UTeach Computer Science

Foundations of Cybersecurity Syllabus and Planning Guide

(2025–2026)

Table of Contents

Curriculum Description

Developers

UTeach Foundations of Cybersecurity has been developed by the UTeach Institute (UTeach Computer Science) in collaboration with Teach Cyber.

Curriculum Overview

UTeach Foundations of Cybersecurity is yearlong high school curriculum designed to introduce students to foundational concepts, principles, and tools of cybersecurity. Based on the High School Cybersecurity Curriculum Guidelines, the course is structured around eight Big Ideas: ethics, establishing trust, ubiquitous connectivity, data security, system security, adversarial thinking, risk, and implications. By the end of the course, students will understand the broad impact of cybersecurity, engage in ethical reflection, and grasp essential principles for security requirements and mechanisms. The curriculum covers historical events and their cybersecurity impacts, relevant laws and policies governing data, and economic trade-offs in decision-making. Additionally, students analyze threats, vulnerabilities, and attacks, evaluate tools for cyber-physical systems, and practice encryption techniques for securing data across networks.

The lessons and materials used throughout this curriculum incorporate project-based learning (PBL), a pedagogical approach that actively engages students in the educational process, improves retention, and develops problem-solving, critical thinking, and group communication skills.

Curriculum Standards

The UTeach Cybersecurity curriculum is based on the High School Cybersecurity Curriculum Guidelines (HSCCG) designed by a team of educators and cybersecurity experts in partnership with the National Cryptologic Foundation.

Textbook

UTeach Foundations of Cybersecurity has an interactive online textbook available for students and teachers. The textbook, assessments, projects, and built-in hands-on lab environment are hosted on the cloud-based Codio platform, which can be integrated with most learning management systems and is FERPA compliant.

Curriculum Standards — Big Ideas

The Big Ideas serve as the foundation of the course. They are overarching concepts or themes that are incorporated throughout the curriculum units and connected to the topics and activities within each unit.

Big Ideas
Big Idea 1: Ethics Cybersecurity has broad implications. Ethical reflection and judgement are required to make decisions about the trade-offs between the benefits and harms of security. Whether a system's design or the use of the system constitutes a benefit or harm depends on the ethical duties and interests of both the designer and user. Designers and users can have differing interests when it comes to deciding what is worth protecting and which cybersecurity resource investments are justified to achieve that protection. All cybersecurity exists within a context of social, organizational, and personal values; these values undergird beliefs about right and wrong. In this course, students have the opportunity to evaluate the ethical implications among all stakeholders.
Big Idea 2: Establishing Trust Knowledge of the fundamental cybersecurity principles is necessary to determine security requirements and mechanisms, as well as to identify vulnerabilities and threats. The principles derive from the ideas of simplicity and restriction. Understanding the related assumptions is also important in considering the strength of a system's security. This course emphasizes the cybersecurity principles, the CIA triad, and how to question assumptions as the basis for establishing trust in cybersecurity. Students in this course evaluate the principles and apply them to systems creating trust within organizations.
Big Idea 3: Ubiquitous Connectivity Networks are used daily by most people in the world. There is no single network, but rather a collection of different network technologies that together form a network of networks called the internet. Conceptually, the internet is divided into layers with protocols and standards that define each layer. This enables a large variety of devices to be connected. This vast number of devices connected over a large number of network technologies is referred to as ubiquitous connectivity. In other words, everything is connected all the time. The more dependent we become on ubiquitous connectivity, the greater the implications if the network becomes compromised. This makes it necessary for students to understand and effectively use the methods and tools for keeping our network secure.
Big Idea 4: Data Security Data is all around us. Keeping it secure and private is essential for individuals, groups, and governments. The concept of what data is and how it can be collected, has changed monumentally with the advent of the internet. As collection has become easier with improved computing power, data can be generated, stored, transmitted, and manipulated at a much greater pace and at an almost immeasurable amount. Keeping those with malicious intent away from data assets and preserving privacy is a major tenet in cybersecurity. Because data can tell us so much about our world, it is important to keep the confidentiality, integrity, and availability of the data intact. Students in this course study relevant laws and policies governing data, evaluate the tools used to connect cyber-physical systems, and practice using the encryption techniques needed to secure data across networks.
Big Idea 5: System Security This Big Idea addresses security flaws and vulnerabilities in hardware and software. Hardware and software work together to achieve an objective. Adversaries may exploit weaknesses in the system to disrupt the systems confidentiality, integrity, or availability. System security includes definitions and explanations of security flaws and vulnerabilities, helps explain why hardware and software have vulnerabilities, introduces students to some specific vulnerabilities, and addresses the consequences of less secure hardware and software.

Big Idea 6: Adversarial Thinking

A primary objective of cybersecurity is to identify critical assets, design and implement systems to protect the assets, identify ways to detect when the protections fail, respond to the failures, and recover to a working state. To accomplish this, one must think about what can go wrong. This Big Idea extends the concept of adversary from a clever cybercriminal who will adapt to a natural disaster to anything that might disrupt the system. Students learn to consider how an adversary might attempt to find key assets, compromise those assets, and avoid detection. The most challenging adversaries adapt to defenses and adjust their attacks based on the system's responses. Students in this course challenge assumptions and practice thinking about opposing forces in terms of intentions (when opposing forces are human adversaries), capabilities, and actions. Students will employ these techniques to analyze threats, vulnerabilities, and attacks.

Big Idea 7: Risk

Risk, as defined in regard to cybersecurity, is a relationship between the chance that harm will occur and the damage that will be done if harm does occur. This Big Idea engages students with the risk assessment process as a methodology for grasping cybersecurity risk. This Big Idea also addresses the inherently uncertain and complex nature of cybersecurity risk due to complexity of systems of systems, the presence of adversaries, the logical malleability of computing, and the dynamic and distributed nature of computing.

Big Idea 8: Implications

Advances and decisions at a local level in computing, connectivity, and big data are driving a global, interconnected phenomenon and have significant cybersecurity implications. Societies face cybersecurity issues regarding infrastructure, law enforcement, and social and cultural issues. Economic concerns and risk management trade-offs drive decisions that significantly impact cybersecurity. Cybersecurity is shaped by critical historical ideas and events. History proves that adversaries can launch attacks from anywhere transcending global borders, requiring adaptation. This course differentiates between the severity of cyber threats and stresses the fact that threats evolve along with the technology which enables the adversary to evolve with their attacks. Students in this course describe historical events and their cybersecurity implications, examining the evolution of the threat environment at the local and global level.

Unit 1: What Is Cybersecurity?

Unit 1 begins with an exploration of early hacks and then transitions into a discussion of cyberspace, engaging students in the notion of cyberspace as a complex system. Next, students delve into what it means for the internet to be an open architecture and explore how this is both a virtue and a vice, using cloud storage to illustrate this complexity. The unit brings into sharp focus why cybersecurity is needed and who it affects. Next, the unit introduces the foundational model of the CIA triad and explores its importance. Then, the unit introduces how cybersecurity impacts the quality of people's lives and the rise of the Internet of Things (IoT). The unit ends by engaging students in the ethical obligations involved in cybersecurity and how complex systems are not easy to predict or model.

Unit 1 Topics and Learning Outcomes

This module includes the following topics:

- Early hacks
- Internet architecture
- Complexity
- CIA triad
- Privacy and security
- Cloud computing

Over the course of this unit, students learn to:

- Explore cybersecurity issues related to the internet, cloud computing, and the Internet of Things (IoT).
- Apply the concepts of confidentiality, integrity, and availability when securing information.
- Explain the role of a professional code of ethics in cybersecurity.

Unit 1 Schedule (12 Days)

Assignment #	Topic	# of Class Days
1.1	Internet Security	1
1.2	What Is Cyberspace?	2
1.3	What Is Cybersecurity?	1
1.4	Security in the Cloud	1
1.5	CIA Triad	2
1.6	Digital Trends	1
1.7	Internet of Things	1
1.8	Ethics and Cybersecurity	1
1.9	Unit 1 Vocabulary Quiz	1
1.10	Unit 1 Test	1

Back to Table of Contents

Unit 2: Risk, Adversity, and Trust

This unit picks up with the question of the value of information. Students identify what information assets need to be protected and how they need to be protected. Then, the unit introduces the idea of threat sources and students identify the vulnerabilities in conjunction with the impacts (i.e., disclosure, deception, disruption, destruction, and/or usurpation). The focus shifts to countering threats, vulnerabilities, and attacks with security services or controls. Security controls are introduced in two ways. First, a few controls are introduced, e.g., authentication, cryptography, access control, firewalls, and intrusion detection. Here, students are engaged in learning about the control and its role in prevention, detection, and response. Then, students consider these same controls but this time through the lens of establishing trust. In order to do that, the unit addresses the question of "What is trust?" It is pointed out that while trust cannot be quantified precisely, it is essential in everyday life and cyberspace. After exploring attacks, vulnerabilities, threats, control measures, and trust, students will have developed an understanding of cyber risk.

Unit 2 Topics and Learning Outcomes

This unit includes the following topics:

- Data classification
- Vulnerabilities, threats, attacks
- APTs
- Social engineering
- Risk
- Adversarial thinking
- Principle of least privilege
- CIA triad
- Identification, authentication, authorization

Hands-on lab:

- Social engineering

Over the course of this unit and the unit project, students learn to:

- Explain how information assets are classified based upon level of sensitivity.
- Prioritize information assets according to their need to be kept confidential, unchanged, and/or available, and their criticality/sensitivity.
- Differentiate between threats, vulnerabilities, and attacks.
- Identify the impact of software vulnerabilities on confidentiality, integrity, and availability.

- Describe adversaries in terms of their resources, capabilities, and motivations.
- Identify threats that do not have malicious intent.
- Distinguish between identification, authentication, and authorization.
- Describe how cryptographic hashing functions can ensure confidentiality and integrity.
- Understand how protection involves prevention, detection, response, and recovery.
- Describe how complexity can affect the vulnerability of a system.
- Describe how the human factor can negate trust in cybersecurity systems and procedures.
- Explain why cybersecurity is a hard problem.
- Describe the risk assessment process and purpose.

Unit 2 Schedule (25 Days)

Assignment #	Topic	# of Class Days
2.1.1	Unmasking Deception: Exploring Social Engineering Project Launch	1
2.2	Information Assets	1
2.3	Attacks, Vulnerabilities, & Threats	1
2.4	Software Vulnerabilities	1
2.5	Advanced Persistent Threats	1
2.6	Insider Attacks	1
2.7	Revisit Concept Map	1
2.8	Social Engineering	1
2.9	Social Engineering Lab	1
2.1.2	Unmasking Deception: Exploring Social Engineering Project Workday 2	1
2.10	Security Controls	1
2.11	Password Policies	2
2.12	Security Protection	1
2.1.3	Unmasking Deception: Exploring Social Engineering Project Workday 3	1
2.13	The NotPetya Case Study	2
2.14	What Is Trust?	1
2.15	Why Is Cybersecurity a Hard Problem	1

	to Solve?	
2.16	Risk	2
2.1.4	Unmasking Deception: Exploring Social Engineering Project Workday 4	1
2.17	Unit 2 Vocabulary Quiz	1
2.18	Unit 2 Test	1
	Unmasking Deception: Exploring Social Engineering Project Presentations	1

Unit 3: The Elements of Cyberspace

In this unit, students explore how hardware and software work together to achieve an overall objective. Students learn how devices communicate across the internet and explore open source versus proprietary protocols. After these basic building blocks of cyberspace are defined, the unit introduces basic concepts of networks and networking. This unit includes introductory labs to introduce students to basic Linux commands and networking concepts. Finally, students examine the growth in society's use of and reliance on computers and networks, ranging from health, commerce, and national defense to entertainment and leisure.

Unit 3 Topics and Learning Outcomes

This unit includes the following topics:

- Overview of hardware and software
- Introduction to operating systems
- Understanding flaws and failures
- Introduction to embedded systems
- Introduction to networks
- Components of a network
- The internet
- Network protocols
- Ubiquitous connectivity

Hands-on Lab:

- Introduction to Linux/Ubuntu
- Linux Networking Commands
- Introduction to Wireshark

Over the course of this unit and the unit project, students learn to:

- Convey that computer hardware refers to the physical parts of a computer and related devices.
- Define software as a set of instructions that execute on hardware and are designed to achieve some objective on a physical device objective.
- Identify how hardware and software work together to achieve an overall objective.
- Explore the operating system Linux.
- Explain that an embedded system is one that has embedded software that is built directly into the physical device.

- Explain how devices connect to a network.
- Understand the types of networks.
- Describe how the internet works.
- Compare networking conceptual models.
- Understand layered network models including Open Systems Interconnect (OSI) and TCP/IP models.
- Identify networking protocols.
- Examine packets with Wireshark.
- Examine the growth in society’s use and reliance on computers and networks in healthcare, commerce, national defense, entertainment, and leisure.

Unit 3 Schedule (22 Days)

Assignment #	Topic	# of Class Days
3.1.1	Designing Tomorrow's Secure Network Today Project Launch	1
3.2	Hardware and Software	1
3.3	Operating Systems	1
3.4	Introduction to Linux/Ubuntu OS	1
3.5	Flaws and Failures	1
3.6	Embedded Systems	1
3.7	Introduction to Networks	1
3.8	Components of a Network	1
3.1.2	Designing Tomorrow’s Secure Network Today Project Workday 2	1
3.9	The Internet	1
3.10	Network Protocols	2
3.11	Linux Networking Commands	1
3.12	Wireshark Lab	1
3.1.3	Designing Tomorrow’s Secure Network Today Project Workday 3	1
3.13	Proprietary vs. Open-Source Protocols	1
3.14	Networks Abound	2

3.1.4	Designing Tomorrow's Secure Network Today Project Workday 4	1
3.15	Unit 3 Vocabulary Quiz	1
3.16	Unit 3 Test	1
	Designing Tomorrow's Secure Network Today Project Presentations	1

Unit 4: Data, Software, Hardware, and Network Security

Unit 4 focuses on concepts of data in cyberspace. Students delve into the technical aspects of cybersecurity including data states and data controls, as well as vulnerabilities and exploits in software, hardware, networks, cyber-physical systems, and human use of data.

Unit 4 Topics and Learning Outcomes

This unit includes the following topics:

- Data security concerns
- Data principles
- Data states
- Common software vulnerabilities
- Hardware vulnerabilities
- Common network vulnerabilities
- Vulnerabilities in cyber-physical systems
- Human vulnerabilities in cybersecurity

Hands-on labs:

- Vulnerability scanning
- SQL injection
- Buffer overflow
- Email tracking

Over the course of this unit and the unit project, students learn to:

- Analyze existing data security concerns and assess methods.
- Use Open Source Intelligence (OSINT) tools from publicly available resources.
- Distinguish between the use of data to help individuals and the misuse of data to harm individuals.
- Analyze existing data security concerns and assess methods to overcome those concerns.
- Describe how the principles of confidentiality, integrity, and availability are applied to protect data.
- Analyze existing data security concerns and assess methods to overcome those concerns by focusing on data at rest, processing, and in transit.
- Describe the requirements for protecting data at rest (storage), in motion (transit), and in use (processing).
- Describe the purpose of common cybersecurity laws at the federal and state level (e.g., HIPAA, CFAA, CCPA, GDPR).

- Describe the purpose of common cybersecurity policies (e.g., Acceptable Use, Data Encryption, Minimum Password Requirements Policies).
- Describe the rules and methods for the physical protection of data.
- Describe software vulnerabilities.
- Explain how an adversary can exploit a vulnerability.
- Describe the process of discovering vulnerabilities and determining the severity of a vulnerability.
- Identify hardware-related vulnerabilities.
- Describe the requirements for tamper-resistance and fail-safety in hardware.
- Identify hardware security issues related to an adversary physically gaining access to a device.
- Identify network vulnerabilities on the OSI layers of internetworking.
- Explain how an adversary can exploit a security-related vulnerability on one or multiple OSI layers.
- Identify some common cyber-physical system vulnerabilities.
- Describe the consequences of unintentional gaps or malicious attacks on cyber-physical systems that could have a severe impact on human lives and the environment.
- Describe how social behaviors and human factors impact the cybersecurity of a system design.
- Explain how social engineering works.

Unit 4 Schedule (27 Days)

Assignment #	Topic	# of Class Days
4.1.1	A Cybersecurity Plan for a Small Business Project Launch	1
4.2	What is Data?	2
4.3	Data Principles	1
4.4	The Three States of Data	1
4.5	Data Controls	1
4.6	Software Vulnerabilities Revisited	2
4.1.2	A Cybersecurity Plan for a Small Business Project Workday 2	1
4.7	Vulnerability Scanning Lab	1
4.8	SQL Injection Lab	1
4.9	Buffer Overflow Lab	1
4.10	Hardware Vulnerabilities	2

4.11	Network Vulnerabilities	2
4.1.3	A Cybersecurity Plan for a Small Business Project Workday 3	1
4.12	Advanced Port Scanning Lab	1
4.12	Email Tracking Lab	1
4.13	Cyber-Physical Systems	2
4.14	Securing IoT Devices	1
4.15	The Human Factor	2
4.1.4	A Cybersecurity Plan for a Small Business Project Workday 4	1
4.16	Unit 4 Vocabulary Quiz	1
4.17	Unit 4 Test	1
	A Cybersecurity Plan for a Small Business Project Workday 5	1

Unit 5: Countermeasures Against Cyberattacks

Unit 5 further develops understanding of data security controls, including authentication, identification, authorization, and access controls. These tools are examined from the perspective of their function when preventing disclosure, deception, disruption, destruction, or usurpation. This unit also introduces important terms and concepts in cryptography and covers how symmetric and asymmetric cryptosystems work. The unit ends with a discussion of policy controls and students will analyze laws to discern what type of data are being protected, for whom, and under what circumstances. The unit also covers physical policies as part of a comprehensive defense-in-depth protection strategy.

Unit 5 Topics and Learning Outcomes

This unit includes the following topics:

- Role-based access control
- Mandatory access control
- Discretionary access control
- Modern cryptographic algorithms
- Organizational policy controls
- Hash functions
- Digital signatures
- Nonrepudiation
- Physical security
- Network security
- Acceptable use
- Defense-in-depth
- Secure protocols

Hands-on labs:

- Access control
- Public key encryption
- Password auditing
- Keylogging
- OS hardening

Over the course of this unit and the unit project, students learn to:

- Describe and articulate differences between authentication, authorization, identification, and access control.
- Identify various factors of authentication and identify pros and cons.
- Implement role-based access control on a Linux system.
- Describe how mandatory access control and discretionary access control each specify a process for securing resources.
- Explain that failure to protect data can be due to faulty authentication, faculty authorization, and/or faulty access control.
- Explain how cryptography is used in data security.
- Use symmetric ciphers to engage in the process of encryption and decryption.
- Explain the process of moving between ciphertext and plaintext.
- Describe the difference between transposition ciphers and substitution ciphers.
- Explain the challenges to symmetric cryptosystems.
- Explain how asymmetric (public key) encryption works.
- Recognize the need for public key cryptography.
- Explain the use of key exchange/agreement protocols in cryptography.
- Identify commonly used algorithms for asymmetric encryption.
- Explain the use of and basic requirements for hash functions in securing information.
- Identify commonly used algorithms for hashing.
- Explain the role of digital certificates and certificate authorities in secure communications.
- Describe the security controls needed for implementation of a policy.
- Identify violations of a security policy.
- Identify physical controls that are used to secure data.
- Describe how physical access controls are implemented as part of defense-in-depth physical security policy.
- Distinguish between the purposes of network security devices and technologies for layered network protection.
- Describe the impact of DevSecOps on software development.
- Perform operating system (OS) hardening and implement common controls in software applications.
- Recognize how controls come together to form a complex system with various weak points.
- Explain that security requires a system to be responsive to change and is only as strong as the weakest link.

Unit 5 Schedule (35 Days)

Assignment #	Topic	# of Class Days
5.1.1	Designing the Future of Secure Communication Project Launch	1
5.2	Access Controls	2
5.3	Access Controls Lab	1
5.4	Faulty Access Controls	1
5.5	Symmetric Cryptography	2
5.6	Substitution Ciphers	1
5.7	Modern Symmetric Ciphers	1
5.1.2	Designing the Future of Secure Communication Project Workday 2	1
5.8	Asymmetric Cryptography	1
5.9	RSA Encryption	1
5.10	Public Key Encryption	1
5.11	Hash Functions	1
5.1.3	Designing the Future of Secure Communication Project Workday 3	1
5.12	Public Key Encryption Lab	1
5.13	Password Auditing Lab	1
5.14	Digital Signatures	1
5.15	Policy Controls	1
5.16	Keylogger Lab	1
5.17	Physical Controls	2
5.18	Network Security Controls	1
5.19	Firewalls	1
5.20	Intrusion Detection Systems	1
5.21	Secure Design Principles	1
5.22	Software Controls	1
5.23	Hardware Controls	1
5.24	OS Hardening Lab	1

5.25	Impact of Failure	2
5.1.4	Designing the Future of Secure Communication Project Workday 4	1
5.26	Unit 5 Vocabulary Quiz	1
5.27	Unit 5 Test	1
	Designing the Future of Secure Communication Project Presentations	1

Pedagogical Approaches

The UTeach Foundations of Cybersecurity curriculum uses project-based learning (PBL) and other research-backed methods to engage all students. PBL fosters critical thinking and problem-solving skills through real-world challenges. The curriculum emphasizes cultural context, teacher facilitation, and mediated instruction. Teachers unfamiliar with PBL can learn more at the Buck Institute for Education website.

Educators are encouraged to use various PBL strategies, including narrative anchoring videos, unit projects, clear rubrics, regular benchmarks, scaffolding activities, final products, and reflection. These tools enhance engagement and help increase comprehension and retention, problem-solving abilities, critical thinking, and group communication skills.

Instructional Sequencing

The yearlong curriculum consists of five instructional units that have been carefully structured to guide students through an introduction to core cybersecurity skills using practical lessons focused on topics like risk assessment, data security, cyberattacks, and more. Students connect classroom learning to real-world application with unit projects, easy-to-understand videos, collaborative research activities, and hands-on labs.

Introduction

The first assignment of each instructional unit opens with an anchor video designed to introduce the driving questions, unit project, and key topics for the next few weeks of study. Students are expected to participate in small-group and/or whole-class discussion to identify areas of focus that will direct and drive learning throughout the unit.

Topic Lessons/Activities

Distributed throughout each unit, individual lessons, daily activities, research assignments, and discussions allow students to explore and practice applying relevant skills and concepts in greater detail.

Project Workdays

Each unit project has between four and five dedicated work periods for students to work on their deliverables. Project workdays are spread throughout the unit, strategically placed after relevant topics have been presented.

Assessments

In addition to informal formative assessments throughout each unit, student learning and progress is also assessed at the end of each unit through a formal summative assessment and evaluation of their independent and collaborative efforts on the unit project. Formal end-of-unit assessments are comprised of multiple-choice questions and free response questions.

Unit Projects

The narrative-driven curriculum immerses students in encounters with cunning adversaries who have intercepted the course with their own agenda. These adversaries challenge students to adopt an adversarial mindset, presenting real-world scenarios and dilemmas that test their skills and ethical boundaries. The students' mission is to resist their temptations, use their growing cybersecurity knowledge to counteract their tactics, and understand the importance of maintaining integrity in the face of cyber threats.

The opening module of each unit serves as a formal launch of the unit project—a product-oriented challenge for students to investigate, research, and solve over the course of the unit. The project launch starts with an anchor video that introduces the fundamental problem or challenge to be solved and is intended to spark the students' imaginations and inspire them to find a solution. Projects are designed to be collaborative, with students working together in groups.

Rubrics

Each unit project is accompanied by a clearly defined rubric that specifies the set of expectations for work throughout the unit, including an exhaustive list of assessment criteria for the artifacts that students will produce and detailed descriptors for each performance level that a student might demonstrate. Teachers should provide students with the rubric at the start of the unit as part of the initial discussion immediately following the anchor video. Giving the students the rubric at the time of the project launch is critical for setting clear expectations early in the research and learning process. Over the course of the unit, teachers should regularly refer to the goals and criteria of the rubric to ensure that students remain focused and on track to meet the stated requirements.

Benchmarks

Each unit provides the teacher with several benchmark activities, or subtasks, that feed into the larger unit project. Each of these subtasks contributes directly to the final product that the students create. Teachers can use these benchmarks as intermediate informal assessments to gauge the progress of each student and/or collaborative group in their mastery of the unit goals.

Scaffolding Activities

The bulk of each unit consists of a series of individual topic lessons, activities, discussions, and hands-on applications that allow the teacher to provide instruction, guidance, and support to students and collaborative groups as they design and implement the deliverables for the unit project. These scaffolding activities serve to introduce, explain, and encourage the use of the unit's core concepts and skills by providing students with structured opportunities and incentives to explore the material in greater depth.

Final Products and Student Portfolio

At the culmination of each unit, student groups are expected to present a final product that represents the body of their work and implementation on the unit project. Students demonstrate their mastery of the core content and skills for the unit by exhibiting the authentic and purposeful artifacts and completing a reflection piece. A key component of the project always includes a public presentation of each student's work before their peers as a way of providing motivation for each student and holding them accountable for their own learning.

Reflection

Students are provided time to reflect at the end of project workdays with thoughtful responses to specific questions about the topics covered in the unit project. This provides students an opportunity to reflect on the challenges and successes during the unit project.

Resources and Technical Requirements

UTeach Foundations of Cybersecurity does not require additional materials for implementation besides the license, which may be purchased or provided through a grant.

Websites Accessed Throughout the Curriculum

The websites below will be accessed in this curriculum. Please advise the school IT department about these websites prior to beginning the course. Always test site access from your device as well as students' devices to ensure a smooth lesson.

*.codio.com, *. codio.io, https://uteachcs.github.io/Cyber-CSS/css/styles.css, https://github.com/nebgnahz/awesome-iot-hacks, youtube.com, *.nist.gov, education.cfr.org, theguardian.com, trendmicro.com, forbes.com, nytimes.com. *.mitre.org, *.wikipedia.org, web.archive.org, ncyte.net, lookup.icann.org, cnet.com, krebonsecurity.com, haveibeenpwned.com, howsecureismypassword.com, legacy.cryptool.org, fileformat.info, crackstation.net, medium.com, ipv6-test.com, whatismyipaddress.com, nordvpn.com, iptrackeronline.com, security.org, osintframework.com, md5calc.com, cybernews.com, ocrportal.hhs.gov, itgovernanceusa.com, iptrackeronline.com, talosintelligence.com, sites.google.com/view/secureco, eia.gov, opendns.com, typingdna.com, dcode.fr, simonsingh.net, planetcalc.com, fileformat.info, freerainbowtables.com, justice.gov, nsa.gov, darkreading.com, sciencedirect.com, smartermsp.com. blog.gigamon.com, owasp.org