CYBERSECURITY SYLLABUS

Course Overview and Goals

As our world becomes increasingly dependent on technology, cybersecurity is a topic of growing importance. It is crucial that companies and individuals take precautions to protect themselves from the growing threat of cyber attacks. This course prepares students with crucial skills to be responsible citizens in a digital future.

The Introduction to Cybersecurity is the first online blended K12 cybersecurity course. The Vigenère year-long version is designed for students with some exposure to computer science, but there are no specific course prerequisites. Students will learn foundational cybersecurity topics including digital citizenship and cyber hygiene, the basics of cryptography, software security, networking fundamentals, and basic system administration and all through the CodeHS web-based platform. Students will complete projects at the end of each module, and a culminating course project where they will complete a simulated hack walkthrough. This is not a coding intensive course, but students will learn basic SQL, and will utilize basic HTML and JavaScript within specific contexts and will be provided supports within those contexts.

Learning Environment: The course utilizes a blended classroom approach. The content is a mix of web-based and physical activities. Students will modify existing code and run it in the browser, investigate cyber related topics and reflect on them and discuss them, create digital presentations, and engage in in-person collaborative exercises with classmates. Teachers utilize tools and resources provided by CodeHS to leverage time in the classroom and give focused 1-on-1 attention to students.

Programming Environment: Students modify and run programs in the browser using the CodeHS online editor. Students will be able to modify text-based programs in HTML, JavaScript and SQL (sand shell commands in the supplementary module). Students will also participate in simulated cyber attacks on safe sites in order to learn how to mitigate cyber attacks. Students will be able to document their processes and discusses best practices for preventing cyber attacks.

Quizzes: Each lesson includes at least one formative short multiple choice quiz. At the end of each module, students take a summative multiple choice quiz that assesses their knowledge of the concepts covered in the module.

Prerequisites: The Introduction to Cybersecurity course is designed for beginners to intermediate computer science students with at least some knowledge and interest in computer science. The course is highly visual, dynamic, and interactive, making it engaging for those new to computer science.

Course Breakdown

Module 1: What is Cybersecurity? (4 weeks/20 hours)
This module gives an introduction to cybersecurity. It focuses on why cybersecurity is important, recent threats to cybersecurity, and different careers in the field.

Objectives / Topics Covered	● Course Overview ● What is Cybersecurity? ● Impact of Cybersecurity ● The CIA Triad
Example Assignments / Labs	● Course Overview ○ Do you use the Internet? ○ How do you use the Internet? ○ What kinds of information are at risk? ○ What are some different CS career fields? ○ Coding as the new literacy ○ What is this course about? ○ Example activity: ■ Lists steps to take to protect yourself on the Internet ■ What is something you want to know or make by the end of the course? ● What is Cybersecurity? ○ Cybersecurity defined ○ Why is cybersecurity important? ○ Cybersecurity in the news ○ Cybersecurity and IoT (Internet of Things) ○ How do we prevent cyber attacks? ○ Example activities: ■ Summarize and discuss recent cyber attacks ■ Explore a threat map to see where cyber attacks are coming from and which countries are being targeted ● Impact of Cybersecurity ○ Why do we care about cybersecurity? ○ What information is at risk? ○ What are the impacts of cyber attacks?

	■ Financial impact ○ Cybersecurity workforce ○ What are current cybersecurity career? ○ Example activities: ■ Review resources and reflect on or discuss ● What information do cyber criminals steal? ● What do cyber criminals do with stolen information? ● The CIA Triad ○ What is the CIA triad? (confidentiality, integrity, availability) ○ What are “secure systems?” ○ What do confidentiality, integrity, and availability mean in cybersecurity? ○ Example activities: ■ Determine where scenarios break part of the CIA Triad

Module 2: Digital Citizenship and Cyber Hygiene (10 weeks/50 hours)
This module includes topics on Internet etiquette and how to stay safe on the world wide web. We will also look at the potential effects of our digital footprints, how to protect information from online risks, and the implications of cyberbullying. Finally, the module includes how to find and cite quality resources online.

Objectives / Topics Covered	● Digital Footprint and Reputation ● Cyberbullying ● Internet Safety ● Privacy and Security ● Information Literacy ● Creative Credit and Copyright ● Hacking Ethics
Example Assignments / Labs	● Digital Footprint and Reputation ○ What is a digital footprint? ○ What is ***your*** digital footprint and reputation? ○ What does it mean that the internet is public and permanent? ○ Who looks at your digital footprint and reputation? ○ What are some recommended social media guideline? ○ How can you maintain your digital footprint? ○ What does your digital footprint say about you? ○ Example activities: ■ What is your digital footprint? ■ Are you going to make any changes in what

	you post on social media? ● Cyberbullying ○ What is cyberbullying? ○ What are the impacts of cyberbullying? ○ Are there cyberbullying roles? ○ What do you do if you are being bullied? ○ What do you do if you see bullying? ○ How can you be an upstander? ○ Example activities: ■ Explore cyberbullying scenarios: What would you do? ● Internet Safety ○ What are some ways to stay safe online? ○ What are some online safety guidelines? ○ Example activities: ■ Explore Internet safety scenarios: What would you do? ● Privacy and Security ○ What are data privacy and security? ○ How can you keep personal data secure and private? ○ What can happen if you data is stolen and what can you do about it? ○ Example activities: ■ Test out various passwords on a site ■ Explore Google's privacy policy: What do they know about you? ● Information Literacy ○ What is information literacy? ○ How can you do effective internet searches? ○ What are some techniques for judging source legitimacy and identifying misinformation? ○ Example activities: ■ Create and test search queries ■ Explore evidence for using sources ● Creative Credit and Copyright ○ What is copyright? ○ What are the different types of copyright licenses ○ Example activities: ■ Create citations for sources ■ Explore image search tools ● Hacking Ethics ○ What are hackers? H ○ Are there different kinds of hackers? (white, black, grey) ○ What are bug bounty programs? ○ Is hacking always illegal? ○ What are the consequences of illegal hacking?

	○ Example activities: ■ Explore what penetration testing is ■ Sign ethical hacker agreement ● Final project: Create a Public Service Announcement ○ Create a Public Service Announcement (PSA) to teach your peers about your selected topic in digital citizenship and cyber hygiene. You can select any of the topics covered in this module. Be creative and make it fun! You could make a video, song, poster, or slideshow.

Module 3: The ABCs of Cryptography (7 weeks/35 hours)

In this module, we will dive into the history of cryptography systems, the motivation behind using encryption systems, and basic cryptography systems. Additionally, we will explore topics on how to use cryptography, cryptology, and cryptanalysis to decode a message without the use of a key. Finally, we will look into more advanced cryptographic topics like public key cryptography and hash functions.

Objectives / Topics Covered	● Cryptography, Cryptology, Cryptanalysis ● History of Cryptography ● Why do we Need to Encrypt Data? ● Basic Cryptography Systems: Caesar Cipher ● Basic Cryptography Systems: Cracking the Caesar Cipher ● Basic Cryptography Systems: Vigenère Cipher ● Advanced Cryptography ● Hash Functions ● Hash Function Development
Example Assignments / Labs	● Cryptography, Cryptology, Cryptanalysis ○ Why do we need some secrecy in our transparent information age? ○ Explain general encryption with data, keys ○ Example activities: ■ Video and discussion on securing the cloud ■ Passing notes in class (offline activity) ● History of Cryptography ○ Why do we encrypt? ○ What are some classic encryption techniques? ○ What is the flaw in substitution ciphers? ○ What was The Enigma during WW2? ○ What is modern cryptography and how has cryptography changed over time? ○ What is 256-bit key encryption and how does this help cryptography overall? ○ Example activities:

	■ How did the Enigma work? ● Why do we Need to Encrypt Data? ○ Explore the CIA Triad and encryption ○ Example activities: ■ Telephone game with math (offline) ■ Modulo math activity sheet ● Basic Cryptography Systems: Caesar Cipher ○ Explore examples of the Caesar cipher ○ Example activities: ■ Practice with a Caesar Cipher JavaScript program ■ Modify the program to create the decrypting Caesar program ● Basic Cryptography Systems: Cracking the Caesar Cipher ○ How do we solve the Caesar Cipher with brute force and using letter frequency analysis? ○ Example activities: ■ Practice cracking Caesar Cipher with brute force ■ Practice cracking Caesar Cipher with letter frequency ● Basic Cryptography Systems: Vigenère Cipher ○ Explore examples of the Vigenère Cipher ○ Example activities: ■ Practice with a Vigenère Cipher JavaScript program ● Advanced Cryptography ○ What are the problems with Caesar cipher? (History recap) ○ What does today's cryptography look like? ○ What does "hard vs. easy problems to crack" mean? ○ What kinds of encryption are there? (symmetric, asymmetric, public key) ○ Example activities: ■ Discuss resources related to public key cryptography ● Hash Functions ○ What is cryptographic hashing? ○ How is hashing used? ○ What is a hash function?n Why are hash functions used? ○ What does the ideal hash function do? ○ How do attackers try to crack a hashing algorithm? ○ Example activities: ■ Use a hash generator to create hashes for various input ● Hash Function Development ○ How can we preventing hash function cracking?

	○ Why is modulo math so important for hash programs? ○ Example activities: ■ Practice module math problems (offline) ■ Test a simple hash program ● Final project: Develop a hash program ○ Modify a hash function program with new math to create different hashes for the same inputs. Explain how your new program works and show before and after results for 3 different input strings that the new hash function changed the hash created.

Module 4: Software Security (9 weeks/45 hours)

In this module, we will learn what happens when running a web application and how to look inside web apps using developer tools, source code, and more. We will learn basic SQL so we can learn about common attacks like SQLi and XSS. and recommend solutions for flawed security systems.

Objectives / Topics Covered	● Inside Web Applications ● Developer Tools ● SQL Overview ○ What is SQL? ○ Structuring Data in SQL ○ Basic Querying in SQL ○ Filtering Queries in SQL ● Clients, Servers, Databases ● Common Security Problems ● SQL Injection ○ SQLi Overview ○ Types of SQLi ○ Preventing SQLi ● Cross-Site Scripting (XSS) ○ XSS Overview ○ Types of XSS ○ Preventing XSS ● Data Exposure
Example Assignments / Labs	● Inside Web Applications ○ View page source (images, navigation and page layout, stylesheets, JavaScript, minified code ○ Example activities: ■ View page source scavenger hunt ■ Getting started with OWASP ● Developer Tools ○ Use the inspect tools to look more deeply inside of

	web apps ○ How does view page source compare to inspect in terms of information about the site / app? ○ Example activities: ■ Practice using the Chrome developer tools ■ Change a favorite site using the Chrome developer tools on your end only. Take a screenshot of your change. ● SQL Overview ○ What is SQL? ○ How do we structuring data using SQL? ○ How do we query databases using SQL? ○ Example activities: ■ Use the SELECT statement to query a database ■ Use the WHERE clause to query a database ● Clients, Servers, Databases ● Common Security Problems ○ What is the “Fortification Principle”? ○ What are some tips about HTTP vs. HTTPS, password fields and CAPTCHA that can help us to navigate more securely on the Web? ● SQL Injection ○ SQLi Overview ■ What is SQLi? ■ Why is SQLi a problem? ■ What happens during a SQLi attack? ■ What is the the fallout of a SQLi attack? ■ How does SQLi work? ■ How do hackers use SQL in a SQLi? ○ What are the types of SQLi (error-based, union-based, blind) ■ What is the underlying SQL behind the scenes that hackers may be trying to hack? ○ How to we mitigate or prevent SQLi? ■ What are the OWASP recommendations? ■ How can we tell if our code is vulnerable? ○ Example activities: ■ Discuss the Equifax SQL injection attack ■ Practice basic SQLi on a safe site ■ Research SQLi prevention ● Cross-Site Scripting (XSS) ○ XSS Overview ■ What is XSS? ■ Why is XSS a problem? ■ What happens during an XSS attack? ■ What is the fallout of a XSS attack? ■ How does XSS works

	■ How do hackers use JavaScript in a XSS attack? ○ What are the types of XSS (reflected XSS, stored or persistent, DOM) ■ What is the vulnerable JavaScript behind the scenes? ○ How do we prevent or mitigate XSS? ■ What are the OWASP recommendations? ■ How can we tell if our code is vulnerable? ○ Example activities: ■ Discuss the XSS bug in Yahoo email attack ■ Practice basic XSS on a safe site ■ Research XSS prevention ● Data Exposure ● Final project: Hack Walkthrough ○ Students will be given a series of SQLi and XSS attacks that they need to perform on the site http://hackyourselffirst.troyhunt.com/ . Students will then reflect on classifying the vulnerabilities that they exploited and how they would mitigate the various attacks.

Module 5: Networking Fundamentals (6 weeks/30 hours)

This module explores the structure and design of the internet and networks, and how this design affects the reliability of network communication, the security of data, and personal privacy. We will learn how the Internet connects computers all over the world. Finally, we will explore basic networking protocols, practical networking, and how networks are secured.

Objectives / Topics Covered	● Introduction to the Internet ● Internet Hardware ● Internet Addresses ● Domain Name System (DNS) ● Routing ● Packets and Protocols ● The Internet and Cybersecurity ● Impact of the Internet ● Network Hacks ● Securing a Network
Example Assignments / Labs	● Introduction to the internet ○ What is the Internet? How does it work? What have been its impact on society? ○ Why do we need protocols for the Internet? ○ Example Activity

	■ Explore the different levels of the internet. ● Internet hardware ○ Vocabulary: bandwidth, bitrate, latency ○ Why are protocols so important? ○ How do we send data over the Internet? ○ Example Activities ■ Explore how data is able to be transmitted across the ocean by using underwater cables ■ Explore the role of simple and complex networks and routers ● Internet Addresses ○ Vocabulary: Internet Protocol (IP) ○ How do IP addresses compare to postal addresses? ○ How IP addresses work? ○ Example Activities ■ Explore the differences between IPv4 and IPv6. Why are we running out of addresses? ■ Trace a website request from the server, through the network, and to your computer ● Domain Name System (DNS) ○ How does DNS help with sending digital information and IP addresses? ○ Example Activities ■ Explore the process of how requesting a web resource works ● Routing ○ How is routing used to send messages / data? ○ Why is redundancy a good thing for the Internet? (fault tolerant) ● Packets and Protocols ○ How data is transmitted? ○ How are internet packets able to find their way to your computer? ○ Example Activities: ■ Explain in your own words how a request from your computer travels through the various levels of servers to reach and return the correct webpage and resources? ■ As a class, create a protocol that will allow one classmate to send another classmate a note, without the need for talking to each other. ○ What are the standard protocols for the Internet and how do they work? (TCP/IP, HTTP) ● The Internet and Cybersecurity ○ What are cybercrime and cyberwarfare? ○ How do we network attacks? (certificate authorities, public key encryption)

	● Network Hacks ○ What are common network attacks? ○ Explain common network attacks and how they happen. (DNS spoofing, DoS/DDoS, Waterhole attacks, fake WAP, eavesdropping) ● Securing a Network ○ How can we detect intrusions? (checking logs, firewall rules, intrusion detection systems - IDS) ○ What are some recommended approaches for mitigating or preventing network attacks? ● Final Project ○ Create a basic network configuration simulation that is optimized for security via the following site: http://malkiah.github.io/NetworkSimulator/simulator01.html# ● Final course Project / Challenge: ○ Walk through a simulated attack from the attacker and defender perspectives and incorporate all techniques and recommendations garnered from the course.