SpyCloud

Case Study

# OU Remediates 1,000 Exposed Email Accounts

## University of Oklahoma

### Overview

Founded in 1890, the University of Oklahoma (OU) is a public research university located in Norman, Oklahoma. With just over 21,000 undergraduate students, 6,000 full-time employees and 80,000 active accounts, the institution realizes the potential for cybercrime activity is a constant threat. It approaches security with a proactive stance but needed automation and good data to make a real difference.

### Challenge

With few internal resources or sufficient tools to identify and remediate exposed student, faculty and staff email accounts, OU was at constant risk for accounts being compromised.

### Solution

OU chose SpyCloud for its user-friendly API and comprehensive and operationalized exposure data it could quickly compare with its Active Directory accounts to automatically stop bad guys from compromising accounts.

### Result

OU is now able to take proper remediation action based on reliable SpyCloud data and student employee ingenuity, saving thousands of accounts from being taken over and causing harm to users and the university.

SpyCloud

## Challenge: Establishing Internal Means of Identifying Exposed Accounts

OU faces the same challenge that most higher education institutions face: students and staff use school email accounts for personal use, often reusing their OU passwords on multiple sites. When they do, they make it easy for cyber criminals to get into not only the personal sites but find their way into the school accounts as well.

OU knew some of its 80,000 active accounts were periodically exposed to cyber criminals. It just didn't have an effective way to monitor these accounts and discover all of the exposures. It was relying on third parties, and open source resources such as Pastebin and Have I Been Pwned sites.

"We look at Pastebin and they will alert us of exposed credentials, but that only gives us part of the story because not everything gets posted publicly when there's a data breach," says Aaron Baillio, deputy CISO at the University of Oklahoma. "There are a lot of dark web and non-public sites that have our information but we can't see it using open sources. We had to find a more reliable way to get alerts and manage exposures."

Managing those credential exposures was no easy feat. Even when OU received a breach alert, they didn't have the resource capacity to investigate and determine if all of the accounts belonged to active students or staff, if the exposed password matched their current OU password, or when the exposure occurred. The institution also had no password policy in place to secure active accounts. Baillio and his team made it a priority to protect the institution on the front and back ends.

## Use SpyCloud API to Integrate SpyCloud Data with Internal Tools

The first thing OU did was establish a campus-wide password policy. Students, faculty and staff are obligated to reset their passwords every year with an eight-character minimum and complexity requirements. The same password cannot be reused for five cycles. Once good password habits were enforced, the school moved on to automating account takeover precautions.

> "Using SpyCloud and the ingenuity of our student employees, we are legitimately preventing bad guys from compromising accounts."

OU had a few credential exposure products in their security stack but none with the scale and capabilities they required. They chose SpyCloud because the solution not only shows them where the credentials are located but gives them plaintext passwords and hashes so exact matches can be more easily found. It also reveals exposures in the dark web, those that aren't listed in open sources. By catching the exposures before they are on public forums, OU can take more preemptive actions before criminals do harm.

"We don't want to block an account if we don't have to, so having such detailed and usable data from SpyCloud helps our security team be more discerning," says Baillio. "We see the date of the breach, when the exposure was discovered, and its severity. If SpyCloud flags an incident with 10 emails affected but leaked more than a year ago, we hope our password policies forced a reset already and we wouldn't need to lock the account."

OU decided to integrate SpyCloud with its internal SOAR platform (security, orchestration, automation and response). Using the SpyCloud API, they pull SpyCloud breach data into their platform. When there is an alert about a particular data breach or credential leak, a ticket is automatically created.

As part of their practical application initiative, instead of using the SpyCloud Active Directory Guardian to generate automated scripts, the school selects a few SOC student employees to practice their skills to create homegrown scripts that check the SpyCloud data against the school's Active Directory. These scripts determine if active accounts and passwords are the same.

"The SpyCloud API automates the heavy lifting and data gathering for us," says Baillio.

"Our student employees integrate SOAR and SpyCloud so we can quickly react. Having the API documentation in Apiary clearly defined, allows our team and students who have limited security experience to build effective automations. We can't get that with other platforms out there."

## Fast Remediation with Minimal Resources

Using the SpyCloud API, a student employee was able to take a list of more than 7,000 exposed emails from SpyCloud, run it through their own script, and discover over 1,000 Active Directory accounts with matching passwords.

"Before SpyCloud, if we were alerted to 7,000 exposed passwords to manually check, we would most likely have had to ignore them due to a lack of resources," says Baillio. "With SpyCloud, we can get that information in less than 30 minutes. We passed that information along to our help desk and in a matter of hours, 1,000 accounts were secured. Using SpyCloud and the ingenuity of our student employees, we are legitimately preventing bad guys from compromising accounts."

Baillio believes the university is in a much better place now that they have SpyCloud in their security stack. Because SpyCloud enables them to quickly and efficiently identify compromised accounts using their own tools and in-house integrations, they can make decisions and remediate much quicker.

He and his team are focusing on training and outreach to educate students, faculty and staff on the dangers of password reuse, as well as phishing campaigns he says can generate up to a 60 percent click rate from students.

"If you get your password compromised in one place, you can bet it's compromised everywhere you reuse passwords. We need users to understand the many dangers that are inherent with emails and passwords. OU is striving to be a place of learning that goes beyond the classroom and impacts their everyday lives."

SpyCloud

## About Aaron Baillio

I've spent the first 10 years of my career with the Department of Defense. With them I traveled the world and supported both in garrison and deployed network operations and information assurance. I've written compliance documents for AF accreditation and NIST accreditation including policy and technical documents. I've also spent a lot of time performing security engineering through the system development process. Currently, I am the managing director of security operations at the University of Oklahoma. We cover the whole range of security operations from day to day sustainment to incident response. We've planned for and developed tool sets for malware detection, DNS security, vulnerability discovery and remediation and incident response maturity. We support the entire university in security operations and advise on departmental security projects.

## About SpyCloud

SpyCloud transforms recaptured data to protect businesses from cyberattacks. Its products leverage a proprietary engine that collects, curates, enriches and analyzes data from the criminal underground, driving action so enterprises can proactively prevent account takeover and ransomware, and protect their business and consumers from online fraud. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to over 150 cybersecurity experts who aim to make the internet a safer place.

### Enterprise Protection

Prevent account takeover that can lead to ransomware.

Learn More

### Consumer Protection

Combat account takeover and online fraud.

Learn More

### Investigations

Unmask criminals attempting to harm your business.

Learn More

### Data Partnerships

Enhance your solution with SpyCloud's data.

Learn More