

Current EduTech Course Offerings

Computational Thinking (8 hours online/asynchronous toward credential)

This course is based on the CYBER.ORG Computational Thinking curriculum which incorporates the four elements of computational thinking (decomposition, pattern recognition, abstraction, and algorithm design) in a project-based approach to learning within core subject areas. Teachers will be provided guidance about how to embed computational thinking vocabulary into everyday learning experiences and upon completion have a developed lesson to incorporate into their classroom. Relevant for grades 3-12.

Outcomes

- Apply the principles of computational thinking, including decomposition, pattern recognition, abstraction, and algorithm design, to analyze and solve real-world problems within core subject areas, effectively demonstrating their understanding through application.
- Create a comprehensive lesson plan that seamlessly integrates computational thinking vocabulary into various learning experiences. Design engaging activities that foster the development of computational thinking skills while aligning with the curriculum goals of their respective subjects.
- Evaluate the effectiveness of a developed lesson plan by analyzing the integration of computational thinking vocabulary, the engagement level of students, and the application of computational thinking skills, using a reflective approach to refine and improve teaching strategies.

Cyber Society (8 hours online/asynchronous toward credential)

Teachers will explore the Cyber Society course within the CYBER.ORG library. Cyber Society has a Media Literacy unit that will be explored in depth that examines how Journalism and Media shape our perspectives. Other topics include Ethics and Communities that explore skills students need to be cyber safe and smart. Understanding how all parts of society are affected by Cyber will be explored. Relevant for grades 9-12.

Outcomes

- Analyze and interpret the various elements of the Media Literacy unit in the Cyber Society curriculum. Demonstrate an understanding of how different forms of media shape perceptions, discern biases, and interpret underlying messages.
- Develop creative ways to contextualize cyber-related concepts across various subjects, fostering a comprehensive understanding of how Cyber impacts diverse aspects of society.
- Integrate the principles of ethics and digital citizenship covered in the Ethics and Communities section of the course into their teaching practices.
- Recall and explain key concepts related to the Cyber Society course within the CYBER.ORG library. Define media literacy, identify its components, and describe how Journalism and Media influence individual and collective perspectives.

Cybersecurity Basics (2023 and prior 8 hours online/asynchronous toward credential; 2024 to present offered as in-person workshop 2-8 hours toward credential)

CYBER.ORG's Cybersecurity Basics introduces students to the foundational concepts of cybersecurity through immersive modules. The course covers Security and Digital Citizenship to provide students with a basic understanding of cybersecurity that affects our everyday life. Teachers will explore this new course to understand how they can incorporate these concepts into their classrooms. Relevant for grades K-8.

Outcomes

- Analyze common cybersecurity threats and propose basic preventive measures to mitigate potential risks in their digital interactions.
- Define and differentiate between foundational cybersecurity concepts, such as encryption, malware, and authentication.
- Demonstrate an understanding of the significance of cybersecurity in daily life by explaining how security breaches can impact personal privacy and digital citizenship.

Cybersecurity Basics – Digital Citizenship (8 hours online/asynchronous toward credential)

Cybersecurity Basics - Digital Citizenship (CYBER.ORG) introduces students to the foundational concepts of cybersecurity through immersive modules. The course covers content from the Digital Citizenship domain from the CYBER.org course and provides students with a basic understanding of cybersecurity that affects our everyday life. Teachers will explore this new course to understand how they can incorporate these concepts into their classrooms. Relevant for grades K-8.

Outcomes

- Analyze common cybersecurity threats and propose basic preventive measures to mitigate potential risks in digital interactions.
- Define and differentiate between foundational cybersecurity concepts, such as threat actors, cyberbullying, personally identifiable information, digital footprints, and digital citizenship ethics.
- Demonstrate an understanding of the significance of cybersecurity in daily life by explaining how security breaches can impact personal privacy and digital citizenship.
- Recall and explain key concepts related to the Cybersecurity Basics course within the CYBER.ORG library relating to the Digital Citizenship domain.

Cybersecurity Basics – Security (8 hours online/asynchronous toward credential)

Cybersecurity Basics - Security (CYBER.ORG) introduces students to the foundational concepts of cybersecurity through immersive modules. The course covers content from the Security domain from the CYBER.org course and provides students with a basic understanding of cybersecurity that affects our everyday life. Teachers will explore this new course to understand how they can incorporate these concepts into their classrooms. Relevant for grades K-8.

Outcomes

- Analyze common cybersecurity threats and propose basic preventive measures to mitigate potential risks in digital interactions.
- Define and differentiate between foundational cybersecurity concepts, such as data security, encryption, malware, and authentication.
- Demonstrate an understanding of the significance of cybersecurity in daily life by explaining how security breaches can impact personal privacy and digital citizenship.
- Recall and explain key concepts related to the Cybersecurity Basics course within the CYBER.ORG library relating to the Security domain.

Cybersecurity with micro:bits (8 hours online/asynchronous toward credential)

Explore cybersecurity skills through coding on the micro:bit. We will take a quick tour of the cybersecurity blocks CYBER.ORG has created for MakeCode then dive into Communicating and Encrypting with Python on the micro:bit. Relevant for grades 4-12.

Outcomes

- Compare and contrast different encryption techniques, considering their implications for data protection and cybersecurity.
- Evaluate the effectiveness and limitations of the MakeCode programming language for implementing encryption and secure communication on the micro:bit.
- Identify and define fundamental cybersecurity concepts and terminologies associated with micro:bit coding, such as encryption, communication security, and cybersecurity blocks.
- Utilize the cybersecurity blocks provided by CYBER.ORG within the MakeCode environment to design and implement secure coding practices on the micro:bit platform, demonstrating an understanding of how to protect data and communication.

Digital Citizenship (2 hours count towards the credential)

Explore resources and information about digital citizenship and cyber security to prepare you and your students. We will also explore appropriate technology usage and become aware of the dangers of the cyberworld. Resources will be identified to best fit your classroom setting. Relevant for all grade levels.

Outcomes

- Evaluate various online scenarios and distinguish between safe and risky behaviors, utilizing critical thinking to assess potential cyber threats and propose strategies for fostering a secure digital environment for both yourself and your students.
- Explain the significance of responsible technology usage and the implications of cyber threats, demonstrating comprehension of the interconnectedness between digital citizenship, cyber security, and personal well-being.
- Recall key concepts related to digital citizenship and cyber security, including terminology, principles, and fundamental practices, to establish a foundational understanding.

Intro to Cybersecurity Part 1 (8 hours online/asynchronous toward the credential)

What do we need to do to keep ourselves safe online? How can we protect our identities and the devices we use? What are others doing online that could cause me harm? These questions and more are discussed in the Introduction to Cybersecurity course to help you lead a safer cyber existence. The hands-on labs utilize the CYBER.ORG Range, which is a no-cost cyber range for all K-12 students and educators. Relevant for grades 9-12.

Outcomes

- Define the CIA Triad and articulate its key principles in the context of cybersecurity.
- Explain social engineering techniques, phishing, and tools for Open Source Intelligence (OSINT) with an understanding of their purposes and potential risks.
- Utilize the Terminal for both Linux and Windows environments to execute commands and employ various tools for practical cybersecurity tasks.
- Break down the process of computing binary and hexadecimal numbers, demonstrating a deep understanding of the underlying principles and the ability to analyze and manipulate these numerical systems.

Intro to Cybersecurity Part 2 (8 hours online/asynchronous toward the credential)

This course will be available soon (by late Spring 2024).

What do we need to do to keep ourselves safe online? How can we protect our identities and the devices we use? What are others doing online that could cause me harm? These questions and more are discussed in the Introduction to Cybersecurity course to help you lead a safer cyber existence. Part 2 is a continuation of the content from Intro to Cybersecurity Part 1, covering Units 5-7 of CYBER.ORG's Intro to Cybersecurity course. The hands-on labs in this course utilize the CYBER.ORG Range, which is a no-cost cyber range for all K-12 students and educators. Relevant for grades 9-12.

Prerequisite: Intro to Cybersecurity Part 1

Outcomes

- Utilize the Terminal for both Linux and Windows environments to execute commands and employ various tools for practical cybersecurity tasks, such as WireShark.
- Define techniques for reconnaissance of digital targets, explore how to capture and analyze network information, and configure network IP addressing.
- Identify how the Internet structure and Domain Name System can be used for reconnaissance and attacks and explore advanced searching methods.
- Explore ethical issues, laws, and rules associated with information security and digital activities.

Intro to Cybersecurity Part 3 (8 hours online/asynchronous toward the credential)

This course will be added soon (by Summer 2024).

What do we need to do to keep ourselves safe online? How can we protect our identities and the devices we use? What are others doing online that could cause me harm? These questions and more are discussed in the Introduction to Cybersecurity course to help you lead a safer cyber existence. Part 3 is a continuation of the content from Intro to Cybersecurity Parts 1 and 2, covering Units 8-10 of CYBER.ORG's Intro to Cybersecurity course. The hands-on labs in this course utilize the CYBER.ORG Range, which is a no-cost cyber range for all K-12 students and educators. Relevant for grades 9-12.

Prerequisites: Intro to Cybersecurity Part 1, Intro to Cybersecurity Part 2

Introduction to micro:bit – block coding (8 hours online/asynchronous toward credential)

Teachers will explore CYBER.ORG's Coding Fundamentals course using the BBC micro:bit and Microsoft MakeCode platform to create builds that incorporate block-based coding. You will learn how to use the CYBER.ORG curricula and explore ways to incorporate computer science in any subject area. Relevant for grades 4-12.

Outcomes

- Analyze the CYBER.ORG curricula and evaluate its suitability for integration across various subject areas.
- Apply knowledge of block-based coding, the BBC micro:bit, and the Microsoft MakeCode platform to design and create functional builds that incorporate these technologies.
- Assess the potential benefits and challenges of incorporating computer science concepts into different disciplines, fostering a deeper understanding of how computer science can enhance diverse educational contexts.
- Demonstrate the ability to translate conceptual understanding into practical applications.
- Recall and understand the foundational concepts of CYBER.ORG's Coding Fundamentals course, including the principles of block-based coding, the functions of the BBC micro:bit, and the features of the Microsoft MakeCode platform.

Intro to Python using the micro:bit (8 hours online/asynchronous toward credential)

Learn to program the micro:bit using Python, a text-based coding language. We will learn how to program the components on the micro:bit using python, including the LED display, push buttons, and sensors. Relevant for grades 4-12.

Outcomes

- Analyze the interactions between different micro:bit components and their corresponding Python code, identifying the cause-and-effect relationships that determine the micro:bit behavior.
- Apply Python programming skills to effectively control and manipulate the micro:bit components, such as programming LED displays to show specific patterns, utilizing push buttons to trigger events, and utilizing sensors to gather input data.
- Develop practical solutions by translating conceptual understanding into functional code.
- Evaluate and troubleshoot code to resolve programming errors and optimize performance. Compare and contrast various programming approaches for achieving desired outcomes on the micro:bit platform.
- Recognize the purpose and functionality of the micro:bit components, such as LED display, push buttons, and sensors, in the context of programming.
- Understand the fundamental concepts of programming by comprehending the syntax and structure of Python.

micro:bit with STEM EDA (8 hours online/asynchronous toward credential)

The micro:bit is a multifunctional tool that can be integrated into many areas of curriculum. The CYBER.ORG STEM EDA (Explore, Discover, Apply) workshop covered Electricity, Coding, and Music. In this workshop, teachers will be guided through ways of using the micro:bit with these topics to incorporate micro:bits and computer science into all classrooms. Relevant for grades 6-8.

Outcomes

- Analyze the alignment between micro:bit-based activities and essential concepts. Evaluate and adapt existing teaching strategies to incorporate micro:bits and computer science principles, fostering interdisciplinary learning experiences across different subject areas.
- Describe the fundamental features and capabilities of the micro:bit, including its integration potential within various curriculum areas, such as Electricity, Coding, and Music.
- Employ the micro:bit effectively in diverse classroom scenarios by designing and implementing hands-on activities that demonstrate the application of micro:bit technology to teach concepts related to Electricity, Coding, and Music.

Minecraft (16 hours – 8 hours count towards the credential)

Minecraft Education Edition 2-day workshop. Teachers must commit to both days to receive credit.

Learn how to use Minecraft Education Edition in the classroom to help students unlock their creative potential. Explore other free resources and tools that will take learning and student engagement to a new level.

Day 1: Participants will learn the basic mechanics of how to function within a Minecraft environment and how to create learning experiences for their students. Minecraft Education Edition can be used to teach concepts in any subject area. Teachers will explore the M:EE website and sift through already developed lesson plans for their classroom and adapt those to their current teaching practices.

Day 2: Participants will continue developing their lesson plans and participants will be introduced to coding in M:EE. Participants will develop an understanding of how Computer Science concepts can be integrated into all learning experiences using M:EE.

Outcomes

- To familiarize participants with the basic game mechanics and provide opportunities for practice.
- Help participants understand how to bring the game in as an educational tool into their classroom.
- Practice navigating and learning to move in the game.
- Utilize and manage Minecraft Education Edition as a digital tool.
- Understand and deliver an activity using Minecraft Education Edition.
- Explore pre-made coding and CS curriculum that can be used in any classroom.

Science+ (8 hours online/asynchronous)

Teachers will explore the CYBER.ORG Science Plus Curriculum. Science Plus is a phenomenon-based, hands-on science curriculum with technology ideas built into it. The modules are designed for students to learn the engineering design process to understand concepts and solutions. This course provides teachers with hands-on experience as to how the course works and provides them with methods of teaching computer science and cybersecurity concepts at the elementary grade levels. Relevant for grades 3-5.

Outcomes

- Explore and experience the CYBER.ORG Science+ curriculum.
- Work toward ND Level III Credential for Computer Science and Cybersecurity.
- Work with combination of text-based and visual programming languages (software).

STEM EDA (8 hours online/asynchronous toward credential)

Teachers will explore the CYBER.ORG STEM EDA Curriculum for students in grades 6 through 8. STEM EDA (Explore, Discover, Apply) explores science, technology, engineering, and mathematics through hands-on projects that build experiences. Relevant for grades 6-8.

Outcomes

- Adapt and implement the curriculum effectively within a classroom, fostering a conducive environment for students to explore, discover, and apply STEM concepts in practical projects.
- Articulate the key components and principles of the CYBER.ORG STEM EDA Curriculum, demonstrating understanding of how it integrates science, technology, engineering, and mathematics concepts for students in grades 6 through 8.
- Determine the extent to which the workshop content can contribute to fulfilling these credential prerequisites, providing valuable insights for both educators and students pursuing these fields.

Code.org Computer Science Fundamentals (CSF) Intro (8 hours toward credential)

Code.org's Computer Science Fundamentals courses blend online and "unplugged" non-computer activities to teach students computational thinking, problem solving, programming concepts and digital citizenship.

Outcomes

- Work toward the Level III Credential for Computer Science and Cybersecurity.
- Explore the Code.org Computer Science Fundamentals curriculum and learning tools.
- Discuss classroom management and teaching strategies.
- Build a community of teachers.
- Develop skills while working in small groups.
- Deepen their understanding of the materials.

Code.org CS Fundamentals (CSF) Deep Dive (8 hours toward credential)

Deep dive into the CSF curriculum that focuses on pedagogy. Participants are encouraged to share what empowers students to create authentic artifacts and engage with computer science as a medium for creativity, communication, problem solving, and fun. The curriculum is recommended for elementary school students (grades K-5) and can be taught either as a semester or full-year offering.

Outcomes

- Reflect and discuss classroom management and teaching strategies.
- Continue to build a community of teachers.
- Deepen their understanding of the Computer Science Fundamentals curriculum.
- Be updated on latest curriculum pieces and learning tools.

Code.org Computer Science Discoveries (CSD) (72 hours toward credential)

Computer Science Discoveries (CS Discoveries) is an introductory computer science course that empowers students to create authentic artifacts and engage with computer science as a medium for creativity, communication, problem solving, and fun.

Outcomes

- Work toward the Level II Credential for Computer Science and Cybersecurity.
- Explore the problem-solving process and the different ways humans and computers solve problems.
- Discover the languages powering the web. Build your own websites in HTML and CSS using Web Lab.
- Learn the powerful constructs underlying programming languages. Build interactive games in JavaScript using Game Lab.
- Follow a design process to identify and empathize with problems faced by a target audience. Prototype an app to help solve that problem using App Lab.
- Develop binary representations of different kinds of information. Collect, analyze, visualize, and make automated decisions using data.
- Explore the relationship between hardware and software, while building interactive projects on Adafruit's Circuit Playground using App Lab.

Code.org Computer Science Principles (CSP) (72 hours toward credential)

Computer Science Principles is a course designed to prepare students (and teachers) who are new to computer science for the AP CS Principles exam. The course covers many topics including the Internet, Big Data and Privacy, and Programming and Algorithms.

Outcomes

- Work toward the Level II Credential for Computer Science and Cybersecurity.
- Students learn how the multi-layered systems of the Internet function as they collaboratively solve problems and puzzles about encoding and transmitting data, both 'unplugged' and using Code.org's Internet Simulator.
- Students learn how complex information like text and images is stored in a computer and the way compression helps reduce the size of those files.
- In this unit, students learn the JavaScript language with turtle programming in Code.org's App Lab. Students are introduced to the general principles of algorithms and program design that are applicable to any programming language.
- Students research current events around complex questions related to public policy, law, ethics, and societal impact. Students are also introduced to the basics of how and why modern encryption works.

- Students continue learning how to program in the JavaScript language. Using Code.org's App Lab environment, students create a series of applications that live on the web. Each app highlights a core concept of programming.

Previous EduTech Offerings that can be used for the CS Credential

Middle School CyberTeacher (32 hours – between 2018-2020 and 2021-2022)

Teachers will explore the CYBER.ORG curricula for middle school, including STEM EDA, Cybersecurity Basics, and Coding Fundamentals. We will learn how to use the CYBER.ORG curricula and discover innovative ways to incorporate the curricula and micro:bits into all learning. A Blended Learning approach will be used during this workshop series.

Outcomes

- Middle school teachers will explore the CYBER.ORG curriculum and work toward CYBER.ORG certification and Level II Credential for Computer Science and Cybersecurity.
- Explore and learn how to integrate the CYBER.ORG curriculum, specifically STEM EDA, Coding Fundamentals, and Cybersecurity Basics into their classroom.
- Practice using a combination of text-based and visual programming languages (software).
- Discover new uses of the micro:bit using Microsoft MakeCode and ways to incorporate into all subject areas.

High School CyberTeacher (32 hours – between 2018-2019 and 2021-22)

Teachers will explore CYBER.ORG's Coding Fundamentals and Cyber Literacy courses using the Parallax cyber:bot and the BBC micro:bit platforms to create complex builds that incorporate blockbased coding, Python coding, and a combination of tactile and infrared sensors. We will learn how to use the CYBER.ORG curricula and explore ways to incorporate computer science and cybersecurity in any subject area.

Outcomes

- High school teachers will explore the CYBER.ORG curriculum and work toward CYBER.ORG certification and Level II Credential for Computer Science and Cybersecurity.
- Explore and learn how to integrate the CYBER.ORG curriculum, specifically Cyber Literacy and Coding Fundamentals into their classrooms.
- Use Microsoft MakeCode to program the BBC micro:bit.
- Practice creating complex circuit builds that incorporate Python coding and the Parallax cyber:bot.
- Discover ways to navigate with the cyber:bot, including using tactile and infrared sensors.

Please Note: Participants from Spring 2021 received 40 hours of training instead of 32 hours of training.