How Proofpoint Helps Protect Colleges and Universities

Defend your students, faculty, researchers and donors against cyber threats

Products

- Proofpoint Email Protection
- Proofpoint Email Fraud Defense
- Proofpoint Threat Response Auto-Pull
- Proofpoint Content Capture
- Proofpoint Email Encryption
- Proofpoint Cloud App Security Broker

Key Benefits

- Protect key people as threats fluctuate throughout the academic year
- Take action quickly when attacks occur to minimize damage
- Address legal and compliance risk by ensuring that relevant content is retained
- Mitigate the risk of infiltration because of human error
- Manage cloud sprawl and achieve centralized visibility

COVID-19 hit the higher-education sector particularly hard. In many cases, schools were forced to close their campuses. Administrations were limited to online operations. Professors taught their classes virtually. And students had to access their classes remotely, many times from places around the globe. With such a dramatic increase in online activity, cybersecurity concerns at institutes of higher learning took center stage.

Colleges and universities are an important part of society. They educate students, conduct research and manage some of the largest events in their regions. But their importance also makes them attractive targets for cyber criminals. So although things have largely returned to normal by fall 2021, the risk of cyber attacks hasn't much abated.

Proofpoint can help your institution protect its most valuable asset—your people. We have solutions that help you respond rapidly to threats, mitigate compliance and legal risks and manage your growing cloud infrastructure.

Higher Education Cybersecurity Challenges

From an IT point of view, a major research university can be as complex as any large enterprise. With tens of thousands of students, faculty and staff, a large campus can have more user accounts than some Fortune 500 companies. A university's advanced scientific research requires massive computing resources. And a diverse set of roles, disciplines and job titles makes it extremely complex to protect the people that criminals target. Moreover, unlike private corporations, students often use campus IT resources not only for their academic work, but also for personal activities. These activities can include streaming entertainment, social media and non-school-related correspondence. This personal use of IT resources only adds to the risk around both network performance and cybersecurity.

Movement of funds

Large amounts of money move within a college or university. The schools receive donations, government funding, foundation grants, revenue from athletic and artistic events and student tuition and fees. School endowments can hold billions of dollars. And school real estate holdings can also be substantial, with many schools owning property away from their main campus. These properties can include branch campuses, research facilities and endowment lands. At a large school, some sort of construction is also almost always taking place. And significant funds must be set aside to pay for that work.

Cyber criminals have their eyes set on school funds. And they often focus on the people who handle the money. Common targets include:

- Employee and volunteer fundraisers
- Accounts receivable and finance professionals who handle payments from students
- People who maintain the physical plant and oversee construction
- Endowment fund managers

Connections with federal government initiatives

Colleges and universities are a key part of the federal supply chain. As such, nation-state threat actors and other cyber criminals target them as a way to infiltrate federal infrastructure or gain access to top-secret information stored on the institution's IT systems.

Many major universities have strong connections with the federal government. Hundreds of them conduct government-funded scientific and healthcare research. Still more schools engage in defense department-related research. The federal government also provides billions of dollars in student grants each year and guarantees the vast majority of student loans.

Enmeshed instruction, research and clinical services

Universities that have a medical school have even more complications. This is because at these schools, the academic, research and clinical functions tend to be comingled. Attackers see the school and the medical center as two paths to the same goal. An individual might be a researcher on the university side and a physician on the medical center side. This person might have separate email addresses for each organization. And this practitioner will likely check both email addresses from a mobile device or over webmail on a single laptop that is connected to both networks.

Human-error on a complex network

As networks become more distributed and complex, higher-education institutions have resources both on premises and in the cloud. Thus, they often lack centralized visibility of the entire network. This, along with typically lean staffing levels, can result in accidental misconfiguration or inadequate security protection for data. Such mistakes can create vulnerabilities on the attack surface. And attackers can exploit these points of weakness through key people in the organization.

Athletic departments and game tickets

Intercollegiate sports bring visibility to a school's brand and often are a profit center for many US universities. Because of the money generated by ticket sales, the athletic department is one of the most targeted groups at a typical university. Attacks tend to surge just prior to the beginning of the American football season. They surge again in the few weeks before end-of-season bowl games and in the leadup to the March Madness NCAA basketball tournament.

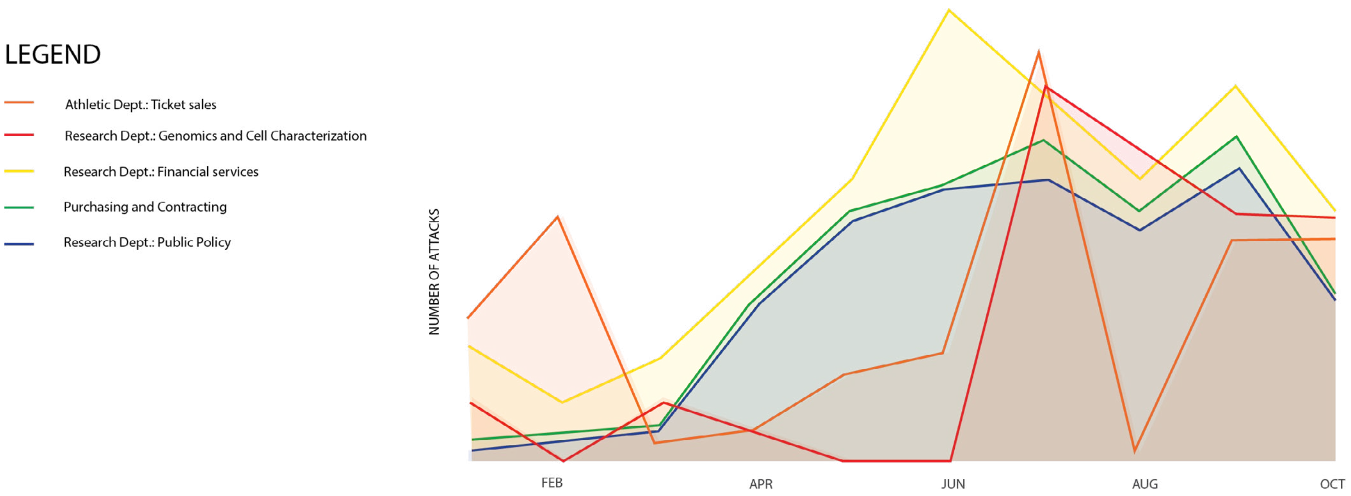

Figure 1: Monthly breakdown of the top five departments attacked at a Big 10 university.

Figure 1 shows the top five departments targeted over the course of a year at a university in the Big 10 athletic conference. Note the cyclical nature of attacks. With a fixed academic calendar, these trends are easy to predict. So security teams can prioritize their efforts to protect the right people at the right time.

Increasingly, these attacks begin with a phishing email. In Proofpoint's 2021 State of the Phish report, 57% of respondents said that their organization experienced a successful phishing attack in 2020. The percentage of organizations for which this attack resulted in data loss ballooned to 60%—a 40% increase over 2019. In an environment that is open to the sharing of ideas, it is perhaps easier for colleges to fall victim to such attacks.

A People-Centric Approach

Cyber attacks increasingly target people, not technology. Because of this, you must take a people-centered approach to secure sensitive data. Your school may value free expression of ideas, but this freedom must be balanced with protection—of individuals and the technology tools they use.

How Proofpoint Can Help

Proofpoint gives your school the tools it needs to defend its people against cyber threats. We have many solutions to help protect faculty, researchers, fundraisers and students.

Rapid threat response

In today's fast-moving threat landscape, real-time response to attacks is key. Cyber criminals use email more than any other vector to attack people in higher education. When schools can't respond quickly, attackers can move laterally in the network and cause even more damage before they are discovered.

Proofpoint offers the following solutions:

- **Proofpoint Email Protection.** As the industry-leading email gateway, Proofpoint Email Protection helps you identify and block malicious email using machine learning and multilayered detection techniques.
- **Proofpoint Email Fraud Defense (EFD).** This product augments email protection with comprehensive brand protection and visibility into attacks in a company's supply chain.
- **Proofpoint Threat Response Auto-Pull (TRAP).** This product brings automation to the manual processes your messaging and security teams use to analyze suspicious email that has made it through filters.

Compliance and legal protection

Colleges must meet multiple standards and experience litigation on a regular basis. To comply with regulations, corporate-governance standards and court-discovery requirements, these schools must retain all content from all tools that employees use to communicate. They must also make the content easily accessible by topic and user.

Proofpoint offers the following solutions:

- **Proofpoint Content Capture.** This solution archives content to your data store or downstream services while maintaining a clear and compliant chain of custody.
- **Proofpoint Email Encryption.** This solution keeps the content of emails from being intercepted by triggered encryption. For example, users can trigger encrypted messages automatically by adding a keyword of choice to the subject line.

Cloud security management

Many colleges have already adopted a cloud-first strategy. Others are in the final stages of launching one. Yet since it is almost impossible to limit cloud-based services to a single cloud, they struggle with visibility and coordination of security across multiple clouds.

Proofpoint Cloud App Security Broker (CASB) gives people-centric visibility and control over cloud apps. This includes monitoring suspicious logins and questionable activity.

Conclusion

Our solutions provide everything you need to defend against today’s most dangerous cyber threats. We protect your institution from email- and cloud-borne threats. We also help you gain visibility into your multicloud infrastructure and give you confidence that your institutional email is preserved for legal protection.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.