Network Security: Four Essential Strategies to Protect Information and Your Network

When students moved back into their dorm rooms this fall, many brought wireless access points. Their motives are positive, perhaps studying companionably in hallways or dorm lounges. But unauthorized wireless access points can also introduce infections and provide an inroad for hackers to wreak havoc on networks and view or steal sensitive information.

Rogue wireless networks are just one example of threats to campus networks. To keep your networks safe, IT departments need to take precautions in four ways to:

- Protect student records and staff personal data from theft.
- Prevent infections that can bring down the campus network. (This becomes even more important when colleges and universities use the IP network for physical security systems like video surveillance and building access controls).
- Protect the network from malware surreptitiously installed on computers when students and faculty unknowingly visit an infected site.
- Quickly identify threats that manage to slip through your layers of defense so that you can prevent or minimize harm.

Cisco is making it easy to learn about and implement these measures through a new program called Cyberspace Action for Education (CAFE). Cisco CAFE provides Internet security awareness to education customers. It also delivers a security architecture with four components.

Stop Online Attackers
Attackers keep inventing new ways to break into campus networks and systems. Cisco ASA 5500 Series Adaptive Security Appliances provide firewall protection to keep these intruders out. You install firewalls between the campus network and the Internet. It’s also a good idea to place another firewall in front of servers that house important student records, research databases, and other sensitive information.

Check PCs Before Letting Them Connect
Mobile students, faculty, and staff can pick up infections on their laptops when they are off-campus and then introduce them onto the campus network the next time they connect. The Cisco Network Admission Control (NAC) solution prevents this problem by automatically checking every computer before allowing it to connect to the campus network. If a laptop is unauthorized, lacks antivirus software, or doesn’t have the proper settings, NAC automatically corrects the problem without any involvement by the IT staff.

Block Bad Websites
Students, faculty, and staff can pick up malware by visiting legitimate-seeming websites. Case in point: In August 2009, it was widely reported that fans searching online for actress Jessica Biel had a one-in-five chance of hitting a Web site with malicious code that could affect their PCs or network. Cisco IronPort Web Security Appliances combine several technologies to block access to malware-laden websites:

- **URL filtering:** The appliance blocks websites already known to have undesirable content.
- **Reputation filtering:** Attackers put up countless new websites every day, and these don’t appear in URL filtering lists. Before connecting to a website, the appliance considers factors such as years of operation, ownership country, history of ownership, and more. It warns campus users when they’re about to visit a website that looks suspicious.
- **Malware filtering:** If a staff member or student does visit a website that attempts to install malicious software, the appliance blocks it.
- **Enforcement of common-sense security policies:** These might include blocking transfer of files over a certain size. This keeps students from downloading audio and video files, which can slow down the network for campus business or research applications.
Gain Early Awareness of Threats

What if your network does become infected, or a freshman computer science student wants to break into university databases? Gain early awareness of these and other threats so that you can stop them, with Cisco Security Monitoring, Analysis, and Response System and Cisco Intrusion Prevention System.

These four simple steps can pay for themselves many times over by preventing even one security incident that takes down campus networks.

To watch a webcast on Cyberspace Action for Education, visit:
https://ciscosales.webex.com/ciscosales/onstage/g.php?t=a&d=201437239

To learn more about Cisco security solutions, visit: www.cisco.com/go/security

To read a case study on Trinity University’s network security initiatives, visit: