarding Educational Data with Security Awareness Training

TitanHQ™

Safeguarding Educational Data with Security Awareness Training

With as much personal data as educational institutions store, they still struggle with cybersecurity infrastructure and training. Teachers, administrators, professors, teaching assistants, and other staff have access to student social security numbers, financial information, and personally identifiable information (PII). Security awareness training gives staff the knowledge to detect and stop phishing and social engineering, but educational institutions still don't have the infrastructure in place to help stop a data breach.

Not only do staff pose a threat, but students unaware of common phishing and social engineering techniques are also perfect targets for cyber-criminals. Students with remote access to class schedules, classes, and their personal information on a school dashboard are targets for data theft. Cybersecurity infrastructure is necessary to detect and stop a data breach, but training students to identify phishing emails reduce their chances of becoming a victim.

Targeting Educational Institutions with Phishing Emails

Because it's well known that schools don't have the cybersecurity infrastructure to stop a data breach, they are a primary target for cyber-criminals. A cyber-criminal group named Vice Society continually targets schools and uses ransomware to extort money from victims. The US Government warned of increasing threats of ransomware on schools from kindergarten to high schools.

In May 2022, a ransomware attack was the tipping point for Lincoln College, an institution in Illinois, to close permanently. The ransomware blocked admissions and stopped students from accessing remote learning tools, which led to transfers out of the school and sluggish admissions for the following semester.

The public school system in Albuquerque, New Mexico was forced to close for two days after a ransomware attack blocked access to critical student data and information for adults given authority to pick up younger students from classes. All 140 Albuquerque schools were forced to suspend learning to replace encrypted data with backups.

Software developers providing applications to schools are also targets. Attackers targeted Finalsite, a developer for hosted web solutions for educational institutions, with ransomware. The ransomware affected 5000 schools after an attacker injected ransomware on Finalsite systems, which disrupted communications, enrollments, and student services.

Ransomware attacks will continue provided schools leave their staff untrained to detect and stop phishing and social engineering. Most ransomware starts with a phishing email tricking a targeted user to download a malicious file or click a link to an attacker-controlled site hosting ransomware files.

Even with cybersecurity infrastructure in place, ransomware works with users permissions and the local machine to provide the malware with access to the network. Some infrastructure will catch the ransomware before it can damage data, but sophisticated attacks bypass cybersecurity controls.

Sophisticated ransomware authors write their malware to bypass security, and educational institutions are known to have fewer effective controls. The lack of cybersecurity controls is what makes schools a primary target for cyber-criminal groups.

Reducing Threats Using Security Awareness Training

Because most ransomware starts with a phishing email, educational institutions must rely on staff to detect malicious messages and avoid clicking links or running file attachments. Having the right cybersecurity infrastructure is necessary, but the second piece to the puzzle is training staff and students so that they know what a phishing email looks like and what can happen if they don't take precautions. Training staff to avoid being a victim of phishing and ransomware is a critical component of a good cybersecurity strategy.

It's not enough to have simple training. Schools need effective security awareness training that covers several aspects of cyber-attacks, phishing, and social engineering. Cyber criminals have several tricks up their sleeves, so schools need to train staff to recognize the many ways threats compromise data storage systems.

A few areas that security awareness training should cover include:

- Shoulder surfing
- Basic data protection best practices
- Email security
- Social engineering detection
- Mobile device security
- Good password security and generation
- Overviews for common threats and attack strategies

In addition to offering initial security training, organizations must offer supplemental materials and continual training in the future. Security awareness training isn't a "one-and-done" strategy. Attackers continually change their tactics and threats evolve to bypass cybersecurity strategies. A school's training program should also adopt changes to cover the latest threats and attack tactics.

43% have had student data attacked, including dissertation materials and exam results.

25% have experienced critical intellectual property theft.

28% have had grant holder research data attacked.

To avoid staff training to become too outdated to be effective, training materials should be reviewed and updated with the latest attack strategies. After reviewing materials and updating them, the new information should be communicated to employees. Communication can be in the form of online materials, or an educational institution could offer offline materials and classes to help with the learning process.

Don't forget to use security awareness training with available metrics and feedback. Schools need training that can offer metrics so that stakeholders see results and know that training is working. Some training offers mock phishing attacks with metrics to determine if any staff members click links or interact with a threat. The results are then used to determine who needs additional training.

Security Awareness Training is Not a Replacement for Infrastructure

Although security training is beneficial for any organization including schools, it's not a replacement for good cybersecurity infrastructure. Training should be used in addition to the installation of firewalls, virtual private networks, encryption, email security, and other infrastructure.

Email security is one of the most effective measures in ransomware and phishing protection. With both email security systems in place and security awareness training for staff, a school's risk of being a ransomware victim is greatly reduced. Should a false negative pass the email security controls installed on a school's environment, the security training awareness empowers staff to detect the malicious content and report it rather than download files or click embedded links.

SafeTitan Security Awareness Training

SafeTitan is an industry-leading, behavior-driven security awareness platform that delivers security training in real time. With SafeTitan you can help bring security awareness training to your staff to help them avoid becoming the next ransomware or phishing victim. We can help fortify any educational institution's cybersecurity strategy to empower administrators and teachers to recognize phishing and social engineering when it happens.

Ready to maximize your ability to secure your school, college, or university and staff to cut security incidents and related costs?

To get started with SafeTitan, book a free demo to see SafeTitans phishing simulation and security training in action.

GET IN TOUCH