Garden State Cyber - Intro Cybersecurity I

Course Details: The goal of this 1/2 year course is to introduce high school students to basic cybersecurity concepts and inspire interest in cybersecurity careers. This course does not require any prerequisite knowledge in computing or cybersecurity for either the student or teacher. The course is able to be delivered completely on Chromebooks with no specialized equipment. It includes access to a cyber range for online labs at zero cost to districts. The course incorporates the 2020 New Jersey Student Learning Standards – Computer Science and Design Thinking.

Catalog Course Description: This course is designed for students who are interested in exploring careers in Cybersecurity. The focus of instruction will include the implementation and monitoring of security on network and computer systems. Students will investigate strategies to identify and protect against security threats such as hackers, eavesdropping and network attacks. The basics of cryptography and logic reasoning will be explored. Hands-on labs in a cyber range provide practice in the configuration and mitigation of system vulnerabilities. Each unit integrates current events and related cyber ethics and law. *Ethics agreement must be signed by all students and parents during the first 2 weeks of class.

Syllabus

Learning Objectives:

Upon conclusion students will be able to:

- Define the CIA Triad and key principles of cybersecurity.
- Identify authentication methods, types of attacks on authentication and best practices for mitigation.
- Identify types of malware and methods of mitigation.
- Define social engineering techniques, phishing and tools for OSINT (Open Source Intelligence).
- Use the Terminal for Linux and Windows commands and tools.
- Apply best practices for secure device configuration.
- Apply threat modeling to home and personal IOT threats
- Compute binary and hexadecimal numbers.
- Apply basic encoding and cryptographic ciphers.
- Identify key parts of a PC and define interaction of PC components.
- Identify the components, major services and protocols deployed on TCP/IP networks.
- Capture and analyze network packets.
- Complete tasks with cyber tools including Wireshark, CyberChef, binwalk, exiftool, hex editor, vulnerability scanner and bash scripting.
- Explore career opportunities in cybersecurity and evaluate the skills and education requirements in areas of career interest.

Instructional Units

Unit 1 - Foundations & Threats
1.0 Cybersecurity Careers, course objectives and Ethics Agreement
1.1 The CIA Triad and Authentication
1.2 Identifying Security Threats
1.3 Introduction to CLI (Command Line Interface)
al
Unit 2 - The Human Factor
2.1 Social Engineering
2.2 OSINT & Phishing

Unit 3 - Data Safety and Best Practices
3.1 System Hardening
3.2 IOT Threat Modeling

Unit 4 - Cryptography and Linux
4.1 Bits, Binary and Encoding
4.2 Basic Concepts of Cryptography
4.3 Advanced Linux Command Line Interface
4.4 Crypto Issues of Privacy vs Security

Unit 5 - Devices and Networking
5.1 Computing Devices
5.2 Networking Fundamentals
5.3 Protocols and Packets

Year End Projects (Extension materials)

- Biometric Authentication Product Pitch
- Social Engineering PSA Video
- Benchmark Selections for OS Hardening
- Making an Impact with Technology

Cyber Competitions: through course labs students will be introduced to cyber competitions including PicoCTF, CyberStart America and CyberPatriot. These events provide students with opportunities to independently expand their cybersecurity learning, to win scholarships and to access career pathways.