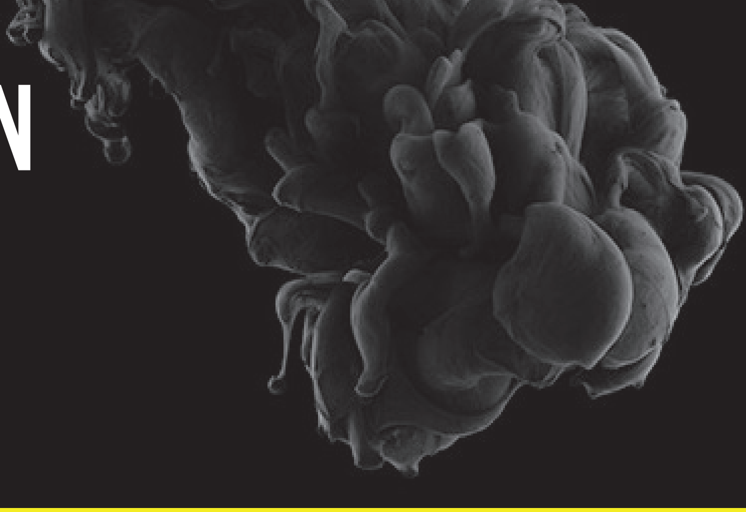
LARGEST EDUCATION SECTOR BREACHES SINCE 2017



CHEGG

Date Disclosed: October 1, 2018

Breach Method: Undisclosed

Chegg.com’s user database was accessed by an unknown third-party, allowing access to user data including name, email, address, username and hashed password. Allegedly no SSNs or financial information was accessed. Additional brands owned by Chegg were also breached in the same attack.

40M

records breached

THE CENTER FOR ELECTION SYSTEMS AT KENNESAW STATE UNIVERSITY

Date Disclosed: March 3, 2017

Breach Method: Undisclosed

In March 2017 the Kennesaw State Center for Election Systems was breach making it the second time in two years. Details on what data was taken or how access was gained has not been made public. Shortly after the event systems were wiped (suspected to be in response to a lawsuit filed against the Center.) the controversy over which heavily distracted from the breach in question.

7.5M

records breached

SAN DIEGO UNIFIED SCHOOL DISTRICT

Date Disclosed: December 21, 2018

Breach Method: Phishing

Malicious actors used phishing to compromise the accounts of over 50 faculty and gain access to personal data of staff and students alike including names, addresses, phone numbers, SSNs, staff payroll and benefits, and student health and discipline records.

500K

records breached

DATA DYNAMICS

314.696.6725 | sales@datadynamics-inc.com

DARKWEB ID

EDUCATION SECTOR BREACHES

ADVANCED LAW ENFORCEMENT RAPID RESPONSE TRAINING, TEXAS STATE UNIVERSITY

150K

records breached

Date Disclosed: July 3, 2018

Breach Method: Negligence

ALERRT is an active shooter training center for law enforcement. In 2018 a database of law enforcement officers was uploaded to an organization web server with no security or password protection. The database contained names, cell phones, work addresses, emails and other personal data of thousands of instructors and law enforcement officers, among other data can only be described as “confusing” for being stored such as last four numbers of SSNs, full emails sent to trainees which contained various PII.

BROWARD COLLEGE

44K

records breached

Date Disclosed: January 10, 2018

Breach Method: Phishing

Several employees fell victim to a phishing scam allowing fraudsters access to a database containing names, dates of birth, addresses, SSNs, financial account details, credit card numbers, and driver’s license numbers.

UCLA

30K

records breached

Date Disclosed: August 5, 2017

Breach Method: Undisclosed

In 2017 an unauthorized party gained access to a university server containing student personal data. UCLA was not forthcoming with information on how the attack occurred or what data was compromised if any.

EDUCATION SECTOR BREACHES

THE UNIVERSITY OF OKLAHOMA

Date Disclosed: June 14, 2017

Breach Method: Negligence

The University of Oklahoma had educational records dating back to 2002 on a campus file-sharing network with little to no privacy or security settings, violating federal law. The records contained names, SSNs, financial aid information and grades.

29K

records breached

PURDUE UNIVERSITY

Date Disclosed: July 13, 2018

Breach Method: Negligence

An employee from Purdue's Financial Aid department emailed the parent of a prospective student a list of names, SSNs, and birthdays for other applicants.

26K

records breached

STANFORD UNIVERSITY

Date Disclosed: December 4, 2017

Breach Method: Misconfiguration

A student staff member of the Stanford Daily was able to access sexual assault reports and promptly reported it. During the response to this event IT discovered an unprotected file containing names, birthdates, SSNs and salary for 10,000 non-teaching employees.

10K

records breached

SOUTH WASHINGTON COUNTY SCHOOL DISTRICT

Date Disclosed: August 17, 2017

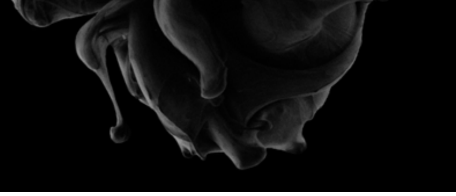
Breach Method: Negligence

Mass "back-to-school" emails were sent out containing a document with names, grades, id numbers, emails, addresses, phone numbers, bus routes, pick up and drop off, and schools of attendance for district students.

9.6K

records breached

EDUCATION SECTOR BREACHES



MONTICELLO CENTRAL SCHOOL DISTRICT

Date Disclosed: January 12, 2018

Breach Method: Phishing

Attackers were able to phish employee accounts allowing access to names, addresses, dates of birth, and SSNs, some affected also had their driver's license information exposed.

2.5K

records breached

UNIVERSITY AT BUFFALO

Date Disclosed: June 12, 2018

Breach Method: Phishing

A coordinated phishing attack at the University of Buffalo was able to get login information for 2500 accounts including 28 staff.

2.5K

records breached

RUTGERS UNIVERSITY

Date Disclosed: December 4, 2017

Breach Method: Negligence

An "Administrative Error" allowed students to view student ID, GPAs, class schedules and other student data.

1.7K

records breached

DARKWEB ID

Contact Us Today for a Free Preliminary Dark Web Scan!

DATA DYNAMICS

314.696.6725 | sales@datadynamics-inc.com