knowbe4

Human Risk Management For Education

In today's digital age, education institutions are prime targets for cyber threats, risking sensitive student and staff data. Human risk management (HRM) is crucial to safeguard these valuable assets. By educating faculty, staff and students on recognizing and responding to cyber threats, institutions can significantly reduce the likelihood of data breaches, phishing attacks and other cyber incidents. Investing in comprehensive security awareness programs not only protects the institution's reputation but also ensures a safe and secure learning environment, fostering trust and resilience against cyber adversaries.

Human Error Is The Primary Cause of Education Cyber Attacks

~70-90%

of **cyber breaches** within education are caused by human error, according to industry research by IBM, Verizon and Ponemon Institute

$20.000 - 1 million

Is the **average cost of a data breach** for schools and education institutions, according to various industry studies

90 days

On average, to **identify and contain a data breach** in schools and education institutions, according to various industry studies

A Social Engineering Assault

Here are **10 examples** of social engineering attacks that educational institutions have suffered in recent years.

1. **California university breach:** Social engineering attack exposed 4.5 million students' and staff's personal data.
2. A phishing attack on a **community college district** exposed the personal data of 2.4 million students and staff.
3. A **Maryland state university** suffered a data breach that affected the personal records of over 300,000 students and staff due to social engineering tactics.
4. **Canadian university** paid a $20,000 CAD ransom after a social engineering campaign targeting university employees led to a ransomware attack.
5. A phishing attack against a **Georgia school district** led to employee payroll and personal data being exposed.
6. A **Nevada county school district** experienced a data breach following a phishing attack targeting employee email accounts, potentially exposing sensitive information of students and staff.
7. A **Virginia public school district** suffered a ransomware attack that disrupted virtual learning platforms and exposed personal data of students and staff, highlighting vulnerabilities to social engineering tactics.
8. **Ivy League breach:** Phishing attacks compromised data across eight schools and administrative units through email phishing scams targeting university affiliates.
9. **Florida university** phishing attack exposed employee Social Security numbers and sensitive data through a phishing attack targeting university employees.
10. A **Montana state university** reported a data breach involving unauthorized access to employee email accounts through a phishing attack, potentially exposing personal information.

The Impact of Security Awareness Training on Education Institutions

Security awareness training (SAT) is the foundation for driving vigilance, building a strong security culture and is the foundation for a HRM strategy.

KnowBe4's Global Phishing By Industry Benchmarking Report measures Phish-prone™ Percentage (PPP), or the number of employees likely to fall for social engineering and phishing scams. Here is the impact that KnowBe4's SAT platform had on education institutions of all sizes based on PPP.

	Small Businesses 1-249 Employees	**Medium Businesses** 250-999 Employees	**Large Businesses** 1000-10,000 Employees	**Enterprises** 10,000+ Employees
Baseline Phishing Security Test Results - No Training	26.6%	28.4%	31.7%	34.2%
After 90 Days of SAT	19.8%	19.7%	19%	17.3%
After One Year of SAT	3.5%	4.5%	4.6%	4.8%
Overall improvement of susceptibility to phishing attacks	**87%**	**84%**	**85%**	**86%**

KnowBe4's HRM+ Platform

The HRM+ platform is KnowBe4's innovative approach to human risk management. HRM+ transforms your largest attack surface — your workforce — into your biggest asset, actively protecting your organization against cybersecurity threats, strengthening your security culture and reducing human risk. It comprises:

Security Awareness Training

AI-powered security awareness training and simulated phishing that allows organizations to drive awareness and change user behavior. Build a stronger security culture by effectively managing the ongoing problem of social engineering.

Cloud Email Security

The only email security platform to continually assess human risk and dynamically adapt security controls, preparing customers to defend against advanced phishing threats, human error and data exfiltration.

Anti-Phishing

Security orchestration and proactive anti-phishing protection to allow your incident response and security orchestration teams to identify and stop phishing threats before they reach your users' inboxes.

Real-Time Security Coaching

The first ever real-time security coaching product that detects and responds to risky end user behavior to provide immediate feedback, improving overall security culture and reducing human risk.

Compliance Plus

Compliance training that delivers continuously updated, engaging, customizable content to users and allows your organization to take a comprehensive approach to security awareness and compliance training.

AI Defense Agents

AIDA is an advanced suite of AI-powered agents that elevates your human risk management strategy.

Learn More About HRM+

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com