Campus Network Security

By Dr. Carolyn Lightfoot, Chief Technology Officer

With the proliferation of computers around the world, coupled with viruses spreading from sharing floppy disks in the early 1980s on network computers, hackers have been trying ever since to bring down computer systems. Whether it was meant as a joke, game, or just nuisance, mischievous folks have been finding ways to hack computer systems, and most times we are unaware of malicious code on our computer.

The rush to be “webvergence” (which is the converging of voice, data and video on the Web) has introduced many different avenues for spyware and key-loggers to attack computer systems leaving them wide open to identify theft and Internet predators.

Every day the local news station top stories are about the latest computer security threats from virtually unknowns due to the anonymous nature of the Internet. Cybercrime is on the increase targeting unsuspecting people via phishing scams, spyware, identify theft and Internet predators. We have seen attempts by hackers to compromise computer systems information as a direct result of focused attacks.

Lee College is constantly working to improve computer security using best practices including user awareness of security issues, promoting the use of security tools and providing workshops and conferences to our students and community. The unfortunate reality today is that cyber crime on the rise and is here to stay.

Cybersecurity takes all of us working together to counter cyber attacks by keeping abreast of vulnerabilities and being aware of your surroundings, Internet activity, suspicious email attachments and offers just too good to be true! You never know who or what’s lurking between the bits and bytes!

Lee College Network

The Lee College (LEEnet) network is composed of a gigabit backbone network with campus buildings connected via single mode and multimode fiber to the network operations centers (NOC). The NOC provides Ethernet connectivity between buildings and its associated switching site. The campus LAN connects routers and PIX firewalls to the Internet. We support Ethernet and high-speed data networking to the desktop. The Office of Information Technology routinely scans the campus network for computers with known vulnerabilities. This scanning is done as unobtrusively as possible. Lee College utilizes Intrusion Detection, Firewalls, ISA, WUS, Filtering, Packet Shaping, DMZ and Radius ACS and numerous other security measures to help detect and respond to information security incidents involving computers connected to the campus network. The Office of Information Technology has responsibility for centralized computing, telephony, network infrastructure including over 2,500 network connections and enterprise database management systems in the areas of finance, human resources and student administration.

Security News & Alerts

- Cyber Security Alerts — US-CERT Alerts Team
- Microsoft Security Alerts — Microsoft TechNet
Security Policy, Copyright and FERPA

- Lee College Policies and Procedures
- Copyright TITLE 17 – U.S. Code Collection from Cornell Law School
- FERPA Guidelines – Family Educational Rights and Privacy Act

Related Links

- U.S. CERT – Computer Emergency Readiness Team
- CERT Coordination Center operated by Carnegie Mellon University

Cyber Safety Tips

1. Make sure you regularly update your anti-virus software.
3. Use strong passwords (letters, numbers, capital letters, and symbols; avoid common words).
4. Do not share passwords.
5. Disable remote access.
6. Encrypt your sensitive files.
7. Protect your identity! NEVER give out personal information to a stranger.

FREE Security Software Desktop Tools

- Spybot – Search and Destroy
- Ad-aware Personal
- Microsoft Windows Defender

Notification

If you suspect a security issue regarding Lee College computers, networking resources or wireless laptops, contact the Office of Information Technology’s Help Desk at 281.425.6874 or 281.425.6451 immediately. If you prefer, email Tom Sandoval, network manager, at tsandoval@lee.edu or Dr. Carolyn Lightfoot at clightfo@lee.edu.