A BIO-key® Solution.

White Paper

# Why New and Returning College Students Present Data Security Issues

# Table of Contents

# Introduction

A study conducted by the National Cybersecurity Alliance (NCSA) and sponsored by Microsoft Corporation found "that schools are ill-prepared to teach students the basics of online safety, security and ethics, skills that are necessary in today's digital times."

With a new semester underway, it is imperative that students understand the threats and are taught how to combat them. After all, new students and students returning from break bring along with them forgotten passwords, the creation of new passwords, and a plethora of IT security issues. In general, students are unaware of most data security issues, making it more likely for attackers to take advantage of compromised user credentials to gain access to student, faculty, administration, and organizations' networks and data.

College students are increasingly becoming a target for phishing attacks. Since they spend a lot of time using the Internet for research, communicating with other students, and participating in class activities (including online classes), they are perfect targets for hackers. (Source: Toni Hunt, Cybersecurity Awareness in Higher Education, Central Washington University)

This is even more concerning since colleges and universities handle large amounts of sensitive data as well as being bound by compliance requirements like FERPA, HIPAA, GLBA, and PCI-DSS.

# Students Are Unaware of Data Security Issues

According to Ray Bendici, writing for University Business, "The majority of college students are not aware of any cybersecurity breaches at their institutions despite most IT departments on campuses reporting such incidents. A survey of 250 higher ed IT professionals and 300 students revealed that 91 percent of IT professionals who have experienced a cybersecurity breach say they have communicated the news to the student body, yet only 26 percent of students say they are aware of the incidents at their institutions."

Michael Corn, Chief Information Security Officer at the University of California, San Diego says, "I don't think we've done a good job of crafting the narrative and telling the story of cybersecurity. College is usually the first place students interact with administrative types of systems and learning management systems, so it's a real change for them."

# Higher Ed Provides Data Security Training for Faculty and Staff—But Not for Students.

Many higher ed institutions have mandatory cybersecurity training for faculty and staff but lack the same for students. Michael Dinger, a cybersecurity researcher and an associate professor of management in the Johnson College of Business and Economics at the University of South Carolina Upstate, says "the scale of a small IT staff providing training for thousands of students often makes such a practice prohibitive."

Colleges and universities must have in place an effective identity access management plan to safeguard against threats—like hacking, ransomware, phishing, and other malware attacks. And this plan should be coupled with a student data security awareness campaign.

# The Times They Are a Changin'...

According to a CIO article, "Top U.S. Universities Failing at Cybersecurity Education," cybersecurity is quickly becoming a priority for organizations."
In current studies on the topic, it has been shown that with the proper education and training, students can learn to change their Internet behavior. Students have shown that they are able to comprehend the importance of cybersecurity and identity protection. (Source: Toni Hunt, Cybersecurity Awareness in Higher Education, Central Washington University)

Mr. Corn suggests covering the subject in classes and guest lectures, since that is where students are most used to learning. Toni Hunt, Stephanie Kumi of EDUCAUSE, National Cybersecurity Alliance (NCSA), and Microsoft Corporation second this view.

# Creating a Successful Data Security Awareness Campaign

A successful data security awareness plan should have four components: technology; policy and procedures; remediation; and training and awareness. Security awareness activities should be coordinated by the Chief Information Security Officer and staff. It is ideal if there is a Student Advisory Group for input and feedback between IT, faculty, staff, and students.

EDUCAUSE puts forth a concise summary of a Security Awareness Plan:

## Technology

Update tools used to defend against illegal computing activities; make greater use of technologies such as more robust intrusion detection, firewalls, and vulnerability scanning tools.

## Policy and Procedures

Implement up-to-date security technologies; modify or create university policies and procedures on the use of computing resources. Because of the concern about computer security, many new laws and regulations are affecting data protection, and these may result in a change of university policies.

## Remediation

Protect and authorize access to private information.

## Training and Awareness

The security awareness plan will affect each member of the university community, and resources should be available to help everyone understand and implement the changes. Training on security issues should be offered as part of the program. This training should include documentation, videos, and courses on both technical and non -technical subjects.

# Identity Access Management and Security Awareness Go Hand in Hand

With an effective identity access management plan and a good data security awareness campaign that includes students, colleges and universities can safeguard their data, substantially cut down or eliminate data breaches, and protect the entire college/university community—faculty, staff, administration, and students.

A BIO-key® Solution.

# About Us

BIO-key's PortalGuard offers both a cloud-based and on-premises turnkey user authentication solution-set for campuses with external-facing web applications for their students, staff, and faculty. This all-in-one integrated design includes Two-Factor methods, Single Sign-On, Centralized Self-Service Password reset/unlock, Password Synchronization, plus transparent barriers to confirm user identities by validating their context.