

Engineering Majors at A&M on Creating a Secure Cyberspace

We live in an age where the world heavily relies on digital connectivity for various purposes, including communication, commerce, and critical infrastructure. This heavy reliance has given birth to a new dangerous threat - cybersecurity. A few facts about cybersecurity threats, as reported by fintechnews.org, are a cause for concern. One statistic is that human error accounts for 95% of all data breaches. This is particularly alarming as we receive numerous phishing emails daily, each with the potential to breach our data. Also, 75% of cyber-attacks are initiated from a simple email, showing the vulnerability of our digital ecosystem. During my past internship at a Fortune 500 company, I participated in extensive training on phishing emails and potential cybersecurity attacks. However, the effectiveness of the training does not guarantee 100% safety as human error leads to many cyber-attacks.

Two specific majors at Texas A&M University can play a pivotal role in addressing the challenge of creating a secure cyberspace for future generations.

The first major, which has increased in popularity, is Computer Science Engineering. Students in this field can contribute by creating a secure cyberspace due to their software engineering and program design knowledge. They can specialize in secure software development, by writing code that lessens cyber threats. By learning coding skills through class projects and understanding the relationship between hardware and software, these future developers can build more secure platforms when creating applications. Computer Science Engineering is a challenging major, developers must consider security, feasibility, and user-friendliness in every application they make. Prioritizing security in coding is important, as human error can easily lead to data breaches. Developing programs that minimize or eliminate human error is important for a safer cyberspace.

Computer Science students can expand their skills in ethical hacking and penetration testing. Events such as "Hackathons" at Texas A&M provide students from various majors the opportunity to engage in ethical hacking challenges. When developing any type of program, it is important to assemble a team of programmers to do ethical hacking tests. These tests aim to identify vulnerabilities in the code rather than looking for personal or private information. Discovering these weaknesses lets developers find impurities in their code and strengthen it against hackers.

Electrical Engineering students at Texas A&M are well-equipped to address cyberspace security's hardware and infrastructure aspects. Their contributions can focus on network and hardware security, both are critical in our new automated systems, networks, and personal computers.

Electrical Engineering students can design more secure network architectures. This specialization involves encryption, intrusion detection, firewalls, and other security measures.

For example, substations are automated to distribute power to areas based on demand, this continuously changes throughout the day. Automating this process introduces vulnerabilities to potential cyberattacks that could compromise our power grid. Creating more effective firewalls and threat assessments is important to enhance the security of these systems.

Another significant contribution is in the field of hardware security. Electrical Engineering students take courses on microprocessors, computer architecture, and digital systems, providing them with an understanding of computer operation and potential weaknesses. While software is the main focus of cybersecurity, addressing vulnerabilities at the hardware level is also important. Developing secure hardware components and microcontrollers is a key strategy for protection against cyber threats.

Collaboration between Computer Science and Electrical Engineering students is important to developing security solutions. Computer Science students focus on securing software, raising security awareness, and identifying vulnerabilities, while Electrical Engineering students concentrate on securing the hardware that allows software to be developed. Together they create a safe and secure digital environment for people to communicate, conduct commerce, and for businesses to operate with confidence and peace of mind.

Sources Cited

moccia. "The 2020 Cybersecurity Stats You Need to Know." *Fintech News*, 20 Aug. 2020, www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/.