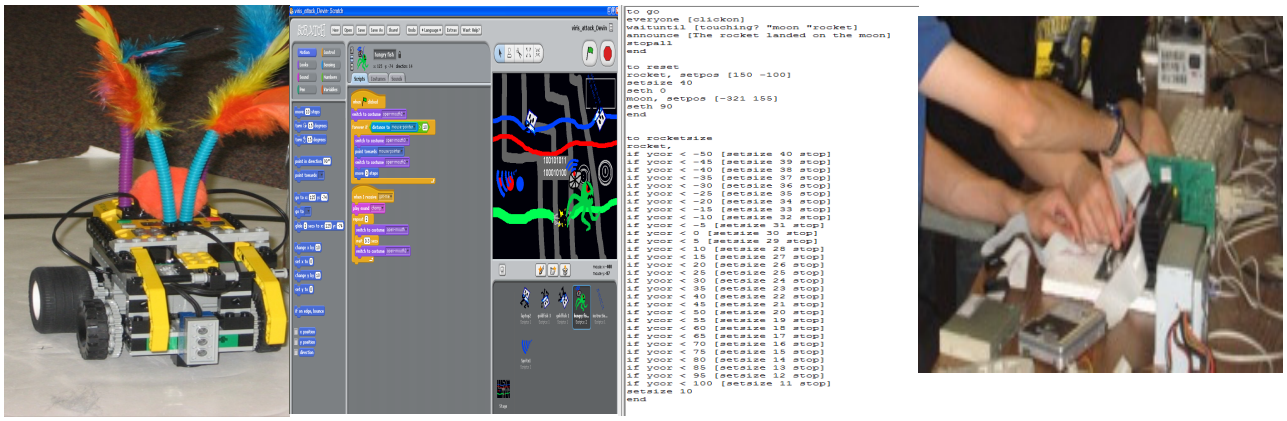
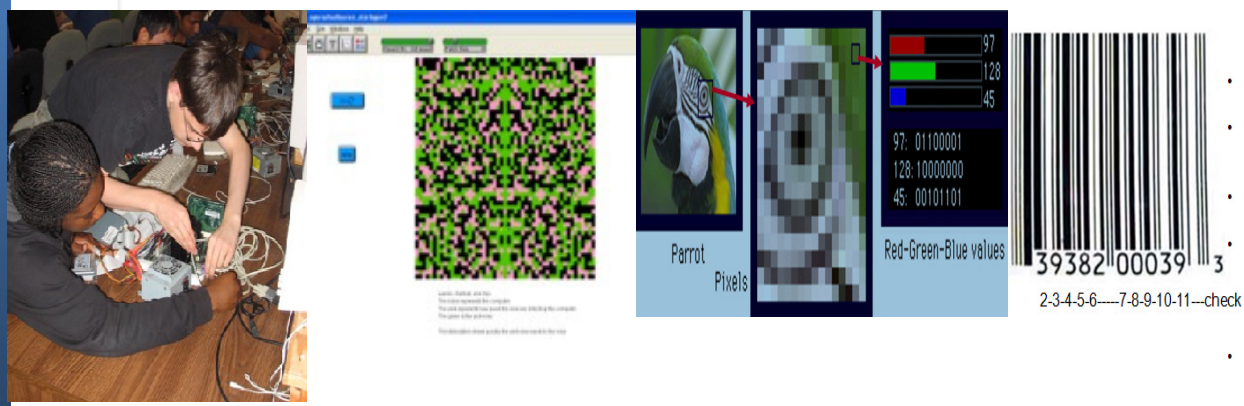
SECURE IT



Strategies to Encourage Careers in Cybersecurity & Information Technology



SECURE IT

Strategies to Encourage Careers in CyberSecurity and Information Technology

Based on Research by

Educational Technology Policy, Research and Outreach

With Partial Funding from

Illustrations by ETPRO

Graphics by ETPRO and the SECURE IT Team

Modified from the Young Scholars Program: Students, Learning and Technology

Davina Pruitt-Mentle
Carla Doernberg
Mike Garza
David Wilson

Kim Reddy
Portia Pusey
CW Consortium

Educational Technology Policy, Research and Outreach
5333 Broadwater
Clarksville, MD 21019

To learn more about the *SECURE IT*: Strategies to Encourage Careers in Cybersecurity and Information Technology Project, contact us:

Web: http://www.edtechpolicy.org/cyberk12/

Email: info@edtechpolicy.org

Educational Technology Policy, Research, and Outreach
SECURE IT is part of ETPRO and CyberWatch

Educational Technology Policy, Research and Outreach, a research and development organization located in Maryland, connects educational technology policy and research to instructional practice. ETPRO brings more than two decades of experience in the educational community, and more than a decade of experience in evaluating both formal and informal educational programs at the K-16 level, and conducting educational technology policy analysis. ETPRO's expertise is founded on a combination of classroom practice across K-16 tied with a solid research base.

ETPRO originated from the Educational Technology Outreach division of the College of Education, at the University of Maryland, and in 2007 was founded as an entrepreneurial entity committed to quality education for all learners, targeting the effective use of cutting edge technology in formal and informal educational settings to increase interest in Science, Technology, Engineering and Mathematics (STEM) fields. The fundamental gap between technology use and understanding of proper practices, lead ETPRO to the forefront of research, program evaluation and development of Cyberethics, Cybersafety, and Cybersecurity (C3™) initiatives.

CyberWatch is an Advanced Technological Education (ATE) Center, funded by a grant from the National Science Foundation (NSF). The CyberWatch mission is to increase the quantity and quality of the Information Assurance/cybersecurity workforce. The CyberWatch goals are focused on Information Assurance (IA) education at all levels, from elementary through graduate school, and include curriculum development, faculty professional development, student development, career pathways, and public awareness. Since its founding in 2005 as a consortium of 10 institutions in the Washington, DC metropolitan area, CyberWatch has expanded to over 60 member institutions across multiple states; acquired multiple partner businesses, government agencies, and professional associations; developed model IA curricula, including complete courses for A.A.S. and A.S. degrees and for two IA certificates; assisted member institutions in mapping their IA courses to the Center for National Security Standards (CNSS) standards; helped lead the national effort to create the Centers of Academic Excellence in Information Security Education for Community Colleges (CAE2Y) with NSF, NSA, and DHS; contunies to assist all eligible CCs to apply for CAE2Y status; trained 450+ faculty through CW workshops and through sponsored courses at member institutions; built the Montgomery College Virtual Lab (MCVL), the University of Maryland Digital Forensics Lab (DFL), and the Bowie State University CW Underground Tunnel System (CUTS); initiated and still conduct these student competitions: Mid-Atlantic Regional Collegiate Cyber Defense Competition (CCDC), Digital Forensics Cup, Security Awareness Poster and Video Contest for higher education (in collaboration with EDUCAUSE) and K12, and host/coordinate the DC Regional High School Network Security Compeition and two Maryland US Cyber Challenge Summer Camps. CW also has created a robust IA program for K-12 students including cybersecurity awareness materials for educators and parents, after school and summer programs, formal content modules, contests and competitions, and STEM related research studies.

SECURE IT:
Strategies to Encourage Careers in CyberSecurity and Information Technology

INTRODUCTION

SECURE IT is a strategies project designed to implement and evaluate a *systemic community development strategy* to address the need for career pathways in Cybersecurity. The project builds on close existing partnerships between the successful NSF funded ATE CyberWatch Center K12 program, and local school districts. SECURE IT promotes whole-community, systemic adoption of a standard-based pedagogically proven curricula, and a multiple-pronged approach to addressing the project's three overarching goals: 1) increasing student's knowledge of essential 21st century skills and digital literacy, including general Cyberethics, safety and security (C3®) education, 2) addressing the critical cybersecurity workforce pipeline shortage, and 3) increasing the STEM research knowledge base. Each prong is designed to increase student access to, and success with, the schools' general education curricula, while prolonging engagement in STEM activities that can lead to a career in Cybersecurity or other STEM related workforce areas.

Goals:

- increase student's 21st century skills and digital literacy, including general awareness and education about Cyberethics, safety and security (C3®) education
- address the critical shortage of the Cybersecurity workforce pipeline by increasing the number and diversity of students pursuing careers in Cybersecurity
- increase the research knowledge base about STEM career preparation, specifically careers in Cybersecurity.

Seven Essential Steps of SECURE IT

7 Essential Steps of SECURE IT:

After-School Programs
Saturday/Enrichment Activities
Summer Programs
Teacher Training
Counselors Workshop
Parent Materials
Integration Topics
Cyber Challenges

The SECURE IT strategy design is comprised of seven essential steps: informal or after-school/Saturday programs for elementary and middle school students; high school cyber clubs; summer programs; teacher professional development; training and materials for counselors and STEM coordinators; integrated core curricular lessons; resources and activities for parents/guardians, and Cybersecurity related challenges/competitions.

The SECURE IT content is the foundation of the project. The content currently includes activities in five areas: *Cryptography; Programming/Computational Logic; Digital Ethics, Safety and Security; System Vulnerabilities; and Digital Forensics.* The five content area resources include activities that have been developed for grade bands 3-5, 6-8 and 9-12. However, it should be noted that SECURE IT is organized around competence rather than seat time and promotes flexible scheduling that fits students' individual needs and interests rather than traditional academic periods and lockstep curriculum pacing. A static age-determined group lesson is discouraged. Tied to national and partnering school system math, technology and science curriculum, students engage in hands-on STEM activities and improve digital literacy skills while learning and applying concepts through gaming, modeling and simulation development. Speakers and field trips are integrated in the content. The central focus is the field of Cybersecurity, but it is supported by the too often neglected topics of citizen awareness of ethics, safety and security.

5 Domains of SECURE IT:

Cryptography

Programming/Computational Logic

Cyber Ethics, Safety and Security

System Vulnerabilities

Digital Forensics

Content Overview

The SECURE IT content is based on the Young Scholars Program (YSP), Students, Learning and Technology, developed by Pruitt-Mentle, initiated in 2001 at the University of Maryland, College of Education. The YSP is a campus wide initiative to attract high school students to pursue academic interests, explore career opportunities, earn three college credits, and discover campus life at the University of Maryland. Each college developed a signature program. The purpose of the College of Education's program was to foster excellence in 21st century skills to help students succeed in college, and prepare themselves with the skills necessary to meet the shifting and constantly changing demands of the future workplace. Students gained valuable skills related to digital literacy while exploring career opportunities related to the STEM fields. Students investigated the design and use

of games and simulations for educational purposes, the research and development issues associated with each, and experienced various modeling and simulation software packages (*MicroWorlds, Excel, RoboLab, Scratch, GoogleSketchUp, StarLogo* and other open source applications). Through the NSF funded CW ATE grant, a similar program was developed specifically exploring career opportunities related to Cybersecurity. Materials were developed, piloted, evaluated, and adjusted. Due to popularity, the summer program for high school students grew to five programs in four Maryland counties in 2009, has expanded well beyond that number in multiple states, and has led to the development of year round after school programs for both elementary and middle schools, and several high school cyber defense and cryptography clubs.

Designing and creating interactive games and simulations, as well as robotics, has shown to be an effective and efficient means for delivering complex instruction and promoting high order thinking skills and problem solving strategies. Robotics, and game and simulation development, " (a) use action instead of explanation, (b) create personal motivation and satisfaction, (c) accommodate various learning styles and skills, (d) reinforce mastery, (e) provide interactive, decision-making context" (Kebritchi, 2008, p. 15[1]), and (f) promote collaboration among learners (Kaptelin & Cole, 2002[2]). SECURE IT allows students to engage with a wide variety of software applications. However, students are not expected to be an expert in any program—the goal is not to teach "Scratch" or "Alice". Instead, the ultimate goal is to allow students to explore and expand their knowledge of essential 21st century skills: technology fluency and applications, team building, collaboration tools, problem based critical thinking, and computational logic. Computational thinking is a way of solving problems, designing systems, and understanding human behavior that draws on concepts fundamental to computer science. "Computational thinking means creating and making

[1] Kebritchi, M. (2008). Effects of a computer game on mathematics achievement and class motivation: An experimental study. Unpublished doctoral dissertation, University of Central Florida

[2] Kaptelin, V., & Cole, M. (2002). Individual and collective activities in educational computer game playing. In T. Kosmann, R. Hall, & N. Miyake (Eds.), g2057CSCL 2:

use of different levels of abstraction, to understand and solve problems more effectively. Computational thinking means thinking algorithmically and with the ability to apply mathematical concepts such as induction to develop more efficient, fair, and secure solutions" (Center for Computational Thinking at Carnegie Mellon University[3]).

PROGRAMS

After School CyberSTEM Programs

The year round after school program typically includes two nine week sessions over the course of the year. Each session runs one hour and a half. At least one teacher from the host school commits to running the program. Professional development and curriculum resources are provided to each teacher. Instructors receive curriculum and training updates. Instructors are usually compensated for both their training time (or sub coverage) and for running the program via a stipend. Parents are encouraged to attend at least one session each semester, in addition to the final Student Showcase event held at the end of each term. Speakers are scheduled for each semester. Students are recruited through school efforts; fliers, PTA bulletin, school newsletters and website. Principals work with teachers to also target students. Past efforts have been fruitful in recruiting girls and special needs students (autistic and dyslexic). The program encourages students to continue to stay with the program by offering small give-aways for class challenges (donated by partners), session certificates and yearly participation awards (trophies-which get larger for each year participating).

Table 1 shows an overview example of the SECURE IT CyberSTEM topics.

[3] Center for Computational Thinking at Carnegie Mellon University, http://www.cs.cmu.edu/~CompThink/

Programming	*Cryptography*	*Digital Ethics, Safety and Security*	*System Vulnerabilities*	*Digital Forensics*	
		Elementary School			
Intro to LOGO – Microworlds/CL/ Syntax	Intro to cryptology & cryptanalysis Transposition cipher	Password/passphrases	Free iPod-Opening Attachments	Decoding/Debugging I/II MW programming	
Interactive PPT	Invisible ink	Cyberbullying	Pop Ups	Learning Binary Name in Computer "Talk"-Binary Numbers	
Scratch	Substitution cipher (cipher wheels)	Who's Who Online	Password Guessing	Bar coding	
Robotics I - RoboLab	NSA Codemakers Codebreakers	Digital Footprints		Real or Unreal (Detecting scams)	
		Middle School			
Computational Logic	Intro to cryptology & cryptanalysis	Passwords/Passphrases /cyberbullying	System Upkeeps/Patching	Recognition of similar patterns	
MicroWorlds/Scratch	Coding/decoding - out of the box				
Robotics II - Mindstorms	Substitution cipher and letter/number frequency	Online Reputation Management	Phishing/Pharming/ Hijacking	Needle in a Hay Stack (where's the bad code)	
Google SketchUp	Cryptography Scavenger Hunt	Dangerous Uploads	Password Cracking		
NetLogo Alice	Geometric cipher	Security Clearances Copyright/Plagiarism Social Networks	SNS Malware		
		High School			
Computational Logic II Rapture	Intro to cryptology & cryptanalysis Substation ciphers	Passphrases/patterns-encryption	Security Layering	Deleted/Hidden Files SIM reader exercise	
MicroWorlds/Scratch Python					
Programming in Excel	Paper Enigma	Cyberbullying	Firewalls	Roadrunner	
StarLogo/NetLogo	Algebraic ciphers	Sexting	Password Cracking II	SamSpade exercise	
				FTK Imager Lite EnCase (CWVDFL)	
Alice	Intro Computer cryptography 2 key cryptography	Online Reputation Management	Ping/Trace Route Reconnaissance		
		Webcams/GoogleHacking	Wireshark Pasco		
Robotics III Mindstorms		Copyright/Plagiarism	Patterns	Reverse Engineering	
		Security Clearances	SamSpade exercise	Steganography/Digital Watermarking	
		File Sharing/LimeWire Social Networks			

Careers in IA/Field Trips/Speakers/Parents Materials/Labor stats-Projections/Pathways

Table 1: SECURE IT Content Overview Example 1

Table 2 provides an example of the 18 week program run at one of the local Elementary Schools and the Fall-Spring schedules.

	Fall		Spring
1	Intro to LOGO programming /MicroWorlds (MW)	10	Robotics
2	MW Intro to cryptology & cryptanalysis /Transposition cipher	11	Robotics NetSmartz speaker Internet safety
3	MW iKeepSafe Speaker Cyberbullying	12	Robotics
4	Interactive PPT Decoding/Debugging I	13	Robotics PopUps CW partner speaker
5	Interactive PPT & computational logic	14	Robotics Attachments
6	Scratch Decoding/Debugging II	15	Robotics CW partner -NSA speaker
7	Scratch CW partner speaker	16	Robotics
8	Scratch	17	Robotics
9	Student Show Case	18	Student Show Case

Table 2: Elementary School Program Example

High School CyberSTEM Clubs

Some schools have chosen to have informal cyber clubs related to cybersecurity; cyber defense, robotics, or cryptography clubs. Cyber clubs usually focus on preparation for various Cyber Defense competitions including the CyberPatriot, US Cyber Foundations/Quest, Network Security Competition, and the DC3Forensic Cup. We also offer support to other related clubs, for example, the North American Computational Linguistics Olympiad (NACLO), First Robotics and American Computer Science League (ACSL), and the FBLA Cybersecurity component, to name just a few. The CyberWatch K12 Division/SECURE IT staff supports these efforts by 1) providing oversight and club development guidance and 2) providing students and advisors with materials, content, coaches, mentors and speakers. Specialized training is also scheduled for high school club advisors.

Summer CyberSTEM Programs

Summer programs are offered and last two to three weeks in duration, depending upon the county. The school district assists in the recruitment of two teachers to serve as instructors within each district. Additionally, SECURE IT staff may help serve in instructor capacity. Professional development and resources are provided to each teacher and they also receive content material and training updates. Instructors/mentors are compensated for both their training time and for leading the program via a stipend. Table 3 provides an example of a two week high school program; up to three speakers and field trips are scheduled during each session. Students are recruited through school/district efforts; fliers, PTA bulletin, school newsletters and website. The program encourages students to continue to stay with the program by having them serve as teacher assistants for the following summer session. Up to two student TA's are chosen.

Table 3: Example of a Two Week High School Program

High School/ CyberSTEM Summer 2 Week
Based 6 hours a day
Week 1

Meeting	Content
1	Welcome & Logistics Hard Drive Introductions Warm-Up Three Questions Overview of Information Assurance, Information Security, and Digital Forensics—Video NSA –4 elements --Integrity Confidentiality Video Snippets/ NSA & CyberWatch DVD Transition to Computational Thinking --Unplugged Activity-- Hook Introduction to Syntax Introduction to MicroWorlds for multimedia creation – Introduction PowerPoint – Where Logo Language fits in – Berkley logo and the other free logos LOGO language: Differences between functional & imperative programming languages Lisp dialect Skill Development with MicroWorlds Hatching a Turtle Basic Commands- Index Card with Basic Commands Shapes Exercise Repeat Converting to Procedure Graphics/ Animation Program the turtle to avoid the hazard Announce command Coordinates of turtle Buttons: New Page/ Add a Page, Reset Sliders: speed and direction MicroWorldsTeam Challenge: Animated Story or Game Related to Cybersecurity
2	Team Challenges Continued: MicroWorlds Identity Management : Digital Footprints/ Digital Fossils Online Reputation Management PowerPoint Digital Dossier Video **Guest Speaker-Security Clearances Cybersecurity Video CyberWatch with Presenter's Guide Programming with Excel Encrypting Files If, And, and Or functions and the connections to MicroWorlds Password Protecting Workbooks Data Validation Conditional Formatting Locking Cells Excel Challenge: Quiz or Crossword Puzzle
3	Disaster Recovery Backing up Teacher PowerPoint and Demonstration using a Thumb drive or external drive Simulation/Game Development in Scratch PowerPoint with build in videos Watch Sample projects Decoding the Samples Conditional Formatting connections with Excel and MicroWorlds Sprite Basics

Meeting	Content
	Creating your own Sprite Name Letter Drop Activity Animating a Sprite Adding Sound Back Spin Activity Scratch Challenge: Create an animation, simulation, game, interactive project to teach someone about an IA/IS/Cybersecurity career or about cyberethics, cybersafety and cybersecurity.
4	CyberWatch exercise on Ping, Traceroute How Internet traffic works video PowerPoint if you can't actually do the ping or tracerout **Guest Speaker: Forensics Digital Forensics using Wireshark, SANS toolkit, FTK Image Lite, or EnCase Digital Forensics: collecting, handling, reporting evidence Cell Phone forensics where available – Citizen engineer
5	Hardware Exploration using Hardware Kits Configuring a Virtual Networking using Cisco Packet Tracer Packets Protocols and Ports Show and Share MicroWorlds, Excel and Scratch Products

*Alice and Google SketchUp can also be included.

High School/ CyberWarrior Summer 2 Week
Based 6 hours a day
Week 2

6	Introduction to Cryptography Cryptography PowerPoints/Exercises Caesar Cipher Substitutions Cipher Steganography Paper Enigma Exercise Robotics Basics Begin Assembling the LEGO Mindstorms Robotics Kits Beginning Syntax
7	**Field Trip: NSA – National Cryptographic Museum and Career/Scholarship talk Finish Assembling the Lego Mindstorms Robotics Kits Mini Challenge: follow a line Mini Challenge: go up to a wall and reverse without touching the wall Mini Challenge: Enter and exit a key Robotics Master Challenge Program the robot to use the sensors to stay within limited area while pushing cans out of this area Introduction to Raptor: Program Structure, Statements/Symbols, Variables, Comments Raptor Programming Challenge: Create a program that prompts a user to input the diameter of the circle and output the area.
8	LegoMindstorm Mini Challenge: follow a line Mini Challenge: go up to a wall and reverse without touching the wall Mini Challenge: Enter and exit a key Robotics Master Challenge Program the robot to use the sensors to stay within limited area while pushing cans out of this area Advanced Raptor Programming: Loops Advanced Raptor Programming Challenge: Work in a team to design and build a Raptor program to create secure passwords or phases Introduce Python Programming: Using the Python Interpreter, Using Python as a Calculator Python Challenge: Create a simple Python calculator
9	Prepare for Student Showcase Day today: Complete any unfinished challenges Queue Excel, MicroWorlds, Scratch, Raptor and Python projects on computers Student Showcase
10	Carefully disassembly the LEGO Mindstorms robot NetSmartz videos: Information Travels, Offline Consequences and Social Networking Student Team Research: Student teams research and present a list of best practices one of the following topics: Social networking; New computer best practice; Reputation and identity management; Disaster prevention and recovery for home computers; Using copyrighted materials legally.

HOW TO USE THIS CONTENT

Integration

SECURE IT is an expanded learning opportunity (ELO); including afterschool and summer activities which have been purposefully aligned with in-school curriculum to support learning and personal success. ELO literature reports benefits to students' academic, behavioral, psychosocial and career development and recommendations for best practice using new tools, such as STEM education support systems and computer simulations which research has shown to be engaging, produce cognitive gains and enhance problem solving skills.

The SECURE IT content is not an independent "curriculum". SECURE IT allows students to explore and expand their knowledge of essential 21st century skills: technology fluency and applications, team building, collaboration tools, and problem based critical thinking, while also exposing them to real-life instances of professionals using these skills in exciting cybersecurity careers that interconnect the fields of science, technology, engineering and mathematics.

SECURE IT provides a means to explore technology applications essential to college success, as well as opportunities to investigate career possibilities in Information Assurance, Cybersecurity, Cryptography and Digital Forensics. **SECURE IT provides dynamic and challenging activities through a variety of computer applications and learning environments - and all while having fun!**

Activities:

- Foster problem-solving skills, including problem formulation, iteration, testing and debugging
- Embrace project-based learning through a variety of software programs and applications
- Include Cybersecurity activities introduced in parallel with programming projects
- Include connections and introductions to career options in IA, Cybersecurity, Cryptography and Digital Forensics

Stand Alone Units, Lessons and Activities

SECURE IT activities have been developed for after school/summer and other enrichment programs. However, programming projects could easily be folded into existing curricula. The following projects have been done by students in the regular core content areas: creating an interactive game in *MicroWorlds* on how to add and subtract fractions (Math), developing a simulation in *StarLogo* regarding deer population with a variety of variables (Biology), creating an interactive Spanish Quiz in *Excel* (Language Arts), and generating an interactive multi-level game regarding cyberbullying (Health). In addition, activities from the SECURE IT content have been "plucked out" by teachers and used in their regular classroom instruction. For example, teachers have used the password cracking probability exercise to teach statistics/probability and tree maps. Another math lesson used often is the virus exercise that highlights exponential speed of spread for worms and viruses. SECURE IT software choices benefit the entire school; MicroWorlds has been used to teach geometry in participating schools.

Grade Level

SECURE IT is organized around competence rather than seat time and promotes flexible scheduling that fits students' individual needs and interests rather than traditional academic periods and lockstep curriculum pacing. A static age-determined group lesson is discouraged. Programming projects can be modified for students based on timeframe, student interest, background knowledge and experience with a particular program. While a variety of software applications are introduced, SECURE IT is not limited to ONLY these programs. If you have another application your school has introduced or there is open source software that you feel would be of interest, by all means, include those in the program. A list of additional programs, resources and materials is available in the Appendix. Additional activities will be added, regularly, to the CW K12 website http://www.edtechpolicy.org/cyberk12/ . While flexibility in programming projects is encouraged, parallel content activities have been written for specific grade bands: grade 3-5, grades 6-8, and grade 9-12. For example, cyberbullying and creating strong passwords can be introduced at the elementary level, however, sexting, encryption of files and using *Wireshark* is more appropriate for the older student.

Sequence

The opening CyberWatch SECURE IT introduction and pre knowledge base exercise occur on day one of each semester. The first semester (fall) focuses on game and simulation development and the second semester (spring) focuses on Robotics[4] - both focusing on the bigger picture, "*computational logic*". *MicroWorlds* is used to introduce the computational logic/programming unit; then students program in *Excel*. These two text syntax specific programming environments/ applications are, followed by *Scratch*, a more visual programming language. This sequence has proven fruitful in promoting computational thinking. Fall and spring semester foci are proposed to best align with local, state and national competitions which some students might find of interest. Table 4 indicates the SECURE IT Program Overview and possible competitions. Description abstracts, links and dates can be found in Appendices.

"Students who were first introduced to *MicroWorlds* and *Excel* easily adapted to other programming languages AND other visual programming languages. They also understood "if", "and" ,"or" functions. However, when students were introduced to visual programming languages first (*Scratch, Alice, Mindstorms Robotics*) they were not able to easily apply the concepts back to 'raw text code', nor were they able to easily debug or decode pieces of code" (Pruitt-Mentle, 2009).

[4] Programming/Computational Logic should be presented prior to Robotics. Therefore, if the first SECURE IT program to run in a school is in the spring semester, the first two SECURE IT programs should be Programming/Computational Logic (first spring, fall) followed by Robotics the second spring.

SECURE IT OVERVIEW
Strategies to Encourage Careers in CyberSecurity and Informational Technology

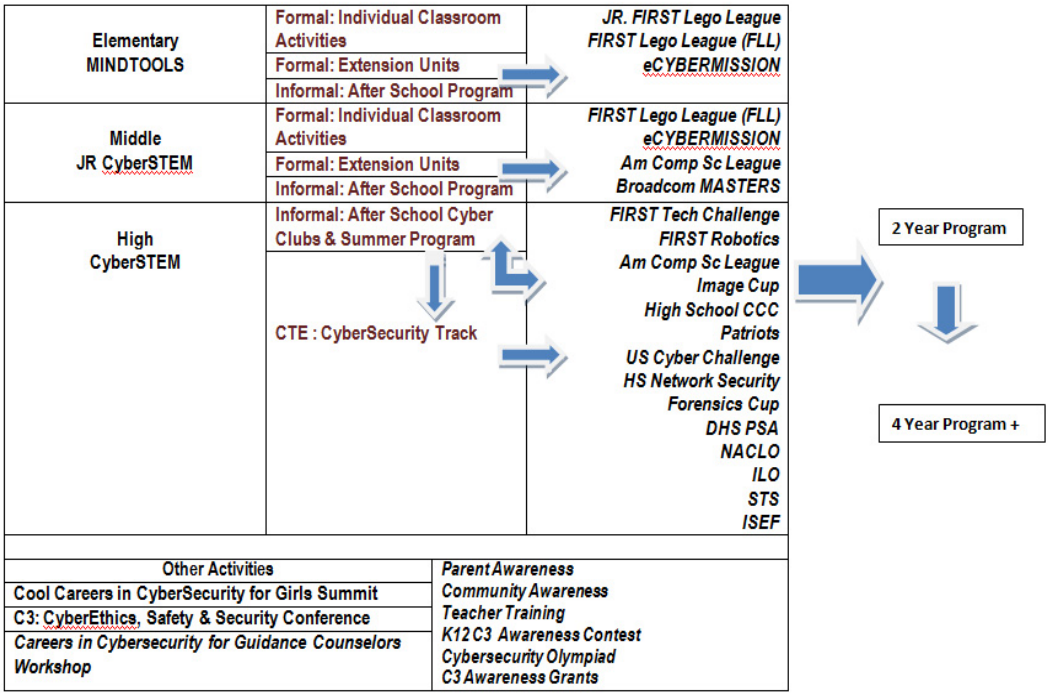


Table 4: SECURE IT Program Overview

Standards

Aligning content and instruction with educational standards is important. Extensive review of national and state standards in math, science, technology, language arts, along with bridging to our CyberWatch Model IA program based on content sequenced with the Committee on National Security Systems (CNSS) National Standards 4011 and 4013. Standards covered in each activity are identified in the Standards Summary Chart found in the Appendices.

Software

Two programs are used at cost: *LCSI's MicroWorlds EX Robotics* and *LEGO MINDSTORMS NXT Robotics.* All other programs, activities and design challenges have purposefully been designed so that they use simple and inexpensive materials and open source software. At cost software licensing is available at a considerable discount through the SECURE IT program in partnership with CyberWatch.

Constructivist Theory: Constructionist Learning

SECURE IT is grounded in constructionist learning through the constructivist theory that individual learners assemble mental models to understand the world around them. Constructionism holds that learning can happen most effectively when people are active in making tangible objects in the real world. In this sense, constructionism is connected with experiential learning and builds on some of the ideas of Jean Piaget.

Seymour Papert, student of Jean Piaget, and founder of the MIT Artificial Intelligence Lab defined constructionism in a proposal to the National Science Foundation entitled Constructionism: A New Opportunity for Elementary Science Education as follows: "The word constructionism is a mnemonic for two aspects of the theory of science education underlying this project. From constructivist theories of psychology we take a view of learning as a reconstruction rather than as a transmission of knowledge. Then we extend the idea of manipulative materials to the idea that learning is most effective when part of an activity the learner experiences as constructing a meaningful product." Seymour Papert was one of the original creators of LOGO, a computer programming language which is the basis of many of the programs SECURE IT uses: *MicroWorlds, Scratch, Alice, and RoboLab/Mindstorms.*

Constructionist learning involves students drawing their own conclusions through creative experimentation and the making of social objects. The constructionist teacher takes on a mentor role rather than a traditional "teacher" position. Teaching "at" students is replaced by assisting them to understand—and help one another to understand—problems in a hands-on way. This is a key, as the SECURE IT instructors are not asked to be experts in any of the activities or programs involved in SECURE IT. Teachers help guide students to debug, find solutions or alternative solutions through a variety of means other than, "the teacher giving the answer away".

When planning SECURE IT activities, instructors are guided by the Madeline Hunter Decision Making Model[5]. This 7 step instructional process provides students with at least three hands-on experiences with the SECURE IT content for every activity. First, instructors model the skill and invite students to participate. Second, the students practice the skill under the direct supervision of the instructor. Lastly, the students complete a final project without direct teacher assistance that reinforces the skill. Consistent with the constructionist theory the students "learn-by-making"[6]; the final project is always a "challenge" that allows students to design and build without a prescribed outcome. The subsequent pages provide a detailed description of how to implement the SECURE IT instructional design process.

[5] Hunter, M. (1994). *Enhancing Teaching.*
[6] Papert, S., & Harel, I. (1991). *Constructionism.* Ablex Publishing Corporation.

The instructional framework for planning activities is guided by the most widely used research-based processes for planning instruction today; Madeline Hunter's Instructional Theory into Practice (ITIP) model. By following the seven steps of the instructional planning process, educators can bring content alive while creating scaffolded learning experiences for the students. Mentors use each of several elements in a sequential order though not all elements need be included in each session. Table 5 lists the 7 steps that should be used in most lessons. More information about implementation of the instructional framework can be found in Appendices.

Instructional Step	Description
Learning Objective	The planning process begins by deciding on your instructional objectives. This is determined by your knowledge of your program and your student group. Do they already know how to work with Microworlds or Mindstorms? Or do they need some starter guidance with the program of choice. Do they understand the bigger picture—connection to computational logic? Working with team members? Figuring things out through trail and error? Includes connections with math, science and technology standards. Ex. Students are being introduced to programming and MicroWorlds will be the application used.
Anticipatory Set	A "hook" to grab the attention of the students (set). These include the activities covering digital forensics, cryptography, system vulnerability and cyberethics, safety and security. These also include career connection activities. Additionally, the prior knowledge or experience of the learners is activated at this time. The SECURE IT materials offer a variety of fun video snippets, interactive or hands on games, or mini team challenges to grab the students' attention and jump start each session.
Lesson Objectives	The purpose for your planned learning activities is shared with your group. Students at all levels need to know what they will be learning and how they will demonstrate what they have learned. (input)
Input	A demonstration activity by the teacher (modeling behavior) that invites active student participation.
Check for Understanding	In addition to specific questions to check for student comprehension (check) the instructor also must observe the students' behavior. You will often use multi-level questioning drawn from Bloom's Taxonomy at this time to help you develop student understanding and adjust your instruction as needed. Peer help/instruction is highly encouraged.
Guided Practice	A project-based student activity is used to pull all the pieces together. Students can work independently or in groups (guided and independent practice).
Independent Practice	A project-based activity similar to the guided practice. Students work independently or with a group without the direct supervision of the teacher (independent practice). A closing summary (closure) and parent follow-up activities should also be planned.

Table 5: Seven Steps of the Madeline Hunter Decision Making Model

SECURE IT INSTRUCTIONAL MATERIALS

SECURE IT includes 5 domains for three grade spans to 1) increase student's knowledge of essential 21st century skills and digital literacy, including general Cyberethics, safety and security (C3®) education, 2) address the critical cybersecurity workforce pipeline shortage, and 3) increase the STEM research knowledge base. Just as C3 awareness and Cybersecurity cannot be isolated in one curricular area or professional field; these 5 domains are not taught in isolation. This section describes the integration philosophy and implementation strategy in four parts:

- Foundational concepts
- Scope and sequence chart
- Recommended content by grade band
- Description and objectives of each domain

Indicated below are suggested activities for the 5 SECURE IT domains. Each activity includes the input, guided and independent practice elements from Madeline Hunter's decision making model. Every activity is designed to be completed in less than 60 minutes. The activities can be executed individually or simplified and combined. Detailed examples of 10 elementary meeting sessions can be found in the Appendices. These example meeting sessions include the following elements:

- Learning objectives
- Standards
- Links to curriculum
- Materials
- Preparation instructions
- Lesson objectives
- Anticipatory sets
- Input
- Handouts for students
- Checks for understanding
- Connections to IA/Cybersecurity careers
- Connections to current technologies and popular culture
- Connections to cyberethics, cybersafety and cybersecurity awareness
- Guided practice
- Independent practice
- Take home activities with links to Information Assurance careers and general cyberethics, cybersafety and cybersecurity handouts

Foundational Concepts

The program goals are accomplished through:

- Acquisition and practice of the skills and knowledge necessary to administrate a personal computing environment, and manage identity and reputation information,
- Acquisition and practice of the skills and knowledge necessary to work for 21st century employers,
- Awareness and exposure to the diverse cybersecurity and other IT related career opportunities,
- Programming in diverse computer languages using several software applications that enable abstract ideas to take concrete forms,
- Acquisition of the principles of computer organization and the major components (input, output, memory, storage, processing, software, operating system, etc.), and
- Acquisition and practice of the skills and knowledge necessary to operate a computer system (CPU, peripherals, operating system, network components, and applications)

At the foundation of the SECURE IT program is computational thinking[7]. Individuals use computational thinking everyday as they complete their daily tasks. Analysis of problems, simplifying procedures, using tools to do repetitive or complex tasks are all part of computational thinking. SECURE IT uses diverse computer applications to allow students to practice the computational thinking process with programming languages or environments that are developmentally appropriate. As students create using programming languages and environments instructors reinforce the fundamental computer science development and testing sequence:

- Decompose problems logically
- Thinking algorithmically
- Planning before implementing
- Recursive processes of testing, problem solving, and implementing

Finally, the collaborative work that is another foundation prong of the SECURE IT program emphasizes the constructionist principal that building a meaningful product translates into effective learning. Students work together to help each other to meet the challenges of the final projects as the teacher assumes a mentor role. This requires students to:

- Understand their work so that they may analyze and assist with the work of others
- Develop 21st century skills of information seeking behavior to solve problems and acquire advanced skills by reading help files or performing Internet research
- Use effective communication to explain their work and thought processes throughout the creative development

[7] Wing, J. (2006). Computational Thinking. *Communications of the ACM,* 49 (3), 33-35.

- Apply skills acquired in one programming environment to diverse programming environments
- Contribute to group projects and work effectively in teams.

Description and Objectives

Cryptography

Topic Description

Cryptography is an important part of Information Assurance -- Not only for the professionals but for everyone in their daily lives. When we use secure websites and programs our data is being encrypted so that no one else can understand the information we are sending. Record labels and movie companies use encryption to protect the copyright of their music and videos. Banks and credit card companies use encryption to protect identity information during online transactions. These protections were created by a cryptographer.

Cryptographers require a diverse training. Cryptographers who specialize in encryption should have advanced skills in math and computer science. But if decryption is what your student wants to do they will also need to be fluent in the language they are decrypting and know a lot about the subject area too. For example, if the cryptographer is trying to decrypt a French art thief's messages, then they should know not only know French but a lot about art and museums and the geographic area where the theft might occur.

Objectives

The student will be able to:

- Encrypt and decrypt messages using basic and advanced cryptographic methods such as substitution, transposition, and computer assisted
- Explore various careers in encryption
- Connect careers in cryptography to the protection of data and communications
- Relate cryptography to the identity protection
- Understand HTTPS as a use for cryptography
- Identify audio and image steganography
- Connect cryptography to strong passwords/ passphrases

Programming/ Computational Logic

Topic Description

Every day we solve problems. Computer programming is merely solving problems using simple instructions called— algorithms. In this module students will use the same skills professionals use to write programs — problem solving, algorithmic thinking, reading, designing, implementing and testing – as they learn and use several computer languages and programs. These skills, also called computational thinking, will be used in every module and in almost every possible career they will hold in the future.

What does computational thinking have to do with Information Assurance? In the process of designing, implementing and testing their programs, students will make mistakes. These mistakes will cause their programs to behave in unexpected ways, for example. Students have to look at the code, find the problem, and fix the mistake – this is what programmers call debugging. Debugging is the same process that Information Assurance professionals use to identify malware (viruses, Trojans etc…). When a computer is infected with malware, the programs that a person uses will not perform as expected – Maybe a delay will occur as a person is typing in their browser -- Maybe there will be pop-up ads-- Maybe emails were sent to everyone in the address list-- or maybe the computer will run slowly. A security professional will use tools to find the source of these problems. If it is malware, they will look at the code that controls the malware to learn how it functions (reverse engineering). They will then create an intervention to delete the malware and prevent the malware from re-installing itself back on the computer. The debugging, reverse engineering, and intervention procedures all require computation logic and are all an important part of Information Assurance.

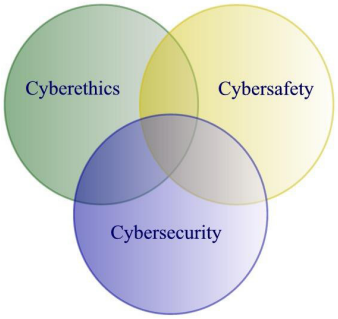
Objectives

The student will be able to:

- Use basic and advanced commands of MicroWorlds, Excel, Scratch, Raptor, Python, Alice, and/or Google SketchUp programs
- Name and explain the process used to decompose problems logically
- Name and explain the algorithmic processes
- Plan before implementing
- Perform the recursive processes of testing, problem solving, and implementing
- Code, test, and execute a program to meet a challenge
- Decode procedures and programs to determine their function
- Build, program and test a robot to meet a challenge

Cyberethics, Cybersafety & Cybersecurity (C3)

Topic Description



The C3 Matrix (c) 1

Promoting socially and ethically responsible use of technology is not a new phenomenon in education. Promoting responsible use has and continues to be acclaimed by many as a strategy under several brands to include *digital citizenship, cyberawareness,* and *cybercitizenship.* Existing strategies that address C3 in K12 education include detailing student, teacher, and administration standards in AUP and student handbooks. Additionally, IT departments have installed Internet filtering and blocking software within state and local education agencies to ensure students' safe and secure technology use. However, some argue that having rules in handbooks and blocking/filtering content is not equivalent to safe practice instruction. Students need to understand the "why" behind the rules, and be able to institute best practices within their normal activities. Once students leave the school and are using unblocked, open systems, they are left unprotected and are not able to make the distinction between safe and dangerous practices. SECURE IT activities are guided by the C3 matrix which assures thorough coverage of C3 content.

Objectives

The student will be able to:

- Practice the technical vocabulary related to the protection of hardware, software, identity, reputation, data, and communications
- Recognize the rights of copyright holders and use copyrighted materials legally
- Describe the consequences of hacking and name opportunities for ethical penetration testing training
- Name methods to avoid Internet and gaming addictions
- Behave ethically and politely online
- Tell a trusted adult if they encountered cyberbullying, inappropriate or objectionable content
- Recognize hoaxes, scams, spoofs, phishing and pharming etc..
- Find, detect, and attempt to eliminate malware and spyware
- Protect and manage identity data and reputation

System Vulnerabilities

Topic Description

The responsibility to prevent system vulnerabilities falls on the shoulders of many professionals. The cryptographer creates unbreakable encryption algorithms to protect users' data and communications; the software developer writes software that minimizes weaknesses; the network security administrator assures the software and operating systems are patched, data is scanned for malware and firewalls are in place – and these are only three of the jobs that protect systems from successful attacks. SECURE IT introduces students to several of the professions that protect a system from being exploited including: security architect, malware analysis, penetration tester, security auditor, and disaster recovery expert. In the process SECURE IT connects the responsibilities of these professionals to the home computer user. Students learn about firewalls, software patches and updates, malware scanning software, social engineering, strong passwords/ passphrases/passpatterns, wireless security, default passwords, HTTPS, and spoofing. They are also introduced to the basics of network security. Exercises include, ping and trace route, email headers and much more.

Objectives

The student will be able to:

- Identify the parts of a computer
- Name hardware and software related to "hardening" systems
- Suggest multiple ideas for "hardening" their own computer system or network
- Implement protective measures on virtual systems
- List several occupations related to protecting computer systems, data and communication
- Recognize national competitions that challenge students to protect systems from vulnerabilities

Digital Forensics

Topic Description

Knowledge of digital forensics is essential in this era of ubiquitous computing. Oftentimes part of a criminal investigation, forensic scientists image and analyze digital media – including hard drives, firmware, cell phones, MP3 players, thumb drives, and even computer systems on cars. SECURE IT activities include examples of the careful investigation of evidence, recovery of deleted data, reconstruction of events/ actions, and reporting on the findings of the investigations. Standard forensic tools such as FTK Image Lite, WireShark, jpegsnoop, and EnCase and the SANS Toolkit are employed within partner virtual environments. In addition, the SANS Toolkit and WireShark can be used by individuals to diagnose home computer and network problems. Steganography is also covered which is a student favorite.

Objectives

The student will be able to:

- Use appropriate vocabulary related to digital forensics
- Identify occupations that need digital forensic skills
- Describe the evidence handling process
- Use neutral language in reporting evidence
- Apply digital forensic skills in virtual environments
- Investigate data or network traffic using standard tools such as FTK Image Lite, EnCase, WireShark, and the SANS Toolkit and EnCase via our CW partner virtual labs
- Acquire free forensic tools and practice forensic analysis on home computers

Career Connection Scope and Sequence

Cybersecurity Career	Content	Elementary MindTools	Middle School Jr CyberSTEM	High School CyberSTEM
		I-Introduce	R-Reinforce	A-Apply
Cryptographer	Vocabulary	I	R	R/A
	Substitution Cipher	I	R	R/A
	Caesar Cipher	I	R	R/A
	Letter Frequency			I/A
	Steganography		I	R/A
	Enigma		I	R/A
	Binary Numbers	I	R	R/A
	UPC/ Bar Codes	I	R	R/A
	Passwords/Phrases	I/R/A	I/R/A	I/R/A
	Excel Programming	I/A	I/R/A	R/A
	Scratch	I/A	I/R/A	
Software Developer	Vocabulary	I	R	R
	Software Development Process	I/A	R/A	R/A
	Help Files	I/A	R/A	R/A
	Introduction to Logo/MicroWorlds	I	R	R/A
	Advanced MicroWorlds		I	R/A
	Raptor			I/R/A
	Python			I/R/A
	Scratch	I/A	I/R/A	
Computer Forensics	Vocabulary	I/R/A	I/R/A	I/R/A
	Investigative Process	I	I/R	I/R
	Cell Phone Forensics		I	I/R/A
	FTK Image Lite			I/R/A
	EnCase (CWDFL)			I/R/A
	Email Header		I	I/R/A
	Deleted/ Hidden Files		I	I/R/A
Incident Responder	Vocabulary	I/R/A	I/R/A	I/R/A
	Malware	I/R/A	I/R/A	I/R/A
	Pop-Up	I/R/A	I/R/A	I/R/A
	Attachments	I/R/A	I/R/A	I/R/A
	Spyware/ Patching	I	I/R	R
	Malware Scanning Software	I	I/R	R
	Software Updates		I	R
	Backing Up		I	R/A
Security Architect	Vocabulary	I/A	I/R/A	I/R/A

Cybersecurity Career	Content	Elementary MindTools	Middle School Jr CyberSTEM	High School CyberSTEM
		I-Introduce R-Reinforce A-Apply		
	Hardware	I/R/A	I/R/A	I/R/A
	Software	I	I/R/A	I/R/A
	New Computers	I	I/R/A	I/R/A
	Networks		I	R/A
	Firewalls	I	I/R	R/A
	Google SketchUp			I/A
Computer Crime Investigator	Vocabulary	I/A	I/R/A	I/R/A
	Logic		I/A	I/R/A
	Handling Evidence		I	I/A
	Collecting and Reporting Evidence		I	I/A
	Reputation Management	I/R/A	I/R/A	I/R/A
	Court			I/A
Malware Analyst	Vocabulary	I/R/A	I/R/A	I/R/A
	Software	I	I/R	I/R/A
	WireShark			I/A
	Malware Scanning Software	I	R	R
	Reverse Engineering			I
	Debugging Code	I/A	R/A	R/A
	Excel Programming			
Network Engineer	Vocabulary	I/R/A	I/R/A	I/R/A
	Hardware	I/R/A	I/R/A	I/R/A
	Software	I	I/R/A	I/R/A
	Networks		I	I/R/A
	Firewalls	I	I/R	I/R/A
	Software Updates		I	R/A
	Google SketchUp		I/A	R/A
	Securing Windows			I/A
Penetration Tester	WireShark			I/A
	Keystroke Loggers	I	R	R
	Social Engineering	I	R	R
	Privacy Settings for Social Networking Sites	I	R/A	A
	Alice		I/A	R/A
Penn Tester cont	HTTPS	I	R	R/A
	Packets Protocols and Ports			I/A

Cybersecurity Career	Content	Elementary MindTools	Middle School Jr CyberSTEM	High School CyberSTEM
		I-Introduce	R-Reinforce	A-Apply
Security Auditor	Vocabulary	I/R/A	I/R/A	I/R/A
	Hardware	I/R/A	I/R/A	I/R/A
	Software	I	I/R/A	I/R/A
	Networks		I	I/R/A
	Firewalls	I	I/R	I/R/A
	Software Updates		I	R/A
	Policy			I/A
	End User Education			I
	Wireless		I	R/A
Disaster Recovery Expert	Vocabulary	I/R/A	I/R/A	I/R/A
	Identifying Threats		I	R/A
	Identifying Assets		I	R/A
	Cost/ Benefit Analysis			I/A
	Making a Plan			I/A
	Testing the Plan			I/A
	Backups	I	R	R/A
	Excel Programming		I/A	R/A
Robotics Engineer	Vocabulary	I/A	I/R/A	I/R/A
	Real-world uses for robots	I	R	R
	Assemble the LEGO Mindstorms robot	I/A	R/A	R/A
	Introduction to Mindstorms sensors		I/A	R/A
	Introduction to Mindstorms NXT software	I/A	R/A	R/A
	Advanced commands of Mindstorms NXT software		I/A	R/A
Computer Crime Prosecutor	Vocabulary	I/A	I/R/A	I/R/A
	Copyright	I/R/A	I/R/A	I/R/A
	Identifying Scams		I	R/A
	Phishing and Pharming		I	R/A
	Identity Theft	I	R	R
	Strangers Online	I/R/A	I/R/A	I/R/A
	Social Networking Privacy Settings		I/A	R/A

Cybersecurity Career	Content	Elementary MindTools	Middle School Jr CyberSTEM	High School CyberSTEM
		I-Introduce R-Reinforce A-Apply		
	Court			I/A
Intelligence Analyst	Vocabulary	I/A	I/R/A	I/R/A
	Clearances	I	R	R
	Reconnaissance			I
	Social Engineering	I	R	R
	Fact or Fiction: Verifying Information Found on the Internet	I/A	R/A	R/A
	Responsible Use of YouTube	I/R/A	I/R/A	I/R/A

Recommended Content by Grade level

One Example Elementary School/ MindTools Fall

Meeting	Content
1	**Information Assurance Career:** Cryptographer **Activity:** Ice Breaker, Three Questions, Cryptography Vocabulary, Substitution Cipher; Caesar Cipher **C3 Connection:** Strong Passwords / Passphrases; Password Security
2	**Information Assurance Career:** Software Developer **Activity:** Directions/Unplugged, Facts about Syntax, Introduction to MicroWorlds (drawing shapes) **C3 Connection:** Digital Footprints
3	**Information Assurance Career:** Malware Analyst **Activity:,** Practicing MicroWorlds (Virus Eater Game) **C3 Connection:** Malware
4	**Information Assurance Career:** Malware Analyst **Activity:** Advanced MicroWorlds Commands (Conditional MicroWorlds operations and slider bars.) **C3 Connection:** Email Safety
5	**Information Assurance Career:** Security Auditor **Activity**: MicroWorlds Challenge: Create a picture, game, program or activity which teaches someone about Information Assurance topics. **C3 Connection:** Reinforcement of the past 4 weeks' careers and topics: cryptography, passwords, software developer, digital footprints, malware analyst, malware, incident responder, email safety
6	**Information Assurance Career:** Computer Crime Investigator **Activity:** Three Questions**,** Introduction to Scratch – Putting pieces together **C3 Connection:** Identity Theft
7	**Information Assurance Career**: Disaster Recovery Expert **Activity:** Scratch Challenge -- Create a picture, game, program or activity which teaches someone about Information Assurance topics. C3 Connection: Reinforcement of the past 4 weeks' careers and topics: cryptography, passwords, software developer, digital footprints, malware analyst, malware, incident responder, email safety, computer crime investigator, identity theft, disaster recovery expert, backing up **C3 Connection:** Back ups
8	**Information Assurance Career**: Intelligence Analyst **Activity:** Three Questions**,** Students should finish their MicroWorlds and Scratch challenge projects. If there is time, students should share their projects with one another. **C3 Connection:** Security Clearances
9	**Student Showcase**

One Example Elementary School/ MindTools Spring

Meeting	Content
1	**Information Assurance Career: Robotics – Locomotion** **Activity:** Ice Breaker**,** Three Questions**,** Introduce the parts of the LEGO Mindstorms kit, decide on rules for assuring that no parts are lost or broken **C3 Connection:** Gaming Safety

2	**Information Assurance Career: Robotics – Sensing** **Activity:** NetSmartz Internet Safety lesson Router's Birthday Surprise**,** Putting the Mindstorms kit together **C3 Connection:** Planning for safe Internet behaviors
3	**Information Assurance Career: Robotics – Actuation and Manipulation** **Activity:** Three Questions**,** Putting the Mindstorms kit together **C3 Connection:**
4	**Information Assurance Career: Robotics: Power Sources** **Activity:** Computer Hardware, putting the kit together, Introduce Mindstorms NXT software **C3 Connection:** Firewalls
5	**Information Assurance Career: Keeping law enforcement safe** **Robotics: Activity:** Three Questions**,** Mindstorms NXT software **C3 Connection:** Revealing too much
6	**Information Assurance Career: Robotics: Doing the heavy lifting – and the boring** **Activity:** Three Questions**,** Robotics Challenge – program your robot to make a shape. **C3 Connection:** Cyberbullying
7	**Information Assurance Career: Robotics: Exoskeletons** **Activity:** Discussion: Real World uses for Robots; Practice challenge for student showcase **C3 Connection:** Inappropriate content
8	**Student Showcase**
9	**Information Assurance Career: Robotics: Power Sources** **Activity:** Carefully disassembling the robot, **C3 Connection:** Protecting the environment: Proper disposal of technology

One Example Middle School/ Jr. CyberSTEM Fall

Meeting	Content
1	**Information Assurance Career:** Cryptographer **Activity:** Ice Breaker, Three Questions, Cryptography Vocabulary, Substitution Cipher; Caesar Cipher, letter frequency, steganography **C3 Connection: Protecting your identity**
2	**Information Assurance Career:** Software Developer **Activity:** Reminder about Syntax, Review Introductory commands to MicroWorlds, Review Advanced MicroWorlds Commands, MicroWorlds Challenge Create a picture, game, program or activity which teaches someone about Information Assurance topics. **C3 Connection:** Reputation Management
3	**Information Assurance Career:** Security Auditor **Activity:** Three Questions**,** Introduce Excel Programming **C3 Connection:** Home computer security check
4	**Information Assurance Career:** Computer Forensics **Activity:** Advanced Excel Programming **C3 Connection:** Email headers
5	**Information Assurance Career:** Penetration Tester **Activity:** Excel Challenge: Create a quiz or a crossword puzzle that teaches about cyberethics, cybersafety, and cybersecurity; or an Information Assurance job. **C3 Connection:** New Computer Checklist
6	**Information Assurance Career:** Computer Crime Investigator **Activity:** Three Questions**,** Speaker: Forensics Investigator, or Penetration tester **C3 Connection:** HTTPS
7	**Information Assurance Career**: Disaster Recovery Expert **Activity:** Review Scratch programming**,** Scratch Challenge -- Create a picture, game, program or activity which teaches someone about Information Assurance topics. **C3 Connection:** Threats to data
8	**Information Assurance Career**: Intelligence Analyst **Activity:** Three Questions**,** Students should finish their MicroWorlds, Excel and Scratch challenge projects. If there is time, students should share their projects with one another. **C3 Connection:** Security Clearances
9	**Student Showcase**

One Example Middle School/ Jr. CyberSTEM Spring

Meeting	Content
1	**Information Assurance Career: Robotics – Locomotion** **Activity:** Ice Breaker, Three Questions, Review the parts of the LEGO Mindstorms kit, decide on rules for assuring that no parts are lost or broken **C3 Connection:** Gaming Addiction
2	**Information Assurance Career: Robotics – Sensing** **Activity:** Putting the Mindstorms kit together **C3 Connection:** Webcams
3	**Information Assurance Career: Robotics – Actuation and Manipulation** **Activity:** NetSmartz Mike-Tosis - Texting, Putting the Mindstorms kit together **C3 Connection:** Texting
4	**Information Assurance Career: Robotics: Power Sources** **Activity:** Three Questions, Computer Hardware, putting the kit together, Introduce Mindstorms NXT software **C3 Connection:** Disposal of Technology: Protecting the environment and your data
5	**Information Assurance Career: Keeping law enforcement safe** **Robotics: Activity:** Three Questions, Mindstorms NXT software using sensors **C3 Connection:** Wireless Safety
6	**Information Assurance Career: Robotics: Doing the heavy lifting – and the boring** **Activity:** Three Questions, Robotics Challenge – program your robot to follow a line. **C3 Connection:** Spyware
7	**Information Assurance Career: Robotics: Exoskeletons** **Activity:** Discussion: Real World uses for Robots; Practice challenge for student showcase **C3 Connection:** Firewalls
8	**Student Showcase**
9	**Information Assurance Career: Robotics: Power Sources** **Activity:** Netsmartz: Beat the Tricks; Carefully disassemble the LEGO Mindstorms robots **C3 Connection:** Internet scams

One Example High School/ CyberSTEM Summer 3 Week
Based 6 hours a day
Week 1

Meeting	Content
1	Welcome & Logistics Overview of Information Assurance, Information Security, and Digital Forensics Video Snippets/ NSA & CyberWatch DVD Cybersecurity Video Introduction to Syntax Introduction to MicroWorlds for multimedia creation LOGO language: Differences between functional & imperative programming languages Lisp dialect Skill Development with MicroWorlds MicroWorlds Team Challenge: Create an Animated Story or Game Related to Cybersecurity
2	Identity Management : Digital Footprints/ Digital Fossils Reputation Management *****Guest Speaker-Security Clearances*** Advanced Microworlds: Conditional Statements, Creating animated graphics Team Challenges Continued: Work in teams and use advanced MicroWorlds skills to create an animated story or game related to cybersecurity or reputation management
3	*****Guest Speaker: Intrusion Detection and Prevention*** Programming with Excel Review Examples Mini Challenge: Reverse engineer an example and create a new game related to Cybersecurity Excel Challenge: Quiz or Crossword Puzzle
4	Ping and Tracerouting *****Guest Speaker: Forensics*** Digital Forensics using Wireshark, SANS toolkit, FTK Image Lite, or EnCase Digital Forensics: collecting, handling, reporting evidence Cell Phone forensics where available
5	*****Field Trip: Lazarus Foundation or*** Hardware Exploration using Hardware Kits Configuring a Virtual Networking using Cisco Packet Tracer Packets Protocols and Ports Show and Share MicroWorlds and Excel Challenge work

High School/ CyberWarrior Summer 3 Week
Based 6 hours a day
Week 2

6	***Guest Speaker: Disaster Recovery or Security Audits*** Disaster Recovery, Backing up Simulation/Game Development in Scratch Watch Sample projects Sprite Basics Creating your own Sprite Animating a Sprite Adding Sound Scratch Challenge: Create an animation, simulation, game, interactive project to teach someone about an IA/IS/Cybersecurity career or about cyberethics, cybersafety and cybersecurity.
7	Cryptography exercises ****Field Trip: NSA – National Cryptographic Museum and Career/Scholarship talk*** Paper Enigma Exercise https and Encryption ****Guest Speaker:* The Impact of Online Public Records on Identity Theft**
8	****Guest Speaker: Wireless Security*** Raptor Programming Introduction to Raptor: Program Structure, Statements/Symbols, Variables, Comments Raptor Programming Challenge: Create a program that prompts a user to input the diameter of the circle and output the area.
9	****Guest Speaker: CyberCrime*** Advanced Raptor Programming Advanced Raptor Programming: Loops Advanced Raptor Programming Challenge: Work in a team to design and build a Raptor program to create secure passwords or phases
10	****Field Trip: National Crimes Museum Trip*** Robotics Basics Assemble the LEGO Mindstorms Robotics Kits

One Example High School/ CyberSTEM Summer 3 Week
Based 6 hours a day
Week 3

11	****Guest Speaker: Secret Service*** Robotics Challenge Program the robot to use the sensors to stay within limited area while pushing cans out of this area Introduction to Python Programming: Basic Syntax, Hello world!, Data types, Operators, Flow Control, Functions
12	****Guest Speaker: Insecurities in Universal Plug and Play*** Python Programming: Using the Python Interpreter, editing a simple python program, creating python programs Python Challenge: Create a simple Python calculator
13	Python or Raptor Team Challenge: Work in a team to Design and implement a Python or Raptor program which teaches someone about cybersecurity or and information assurance job.
14	***Prepare for Student Showcase Day today:*** Complete any unfinished challenges Queue Excel, MicroWorlds, Scratch, Raptor and Python projects on computers **Student Showcase**
15	Carefully disassembly the LEGO Mindstorms robot NetSmartz videos: *Information Travels*, *Offline Consequences* and *Social Networking* Student Team Research: Student teams research and present a list of best practices one of the following topics: Social networking; New computer best practice; Reputation and identity management; Disaster prevention and recovery for home computers; Using copyrighted materials legally.

**** Field trips and Speakers are based on availability.**

Suggested tours for the Baltimore-Washington Metropolitan area include:

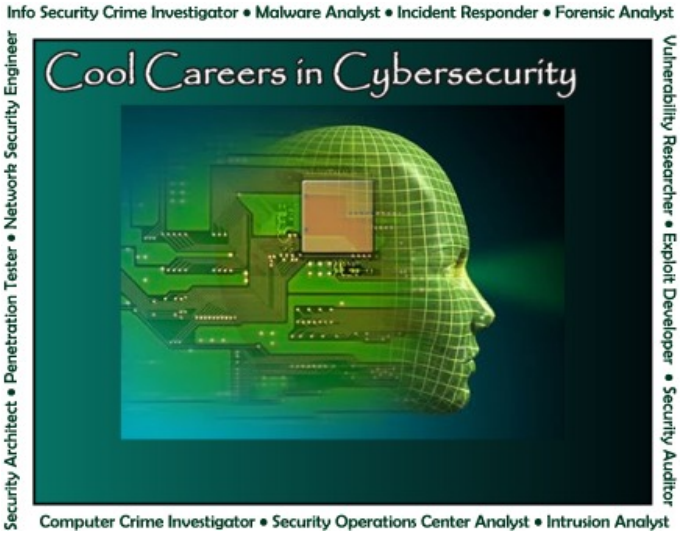
International Spy Museum http://www.spymuseum.org/
National Cryptologic Museum and NSA Career/Scholarship Talk
http://www.nsa.gov/about/cryptologic_heritage/museum/
National Electronics Museum http://www.nationalelectronicsmuseum.org/
National Museum of Crime and Punishment: http://www.crimemuseum.org/
The Lazarus Foundation: http://www.lazarus.org/

Suggested Speakers for the Cyber program include:

Security Clearances
Digital Forensics
Secret Service
Penetration Testing
Disaster Recovery
CyberCrime
Network Security and the Information Security CTE track
Security Audits
The impact of Online Public Records on Identity Theft
Social Engineering Techniques
Protection of Personally Identifiable Information
Updates and Patch Management
Insecurities in Universal Plug and Play
Operational Security
Careers in CyberSecurity
Incident Response
Intellectual Property Issues
Wireless Security
Intrusion Detection and Prevention

SECURE IT

Strategies to Encourage Careers in CyberSecurity and Information Technology



INTRODUCTION TO CYBERSECURITY

Envision the following two scenarios. It's a regular day in your middle school. The students have filed into the computer lab and have logged in. One computer doesn't seem to be connecting to the network, so the technology instructor works to re-establish the network connection. Meanwhile, a few students in the back of the room use a proxy server to check their social networking site and email. One student clicks on an attachment marked "Go Ravens" which is actually a Trojan. It pops up a pornographic website on his computer, and sends a similar message to every person in his contact list. Just then, the technology coordinator walks in to help with the network, sees the website, and tells the student to take off his headset and shut the monitor. "Not again" she thinks. Meanwhile, the principal comes in to

request an updated list of software installed on the school computers as the district has detected too many copies of a language learning program installed at the school. With only one technology teacher and one technology coordinator to help resolve the technology problems at the school, how will she manage to keep the school computers running, secure and virus free, software compliant, while also having to deal with the parent who is calling because her child received a text with a sexually explicit picture of another student at the school?

You've just sat down at your terminal at the Cyber Command. You look over your monitors showing status of various networks you are monitoring. All green. You check the main servers, and they show a process running you don't recognize. It has connected to one of the Department of Defense email servers and is transferring data outside the network. You shutdown the outgoing traffic, and lock down the server so it can't contaminate another server. You track its origin and it seems to have come from an outside server originating in a foreign country. I guess it looks like another interesting day. You sigh, alert your supervisor and settle down to tracking the source, and minimizing the damage from another hacker trying to penetrate the United States Department of Defense infrastructure.

While the above cases may seem extreme, both are typical in the day and life of personnel in the field of Information Assurance (IA). These scenarios present the reader with a potential conundrum related to both general citizenship awareness about cyberethics, safety and security and the growing need for a trained workforce in the IA, information systems and digital forensics field; often referred to as Cybersecurity. Unfortunately, few students know about the field and in many cases educators, parents, and career counselors are not informed of the career tracks available, requirements for and even what the jobs entail. Each session will allow students to learn more about the field of cybersecurity, and sharpen the skills required to do jobs in fast growing field.

For SECURE *IT*, we will refer to the various fields in this workforce area as Cybersecurity. Industry professionals confuse definitions of Cybersecurity and Information Assurance. In some, Cybersecurity focuses on the technical aspects of computer defense: the safety of computers and computer systems in a networked environment, while Information Assurance focuses on confidentiality, integrity, availability and validation of data, and therefore Cybersecurity is a subset of Information Assurance. However, others, particularly the Department of Defense, state that IA is a subset of Cybersecurity, and Cybersecurity includes management of the risks associated with computers and networks and mission assurance. SECURE IT does not concern itself with the subtleties of the differences; it lives in the intersection of the definitions.

Each session will allow students to learn more about the field of cybersecurity, and sharpen the skills required to do jobs in fast growing field.

Why cybersecurity?

It seems that everything relies on computers and the Internet now — communication (email, cell phones), entertainment (digital cable, mp3s), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards), medicine (equipment, medical records), and the list goes on. How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else's system?

Cybersecurity involves protecting that information by preventing, detecting, and responding to attacks. In the most general terms, it involves protecting data and communications, but fields which may not necessarily fit everyone's definition of cybersecurity may be involved. These include accounting, forensic science, law enforcement, bioengineering, intelligence, communications, management science, systems engineering, criminology, security engineering, computer science, and robotics. But why are these jobs important?

The Director of National Intelligence (DNI) recently testified before Congress, stating: "The growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures. The Intelligence Community assesses that a number of nations already have the technical capability to conduct such attacks" (Cyberspace Policy Review, 2009, p. 1) .The globally-interconnected digital information and communications infrastructure known as "cyberspace" underpins almost every facet of modern society and provides critical support for the US economy, civil infrastructure, public safety, and national security. Cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century. These challenges are captured in US Bureau of Labor Statistics (BLS) employment projections. Overall, the BLS estimates total US employment to increase by 10 percent from 2008 to 2018. However, cyber related jobs are expected to grow at significantly higher rates. The need for network systems and data communications analysts is expected to grow by 53.4%, and the need for computer software engineers is expected to grow by 34% over the same time period. The BLS attributes this growth to the increased need for workers with information security skills-the group which CW K12 targets. Overall, the BLS estimates computer and mathematical science occupations will grow by 22.2%. This parallels similar data for almost all STEM fields. Clearly, the available workforce is not growing with the demand.

Table 6 shares the US Department of Labor 2018 Employment Projections for the US. The largest growth changes are in: computer science/engineering, network systems, and home health career careers. However, note that the median annual wages for home health care is between $19-30,000.00 vs. $70,000-90,000 for technology related fields. Also note that income data is based on training no higher than a Bachelors degree. Income would increase with increased levels of training, certifications and degrees.

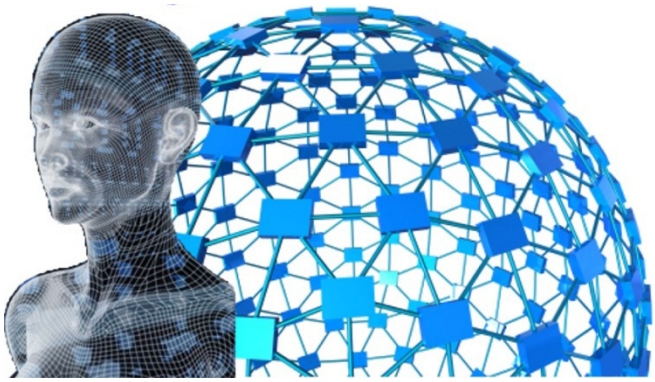
Table 1.6 Occupational Employment and Job Openings Data, 2008—18, and worker characteristics, 2008
(Numbers in thousands)

2008 National Employment Matrix title and code		Employment		Change, 2008-18		Job openings due to growth and replacement needs (in thousands)	Median annual wages	Median annual wage quartile	Most significant source of education and training category
		2008	2018	Number	Percent				
Financial examiners	13-2061	27.0	38.1	11.1	41.16	16.0	$70,930	VH	Bachelor's degree
Computer software engineers	15-1030	909.6	1,204.8	295.2	32.46	371.7	-	-	-
Computer software engineers, applications	15-1031	514.8	689.9	175.1	34.01	218.4	$85,430	VH	Bachelor's degree
Computer software engineers, systems software	15-1032	394.8	515.0	120.2	30.44	153.4	$92,430	VH	Bachelor's degree
Network systems and data communications analysts	15-1081	292.0	447.8	155.8	53.36	208.3	$71,100	VH	Bachelor's degree
Biomedical engineers	17-2031	16.0	27.6	11.6	72.02	14.9	$77,400	VH	Bachelor's degree
Environmental science and protection technicians, including health	19-4091	35.0	45.2	10.1	28.91	25.2	$40,230	H	Associate degree
Self-enrichment education teachers	25-3021	253.6	334.9	81.3	32.05	120.3	$35,720	H	related occupation
Physician assistants	29-1071	74.8	103.9	29.2	38.99	42.8	$81,230	VH	Master's degree
Surgical technologists	29-2055	91.5	114.7	23.2	25.32	46.3	$38,740	H	award
Veterinary technologists and technicians	29-2056	79.6	108.1	28.5	35.77	48.5	$28,900	L	Associate degree
Home health aides	31-1011	921.7	1,382.6	460.9	50.01	552.7	$20,460	VL	training
Dental assistants	31-9091	295.3	400.9	105.6	35.75	161.0	$32,380	L	training
Personal and home care aides	39-9021	817.2	1,193.0	375.8	45.99	477.8	$19,180	VL	training

Source: Employment Projections Program, U.S. Department of Labor, U.S. Bureau of Labor Statistics

Table 6: US Department of Labor, Occupational Employment and Job Openings from 2008-2018

GETTING STARTED



SECURE IT content is designed to introduce and reinforce the job skills necessary for students to experiment with cyber careers. The activities are hands-on and provide students the opportunity to explore and learn for themselves. In addition, there are several mini-activities that are completed each day which reinforce the goal of exploring Information Assurance while providing the instructor with an opportunity to assess students' understanding of the topic. For example, on the first day, these activities are: the Ice Breaker/"Storage Device" and "Three Questions"

In the Icebreaker/ "Storage Device" activity students are given a large 9X12 envelope. Students write their name on the envelope, they introduce themselves to each other using an alliterative adjective before their name and then justify the use of that adjective. This envelope becomes their storage device, a physical representation of a hard drive, for the duration of the activities because, we have found that students need a place to keep all the handouts and notes they take during the modules. At the end of the program, students have a resource to share with their parents or, to refer to when they use the software at home.

The "Three Questions" activity is a review and assessment tool that is used at the end of each meeting (or several meetings throughout the sessions). After the ice breaker on the first day, instructors will ask students to brainstorm the answer to three questions about Cybersecurity.

- What is the INFORMATION we are SECURING (protecting)?
- Who wants the INFORMATION?
- What kinds of jobs need to know about CYBERSECURITY?

Throughout the sessions, as the students learn more about the field of Cybersecurity, they will answer these three questions on sticky-notes. They will stick their answers to a poster with the corresponding question on it. As they post their responses they can read other students' responses

and remove the responses that they created but no longer believe is true. Students will use inductive reasoning to create a definition of Cybersecurity. Student responses can be used as a formative assessment during the instructional process to guide students to a more accurate definition for Cybersecurity. The last day students will discuss their theories and answer the questions together.

The activities in this document are organized in chapters according to topic. However, the sequence is determined by the instructor. Student interest and questions should drive the activities. In general, leading off with a general cyberethics, cybersafety, cybersecurity (C3) topic followed by a computational thinking activity is a way to maintain the connection between Cybersecurity and the fun activities. Student projects should always be focused on C3 and Cybersecurity to build knowledge and interest in these topics and fields.

Supporting materials are also provided to help the instructor facilitate the activities. Many of the activities have accompanying PowerPoint presentations and videos. Sample projects have been included for some of the computational thinking activities. We have also included a few videos for instructors to integrate into existing activities when there is time. These videos are included as resources for instructors who want to create their own activities directed to individual student interests.

Cybersecurity is an emerging and evolving field. This document will grow and change along with the skills and knowledge required to maintain general C3 awareness and grow the Cybersecurity career pipeline. Securing the national infrastructure is going to require a collaborative effort so, we encourage you to share your ideas and resources with us and the SECURE IT community so that we all can contribute to this important effort.

Introductory Ice Breaker and "Three Questions"

Ice Breaker

Objective

Students will learn each other's names and configure the envelope that they will use to store SECURE IT notes.

Materials

- One 9X12 envelope per Student
- Several chisel tipped markers

Activity

Give each student a large envelope. This will serve as the **hard drive of their computer**. The student's brains are the computer systems and this hard drive is part of their configuration.

- When talking about computers, "configuration" refers to the technical specifications of a computer. If someone asks about the configuration of your machine, they will want to know statistics about the processor speed, the amount of RAM, hard drive space, and the type of video card.
- In this case, the envelope is the storage device for the knowledge we are acquiring about Information Assurance.

Distribute large markers to the students and ask them to write their first name in very large letters on both sides of the envelope.

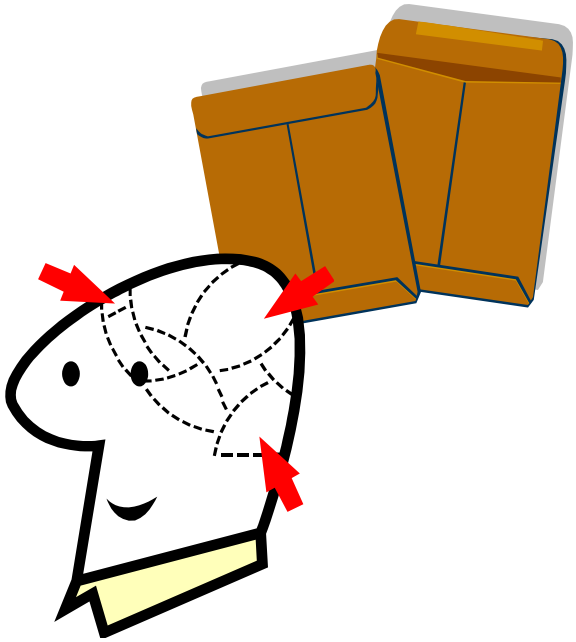
- **A student's name is their URI (Uniform Resource Identifier)**. A URI is a standard format that computers use to designate the name and location of a file or resource. A URI is a string of characters which represent the file name and may also have characters which represent the path to the directory of the file. If the URI contains the location it is called an absolute URI. An example of a URI is cyberwarrior.docx; and example of an absolute URI is documents/summerprograms/cyberwarrior.docx

Describe the envelope as the student's brand of hard drive. The slogan of the brand is an alliterative adjective that describes the student.

- Alliteration is a series of words that begins with the same letter or sound – as in Pathologically Perky Portia.

Have each student explain their choice of alliterative adjective.

- To help each student learn their fellow students' name, each student recalls the proceeding student's name and their adjective before they announce and explain their own.



"Three Questions"
Session Review and Assessment

Introducing Information Assurance

Students will use inductive methods to understand Information Assurance

Materials

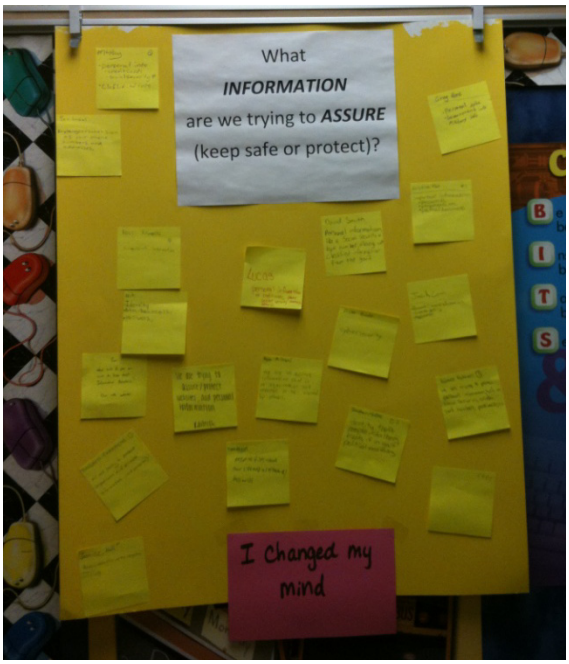
- Three sticky notes for each student
- Pencil or Pen
- Three posters: each with a different question at the top and a square of paper taped to the bottom with "I changed my mind"
    - What is the INFORMATION we are SECURING (protecting)?
    - Who wants the INFORMATION?
    - What kinds of jobs need to know about CYBERSECURITY?

Activity

Each session students learn more and more about the field of Cybersecurity. As they learn, they will build a working definition.

After the ice breaker on the first day, have the students answer three questions about Cybersecurity.

Throughout your sessions, as students learn more about the field of Cybersecurity, they will answer these three questions again.



Instruct students, as they put their current hypothesis on the on the board, they should read a few of the other ones posted and look for their past ideas. If they change their minds, that is ok. They can move the discarded hypothesis to the "I changed my mind card." **That is what inductive investigation is all about. As patterns start to emerge hypotheses are rejected.** Forensic scientists do this all the time as more evidence becomes available.

Distribute three sticky notes to each student, and ask them to label their notes “what”, “who”, and “jobs”

- Ask the students to write their response to the following question on the “what” note
    - What is the INFORMATION we are SECURING (protecting)?
- Ask the students to write their response to the following question on the “Who” note
    - Who wants the INFORMATION?
- Ask the students to write their response to the following question on the “Jobs” note
    - What kinds of jobs need to know about CYBERSECURITY?

Students should post their beginning hypothesis on the three posters. As this is an inductive activity, there is no further discussion required. Students will use the information throughout the sessions to sharpen their hypothesis about the three questions. The last day you will discuss their theories and answer the questions together.

Inductive reasoning requires looking for patterns in observations to generate tentative hypotheses which eventually we confirm to become a general conclusion or a theory.