

TRUMBULL PUBLIC SCHOOLS

Trumbull, Connecticut

CYBERSECURITY

Grades 9-12

Computer Science Department

2020

Curriculum Writing Team

Scott Kaminski

Teacher

Jonathan S. Budd, Ph.D.

Assistant Superintendent

Cybersecurity

Property of Trumbull Public Schools

**Cybersecurity
Grades 9-12
Table of Contents**

Core Values & Beliefs	2
Introduction & Philosophy	2
Course Goals.....	2
Course Enduring Understandings	5
Course Essential Questions.....	5
Course Knowledge & Skills.....	5
Course Syllabus	8
Unit 1: What Is Cybersecurity?	9
Unit 2: Digital Citizenship and Cyber Hygiene	11
Unit 3: The ABCs of Cryptography	14
Unit 4: System Administration	17
Unit 5: Software Security	19
Course Credit	22
Prerequisites	22
Supplementary Resources	22
Current Reference	22
Assured Student Performance Rubrics	22

The Trumbull Board of Education promotes non-discrimination in all of its programs, including educational opportunities and services provided to students, student assignment to schools and classes, and educational offerings and materials.

CORE VALUES AND BELIEFS

The Trumbull High School community engages in an environment conducive to learning which believes that all students will **read and write effectively**, therefore communicating in an articulate and coherent manner. All students will participate in activities **that present problem-solving through critical thinking**. Students will use technology as a tool applying it to decision making. We believe that by fostering self-confidence, self-directed and student-centered activities, we will promote **independent thinkers and learners**. We believe **ethical conduct** to be paramount in sustaining the welcoming school climate that we presently enjoy.

Approved 8/26/2011

INTRODUCTION & PHILOSOPHY

As our world becomes increasingly dependent on technology, cybersecurity is a topic of growing importance. Cybersecurity prepares students with crucial skills to be responsible citizens in a digital future.

Cybersecurity is a semester-long course designed for students with some exposure to computer science, but there are no specific course prerequisites. The course is entirely web-based, provided by CodeHS. Students will learn foundational cybersecurity topics including digital citizenship, software security, and the basics of cryptography. The entirely web-based curriculum is made up of a series of learning modules that cover the fundamentals of cybersecurity. Each module is comprised of short video tutorials, example programs, quizzes, simulations, programming exercises, and free-response prompts. Cybersecurity is not a coding-intensive course, but students will learn very basic SQL, JavaScript, and HTML in order to protect against simulated cyber attacks.

COURSE GOALS

The following course goals derive from the 2017 Computer Science Teachers Association (CSTA) K-12 Computer Science Standards.

Computing Systems

CSTE.3A-CS-02 Compare levels of abstraction and interactions between application software, system software, and hardware layers.

CSTE.3B-CS-01 Categorize the roles of operating system software.

Networks and the Internet

CSTA.3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.

CSTA.3A-NI-06 Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

- CSTA.3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system.
- CSTA.3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations.
- CSTA.3B-NI-04 Compare ways software developers protect devices and information from unauthorized access.

Data and Analysis

- CSTA.3A-DA-10 Evaluate the tradeoffs in how data elements are organized and where data is stored.

Algorithms and Programming

- CSTE.3A-AP-18 Create artifacts by using procedures within a program, combinations of data and procedures, or independent but interrelated programs.
- CSTA.3A-AP-20 Evaluate licenses that limit or restrict use of computational artifacts when using resources such as libraries.
- CSTE.3B-AP-10 Use and adapt classic algorithms to solve computational problems.
- CSTE.3B-AP-11 Evaluate algorithms in terms of their efficiency, correctness, and clarity.
- CSTE.3B-AP-14 Construct solutions to problems using student-created components, such as procedures, modules and/or objects.
- CSTA.3B-AP-18 Explain security issues that might lead to compromised computer programs.
- CSTE.3B-AP-22 Modify an existing program to add additional functionality and discuss intended and unintended implications (e.g., breaking other functionality).

Impacts of Computing

- CSTA.3A-IC-24 Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
- CSTA.3A-IC-25 Test and refine computational artifacts to reduce bias and equity deficits.
- CSTE.3A-IC-26 Demonstrate ways a given algorithm applies to problems across disciplines.

CSTA.3A-IC-28	Explain the beneficial and harmful effects that intellectual property laws can have on innovation.
CSTA.3A-IC-29	Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users.
CSTA.3A-IC-30	Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.
CSTA.3B-IC-25	Evaluate computational artifacts to maximize their beneficial effects and minimize harmful effects on society.
CSTA.3B-IC-26	Evaluate the impact of equity, access, and influence on the distribution of computing resources in a global society.
CSTA.3B-IC-27	Predict how computational innovations that have revolutionized aspects of our culture might evolve.
CSTA.3B-IC-28	Debate laws and regulations that impact the development and use of software.

The following course goals derive from the 2016 International Society for Technology in Education Standards.

ISTE Empowered Learner (Standard 1)	Students leverage technology to take an active role in choosing, achieving, and demonstrating competency in their learning goals, informed by the learning sciences.
ISTE Digital Citizen (Standard 2)	Students recognize the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world, and Act and model in ways that are safe, legal, and ethical.
ISTE Knowledge Constructor (Standard 3)	Students critically curate a variety of resources using digital tools to construct knowledge, produce creative artifacts, and make meaningful learning experiences for themselves and others.
ISTE Computational Thinker (Standard 5)	Students develop and employ strategies for understanding and solving problems in ways that leverage the power of technological methods to develop and test solutions.
ISTE Creative Communicator (Standard 6)	Students communicate clearly and express themselves creatively for a variety of purposes using the platforms, tools, styles, formats, and digital media appropriate to their goals.
ISTE Global Collaborator (Standard 7)	Students use digital tools to broaden their perspectives and enrich their learning by collaborating with others and working effectively in teams locally and globally.

COURSE ENDURING UNDERSTANDINGS

Students will understand that . . .

- cybersecurity risk is a measure of the potential damage or loss a vulnerability could cause weighed against the likelihood an adversary will exploit the vulnerability.
- cybersecurity shapes and is shaped by significant historical ideas and events.
- cybersecurity is global and always evolving.
- data security deals with the integrity of data, the privacy of data, and data confidentiality.
- data security uses non-technical and technical controls and techniques to protect data that is being processed, transmitted, and stored.
- cryptography techniques are necessary to keep data private and secure, and evolve with changes in technology.
- systems consist of a combination of hardware and software that together achieve some objective, and security requires integration of both.
- security vulnerabilities in software are weaknesses in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.
- adversarial thinking is the process of reasoning about how opposing forces could prevent a systems from meeting both its functional and its security goals.

[All retrieved from the *Cyber Center for Education & Innovation*,
<https://cryptologicfoundation.org>.]

COURSE ESSENTIAL QUESTIONS

- What is cybersecurity, and why is it necessary?
- What is a digital footprint, and how can it be protected?
- How does cryptography work?
- How does computer system administration work?
- What are the components of software security?

COURSE KNOWLEDGE & SKILLS

Students will know . . .

- the definition of cybersecurity.
- details of current cyber attacks and how they affect society.
- the definition of the Internet of Things (IoT).
- the three parts of the CIA Triad.
- the different ways that everyone leaves digital footprints.
- the definition of cyberbullying and what to do if they experience it or witness it.
- safety guidelines to keeping personal information secure while online.
- strategies for effective Internet searches.
- multiple techniques for judging source legitimacy and identifying misinformation.
- different types of copyright licenses.
- what a hacker is, and the difference between ethical and illegal hacking.
- the definition of encryption.
- how to encrypt and decrypt messages using a Caesar cipher and the Vigenère cipher.

- the three main operating systems used in most computers.
- how the file management systems work in operating systems.
- techniques for using the developer tools of web browsers.
- the differences between basic databases and SQL.
- basic SQL commands to perform a SQL Injection (SQLi) attack on a virtual machine.

Students will be able to . . .

- explain why it is important to learn computer science, regardless of their goals for college and career.
- define cybersecurity.
- describe how the Internet of Things (IoT) makes people more vulnerable to cyber attacks.
- reflect on recent cyber attacks and identify the financial and societal impact of the attacks.
- evaluate recent cyber attacks and understand the negative consequences of these attacks.
- understand career opportunities in the field of cybersecurity.
- identify what the CIA Triad is and how it relates to cybersecurity.
- identify which part of the CIA Triad has been broken in a given scenario.
- understand how their online activity contributes to a permanent and public digital footprint.
- articulate their own social media guidelines to protect their digital footprint.
- understand the impact of cyberbullying, and identify unacceptable bullying behavior.
- identify proper actions to take if they are victims of cyberbullying or if they observe someone being cyberbullied.
- identify predatory behavior and how to respond to it online.
- use best practices in personal privacy and security, including strong passwords, using https, and reading privacy policies.
- effectively search for and evaluate resources.
- explain what copyright laws are and why they are important.
- find images they are legally allowed to use in their projects.
- accurately attribute images they find and want to use.
- identify the difference between white hat hacking and black hat hacking.
- explain career opportunities in cybersecurity.
- define cryptography, cryptology, and cryptanalysis.
- explain the need for encryption and how basic encryption and decryption works.
- relate encryption to the CIA Triad.
- explain the purpose of cryptography and how different crypto systems have been used throughout history.
- encrypt and decrypt messages using a Caesar cipher.
- explain why a Caesar cipher is so easy for a computer to crack.
- use basic distribution analysis to decrypt a simple message.
- explain how the Vigenère cipher works and why it is not as easy to crack as a Caesar cipher is.
- explain the purpose of operating systems.
- identify the main types of operating systems.
- analyze the upgrade and installation process for operating systems.

- compare and contrast the interface of Mac, Windows, and Linux operating systems.
- explain how operating systems use file systems to manage data.
- explain the importance of application security.
- explain the multiple methods for protecting software.
- configure their browsers to enhance security and privacy.
- explain how the following features impact their browser security: cache, client-side scripting, browser extensions, private browsing, proxy settings, certificates, and popup blockers.
- describe how creating user accounts and permissions enhances security.
- define system hardening
- explain the importance of establishing baseline security, including deciding rules around authentication and authorization.
- explain the importance of performing security audits.
- identify major sections of code within the view source of a web page/app.
- understand the importance of OWASP and how it relates to the field of cybersecurity.
- identify major developer tools within the inspect element.
- explain the major difference between view page source and what is rendered in the inspect tools.
- explain in general terms what each major tool in the inspect area can show a developer.
- explain how the developer tools can help web developers build and maintain sites, and how understanding the tools can potentially help cyber professionals who are trying to keep sites and data secure.
- explain the primary purposes of a database.
- identify and explain the major parts of a database.
- understand the implications of database storage on the protection of data within the field of cybersecurity.
- explain what the SQL programming language does.
- define the different parts of a database (table, column, row).
- define what a schema is in relation to a database.
- explain what security means on a personal and organizational level.
- understand and explain what a SQL injection attack is and the ongoing, pervasive impact of SQLi cyber attacks.
- explain the 3 types of SQLi and the vulnerability associated with each.
- understand the fundamentals of how SQL injections are prevented or at least mitigated.

COURSE SYLLABUS

Course Name

Cybersecurity

Level

Grades 9-12

Prerequisites

None

Materials Required

None

General Description of the Course

As our world becomes increasingly dependent on technology, cybersecurity is a topic of growing importance. This course will prepare students with crucial skills to be responsible citizens in a digital future. Students will learn foundational cybersecurity topics including digital citizenship, cyber hygiene, classic and modern cryptography, software security, networking fundamentals, and basic system administration. The course is designed for students with interest in computer science, and beginning to intermediate computer science skill.

Assured Assessments

Formative Assessments:

- Responses to simulated experiences (Units 1, 2, 4, 5)
- Reading and discussion of case studies (Units 1, 2, 3, 4, 5)

Summative Assessments:

- End-of-unit assessment (Units 1, 2, 3, 4, 5)
- “Public Service Announcement” project related to digital citizenship and cyber hygiene (Unit 2)
- Creation of a modified version of an Enigma Machine (Unit 3)
- “Security Assessment” project related to SQLi hacking techniques (Unit 5)

Core Text

- CodeHS. *CodeHS: Fundamentals of Cybersecurity*. <https://codehs.com/course/6560>. Accessed October 9, 2020. Web.

UNIT 1

What Is Cybersecurity?

Unit Goals

At the completion of this unit, students will:

CSTA.3A-IC-24	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
CSTA.3A-IC-29	Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users.
CSTA.3A-IC-30	Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.
CSTA.3A-NI-05	Give examples to illustrate how sensitive data can be affected by malware and other attacks.
CSTA.3A-NI-06	Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.
CSTA.3A-NI-07	Compare various security measures, considering tradeoffs between the usability and security of a computing system.
CSTA.3B-IC-25	Evaluate computational artifacts to maximize their beneficial effects and minimize harmful effects on society.
CSTA.3B-IC-26	Evaluate the impact of equity, access, and influence on the distribution of computing resources in a global society.
CSTA.3B-IC-27	Predict how computational innovations that have revolutionized aspects of our culture might evolve.
CSTA.3B-NI-04	Compare ways software developers protect devices and information from unauthorized access.
ISTE Empowered Learner (Standard 1)	Leverage technology to take an active role in choosing, achieving, and demonstrating competency in their learning goals, informed by the learning sciences.
ISTE Digital Citizen (Standard 2)	Recognize the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world, and act and model in ways that are safe, legal, and ethical.
ISTE Knowledge Constructor (Standard 3)	Critically curate a variety of resources using digital tools to construct knowledge, produce creative artifacts, and make meaningful learning experiences for themselves and others.

Unit Essential Questions

- What is cybersecurity, and why is it necessary?
- What types of information are sent over the Internet?
- What is the Internet of Things (IoT)?
- What are the risks of using IoT devices?
- What are the consequences of cyber attacks?
- How do cyber attacks affect individuals and organizations?
- What is the CIA Triad, and why is it important?

Scope and Sequence

- Course overview
- What is cybersecurity?
- Impact of cybersecurity
- Internet of Things
- Newsworthy cyber attacks
- CIA Triad

Assured Assessment

Formative Assessment:

- Students will experience and respond to simulated cyber attacks: password cracking, ransomware, and phishing e-mails.
- Students will read and discuss case studies from CYBER.ORG.

Summative Assessment:

- Students will take a common end-of-unit assessment scored via a common scoring guide.

Resources

Core

- CodeHS. *CodeHS: Fundamentals of Cybersecurity*. <https://codehs.com/course/6560>. Accessed October 9, 2020. Web.

Supplemental

- CYBER.ORG. *Cyber.org: Cybersecurity*. <https://cyber.org/cybersecurity>. Accessed October 9, 2020. Web.

Time Allotment

- Approximately 12 school days

UNIT 2

Digital Citizenship and Cyber Hygiene

Unit Goals

At the completion of this unit, students will:

CSTA.3A-AP-20	Evaluate licenses that limit or restrict use of computational artifacts when using resources such as libraries.
CSTA.3A-DA-10	Evaluate the tradeoffs in how data elements are organized and where data is stored.
CSTA.3A-IC-24	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
CSTA.3A-IC-25	Test and refine computational artifacts to reduce bias and equity deficits.
CSTA.3A-IC-28	Explain the beneficial and harmful effects that intellectual property laws can have on innovation.
CSTA.3A-IC-29	Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users.
CSTA.3A-IC-30	Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.
CSTA.3A-NI-05	Give examples to illustrate how sensitive data can be affected by malware and other attacks.
CSTA.3A-NI-06	Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.
CSTA.3A-NI-08	Explain tradeoffs when selecting and implementing cybersecurity recommendations.
CSTA.3B-AP-18	Explain security issues that might lead to compromised computer programs.
CSTA.3B-IC-25	Evaluate computational artifacts to maximize their beneficial effects and minimize harmful effects on society.
CSTA.3B-IC-26	Evaluate the impact of equity, access, and influence on the distribution of computing resources in a global society.
CSTA.3B-IC-27	Predict how computational innovations that have revolutionized aspects of our culture might evolve.

CSTA.3B-IC-28	Debate laws and regulations that impact the development and use of software.
CSTA.3B-NI-04	Compare ways software developers protect devices and information from unauthorized access.
ISTE Empowered Learner (Standard 1)	Leverage technology to take an active role in choosing, achieving, and demonstrating competency in their learning goals, informed by the learning sciences.
ISTE Digital Citizen (Standard 2)	Recognize the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world, and act and model in ways that are safe, legal, and ethical.
ISTE Computational Thinker (Standard 5)	Develop and employ strategies for understanding and solving problems in ways that leverage the power of technological methods to develop and test solutions.
ISTE Creative Communicator (Standard 6)	Communicate clearly and express themselves creatively for a variety of purposes using the platforms, tools, styles, formats, and digital media appropriate to their goals.
ISTE Global Collaborator (Standard 7)	Use digital tools to broaden their perspectives and enrich their learning by collaborating with others and working effectively in teams locally and globally.

Unit Essential Questions

- What is a digital footprint?
- What are some good rules to follow to protect your digital footprint?
- What are some possible consequences of having a negative digital footprint?
- How is cyberbullying different from in-person bullying?
- What should you do if you are being cyberbullied, or you know someone else who is being cyberbullied?
- What is the difference between data security and data privacy?
- What are a few password strategies to ensure the strength of your password?
- What are you agreeing to when you sign a privacy policy?
- What rules or criteria can be used to evaluate online sources?
- What are the risks if we're not able to evaluate sources effectively?
- What does it mean to be protected by copyright laws?
- What is a "hacker"?
- What is the difference between "white hat" and "black hat" hackers?
- What are the potential consequences of hacking illegally?

Scope and Sequence

- Digital footprint and reputation

- Cyberbullying
- Internet safety
- Privacy and security
- Information literacy
- Creative credit and copyright
- Hacking ethics

Assured Assessment

Formative Assessment:

- Students will respond to simulated experiences: social media clean-up, hacking passwords, and source evaluation.
- Students will read and discuss case studies from CYBER.ORG.

Summative Assessment:

- Students will complete the “Public Service Announcement” project related to digital citizenship and cyber hygiene.
- Students will take a common end-of-unit assessment scored via a common scoring guide.

Resources

Core

- CodeHS. *CodeHS: Fundamentals of Cybersecurity*. <https://codehs.com/course/6560>. Accessed October 9, 2020. Web.

Supplemental

- CYBER.ORG. *Cyber.org: Cybersecurity*. <https://cyber.org/cybersecurity>. Accessed October 9, 2020. Web.

Time Allotment

- Approximately 15 school days

UNIT 3

The ABCs of Cryptography

Unit Goals

At the completion of this unit, students will:

- | | |
|---------------|---|
| CSTE.3A-AP-18 | Create artifacts by using procedures within a program, combinations of data and procedures, or independent but interrelated programs. |
| CSTE.3A-IC-24 | Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices. |
| CSTE.3A-IC-26 | Demonstrate ways a given algorithm applies to problems across disciplines. |
| CSTE.3A-IC-29 | Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users. |
| CSTE.3A-IC-30 | Evaluate the social and economic implications of privacy in the context of safety, law, or ethics. |
| CSTE.3A-NI-05 | Give examples to illustrate how sensitive data can be affected by malware and other attacks. |
| CSTE.3A-NI-06 | Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts. |
| CSTE.3A-NI-07 | Compare various security measures, considering tradeoffs between the usability and security of a computing system. |
| CSTE.3B-AP-10 | Use and adapt classic algorithms to solve computational problems. |
| CSTE.3B-AP-11 | Evaluate algorithms in terms of their efficiency, correctness, and clarity. |
| CSTE.3B-AP-14 | Construct solutions to problems using student-created components, such as procedures, modules and/or objects. |
| CSTE.3B-AP-18 | Explain security issues that might lead to compromised computer programs. |
| CSTE.3B-AP-22 | Modify an existing program to add additional functionality and discuss intended and unintended implications (e.g., breaking other functionality). |
| CSTE.3B-IC-25 | Evaluate computational artifacts to maximize their beneficial effects and minimize harmful effects on society. |

CSTE.3B-IC-27	Predict how computational innovations that have revolutionized aspects of our culture might evolve.
CSTE.3B-NI-04	Compare ways software developers protect devices and information from unauthorized access.
ISTE Empowered Learner (Standard 1)	Leverage technology to take an active role in choosing, achieving, and demonstrating competency in their learning goals, informed by the learning sciences.
ISTE Knowledge Constructor (Standard 3)	Critically curate a variety of resources using digital tools to construct knowledge, produce creative artifacts, and make meaningful learning experiences for themselves and others.
ISTE Computational Thinker (Standard 5)	Develop and employ strategies for understanding and solving problems in ways that leverage the power of technological methods to develop and test solutions.
ISTE Creative Communicator (Standard 6)	Communicate clearly and express themselves creatively for a variety of purposes using the platforms, tools, styles, formats, and digital media appropriate to their goals.

Unit Essential Questions

- How do encryption and decryption work?
- What are the risks of sending unencrypted information?
- What is cryptanalysis?
- What is a Caesar cipher, and how does it work?
- What is a flaw in a substitution method of cyphering such as the Caesar cipher?
- What is the Vigenère cipher, and how does it work?
- What makes the Vigenère cipher a stronger cipher than the Caesar cipher?

Scope and Sequence

- Cryptography, cryptology, cryptanalysis
- History of cryptography
- Basic crypto systems: Caesar cipher
- Basic crypto systems: Cracking cipher
- Basic crypto systems: Vigenère cipher

Assured Assessment

Formative Assessment:

- Students will read and discuss case studies from CYBER.ORG.

Summative Assessment:

- Students will create a modified version of an Enigma Machine, an encryption device used by the German military during World War II.

- Students will take a common end-of-unit assessment scored via a common scoring guide.

Resources

Core

- CodeHS. *CodeHS: Fundamentals of Cybersecurity*. <https://codehs.com/course/6560>. Accessed October 9, 2020. Web.

Supplemental

- CYBER.ORG. *Cyber.org: Cybersecurity*. <https://cyber.org/cybersecurity>. Accessed October 9, 2020. Web.

Time Allotment

- Approximately 20 school days

UNIT 4

System Administration

Unit Goals

At the completion of this unit, students will:

CSTE.3A-CS-02	Compare levels of abstraction and interactions between application software, system software, and hardware layers.
CSTE.3A-DA-10	Evaluate the tradeoffs in how data elements are organized and where data is stored.
CSTE.3A-IC-24	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
CSTE.3A-IC-26	Demonstrate ways a given algorithm applies to problems across disciplines.
CSTE.3A-IC-29	Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users.
CSTE.3A-IC-30	Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.
CSTE.3A-NI-06	Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.
CSTE.3A-NI-07	Compare various security measures, considering tradeoffs between the usability and security of a computing system.
CSTE.3B-AP-18	Explain security issues that might lead to compromised computer programs.
CSTE.3B-CS-01	Categorize the roles of operating system software.
CSTE.3B-IC-25	Evaluate computational artifacts to maximize their beneficial effects and minimize harmful effects on society.
CSTE.3B-NI-04	Compare ways software developers protect devices and information from unauthorized access.
ISTE Empowered Learner (Standard 1)	Leverage technology to take an active role in choosing, achieving, and demonstrating competency in their learning goals, informed by the learning sciences.
ISTE Digital Citizen (Standard 2)	Recognize the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world, and act and model in ways that are safe, legal, and ethical.

ISTE Knowledge Constructor (Standard 3)	Critically curate a variety of resources using digital tools to construct knowledge, produce creative artifacts, and make meaningful learning experiences for themselves and others.
ISTE Creative Communicator (Standard 6)	Communicate clearly and express themselves creatively for a variety of purposes using the platforms, tools, styles, formats, and digital media appropriate to their goals.

Unit Essential Questions

- What things is a computer's operating system in charge of?
- What are the main types of operating systems?
- What do all operating systems have in common, and what are their differentiating factors?
- What are the main features of all file management systems?

Scope and Sequence

- Operating systems
- Comparing operating systems
- Application security
- Browser configuration
- System administration

Assured Assessment

Formative Assessment:

- Students will respond to simulated experiences: detecting an OS, Windows installation, Windows and Mac desktops, Windows update, and Popup Blocker.
- Students will read and discuss case studies from CYBER.ORG.

Summative Assessment:

- Students will take a common end-of-unit assessment scored via a common scoring guide.

Resources

Core

- CodeHS. *CodeHS: Fundamentals of Cybersecurity*. <https://codehs.com/course/6560>. Accessed October 9, 2020. Web.

Supplemental

- CYBER.ORG. *Cyber.org: Cybersecurity*. <https://cyber.org/cybersecurity>. Accessed October 9, 2020. Web.

Time Allotment

- Approximately 10 school days

UNIT 5 Software Security

Unit Goals

At the completion of this unit, students will:

CSTE.3A-DA-10	Evaluate the tradeoffs in how data elements are organized and where data is stored.
CSTE.3A-IC-24	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
CSTE.3A-IC-29	Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users.
CSTE.3A-IC-30	Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.
CSTE.3A-NI-05	Give examples to illustrate how sensitive data can be affected by malware and other attacks.
CSTE.3A-NI-06	Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.
CSTE.3A-NI-07	Compare various security measures, considering tradeoffs between the usability and security of a computing system.
CSTE.3A-NI-08	Explain tradeoffs when selecting and implementing cybersecurity recommendations.
CSTE.3B-AP-18	Explain security issues that might lead to compromised computer programs.
CSTE.3B-NI-04	Compare ways software developers protect devices and information from unauthorized access.
ISTE Empowered Learner (Standard 1)	Leverage technology to take an active role in choosing, achieving, and demonstrating competency in their learning goals, informed by the learning sciences.
ISTE Digital Citizen (Standard 2)	Recognize the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world, and act and model in ways that are safe, legal, and ethical.
ISTE Knowledge Constructor (Standard 3)	Critically curate a variety of resources using digital tools to construct knowledge, produce creative artifacts, and make meaningful learning experiences for themselves and others.

ISTE Computational Thinker (Standard 5)	Develop and employ strategies for understanding and solving problems in ways that leverage the power of technological methods to develop and test solutions.
ISTE Creative Communicator (Standard 6)	Communicate clearly and express themselves creatively for a variety of purposes using the platforms, tools, styles, formats, and digital media appropriate to their goals.

Unit Essential Questions

- Why is it important to regularly check for updates on your software?
- Is antivirus software a worthwhile investment?
- How does browser security connect to your digital footprint?
- In what ways can applications be secured?
- What kinds of code are used to build websites?
- How does having access to a website’s source code affect the privacy and security of the website?
- What is OWASP, and in what ways does it influence the field of cybersecurity?
- What important things can be observed in the developer tools of a web browser, and how do these tools help cyber experts?
- What is a database, and how are databases designed?
- What is SQL?
- How might a user interact with an SQL database just by using the associated website?
- How is SQL injection (SQLi) used to gain access to a database?
- What makes blind SQLi different from error-based or union-based SQLi?

Scope and Sequence

- Inside web apps
- Browser developer tools
- Databases
- SQL
- Common security problems
- SQL injection (SQLi)
- Types of SQLi and prevention

Assured Assessment

Formative Assessment:

- Students will respond to simulated experiences: recreating a webpage, console secrets, local storage, and SQL tables.
- Students will read and discuss case studies from CYBER.ORG.

Summative Assessment:

- Students will complete the “Security Assessment” project by using a simulated website to employ SQLi hacking techniques.

- Students will take a common end-of-unit assessment scored via a common scoring guide.

Resources

Core

- CodeHS. *CodeHS: Fundamentals of Cybersecurity*. <https://codehs.com/course/6560>. Accessed October 9, 2020. Web.

Supplemental

- CYBER.ORG. *Cyber.org: Cybersecurity*. <https://cyber.org/cybersecurity>. Accessed October 9, 2020. Web.
- Hunt, Troy. *Supercar Showdown: SQL Injection Testing*. <https://hack-yourself-first.com/>. Accessed October 9, 2020. Web.

Time Allotment

- Approximately 24 school days

COURSE CREDIT

One-half credit in computer science / STEM
One class period daily for a half year

PREREQUISITES

None

SUPPLEMENTARY RESOURCES

- Laptop or desktop with an Internet connection and web browser (preferably Google Chrome)

CURRENT REFERENCE

- Cyber Center for Education & Innovation. *High School Cybersecurity Curriculum Guidelines*. <https://cryptologicfoundation.org>. Accessed October 9, 2020. Web.

ASSURED STUDENT PERFORMANCE RUBRICS

- Trumbull High School School-Wide Writing Rubric (attached)
- Trumbull High School School-Wide Problem-Solving Rubric (attached)
- Trumbull High School School-Wide Independent Learning and Thinking Rubric (attached)

Trumbull High School School-Wide Writing Rubric

Category/ Weight	Exemplary 4 Student work:	Goal 3 Student work:	Working Toward Goal 2 Student work:	Needs Support 1-0 Student work:
Purpose X_____	<ul style="list-style-type: none"> Establishes and maintains a clear purpose Demonstrates an insightful understanding of audience and task 	<ul style="list-style-type: none"> Establishes and maintains a purpose Demonstrates an accurate awareness of audience and task 	<ul style="list-style-type: none"> Establishes a purpose Demonstrates an awareness of audience and task 	<ul style="list-style-type: none"> Does not establish a clear purpose Demonstrates limited/no awareness of audience and task
Organization X_____	<ul style="list-style-type: none"> Reflects sophisticated organization throughout Demonstrates logical progression of ideas Maintains a clear focus Utilizes effective transitions 	<ul style="list-style-type: none"> Reflects organization throughout Demonstrates logical progression of ideas Maintains a focus Utilizes transitions 	<ul style="list-style-type: none"> Reflects some organization throughout Demonstrates logical progression of ideas at times Maintains a vague focus May utilize some ineffective transitions 	<ul style="list-style-type: none"> Reflects little/no organization Lacks logical progression of ideas Maintains little/no focus Utilizes ineffective or no transitions
Content X_____	<ul style="list-style-type: none"> Is accurate, explicit, and vivid Exhibits ideas that are highly developed and enhanced by specific details and examples 	<ul style="list-style-type: none"> Is accurate and relevant Exhibits ideas that are developed and supported by details and examples 	<ul style="list-style-type: none"> May contain some inaccuracies Exhibits ideas that are partially supported by details and examples 	<ul style="list-style-type: none"> Is inaccurate and unclear Exhibits limited/no ideas supported by specific details and examples
Use of Language X_____	<ul style="list-style-type: none"> Demonstrates excellent use of language Demonstrates a highly effective use of standard writing that enhances communication Contains few or no errors. Errors do not detract from meaning 	<ul style="list-style-type: none"> Demonstrates competent use of language Demonstrates effective use of standard writing conventions Contains few errors. Most errors do not detract from meaning 	<ul style="list-style-type: none"> Demonstrates use of language Demonstrates use of standard writing conventions Contains errors that detract from meaning 	<ul style="list-style-type: none"> Demonstrates limited competency in use of language Demonstrates limited use of standard writing conventions Contains errors that make it difficult to determine meaning

Trumbull High School School-Wide Problem-Solving Rubric

Category/ Weight	Exemplary 4	Goal 3	Working Toward Goal 2	Needs Support 1-0
Understanding X_____	<ul style="list-style-type: none"> • Student demonstrates clear understanding of the problem and the complexities of the task 	<ul style="list-style-type: none"> • Student demonstrates sufficient understanding of the problem and most of the complexities of the task 	<ul style="list-style-type: none"> • Student demonstrates some understanding of the problem but requires assistance to complete the task 	<ul style="list-style-type: none"> • Student demonstrates limited or no understanding of the fundamental problem after assistance with the task
Research X_____	<ul style="list-style-type: none"> • Student gathers compelling information from multiple sources including digital, print, and interpersonal 	<ul style="list-style-type: none"> • Student gathers sufficient information from multiple sources including digital, print, and interpersonal 	<ul style="list-style-type: none"> • Student gathers some information from few sources including digital, print, and interpersonal 	<ul style="list-style-type: none"> • Student gathers limited or no information
Reasoning and Strategies X_____	<ul style="list-style-type: none"> • Student demonstrates strong critical thinking skills to develop a comprehensive plan integrating multiple strategies 	<ul style="list-style-type: none"> • Student demonstrates sufficient critical thinking skills to develop a cohesive plan integrating strategies 	<ul style="list-style-type: none"> • Student demonstrates some critical thinking skills to develop a plan integrating some strategies 	<ul style="list-style-type: none"> • Student demonstrates limited or no critical thinking skills and no plan
Final Product and/or Presentation X_____	<ul style="list-style-type: none"> • Solution shows deep understanding of the problem and its components • Solution shows extensive use of 21st-century technology skills 	<ul style="list-style-type: none"> • Solution shows sufficient understanding of the problem and its components • Solution shows sufficient use of 21st-century technology skills 	<ul style="list-style-type: none"> • Solution shows some understanding of the problem and its components • Solution shows some use of 21st-century technology skills 	<ul style="list-style-type: none"> • Solution shows limited or no understanding of the problem and its components • Solution shows limited or no use of 21st-century technology skills

Trumbull High School School-Wide Independent Learning and Thinking Rubric

Category/ Weight	Exemplary 4	Goal 3	Working Toward Goal 2	Needs Support 1-0
Proposal X_____	<ul style="list-style-type: none"> • Student demonstrates a strong sense of initiative by generating compelling questions, creating uniquely original projects/work 	<ul style="list-style-type: none"> • Student demonstrates initiative by generating appropriate questions, creating original projects/work 	<ul style="list-style-type: none"> • Student demonstrates some initiative by generating questions, creating appropriate projects/work 	<ul style="list-style-type: none"> • Student demonstrates limited or no initiative by generating few questions and creating projects/work
Independent Research & Development X_____	<ul style="list-style-type: none"> • Student is analytical, insightful, and works independently to reach a solution 	<ul style="list-style-type: none"> • Student is analytical, and works productively to reach a solution 	<ul style="list-style-type: none"> • Student reaches a solution with direction 	<ul style="list-style-type: none"> • Student is unable to reach a solution without consistent assistance
Presentation of Final Product X_____	<ul style="list-style-type: none"> • Presentation shows compelling evidence of an independent learner and thinker • Solution shows deep understanding of the problem and its components • Solution shows extensive and appropriate application of 21st-century skills 	<ul style="list-style-type: none"> • Presentation shows clear evidence of an independent learner and thinker • Solution shows adequate understanding of the problem and its components • Solution shows adequate application of 21st-century skills 	<ul style="list-style-type: none"> • Presentation shows some evidence of an independent learner and thinker • Solution shows some understanding of the problem and its components • Solution shows some application of 21st-century skills 	<ul style="list-style-type: none"> • Presentation shows limited or no evidence of an independent learner and thinker • Solution shows limited or no understanding of the problem and its components • Solution shows limited or no application of 21st-century skills