CAMPUSWORKS
Insight. Ingenuity. Impact.

IT Security Clients

Aims Community College, CO

Chesapeake College, MD

Clark State Community College, OH

Graduate School USA, DC

Grayson College, TX

John A. Logan College, IL

Lakeland Community College, OH

North Iowa Area Community College, IA

Parkland College, IL

SUNY Orange, NY

Vermont State Colleges, VT

Washtenaw Community College, MI

Increasingly Complex Security Threats Impact Higher Ed IT Strategy

According to EDUCAUSE's 2019 Trend Watch, "the growing complexity of security threats" is the number one trend influencing higher education's IT strategy this year. Gone are the days of hackers simply trying to gain notoriety by unleashing annoying viruses and spam. The sophistication of today's attacks is high, and the stakes are even higher. Cybercriminals are on the hunt for sensitive data they can sell or exploit for financial gain. Higher education institutions as prized targets because they collect robust data about their students and employees and often lack the security measures to protect it.

Cybercriminals are typically after two types of data: **personally identifiable information (PII)**, which includes names, addresses, email addresses, phone numbers, birthdays, and Social Security numbers, and **personal financial information**, such as credit card numbers and bank account information. However, hijacking sensitive data is not the only goal; some attacks are engineered to interrupt operations or leech off the institution's resources. Regardless of the intent, a cyberattack can be operationally and financially crippling. Victims of such attacks commonly experience campus-wide network outages, encrypted data, lawsuits, fines, restoration costs, tarnished reputations, and public embarrassment.

"Hijacking sensitive data is not the only goal; some attacks are engineered to interrupt operations or leech off the institution's resources."

At CampusWorks, we believe in taking a proactive approach to prevent institutions from becoming victimized. Our cybersecurity experts have identified five prevalent security threats facing higher education right now and preventative measures you can take to help protect your institution:

5 Prevalent Security Threats Facing Higher Ed Right Now

1. **SOCIAL ENGINEERING**
2. **SHADOW IT**
3. **RANSOMWARE**
4. **CRYPTOJACKING/CRYPTOMINING**
5. **INTERNET OF THINGS (IoT)/MOBILE DEVICE THREATS**

CAMPUSWORKS
Insight. Ingenuity. Impact.

1. Social engineering

What is it? A ploy that uses psychology to trick people into divulging personal information or downloading malware. Social engineering includes schemes like **phishing**, **pretexting, baiting,** and more ➲

How does it work? Tactics are most commonly deployed via an email or phone call and often appear to be from a legitimate source (e.g., the IT help desk). Social engineering is the culprit behind many of the security breaches in the news.

How to prevent it: Perform a cybersecurity assessment using popular social engineering techniques to try and trick users into taking the bait. This is an effective way for institutions to identify their greatest risks and understand where more training is needed.

Did you know...

Colleges and universities are prime targets for social engineering attacks because they store a wealth of sensitive information about their students, employees, and operations.

2. Shadow IT

What is it? Systems, software, or applications that are adopted by members of an institution without the IT department's knowledge or approval. Shadow IT can be as seemingly innocuous as a department establishing its own mailing list, or it can happen on a much larger scale—when a department sets up an autonomous IT shop, hiring their own programmers and network administrators, or uses their own accounting system.

How does it work? When employees use unsanctioned applications, it can create security gaps, be non-compliant, and can employ endpoint vulnerabilities that hackers can exploit. In addition to security threats, shadow IT can impede the institution's reporting capabilities when people or departments begin keeping their own unique data sets.

How to prevent it: Conduct an IT security and risk assessment to gain a comprehensive understanding of all the software, hardware, and technical assets currently in use at your institution. Prevent your community members from unintentionally implementing shadow IT by establishing formal technology adoption policies, processes, and procedures, and educate them about the dangers and inefficiencies associated with shadow IT through regular cybersecurity awareness training and refresher workshops.

Phishing:
manipulating users into providing sensitive personal data

Baiting:
dangling something people want to entice them to download malware

Pretexting:
using a compelling story to get users to send money

Human error
is one of the greatest threats to an institution's IT security.

1767 Lakewood Ranch Blvd, #305
Bradenton, FL 34211
Phone: (941) 316-0308
success@campusworksinc.com

3. Ransomware

What is it? Malicious software that holds data hostage using proprietary encryption until the victim pays for its release.

How does it work? A user typically installs ransomware by accident—often by downloading a file that appears to be legitimate (e.g., a resume) or by clicking on an infected link or pop-up window. Ransomware is then downloaded onto the user's device where it encrypts the hard drive and shared drives people use to store critical information, blocking the entire institution from accessing it. The server generates a message that notifies the victim about the encryption and demands payment in exchange for a key to unlock the data (with no guarantee of receiving the key once the ransom has been paid). Some ransomware attacks employ a countdown clock to pressure the victim to act quickly. If and when the data is restored, there is the possibility that additional malware has been installed on the victim's system and is working behind the scenes to steal sensitive data or lying in wait to launch another attack in the future.

How to prevent it: Cybersecurity awareness training can teach your community members about the most prevalent threats and how to avoid becoming a victim. It deploys controlled test attacks to help identify vulnerabilities and understand where more training is needed. Behavioral analysis technologies provide network visibility that enables you to analyze traffic for unusual activity, which can help detect and prevent an attack.

4. Cryptojacking/cryptomining

What is it? Cryptojacking (also known as cryptomining) is a newer offspring of ransomware that hides on a computer or mobile device, often unnoticed, and uses the machine's computing power to mine for cryptocurrencies.

How does it work? Similar to ransomware, users are often tricked into clicking on a malicious link or infected website that loads cryptomining code directly onto the device. Once the computer or device is infected, the cryptojacker starts using its resources to mine cryptocurrency while staying hidden in the background, often impacting performance.

How to prevent it: Similar to ransomware, a combination of preventive measures—in the form of cybersecurity awareness training and detective controls using behavioral analysis technologies—can be effective mitigation strategies. A comprehensive cybersecurity program can add an extra layer of protection by preventing a number of threats, including cryptojacking.

5. Internet of Things (IoT)/Mobile Device Threats

What is it? Hackers target internet-connected devices with weak security protocols to open the door for a more widescale attack on the network and other connected devices.

How does it work? Members of your institution's community, especially students, use internet-connected devices in most aspects of their daily lives—think smartphones, fitness trackers, and virtual assistants. Many IoT devices offer little in terms of security and can create an inroad for hackers to exploit and infect other devices on the network, creating a domino effect.

How to prevent it: Conduct regular vulnerability assessments and penetration testing to evaluate and test the institution's technology architecture and identify ways to strengthen it against this type of attack.

CAMPUSWORKS
Insight. Ingenuity. Impact.

Security Checklist

CampusWorks' cybersecurity experts have identified three areas in which many institutions are vulnerable. When developing your IT Security Strategy, be sure to consider the following:

☑ Security controls

A lack of proper security controls can put your institution at greater risk for an attack. A major culprit is security patches that were issued but not applied, which gives hackers open access to your network and serves as a gateway to bigger problems.

Recommendation: Conduct a cybersecurity assessment to highlight the existing holes and weaknesses in your network.

☑ Security policies

Outdated security policies can leave your institution exposed and vulnerable. However, with technology changing so quickly, it can be difficult for security policies to keep up.

Recommendation: Conduct a policies, procedures, and documentation review at least once a year to identify where gaps exist and the necessary steps to keep your institution safe.

☑ Vendor management

Poor vendor management endangers institutions that outsource IT or use cloud-based systems because vendors may lack the necessary security controls to properly safeguard your institution's data and meet security compliance requirements.

Recommendation: Conduct a comprehensive vendor risk assessment and service level agreement (SLA) review to ensure your vendor has the proper security controls in place to meet your institution's security compliance requirements. If your institution is thinking about outsourcing IT or moving to the cloud, you should conduct this review before engaging a vendor.

Need help protecting your institution from increasingly complex security threats? Contact CampusWorks today for a free consultation.

CampusWorks' IT Security Assessment

A CampusWorks chief information security officer (CISO) conducts a comprehensive 7-point assessment:

1. Internet-based threats assessment and penetration testing
2. Network infrastructure assessment
3. Critical network and computing assets assessment
4. User computing environment assessment
5. Physical and environmental security assessment
6. Wireless network security assessment
7. Policies, procedures, and documentation assessment

Outcomes:

- *Security findings*
- *Information security action plan*
- *Remediation support*

1767 Lakewood Ranch Blvd, #305
Bradenton, FL 34211
Phone: (941) 316-0308
success@campusworksinc.com