Data breaches and identity theft in the **education** industry

Why is the education industry targeted?

- Educational institutions store a tremendous amount of personal, financial, and medical data on each employee, student and faculty member — creating a treasure trove of data for criminals

- Cybercriminals stealing credentials could gain access to thousands of student and employee records

- In addition to being targeted by for-profit hackers, cyber-espionage can also be a threat for institutions engaging in cutting-edge research

Must-know data breach statistics for the education industry
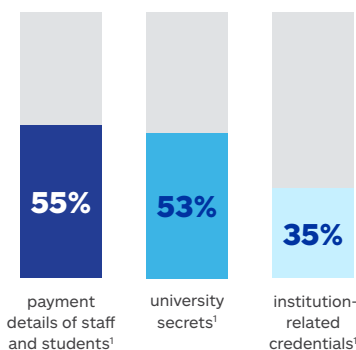
382 security incidents occurred in 2018[1]

99 confirmed data breaches occurred in 2018[1]

80% of attacks appear to have financial motivations, but cyber-espionage remains a persistent problem, particularly for research institutions[1]

Security incidents in 2019: what data was exposed?

55% payment details of staff and students[1]

53% university secrets[1]

35% institution-related credentials[1]

## Take a closer look at some recent industry breaches

- In 2019, Georgia Tech announced that it experienced a data breach exposing the personal information of 1.3 million former and current students, faculty, staff and student applicants[2]

- Educational software company Pearson experienced a breach in 2018, exposing more than 13,000 school accounts, each containing the personal information of up to thousands of students[3]

- In 2018, the FBI issued a public service announcement about cybercriminals targeting online payroll accounts, pointing out the education industry as one of the most vulnerable sectors[4]
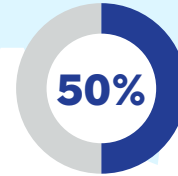
Allstate IDENTITY PROTECTION

Protect your employees, protect your institution

Empower your employees with the protection they're looking for. High quality, valuable privacy protection improves public perception and trust. Plus, it may reduce the probability of litigation for your organization and increase your employees' security awareness and safety.
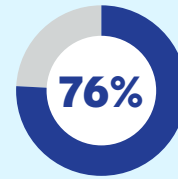
76% of Americans don't believe companies are doing their part to protect data[6]

50% of Americans say they don't know who to trust[5]

Why choose Allstate Identity Protection

Best-in-class technology, innovation and expertise

91.4
Net Promoter Score (NPS)

98%
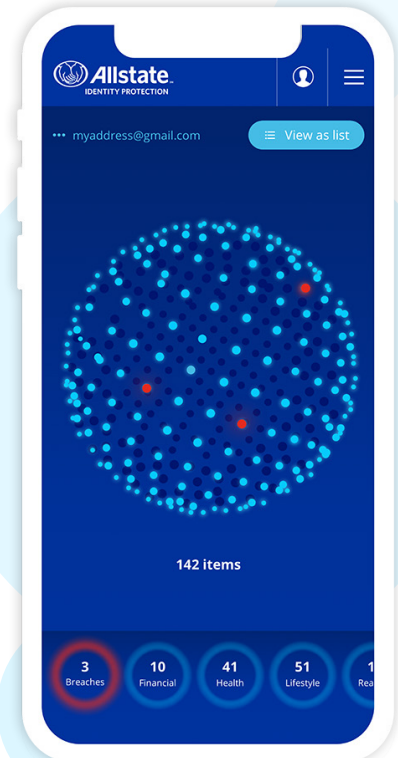implementation satisfaction rate

99%
account management satisfaction rate

99%
client retention

- Comprehensive and ongoing administrative support

- Easy onboarding that includes comprehensive product education and a dedicated client relationship advisor

- Scalable and flexible payment models that minimize risk

- Expert customer service representatives based in the U.S.

- Proactive, real-time alerts that help employees manage their privacy

- In-depth monitoring of the dark web for employees' compromised personal data, plus high risk transactions, data breach notifications, and more

- Tools to monitor and preserve an employee's reputation across social networks

- A dedicated advocate to guide and manage an employee's full recovery process

myaddress@gmail.com   ☰ View as list

142 items

3 Breaches   10 Financial   41 Health   51 Lifestyle

Ready to get started?

Contact us at sales@infoarmor.com

1 Verizon Enterprise, "2019 Data Breach Investigations Report," May 2019
2 Identity Theft Resource Center, "10,000 Data Breaches Later: Top Five Education Data Breaches," November 2019
3 Wall Street Journal, "Pearson Hack Exposed Details on Thousands of U.S. Students," July 2019
4 Federal Bureau of Investigation, "Public Service Announcement: Cybercriminals utilize social engineering techniques to obtain employee credentials to conduct payroll diversion," September 2018
5 Allstate Data Privacy and Consumer Expectations Survey
6 Allstate Digital Safety Offering Study, MARA

Allstate
IDENTITY PROTECTION