Foundations of Information Security

Huntsville High School 2020 - 2021

Instructor: Jim Morse, james.morse@hsv-k12.org, 256.428.8050 ext. 237

Course Number: 520038 Prerequisite: Geometry, Exploring CS or similar class. Fee: $45

I. Course Description:

This is a one-credit course designed to provide students with a basic understanding of computer structure, functionality, security, and ethical concerns which can be used to study cybersecurity as a career in high school and beyond. Students will be involved with hands-on activities to explore hardware and software while implementing sound security principles.

Students will discover and investigate College and Career pathways that are related to cybersecurity and computer science fields. Students complete their course by preparing for and taking the CompTIA IT Fundamentals+ certification exam or another similar exam.

Student involvement and in Skills USA, a career tech student organization, and/or security-based competitions is a requirement of the course and will enhance the concrete benefits of the classroom. This involvement will expand work-place readiness skills and broaden opportunities for personal and professional grow.

Topics Covered:

- Ethics and Safety in the Information Age
- Career and College Pathways
- IT Concepts and Terminology
- Security Concepts and Terminology
- Computer Hardware Basics
- Hardware Virtualization Concepts
- Securing the Operating System
- Digital Numbering Systems
- Applications and Software Development
- Database Concepts
- Client/Server Networking and Services
- Wireless Setup and Security

II. Course Objective

Students successfully finishing this course should have the knowledge to test and pass the CompTIA IT Fundamentals Certification, compete in the Platinum Division of the CyberPatriot competition, complete in the Skills USA State Cybersecurity competition and enroll into the Principles of Information Security Class for the 2022 - 2023 School year.

III. Resources, Materials and Tools:

- EBook: IT Fundamentals, CompTIA Academy
- Microsoft Academy
- Cisco Academy
- Other online resources

IV. Classroom Expectations: Students are expected to:

- **respect** others.
- follow the Huntsville City Schools and Huntsville High School's Disciplinary Guidelines as laid out in the student and parent handbook and the BLOOM documentation.
- follow the Huntsville City Schools Computer Use Policy that the student and parent signed when picking up their student computer.
- follow the Huntsville City Schools Cyber Academy's **Code of Conduct**.
- attend class as directed by their schedules, arrive on time and be ready to learn something new each day the class meets.
- understand that cybersecurity is a **difficult subject,** and they are expected to use the class time on cybersecurity.
- check the SCHOOLOGY page for this class daily, realizing that even if they miss a class, they are responsible for the materials presented and for completing assignments. All class resources used in class will be posted to the class Schoology page.
- follow the **Honor Code** by doing their own work and by not plagiarizing when completing assignments and projects. Follow copyright laws.
- be responsible for their education. Do your work, study for tests, ask questions, do not let others distract you and research subjects you are having difficulty with.

V. Grading Policy

Students will receive grades for completing assignments, assessment, and class activities as well as creating individual and group projects, and preparing for and competing in Skills USA and/or CyberPatriot. Official grades will be posted to PowerSchool weekly.

Assignments:

- Make up 40% of each 9 week's grade.
- Includes: class assignments, competition assignments, minor projects, minor labs
- All assignments will be posted on the Schoology class page and should be submitted to the Schoology class page for credit.
- Assignments may direct the student to another resource to complete an activity, with proof of completion submitted on Schoology.
- Assignments are expected to be turned in on due date unless circumstances prohibit the student from doing so OR the student has an IEP or 504 plan that allows extended time for completion.
- Assignments missed will receive a zero (0) for the assignment until completed.
- Assignments submitted after the due date will receive a maximum grade based on the following:
    - One class day late: 30% deduction.
    - Two class day: 40% deduction.
    - Three or more days late: 50% deduction.
    - No late work accepted after 5 class days late.
- Typical Assignment of points:
    - Class Activities: 5pts
    - Class Assignments: 10 – 20 points
    - Projects and Labs: 25 to 50 points

- Late assignments will NOT be accepted during the last week of each grading period.

Assessments:

- Make up 60% of each 9 week's grade.
- Assessments will be posted on Schoology as a calendar event and as an assignment,
- Assessment delivery:
    - Online Question/Answer or Simulated labs
    - In person, hands-on labs
- Assessments should be completed using the student's skills, abilities, and knowledge. Phones, and use of other web pages other than the test page will be deemed as a violation of the Honor Code.
- Assessments may be timed to limit the opportunity for students to use outside resources to complete the assessment as well as prepare for the certification exam at the end of the course which is timed.
- With some assessments, students will have the opportunity to have additional attempts to receive a satisfactory grade. When this occurs, grades will be determined by averaging the attempts together or accepting the first attempt's score if it is higher.
- If an assessment is missed with a school related or excused absent, students will have until the next assessment to complete it. If it is not completed in time, a zero will be posted for the assessment grade.
- If an assessment is missed with an unexcused absence, students will take the exam during the next 48 hours, either before school, after school, during Panther hour or lunch.

Exams:

Exams are assessments that are given at the end of each semester of the course to assess the long-term understanding of the concepts presented in the class thus far.

- Exams may be Q/A type, Hands-on, or a combination.
- If a student misses an exam, their exam score will be a 0%

Final Grade Calculations:

- Semester Grade Make-up:
    - First 9 weeks: 45%
    - Second 9 weeks: 45%
    - Semester Exam: 10%
- Final Grade Make-up:
    - First Semester: 50%
    - Second Semester: 50%

VI. Sample Lessons

- Students will demonstrate their understanding of computer hardware but dismantling and identify all hardware followed by reassembly of computer to working form.
- Students will demonstrate their understanding of "computer math" by competing in a class competition on the Cisco Binary Game.
- Students will read and review various cybersecurity articles.
- Students will choose an entry level cybersecurity career and complete a written research report on it's:
    - Employment Requirements
    - Average national salary

- Best location to work based on employability, cost of living, etc…
- Time requirements

VII. Learning Standards

1. Explain professional, legal, and ethical responsibilities in the field of cyber security, including the need for a diverse work force.
2. Utilize research results to determine career and entrepreneurial opportunities, responsibilities, and educational and credentialing requirements in entry-level information technology professions.
3. Describe ethical considerations resulting from technological advances.
4. Utilize mathematics skills to convert between two number systems, including decimal, binary, and hexadecimal.
5. Demonstrate the construction of a computer system, including the installation of hardware and software.
6. Exhibit proper use of basic computer components, including hardware, operating systems, software, file management, and network functions.
7. Identify security features of Windows, Cisco, and Linux operating systems.
8. Perform basic security hardening and configuration of multiple operating systems.
9. Utilize the troubleshooting and vulnerability assessment process.
10. Identify fundamental principles of networks.
11. Perform basic TCP/IP configuration of operating systems for access to network resources.
12. Identify tools, diagnostic procedures, and troubleshooting techniques for networks.
13. Perform basic configuration of home wireless networks.
14. Create simple applications use secure and functional programming techniques.
15. Secure and use databases.
16. Create written technical reports.