NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CURRICULUM MODULES IN SUPPORT OF TABLETOP CYBERSECURITY GAMES

by

Jose Calderon Coria

September 2013

Thesis Co-Advisors: Mark Gondree
Zachary Peterson

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)* 18–7–2013	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From — To)* 2102-06-01—2104-10-31

4. TITLE AND SUBTITLE

Curriculum Modules in Support of Tabletop Cybersecurity Games

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Jose Calderon Coria

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Postgraduate School
Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

The National Science Foundation
4201 Wilson Blvd,
Arlington, VA 22230

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

14. ABSTRACT

The number of bachelor degrees in computer science has continued to decline over the past decade. These trends similarly affect cyber security sub-discipline of computer science. The non-digital computer security board game *[d0x3d!]* aims to teach cyber security concepts to a young, non-CS audience, to increase interest in the subject, and have a positive effect on computer science education. We develop curriculum modules in the form of lesson plans to complement this game. This demonstrates how the game can be used in an academic setting to scaffold instruction that introduces security concepts to K-12 audiences, more formally.

15. SUBJECT TERMS

Cyber Security Education, Lesson Plans, Digital Assets, Social Engineering, Hackers, Non-Digital Computer Security Games, Cyber Security Concepts

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified	UU	73	

THIS PAGE INTENTIONALLY LEFT BLANK

CURRICULUM MODULES IN SUPPORT OF TABLETOP CYBERSECURITY GAMES

Jose Calderon Coria
Civilian, Department of the Navy
B.S., University of California, Los Angeles, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2013

Author:	Jose Calderon Coria
Approved by:	Mark Gondree Thesis Co-Advisor
	Zachary Peterson Thesis Co-Advisor
	Peter Denning Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The number of bachelor degrees in computer science has continued to decline over the past decade. These trends similarly affect cyber security sub-discipline of computer science. The non-digital computer security board game *[d0x3d!]* aims to teach cyber security concepts to a young, non-CS audience, to increase interest in the subject, and have a positive effect on computer science education. We develop curriculum modules in the form of lesson plans to complement this game. This demonstrates how the game can be used in an academic setting to scaffold instruction that introduces security concepts to K-12 audiences, more formally.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgements

I would like to thank my thesis advisors Dr. Mark Gondree and Dr. Zachary Peterson for their guidance through this entire thesis. Their insight and expertise was invaluable in developing and completing this thesis. I would also like to thank the panel of teachers who took the time to read and give feedback on the lessons. Finally, a special thanks to Nicole, whose patience and support was steafast through this thesis.

Partial support for this work was provided by the National Science Foundation's CyberCorps®: Scholarship for Service (SFS) program under Award No. 0912048. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

As confirmed by a recent study by (ISC)^2 [2] , there is a global shortage of qualified information security professionals. While strong causation has not been shown, there is some evidence that traces this shortage in the United States back to high school education, where computer science is the only one of the Science, Technology, Engineering and Mathematics (STEM) fields that has experienced a decrease in student participation over the last 20 years, going from 25 percent of high schools to only 19% [3]. Similar data is seen in the number of students taking the AP Computer Science exam, where the Computer Science AB exam showed a decrease in the number of students taking the exam until it was discontinued in 2009, due to this disinterest [4,5]. Perhaps not surprisingly, similar trends have been seen in the production of CS bachelor's degrees [6]. The Bureau of Labor Statistics projects a growth of positions of 22 percent from 2010 to 2020 for information security analysts [7], which indicates the shortage of these jobs will only increase.

Creating a way to generate interest in STEM disciplines in high school could help to curtail the declining trend of non computer science majors. With an increase in students pursuing STEM fields, there would be more people qualified for a job in computer science, and computer security. An obstacle in this is that computer science courses are offered in so few high schools in the United States, with just 2,100 out of a total of over 42,000 high schools in the United States offering a AP computer science course in 2011 [8]. Part of this issue is that there just aren't enough qualified teachers to teach computer science [9], a problem which the CISE Directorate of the National Science Foundation (NSF) is planning to curtail via the CS 10K project [10]. The project will support the development new computer science high school curricula and also looks to prepare 10,000 teachers to teach that material in 10,000 high schools by 2015.

The question of how to provide broader access to computer science (specifically, to computer security concepts) in high school motivates our work. We have developed three lesson plans exploring different aspects in computer security, to be used in conjunction with *[d0x3d!]*, a board game with a network security narrative [11]. We have aligned these lesson plans with some of the common core standards, since this is what educators will primarily be using in their classrooms. We evaluate these proposed lesson plans using feedback from a cohort of local high school teachers. We believe this work is a modest step toward developing an ecosystem of tools that are accessible to teachers without a computer science background. We hope, through use, these tools may develop into instruments that become adopted by teachers, are supportive of existing curricular objectives, engage young students and inspire them to continued study. We leave evaluation of these instruments in the classroom as future work.

CHAPTER 2:
Background

2.1 Games in Computer Security Education

Previous work has attempted to leverage gameplay for computer security education and IA training. We review some notable examples.

Carnegie Mellon University's *Anti-Phishing Phil* [12] is an interactive game teaching patterns and practices to identify phishing attempts. A number of video games have been proposed in which students engage in focused lessons via simulation, while playing the role of a system administrator in a virtual world [13–16]. Microsoft's *Elevation of Privilege* is a card game in which players perform the threat modeling phase of the Microsoft Security Development Lifecycle, earning points by finding vulnerabilities in a software system [17].

The University of Washington's *Control-Alt-Hack* is a card game where players engage in missions as security consultants [18]. It is a competitive game intended for young audiences, based on Steve Jackson's *Ninja Burger*. The game is for sale in a limited print run. The game is intended to expose its audience to the breadth of technologies for which security is a concern, and the variety of professional opportunities in the field.

The game *[d0x3d!]* is a modular board game with a network security narrative, intended to introduce network security terminology, to engage students in security role playing, and to introduce the basic concepts of network attack and defense [19]. In the game, players assume the role of hackers, from whom some digital assets have been stolen. Players work collaboratively to infiltrate an adversarial network to reclaim these assets. The game materials are released online under a Creative Commons license. The game is inspired by Matt Leacock's *Forbidden Island*, published by Gamewright.

Each of these games demonstrates a broad interest in using games in the context of security education and IA training. To our knowledge, however, none of these games have accompanying lesson plans with learning objectives appropriate for curricular objectives at the secondary school level. We have selected *[d0x3d!]* as the context for our work, largely due to its low cost, relative simplicity and collaborative game play, all of which we believe make it attractive to integrate into a classroom.

2.2 Standards and Assessment

The Common Core State Standards (CCSS) were released in 2010, intended to bring states under a uniform set of curriculum standards. Of the 45 states currently planning to adopt these standards, most will have done so by 2015 [20]. The Common Core does not include a computer science content standard.

Mid-continent Research for Education and Learning (McRel) is a nonprofit education research and development organization that hosts a compendium of content standards and benchmarks for K-12 education [21]. Of particular note are the McRel standards for technology, which subsume previously proposed technology content standards such as those put forth by the International Technology Education Association and the International Society for Technology in Education. These standards cover various broad categories including technology and society, technology and ethics, technology communication tools and abilities needed in a technological world.

The College Board's Advanced Placement Computer Science course and exam are offered to high school students as an opportunity to earn college credit for a college-level computer science course [22]. The exam emphasizes object-oriented programming methodology, while emphasizing problem solving and algorithm development. With the discontinuation of the AP Computer Science AB exam, the current AP Computer Science A exam is undergoing revision [23]. Furthermore, there is a new AP Computer Science Principles exam being developed [24]. Due to their current state of modification, we decided not to map to AP computer science objectives.

2.3 Curriculum Modules for Security

A number of educational modules have been developed, related to computer security topics. *CS Unplugged* is a set of activities designed to introduce fundamental computer science principles without the use of computers [25, 26], including those on topics like public key encryption and cryptographic protocols. Syracuse University's SEED Project has developed instructional materials for hands-on lab activities to be used in undergraduate security curricula [27]. Towson University's Security Injections project has developed security-related activities that can be included into "core" computer science courses (operating systems, introductory programming) in undergraduate programs [28].

Capture the Flag (CTF) competitions are ubiquitous in the security industry. DEF CON and UC Santa Barbara hold annual CTF competitions [29, 30], and classes have been developed incorporating these type of games, as they utilize real hacking techniques and reinforce general computer security concepts. Chris Eagle of the Naval Postgraduate School argues it is appropriate to use these types of cyber exercises as early as high school, to attract students at an entry level into computer security [31].

2.4 Board Games for Education

The Academic Games League of America hosts a yearly national tournament on academic games, consisting of math games, social studies games, and language games [32]. This tournament is intended to spark an interest in math and logic for its participants, who range from elementary to high school students. Games For Thinkers is another organization that advocates the use of board games in order to teach math, logic scientific reasoning and language structure at deeper, more profound levels than traditional methods [33]. They publish a series of games, which they say can be integrated to meet standards and CORE curriculum. Games in Education hosts a yearly symposium which focuses on supplementing classroom material with video games to interest students in core curriculum topics [34].

Several researchers have observed that board game strategies are a useful context for exploring computer science concepts. Berland and Lee describe how complex computational thinking can develop spontaneously during board game play [35]. Bezáková et al. used digital simulations of board games in an introductory computer science course, noting board games are small, intuitive discrete systems that provide a rich context for discussing data structures, algorithms and other core topics [36]. They found that students were able to look beyond a “computer science is just programming” paradigm to, instead, appreciate that computer science included other interesting concepts, such as artificial intelligence and experimenting.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3:
Methodology and Design

Appreciating the value of digital data is a fundamental prerequisite to understanding why the field of computer security exists: the need to protect digital systems stems from the motivation that data has value. But, why do we value digital information? Do we value different data in different ways? Does how we value data change based on the situation or over time? What are the repercussions of having that data lost or stolen? These are important initial investigatory questions, the answers to which provide context for later understanding basic security requirements (confidentiality, integrity, availability) and the technical components implementing the systems that provide those properties. These reasons motivated our initial lesson on the value of digital assets, and its associated learning objectives.

Like the value of data, the concept of an adversary provides the necessary context for protecting digital systems. But, who are hackers? Do different hackers have different goals? Can "good guys" think or act like hackers? Information assurance policies are created with hackers in mind. As assets should be protected in a manner commensurate with their value and the environmental threats, understanding the motivations and resources of hackers is important for security planning. These motivated our lesson on the term "hacker," exploring hackers and their motivations.

In our final lesson, we bridge the gap between valued data and hacker threats in the context of exploits: actions by hackers that exploit system vulnerabilities to steal valuable data. Vulnerabilities in digital systems, however, tend to be highly technical and young students lack the prerequisite context to understand how the exploits are achieved. Thus, we focus on non-technical exploits that target the human component of a system: social engineering. We use this because it is an accessible lesson on exploits, and because it relevant and informs students how to better protect themselves and their data. For example, social engineering attacks suggest a trade-off between what information we share on social networks and the answers we choose for our password reset questions.

3.1 Outcomes and Requirements

We adopt an outcome based approach to designing our lesson learning objectives. Wiggins [37] discusses the importance of outcome based assessment with a few key ideas. Wiggins argues that assessment should “center on the purpose, not merely on the technique or tools, of assessment.” During learning, assessment is considered throughout, so as to facilitate student learning and teacher instruction. Another key point presented by Wiggins is that “assessment is central, not peripheral, to instruction.” The goals provided by the assessment help to shape the learning. The feedback received from these assessments also facilitates learning. “Assessment anchors teaching, and authentic tasks anchor assessment.” Having teachers perform genuine tasks gives students insight into how teachers use their knowledge. They can see that accomplishing tasks requires more than just drill work to develop discrete knowledge and skill. Wiggins writes that by taking an outcome based approach, students become effective in learning material, and are able to form, present, and defend opinions. These types of skills translate into performance in a realistic situation more effectively than rote memorization of concepts and regurgitation of ideas. Students will form personal ideas and have the ability to justify them.

It is important to us that lessons be accessible to teachers. A hurdle to this is that teachers may not have a computer science or security background. Without a background in the subjects, teachers may choose not to approach a lesson. Even if they decided to attempt the lesson, teachers may find difficulty with the language and the ideas presented without some experience in the area. Another obstacle to teacher receptiveness is lack of accessibility to technology. School districts in low socioeconomic status communities may not have access to computers and the Internet, either at school or at home. Terms and ideas referenced in the lessons may be foreign, making them difficult for someone to teach and for students to understand. To facilitate accessibility for teachers, we leveraged popular and familiar teaching methods. We presented instruction using the direct instruction methods. Project Follow Through, the world’s largest educational experiment, found that “no educational model has ever been documented to achieve such positive results with such consistency across so many variable sites as direct instruction.” [38].

We use direct instruction to facilitate teacher accessibility. In direct instruction, the teacher’s primary responsibility is to present the information. This flexible strategy and allows teachers to present information in a straightforward, organized manner. This will give teachers the ability to teach the subject comfortably, in a manner they feel is best suited for themselves, and the class. Direct instruction includes three main phases which are colloquially referred to as the “i do,” “we do,” “you do” phases. In the first phase of this model, the teacher spends time modeling new concepts. This progresses into a phase known as “guided practice,” where both the teacher and students are working together mastering the concept. Finally, the student independently works on the concept. This phase also gives the teacher an opportunity to see how well the students grasp the material. We incorporate these three phases throughout our lesson plans.

Cooperative learning strategies are used in the lesson plans to help teachers lead group discussion and partner assignments. Cooperative learning strategies have been suggested as a means to introduce higher level skills into the curriculum [39]. They also ensure students an adequate level of basic skills and give students the collaborative skills necessary in an increasingly interdependent society. Furthermore, cooperative learning strategies are necessary to implement Common Core State Standards [40]. By creating these assignments with collaboration in mind, students should have a better grasp on the subject being covered.

It is important that the lesson plans "fit" into the classroom. The fact that some schools have severe funding constraints imposes a barrier to adoption and obstacles to fitting them into the classroom. As a response, our lessons and materials are publicly available at no cost, and utilize materials that can already be found in most classrooms. In particular, the lesson plans do not require actual use of a computer to complete. Activities throughout the lesson plans are focused on analysis and discussion; we try to eliminate the need for technology to teach the subject, despite the topics being themselves technical. News articles can be printed and copied to introduce them to students, removing the need for the Internet to read lesson materials. By avoiding expensive tools to teach concepts, we've removed a financial barrier in using these lesson plans. A lack of time and support in the classroom force teachers to prioritize objectives aligned with educational standards. Thus, our lesson plans are aligned to standards. This also allows the lesson plans to be taught in non-computer science or security classes, since they will align with the curriculum via standards.

3.1.1 Defining Learning Objectives

We employ Bloom's Taxonomy to craft learning objectives. Bloom's Taxonomy is supported by research which strongly suggests that successful academic achievement and lifelong learning depend on a student's ability to effectively use language to analyze, synthesize, and evaluate. [41]. Bloom's Taxonomy gives language for target outcomes [42] and is widely employed [43–52]. Bloom's Taxonomy describes six levels of cognitive learning, with language associated with each level. The levels are described in Figure 3.1.

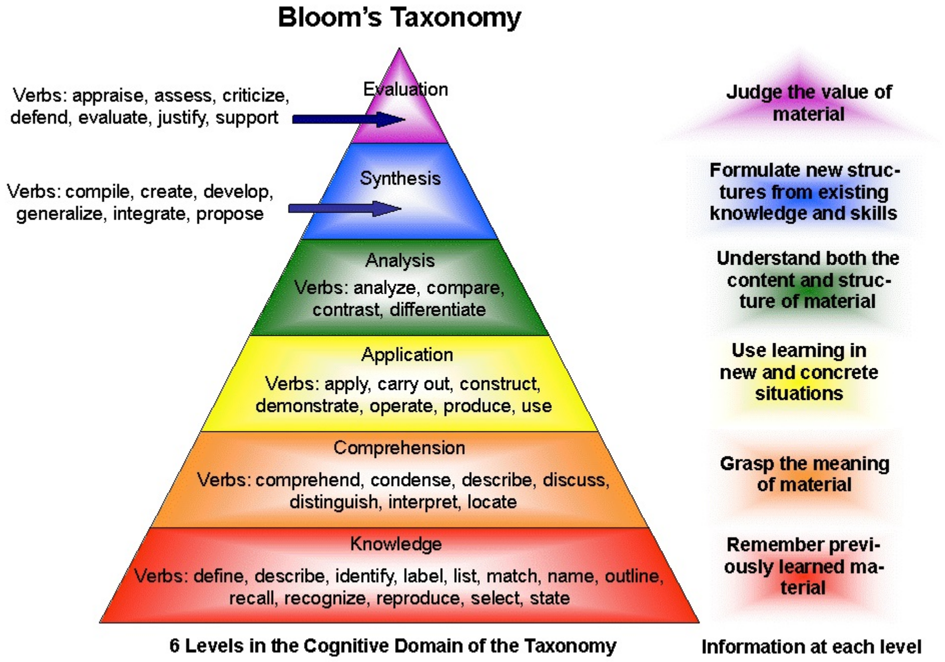

Bloom's Taxonomy
Verbs: appraise, assess, criticize, defend, evaluate, justify, support
Evaluation
Verbs: compile, create, develop, generalize, integrate, propose
Synthesis
Analysis
Verbs: analyze, compare, contrast, differentiate
Application
Verbs: apply, carry out, construct, demonstrate, operate, produce, use
Comprehension
Verbs: comprehend, condense, describe, discuss, distinguish, interpret, locate
Knowledge
Verbs: define, describe, identify, label, list, match, name, outline, recall, recognize, reproduce, select, state
Judge the value of material
Formulate new structures from existing knowledge and skills
Understand both the content and structure of material
Use learning in new and concrete situations
Grasp the meaning of material
Remember previously learned material
6 Levels in the Cognitive Domain of the Taxonomy
Information at each level

Figure 3.1: Bloom's Taxonomy(From [1])

The verbs within the levels are used to appropriately describe the objectives for each lesson. They can be seen in Table 3.1.

Lesson	Objectives (Bloom Level in parentheses)
Introduction to Digital Assets	1. Student will be able to define what a digital asset is, generically. (Knowledge) 2. Students will be able to describe some characteristics of the four types of digital assets present in the game *[d0x3d!]*. (Comprehension) 3. Students will be able to give some examples of digital assets in their own lives. (Application) 4. Students will be able to describe and compare scenarios where digital assets have been compromised, in terms of potential effects or damages in the real world. (Analysis)
Who Are Hackers?	1. Students will be able to define the terms black-hat hacker, white-hat hacker, and gray-hat hacker. (Knowledge) 2. Students will be able to distinguish among types of hackers based on their motivations and actions. (Application) 3. Students will be able to discuss different perspectives related to a court case about hacking, and use evidence to defend a position. (Evaluation)
Introduction to Social Engineering	1. Student will define what social engineering is. (Knowledge) 2. Students will illustrate how social engineers gain information to carry out their hacks. (Comprehension) 3. Students will research information to gain access to "hack" simulated e-mail accounts. (Analysis) 4. Students will evaluate the strength of their peers' password reset questions. (Evaluation)

Table 3.1: Lessons and Objectives

We use differentiated learning objectives because it's important for engaging students at different cognitive levels. This is demonstrated as effective, generally [53] and in computer science specifically by Lister and Leaney [54]. Differentiated learning objectives allow the strongest students to be challenged, while allowing struggling students to meet tasks that relate to lower levels of Bloom's Taxonomy. We create different objectives, using language found in Bloom's Taxonomy, to craft them in a manner that will engage different students at different levels. This helps make the lesson accessible to students at different stages of cognition in the material.

3.1.2 Design and Structure

We structure our lesson plans leveraging Dr. Madeline Hunter's Instructional Theory into Practice (ITIP) model for direct instruction. There are other ways [55] to present instruction, but they are less common and we believed Hunter's template matched a methodology that teachers found more comfortable. We will investigate this belief further in Section 5.1.

The template for our lesson plan has the following structure: Introduction, Summary, Objectives, Standards, Assumed Student Prior Knowledge, Materials, Vocabulary, Background for Teacher, Engage, Activity, Discussion, Check for Understanding, Assessment, Extension Activities. The Objectives, Materials, Check for Understanding and Assessment are borrowed from Madeline Hunter's template. The Discussion section takes ideas from cooperative learning strategies. The Engage portion of the lesson plan borrows elements from the Engage and Explore stages of the learning cycle model [56].

Different sections in each lesson plan have different purposes. The Background for Teacher is included to have the lesson be accessible to teachers. The Engage portion intends to pique the student's interest and establish the topic to be covered. By having a section dedicated to capturing their interest, there is a better opportunity for student participation. There are also student-facilitated questioning to begin constructing knowledge on the topic. This is an example of direct instruction to facilitate learning. The tools are given to students to begin understanding the material, with the expectation that they will able to take additional steps with less direction. The Activity section is part of the "We Do" portion of direct instruction. The teacher provides partial modeling for the activity. The students are able to see how the activity can be completed, and then feel comfortable enough to do it on their own. For more difficult concepts, more time is spent in this phase. The Discussion portion aims to have students engaged and learning from each other. We incorporate media articles and a video into class discussions. By creating these assignments with collaboration in mind, students have a better grasp on the subject being covered. The Check for Understanding section is an informal assessment or the teacher to ensure the students understand the material. If the teacher notices students are not grasping concepts, more time can be spent in this section. The Assessment section gives the students the opportunity to independently work on the concepts. This is part of the "You Do" portion of direct instruction. As the name implies, this also gives the teacher a chance to see how well students are grasping the material. The Extension Activities was a special section added to go further into the subject material, in a way that might be normally permissible due to time constraints in the classroom, or student disinterest. For this reason, the activities in this section are optional. All these sections are meant to work cohesively to facilitate teacher, and student, understanding.

3.1.3 Aligning with Standards

We align our learning objectives with the Common Core State Standards (CCSS), as well as standards from Mid-continent Research for Education and Learning (McRel). The CCSS will be adopted by 45 states by 2015 [20]. Districts are currently working towards creating curriculum that includes these standards. By aligning the lesson plans with these standards, the lesson plans will be relevant in most states. The McRel standards for Technology were released in 2000. Their popularity is not as widespread as the CCSS, and some of their content is subscription based.

Properties of the standards we used in the lesson plans help us align to those standards. The CCSS has Literacy standards. These literacy standards have students write arguments to support claims, or work with peers to have discussion. These skills are useful for teaching computer security lessons. We can present information in the form or articles or data and have students work together to analyze them, which aligns with those standards. McRel contains Technology standards that deal with the impact of the Internet on society. Lessons where we discuss the impact of digital assets or hacking in the context of the Internet directly relate to this standard. Another standard that was useful for us to map to was one asking students to use technology to produce and publish writing and to interact and collaborate with others. Access permitting, students can complete activities throughout the lesson plans via a computer and the Internet. The standards provide properties which helps up align them to topics that synergize, and can be used in different domains.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4:
Developing Computer Security Lesson Plans

In this chapter, we summarize the choices made during the creation of each lesson, as well as our motivations for selecting specific topics, activities and discussion questions. Additionally, we discuss lesson assessments and the extension activities.

4.1 Digital Assets

The first lesson explores different types of digital assets in daily life. Living in a digital age, this topic is relatable to high school students. By realizing the value of personal assets, students can make the connection on a global scale - i.e. a compromise of national security data.

The lesson opens with the teacher engaging student interest by posing discussion questions regarding personal data. Relating the topic to students' everyday life motivates learning. We wanted students to care about the topic. After students become "hooked," the teacher leads students to categorize the types of digital assets. As a class or in groups, students discuss the similarities of what encompasses each of the categorizes, such as "financial data." This discussion on classifying data assets serves two purposes: students use higher cognitive skills by justifying where each asset belongs. Additionally, by having students generate examples of each category, they become more likely to internalize the information. In the lesson plan, we include a list of examples to guide the teacher. However, the lesson notes that this is a flexible list that may include overlapping.

After students have internalized the value of personal digital assets, the Discussion portion asks students to analyze digital assets on a national scale. We include a 2011 Data Breach Investigations Report by the US Secret Service and Verizon [57] to prompt a class discussion. Many of these discussion questions require accessing higher levels of Bloom's Taxonomy and may need to be scaffolded for student understanding based on student needs. Students can see that there are some digital assets that are at greater risk of being compromised. Through this discussion, the teacher introduces the subject of risk management - higher risk data may need additional protection. The cost of protection should commensurate with both the risk of the digital asset as well as its value.

As a conclusion to the lesson, the teacher measures student learning through a complex assessment task. We include a “bank” of articles to illustrate the many examples and effects of stolen digital assets. Essentially, the assessment calls for students to define which digital assets are being compromised and discuss the possible ramifications. We have scaffolded the questions as a way to differentiate the assignment based on abilities. Teachers may also choose to make adjustments to the the assignment as needed, such as limiting the article selection.

We have also added Extension Activities for teachers and students to explore the subject further. Some of the activities require additional research time, such as interviewing a victim of digital asset theft. Personal Narrative activity explores the effects of personal data being compromised. A narrative about a stolen Facebook password would work well for this activity. Students may closely relate with this activity, but aspects may not be appropriate for class discussion.

We intended for the Digital Assets lesson to be relatable to students. Our expectation is that students will understand the value of digital assets and realize the necessity to protect them.

The Introduction to Digital Assets lesson is included in Appendix A.

4.2 Who Are Hackers?

The second lesson explores the societal definition of hacker versus a professional computer security hacker. We assume high school students’ prior knowledge extends to the media’s coverage of hackers. Students will learn the types of hackers and their motivations for hacking.

The lesson opens with the teacher introducing the court case Massachusetts Bay Transportation Authority v. Anderson. We chose this case as an introduction to the lesson because young college students in an academic setting would be a relatable situation for the students. Purposefully, we chose not to include the outcome of the case until the closure of the assignment as a way to measure if opinions on hackers changed. Based on the information presented, we pose discussion questions that would stimulate discussion on the motivations of the hackers. Additionally, we scaffold the discussion questions with the lower cognitive questions being addressed first. Based on student needs, teachers may need to ask even more leading questions such as “Could a hacker think what they are doing is benefiting society?” The aim is for students to think critically about the motivation of a hacker.

The main activity in the lesson centers around the TED Talk video, Hire the Hacker, by journalist Misha Glenny [58]. TED Talks videos serve as a free, entertaining resource to supplement lecture from an industry insider. Hire the Hacker begins with a highly fascinating clip from

“Anonymous.” The video briefly discusses corporations that have been recent victims of hacking and the need to reach out professionally to hackers. While some components of the video may be higher level for all students, the teacher may adapt the lesson by preteaching relevant vocabulary in the video or assign the video for homework assignment. The corresponding assignment asks students to summarize, apply vocabulary, and construct a counter argument against Glenny’s position. We don’t specify whether this should be done in discussion or written form as it is up to the discretion of the teacher and abilities of the students.

After students develop an understanding of the types of hackers, the assessment focuses on the discussion from the Engagement section. The lesson plan includes two articles with competing perspectives relating to the court case. Returning to the court case provides closure to the lesson as well as gives students an opportunity to revisit their initial opinion on hacking. Asking students to metacognitively explain their thought-process is intended to help students become self-regulated learners. The lesson gives students a purpose for reading. We wrote the language somewhat ambiguous in order to give the teacher flexibility. Perhaps, the teacher may choose to split the class into two groups and assign an article to each. Students may write and present their findings to the class or instead discuss it with a partner. We intentionally left room for the teacher to make decisions based on the needs of the class. Additionally, we wrote the discussion questions to align with Bloom’s Taxonomy as a way to differentiate learning.

We also include the Extension Activities as supplemental material. For this particular lesson, we felt each of the four activities would be effective and engaging for students, but aren’t necessary to the central topic of hacking. For instance, students could conduct a mock trial of the MBTA v. Anderson court case; however, much preparation and time would be needed. Similarly, students could research the Anonymous hacking group or read an interview with an ex-hacker, but aren’t necessary to understanding the motivations of hacking. Likewise, the Policy Essay assignment requires higher cognitive and writing skills. It is geared towards the Gifted and Talented Education (GATE) students. With the extension activities, we intended the lesson to contain room for adaptations or to expand the topic of hackers based on students’ needs and interests.

We created this lesson with the outcome that that students will understand the diverse motivations of hackers and develop a deeper understanding of the definition of hacker.

The Who are Hackers? lesson is included in Appendix C.

4.3 Social Engineering

The final lesson explores an attack a malicious hacker might use, known as Social Engineering. While students may be unfamiliar with the vocabulary associated with this subject, we assume students have heard of cases where email and social media accounts have been "hacked." In this lesson, students will learn the attack tactics of social engineers. Furthermore, students will relate the learning to their own personal online use.

The lesson begins with a case study regarding how a young hacker infiltrated 2008 Vice President candidate Sarah Palin's email. This case has become an infamous example of social engineering because it shows the ease in obtaining a password through reset options. Additionally, this case illustrates how even a vice-presidential candidate is vulnerable to this type of hack. Similarly, it lends itself to the main activity in which students will be obtaining passwords through reset questions. We provide a summary of how the attack worked, as well as a web link to a media article. The teacher is given the liberty to make a decision on how much information to provide to the students and how deeply to explore the topic.

The central activity in this lesson allows students to take on the role of a social engineering hacker by recovering faux email accounts of historical figures based on readily available information. Teachers may decide to use figures related to the time period being studied or use the handouts we have provide. This flexibility in choosing figures is also helpful in applying this lesson to different subjects, for example in an English or History class. The handouts are designed in a format that is easy to replicate, but available to copy. We use real world examples to provide motivation for students - an answer to the question, "Why do we need to know this?"

After much guided practice and discussion, the Assessment asks students to analyze the Activity. The teacher poses tiered Discussion questions based on Bloom's Taxonomy. After ample discussion time, the teacher poses a Kevin Mitnick quote which states, in summary, that humans are the greatest weakness in any computer system. For both assessment pieces, the teacher has the flexibility to assign this as a journal response, an essay, or a partner activity. Students must summarize and then evaluate Mitnick's position using evidence from the class discussions and activities. We chose this as our assessment because it illustrates how powerful these simple attacks are, yet may be relevant in the social media lives of teenagers.

We also include the Extension Activities so that teachers can explore the subject of social engineering further. The Social Engineering Role Play is a creative way for students to showcase their learning. Additionally, “Creating” is a higher Bloom’s Taxonomy domain. We chose not to add it to the main lesson as students may not have access to “movie making” technology and the activity may take up too much class time.

Our purpose for creating this lesson is to illustrate that while social engineering hacks require little technical knowledge, they can produce damaging results. After this lesson, we expect students to realize the importance of a strong password reset question, as well as understand how threats to digital data can manifest in their lives.

The Introduction to Social Engineering lesson is included in Appendix B.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5:
Evaluation

To evaluate the lesson plans created, we enlisted a cohort of local high school teachers and educators to review the lesson plans and provide feedback. The six teachers represent a variety of educational experiences, both in terms of length and breadth. We refer to our evaluators using nicknames (A, B, C, D, F, G), decorated with their current subject areas. AE, who has taught for 4 years, is a freshman English teacher. She is also part of the technology team at her site. She has a masters in teaching and teacher education. Currently, AE teaches at a public high school with 96% Hispanic population in a lower economic neighborhood. BEH teaches English and U.S. History. She is GATE certified and a National Board Certification candidate. She has been teaching for 7 years and holds a masters in education. Presently, she teaches at a STEM-focused public high school. CEB teaches senior English and Biology, and has a masters in instructional technology. She also has experience working for Educational Testing Services as both a curriculum writer and test developer. CEB has over 35 years of educational experience. FE teaches freshmen English and language arts development. She has a masters degree in education with an emphasis in cross cultural education. She has been teaching for 5 years. GP teaches Psychology to juniors, seniors, and college freshmen and has a masters in education. She has been teaching for 20 years. CEB, FE, and GP teach at a public high school with a diverse student population. DA is currently a school administrator with a masters degree in education. She has been working in the field of education for 35 years. Currently, she is a principal at a public school with 40% English language learners and a lower middle class population.

We gave each of our evaluators the lessons plans, a copy of *[d0x3d!]*, and a list of topics and questions to consider while reviewing the lessons. Each evaluator was allowed a month to review these materials. Then we met with each to gather feedback. We were primarily interested in feedback regarding whether students would be able to understand the concepts found in the lessons. We also wanted feedback on whether teachers thought the material would be interesting to students. Additionally, we wanted responses on whether we had provided enough background material and appropriate activities throughout the lessons so that teachers felt they could be effective at teaching these new subjects. These were the primary concerns we had about the lesson plans after they were completed.

5.1 Feedback

Overall, the evaluators felt that the material would be accessible to students and they would be successful completing the assignments. Several teachers, however, believed that some students might struggle with certain aspects of the lessons, needing more time than indicated. BEH felt lower-performing students would need time for vocabulary scaffolding and homework. AE felt many of her students would need more time with processing the material, as they are from an English Learner population. Despite this, AE felt the lessons were sufficiently broken down that they could be effectively taught. All evaluators thought that the lessons would take longer than indicated. Specifically, BEH and FE estimated that each lesson would take 3 class periods; AE, CEB, and MP thought that each lesson may take 4 class periods; and DA estimated that it may take up to 5 days per lesson. These comments generally reflect the opinion that these lessons are accessible to high school students, and that the expected timeframe for each lesson should be around four 50 minute sessions.

The teachers expressed that the students' background knowledge and personal computers use relates to the amount of time needed to teach the lesson. BEH's school has many classes that use computers, including robotics, architecture, digital imagery, and computer programming (Scratch). Their daily technology use would provide them with an advantage in the assumed student prior knowledge. This contrasts strongly with AE's experience. Many of AE's students have trouble with their typing skills. Not only that, but her students have limited access to computers at school, and even at home, so access to technology may be a barrier to students contextualizing the lesson and understanding the concepts. This would impact both the amount of time taken to teach the lesson, as well as students' ability to understand the material.

The evaluators believed the material would be interesting to students. DA wrote that the variety of activities were meaningful, relevant, and fun for high school students, and gave students multiple ways of understanding the concepts. An interesting point was brought up by AE, who thought her students would not know who 2008 vice president Sarah Palin was, and suggested the Engage section be revised to include a sentence relating it to students' own password usage. By relating it to their own experiences, the students would become more engaged and the lesson more effective. FE felt that the social engineering lesson would be particularly engaging for students. The activity where the students attempt to hack the email password reset feature of a historical figure would be particularly enjoyable. FE's colleague, CEB, said that her English and Biology students would find the lessons appropriate, except for "perhaps 1% of students," who she thought already would know a lot of these things. CEB explained that she has some students who freely admit to "hacking," and would not be engaged by this material. As the lesson plans are written as introductory lessons, this feedback is justifiable.

All teachers felt they would be able to deliver the material to students based on the background for teacher section and the lessons themselves. FE commented that she found the background for teacher section very interesting, learning a lot herself that caused her to do additional reading on her own. She also liked that the lesson plans were written in such a way that she could apply a Gradual Release of Responsibility model, which was unintended but a side effect of organizing the lesson plans using direct instruction. The amount of articles provided to chose from was also a strong point, she felt, that would help her to teach the concepts with writing assignments. DA thought the lessons gave teachers a framework with resources that would make teachings these lessons feasible. While reviewing the lessons, she looked for additional teaching practices to incorporate, but found that almost all had been incorporated. This was encouraging, as other educators should pick up on that as well. BEH mentioned that her content areas of English and U.S. History would not directly align with the objectives of the lessons; however, by mapping the lesson plans to CCSS standards, she believed that they could make it fit with the curriculum.

Generally, the cohort viewed the lessons favorably. The lesson plans would be accessible to students but require more time to complete than we anticipated. The teachers also felt the plans were interesting, easy to follow, and clearly written. In fact, three evaluators asked permissions to use the lesson plans in the future. FE commented that she would be using the Social Engineering lesson plan in the her english class next year. AE wanted to use all three plans, particularly because she broke the lesson plans into four days of instruction. Her district's new benchmarks, which are slated to be implemented next year, were also built on four day modules. The next step would be to have the lessons be used in a classroom setting, which we leave as future work.

THIS PAGE INTENTIONALLY LEFT BLANK

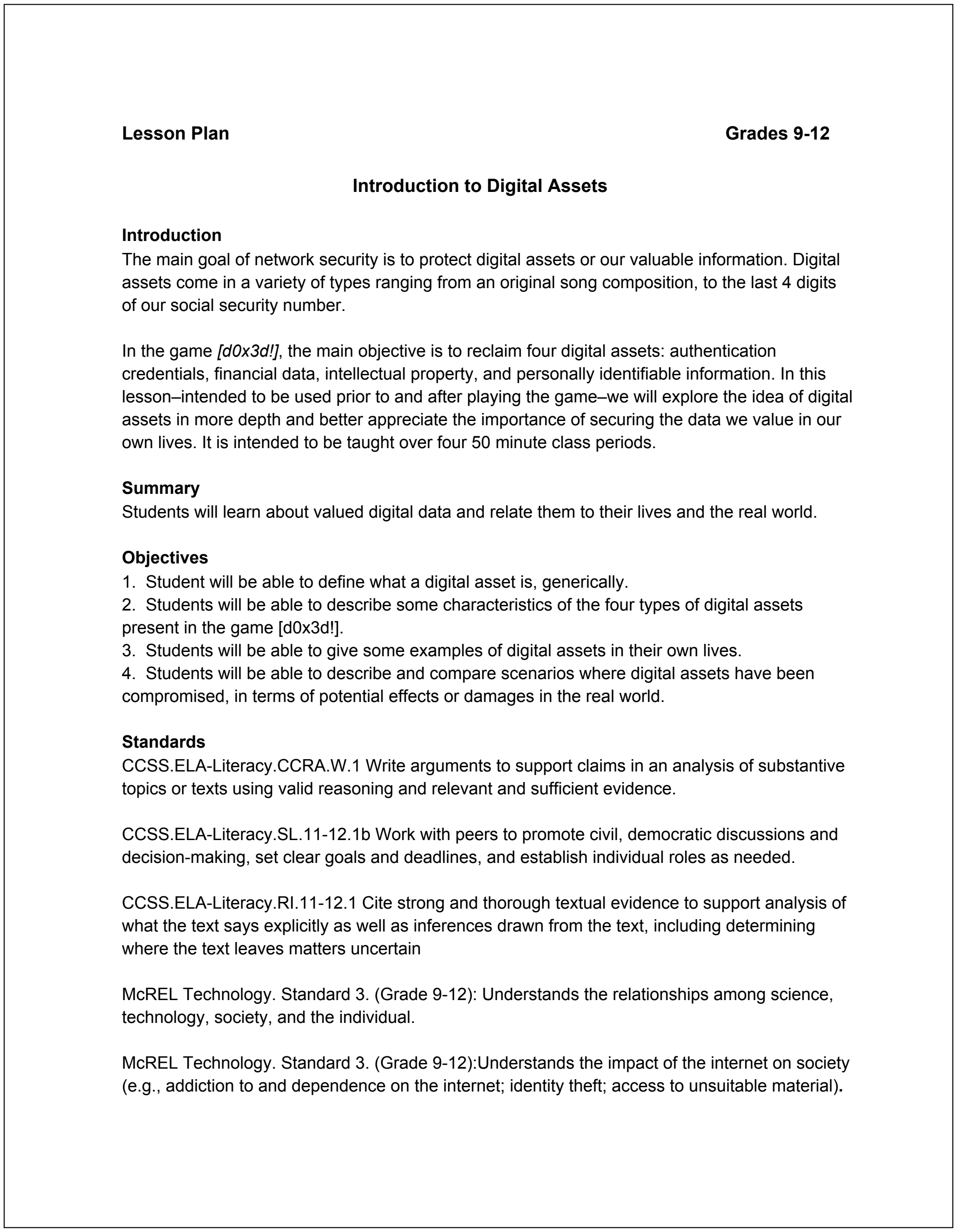
CHAPTER 6:
Conclusion and Future Work

This work has made a modest contribution to addressing a national need for computer security professionals, by developing tools for engaging and educating students early in their careers. These tools take the form of lesson plans, the topics for which were motivated by those significant questions foundational to computer security that we believed would be understandable and engaging to a high school age group. The culmination of our work are three lesson plans: Introduction to Digital Assets, Who are Hackers?, and Introduction to Social Engineering. These lesson plans may be presented as individual lessons, or as a three lesson module on computer security. The lesson plans have explicit learning objectives, have been mapped to standards, borrow design and structure from established pedagogical best practice, and do not rely on any significant use of classroom technology (i.e., can be adopted by schools in low SES communities). Our lessons were assessed by a panel of evaluators with experience in teaching our target age group. The evaluators opined our lessons could be implemented in a classroom setting with our target age group, with little modification. All evaluators felt they would be able to deliver the material to students based on the lesson's background sections and the lessons themselves. In fact, many evaluators wanted to use the lessons the following year in their own classrooms.

While our evaluator feedback is positive evidence suggesting that the lesson plans may have the appropriate form and content for our target group, evaluation of the lessons in a classroom context is required. Specific qualities to assess include validating that students are meeting the lesson's learning objectives, are engaged by the material, and to see how many students without previous interest in security have become interested in learning more about the topic. How to appropriately gather this feedback would likely require partnership with an educational evaluator and appropriate study design. Additional future work includes developing sample grading rubrics, to assist teachers in implementing the assessments for lessons. Also, our three lessons could be used as working models to write additional lesson plans on computer security. Example lessons that may be particularly appealing are lessons related to the other "hacker" characters in the game *[d0x3d!]*, lessons about computer security ethics and responsible disclose. We leave pursuing these ideas as future work.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A. Introduction to Digital Assets



Lesson Plan **Grades 9-12**

Introduction to Digital Assets

Introduction
The main goal of network security is to protect digital assets or our valuable information. Digital assets come in a variety of types ranging from an original song composition, to the last 4 digits of our social security number.

In the game *[d0x3d!]*, the main objective is to reclaim four digital assets: authentication credentials, financial data, intellectual property, and personally identifiable information. In this lesson–intended to be used prior to and after playing the game–we will explore the idea of digital assets in more depth and better appreciate the importance of securing the data we value in our own lives. It is intended to be taught over four 50 minute class periods.

Summary
Students will learn about valued digital data and relate them to their lives and the real world.

Objectives
1. Student will be able to define what a digital asset is, generically.
2. Students will be able to describe some characteristics of the four types of digital assets present in the game [d0x3d!].
3. Students will be able to give some examples of digital assets in their own lives.
4. Students will be able to describe and compare scenarios where digital assets have been compromised, in terms of potential effects or damages in the real world.

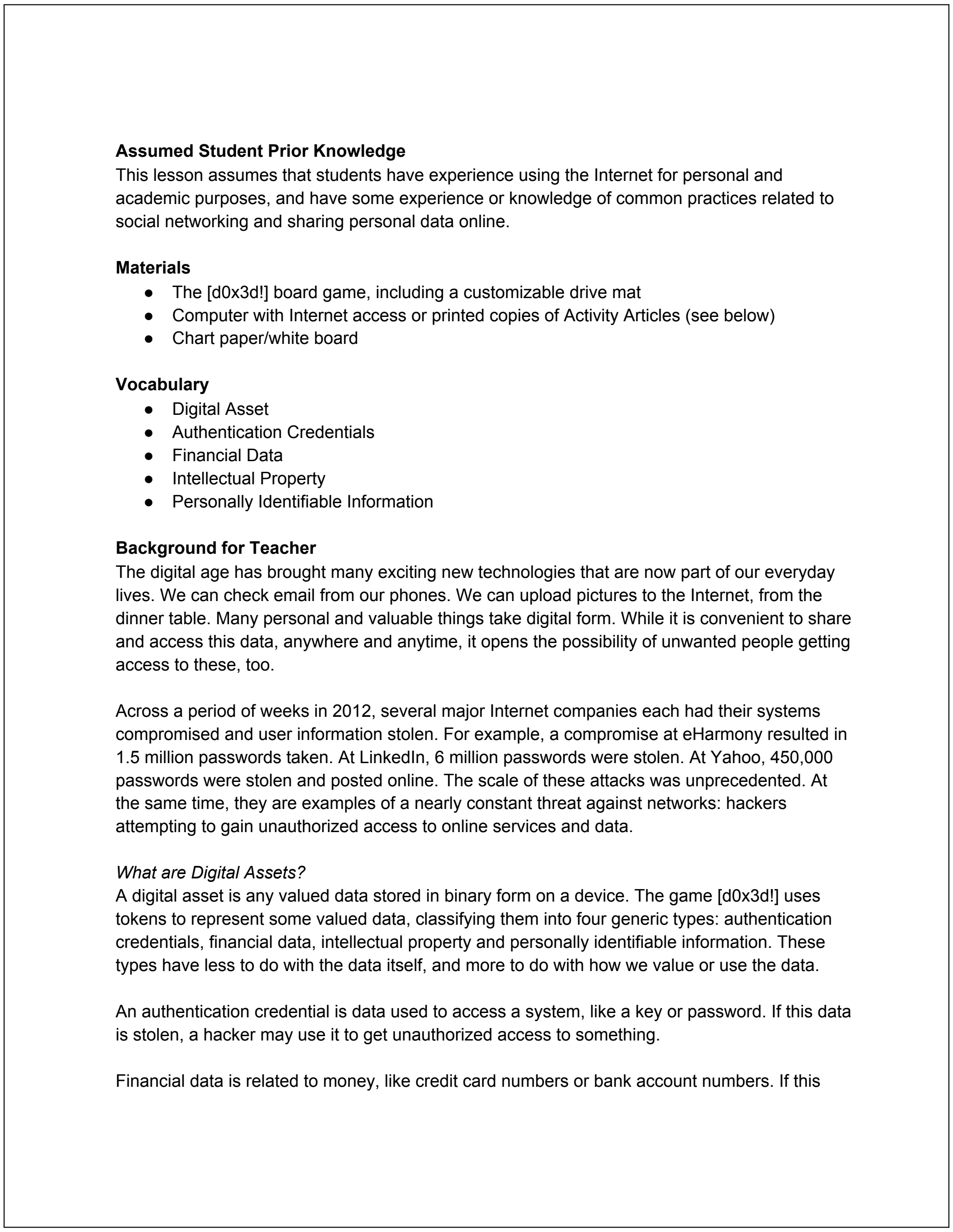
Standards
CCSS.ELA-Literacy.CCRA.W.1 Write arguments to support claims in an analysis of substantive topics or texts using valid reasoning and relevant and sufficient evidence.

CCSS.ELA-Literacy.SL.11-12.1b Work with peers to promote civil, democratic discussions and decision-making, set clear goals and deadlines, and establish individual roles as needed.

CCSS.ELA-Literacy.RI.11-12.1 Cite strong and thorough textual evidence to support analysis of what the text says explicitly as well as inferences drawn from the text, including determining where the text leaves matters uncertain

McREL Technology. Standard 3. (Grade 9-12): Understands the relationships among science, technology, society, and the individual.

McREL Technology. Standard 3. (Grade 9-12):Understands the impact of the internet on society (e.g., addiction to and dependence on the internet; identity theft; access to unsuitable material)**.**



Assumed Student Prior Knowledge
This lesson assumes that students have experience using the Internet for personal and academic purposes, and have some experience or knowledge of common practices related to social networking and sharing personal data online.

Materials

- The [d0x3d!] board game, including a customizable drive mat
- Computer with Internet access or printed copies of Activity Articles (see below)
- Chart paper/white board

Vocabulary

- Digital Asset
- Authentication Credentials
- Financial Data
- Intellectual Property
- Personally Identifiable Information

Background for Teacher
The digital age has brought many exciting new technologies that are now part of our everyday lives. We can check email from our phones. We can upload pictures to the Internet, from the dinner table. Many personal and valuable things take digital form. While it is convenient to share and access this data, anywhere and anytime, it opens the possibility of unwanted people getting access to these, too.

Across a period of weeks in 2012, several major Internet companies each had their systems compromised and user information stolen. For example, a compromise at eHarmony resulted in 1.5 million passwords taken. At LinkedIn, 6 million passwords were stolen. At Yahoo, 450,000 passwords were stolen and posted online. The scale of these attacks was unprecedented. At the same time, they are examples of a nearly constant threat against networks: hackers attempting to gain unauthorized access to online services and data.

What are Digital Assets?
A digital asset is any valued data stored in binary form on a device. The game [d0x3d!] uses tokens to represent some valued data, classifying them into four generic types: authentication credentials, financial data, intellectual property and personally identifiable information. These types have less to do with the data itself, and more to do with how we value or use the data.

An authentication credential is data used to access a system, like a key or password. If this data is stolen, a hacker may use it to get unauthorized access to something.

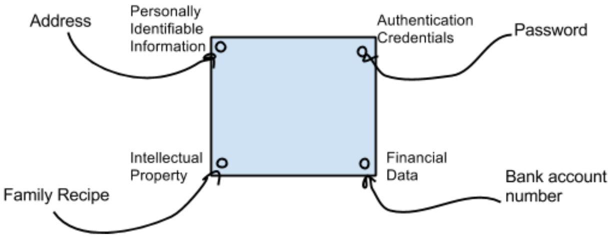
Financial data is related to money, like credit card numbers or bank account numbers. If this data is stolen, a hacker may use it to launder money or commit fraud.

Intellectual property covers a broad range of topics, including copyright, trademark, design rights, inventions, and treatment of creative works. Intellectual property is any product of the mind over which a creator retains some right. Examples include a piece of music, piece of software, or a scientific invention. Sometimes, technology is used to protect the data or keep it secret. For example, trade secrets, once lost, cannot be easily re-claimed. Piracy occurs when the creator's rights are abused in some way. This may happen when some intellectual property is shared or modified without permission.

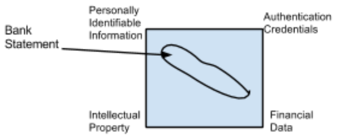
Personally identifiable information is any data that, if clost, may damage your privacy, reputation or identity. Examples include your date of birth, your address, your phone number, or medical records. If this data is stolen, a hacker may use it to (among other things) commit identity theft.

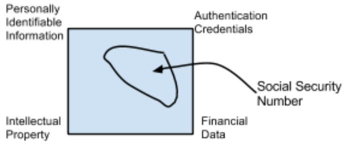
Example Digital Assets

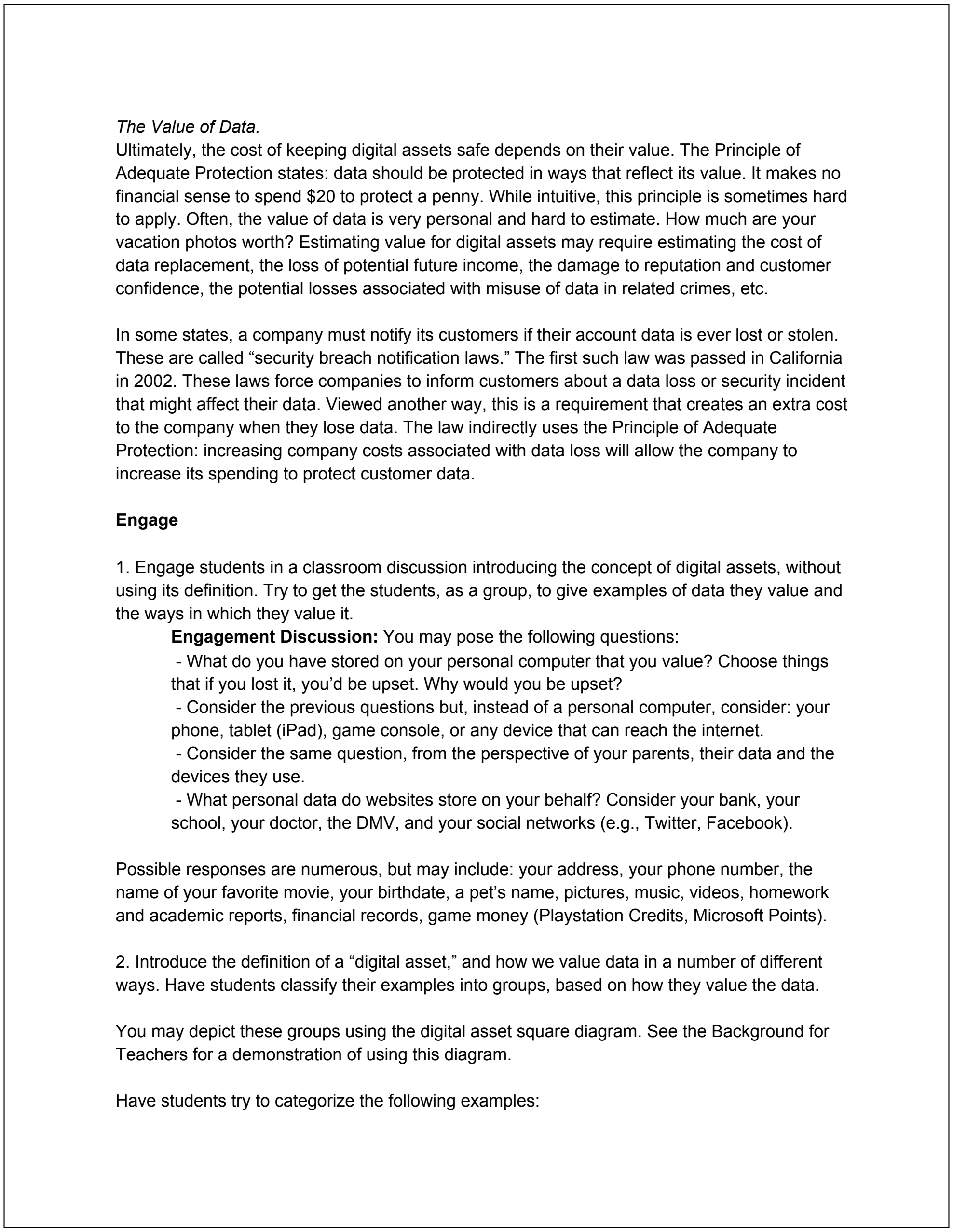
The previous four asset categories are not strict and sometimes overlap. Some valued data doesn't fall into one of these categories, and some fall into several. During the Engage activity, we use a diagram to characterize example assets in terms of the game's four types. If some example fits neatly into one of these categories, we can illustrate this using a point (or a small circular shape) in the appropriate corner. Many natural examples fall into these corners:



When an example asset contains characteristics of more than one type, we draw a shape that has been "stretched" toward several corners. The result is a "blob," whose size and shape reflects our thoughts about how each of these types relates to the data, for example:


Bank Statement
Personally Identifiable Information
Authentication Credentials
Intellectual Property
Financial Data


Personally Identifiable Information
Authentication Credentials
Social Security Number
Intellectual Property
Financial Data



The Value of Data.
Ultimately, the cost of keeping digital assets safe depends on their value. The Principle of Adequate Protection states: data should be protected in ways that reflect its value. It makes no financial sense to spend $20 to protect a penny. While intuitive, this principle is sometimes hard to apply. Often, the value of data is very personal and hard to estimate. How much are your vacation photos worth? Estimating value for digital assets may require estimating the cost of data replacement, the loss of potential future income, the damage to reputation and customer confidence, the potential losses associated with misuse of data in related crimes, etc.

In some states, a company must notify its customers if their account data is ever lost or stolen. These are called “security breach notification laws.” The first such law was passed in California in 2002. These laws force companies to inform customers about a data loss or security incident that might affect their data. Viewed another way, this is a requirement that creates an extra cost to the company when they lose data. The law indirectly uses the Principle of Adequate Protection: increasing company costs associated with data loss will allow the company to increase its spending to protect customer data.

Engage

1. Engage students in a classroom discussion introducing the concept of digital assets, without using its definition. Try to get the students, as a group, to give examples of data they value and the ways in which they value it.

> **Engagement Discussion:** You may pose the following questions:
> - What do you have stored on your personal computer that you value? Choose things that if you lost it, you’d be upset. Why would you be upset?
> - Consider the previous questions but, instead of a personal computer, consider: your phone, tablet (iPad), game console, or any device that can reach the internet.
> - Consider the same question, from the perspective of your parents, their data and the devices they use.
> - What personal data do websites store on your behalf? Consider your bank, your school, your doctor, the DMV, and your social networks (e.g., Twitter, Facebook).

Possible responses are numerous, but may include: your address, your phone number, the name of your favorite movie, your birthdate, a pet’s name, pictures, music, videos, homework and academic reports, financial records, game money (Playstation Credits, Microsoft Points).

2. Introduce the definition of a “digital asset,” and how we value data in a number of different ways. Have students classify their examples into groups, based on how they value the data.

You may depict these groups using the digital asset square diagram. See the Background for Teachers for a demonstration of using this diagram.

Have students try to categorize the following examples:

financial data	*authentication credentials*	*personally identifiable information*	*intellectual property*
bank statement credit card number bank account data gift certificate	password driver's license photo ID school ID library card	phone number address grades/transcript medical record family photos	English report original song secret recipe original video artistic photos

The following list are items that aren't as easily classifiable, and may provoke an interesting debate:

- a driver's license (personally identifiable information, sometimes an authentication credential)
- social security number (personally identifiable information, sometimes an authentication credential, perhaps financial data as well)

3. **Activity:** Using the list you developed as a group, have students (in groups or pairs) define each classification of "digital assets." Discuss student results. Have students defend which assets belong in each category.

Activity Discussion:

Using the examples in each category, can we write a definition for each type of digital asset: *financial data, authentication credentials, personally identifiable information, and intellectual property.*

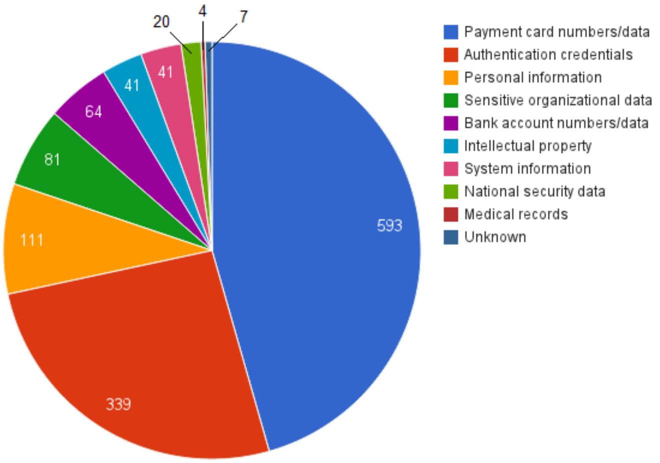
Can assets be in more than one category? Defend your position using examples.

4. **Discussion:** When students appear to understand what digital assets are, interpret this data from the "2011 Data Breach Investigations Report," by the US Secret Service and Verizon.

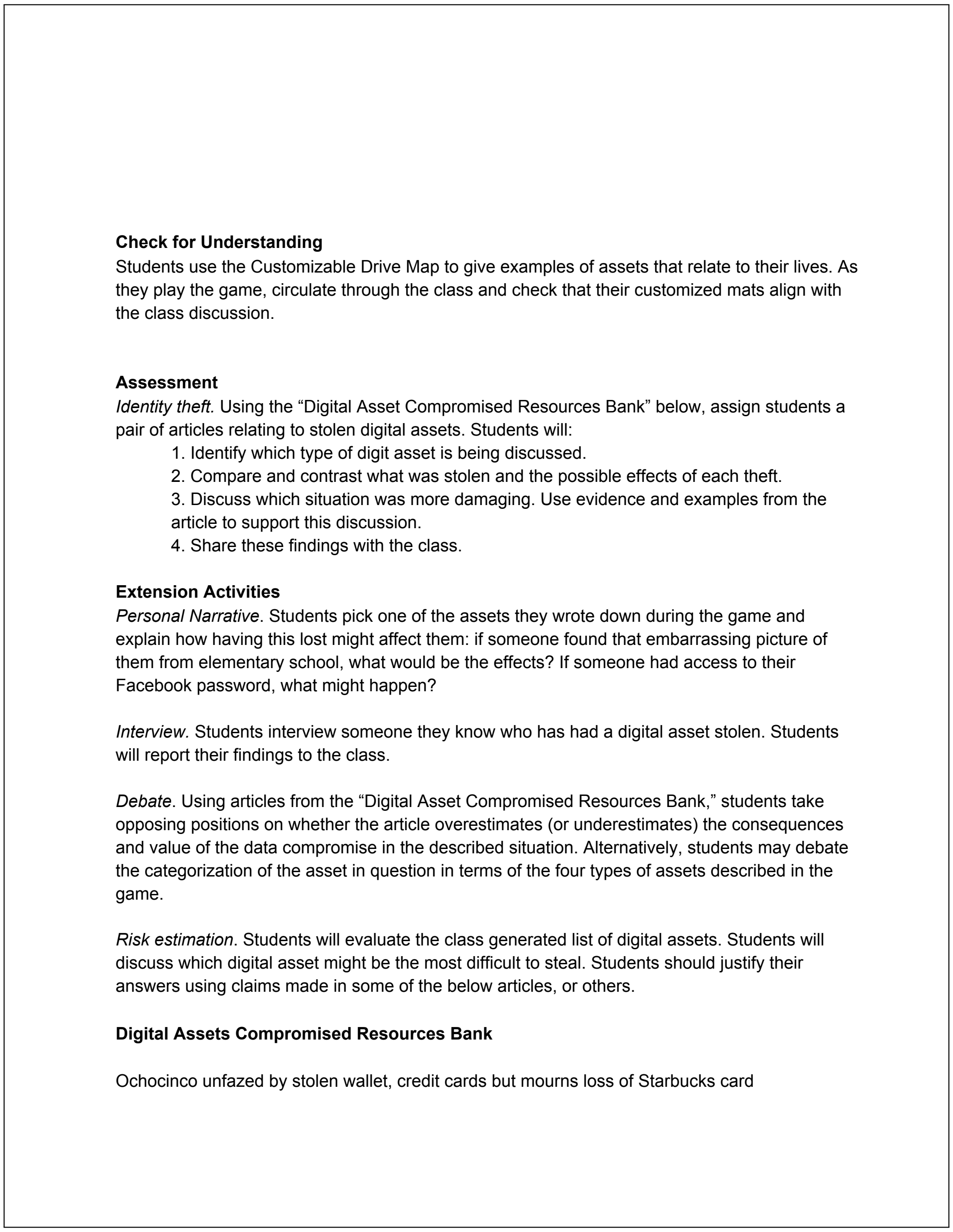
Based on this graph:

- Based on these historical trends, what data seems to have the greatest *risk* for being lost or stolen?
- Why do you think that that category made up almost half of all breaches?
- Consider the possible value of the data represented as lost in this graph. How might you being to create a lower-bound for the total value? An upper bound?
- If something is at low risk of being lost and has low value, does it make sense to spend a lot of money to protect it? How about something with high risk and high value? Low risk and high value?
- Give an example asset represented in the graph, and assign it a value. Assumption: let its risk (likelihood of it being lost during the year) be equal to the likelihood that a random data compromise in 2010 was associated with your example's type. Under this assumption, how much should you spend to protect your asset, per year? Is this assumption good or bad? Why?

Compromised Data Types By Number Of Breaches



Compromised data type	Number of breaches in 2010
Payment card numbers/data	593
Authentication credentials	339
Personal information	111
Sensitive organizational data	81
Bank account numbers/data	64
Intellectual property	41
System information	41
National security data	20
Medical records	4
Unknown	7



Check for Understanding
Students use the Customizable Drive Map to give examples of assets that relate to their lives. As they play the game, circulate through the class and check that their customized mats align with the class discussion.

Assessment
Identity theft. Using the “Digital Asset Compromised Resources Bank” below, assign students a pair of articles relating to stolen digital assets. Students will:

1. Identify which type of digit asset is being discussed.
2. Compare and contrast what was stolen and the possible effects of each theft.
3. Discuss which situation was more damaging. Use evidence and examples from the article to support this discussion.
4. Share these findings with the class.

Extension Activities
Personal Narrative. Students pick one of the assets they wrote down during the game and explain how having this lost might affect them: if someone found that embarrassing picture of them from elementary school, what would be the effects? If someone had access to their Facebook password, what might happen?

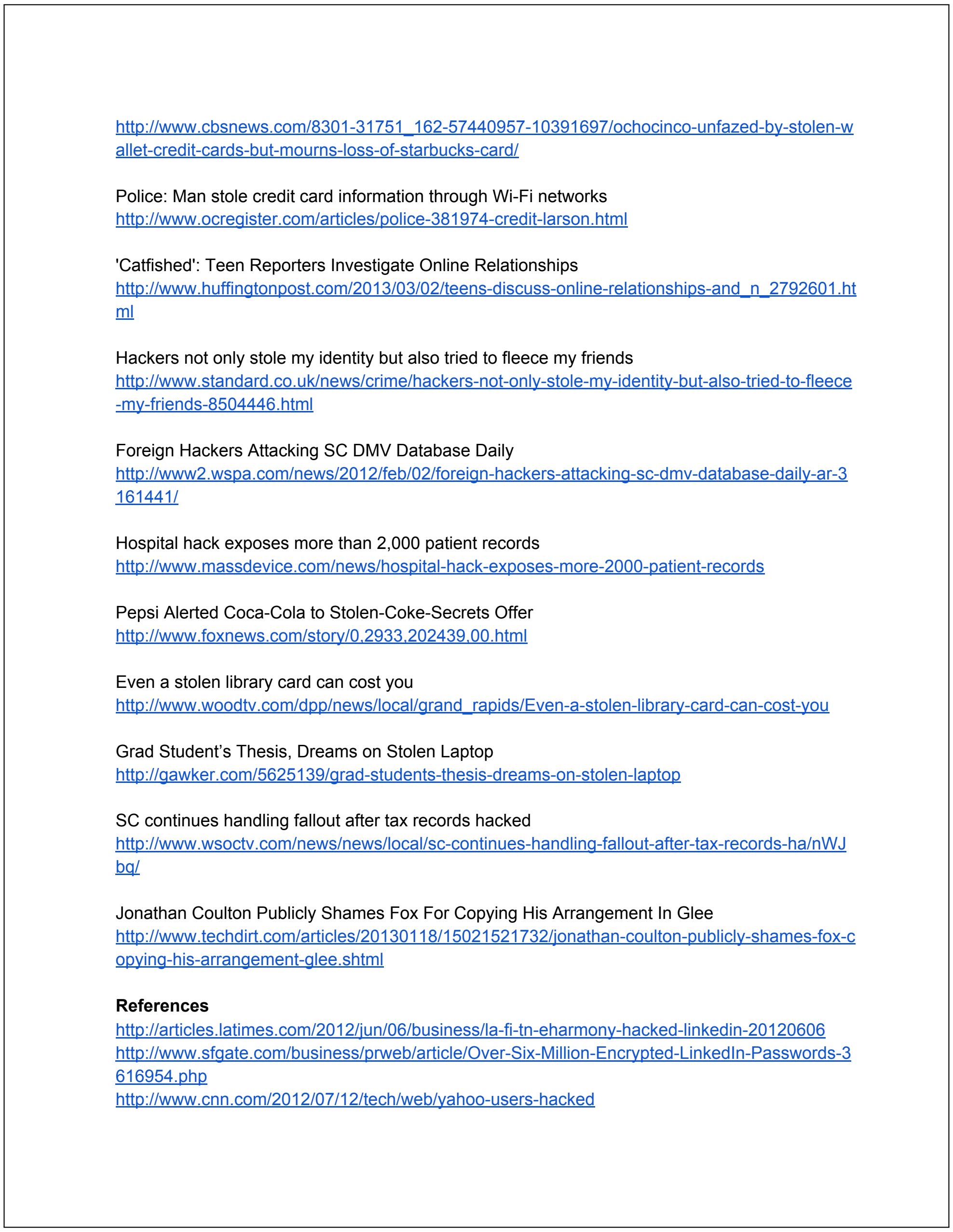
Interview. Students interview someone they know who has had a digital asset stolen. Students will report their findings to the class.

Debate. Using articles from the “Digital Asset Compromised Resources Bank,” students take opposing positions on whether the article overestimates (or underestimates) the consequences and value of the data compromise in the described situation. Alternatively, students may debate the categorization of the asset in question in terms of the four types of assets described in the game.

Risk estimation. Students will evaluate the class generated list of digital assets. Students will discuss which digital asset might be the most difficult to steal. Students should justify their answers using claims made in some of the below articles, or others.

Digital Assets Compromised Resources Bank

Ochocinco unfazed by stolen wallet, credit cards but mourns loss of Starbucks card



http://www.cbsnews.com/8301-31751_162-57440957-10391697/ochocinco-unfazed-by-stolen-wallet-credit-cards-but-mourns-loss-of-starbucks-card/

Police: Man stole credit card information through Wi-Fi networks
http://www.ocregister.com/articles/police-381974-credit-larson.html

'Catfished': Teen Reporters Investigate Online Relationships
http://www.huffingtonpost.com/2013/03/02/teens-discuss-online-relationships-and_n_2792601.html

Hackers not only stole my identity but also tried to fleece my friends
http://www.standard.co.uk/news/crime/hackers-not-only-stole-my-identity-but-also-tried-to-fleece-my-friends-8504446.html

Foreign Hackers Attacking SC DMV Database Daily
http://www2.wspa.com/news/2012/feb/02/foreign-hackers-attacking-sc-dmv-database-daily-ar-3161441/

Hospital hack exposes more than 2,000 patient records
http://www.massdevice.com/news/hospital-hack-exposes-more-2000-patient-records

Pepsi Alerted Coca-Cola to Stolen-Coke-Secrets Offer
http://www.foxnews.com/story/0,2933,202439,00.html

Even a stolen library card can cost you
http://www.woodtv.com/dpp/news/local/grand_rapids/Even-a-stolen-library-card-can-cost-you

Grad Student's Thesis, Dreams on Stolen Laptop
http://gawker.com/5625139/grad-students-thesis-dreams-on-stolen-laptop

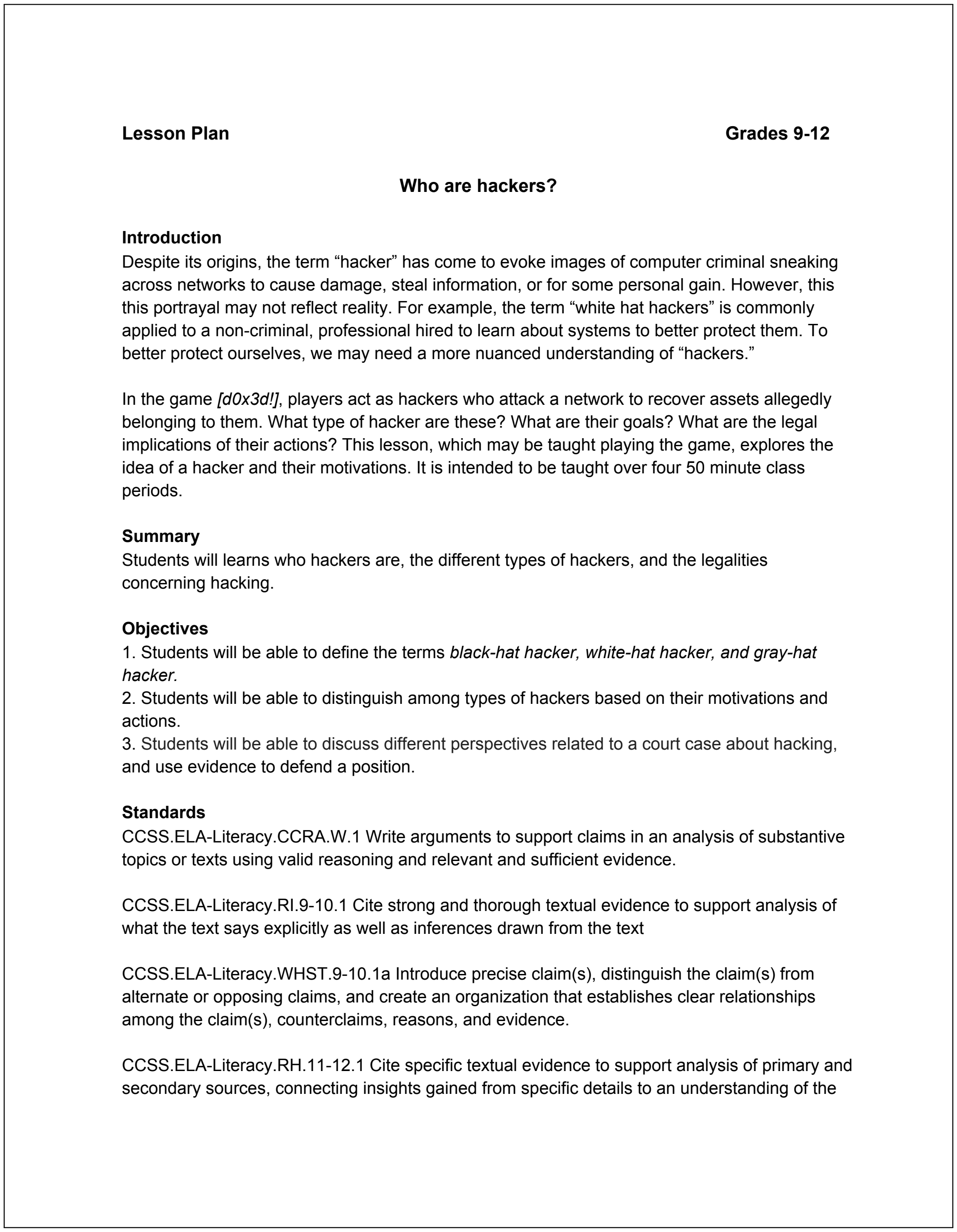
SC continues handling fallout after tax records hacked
http://www.wsoctv.com/news/news/local/sc-continues-handling-fallout-after-tax-records-ha/nWJbq/

Jonathan Coulton Publicly Shames Fox For Copying His Arrangement In Glee
http://www.techdirt.com/articles/20130118/15021521732/jonathan-coulton-publicly-shames-fox-copying-his-arrangement-glee.shtml

References

http://articles.latimes.com/2012/jun/06/business/la-fi-tn-eharmony-hacked-linkedin-20120606
http://www.sfgate.com/business/prweb/article/Over-Six-Million-Encrypted-LinkedIn-Passwords-3616954.php
http://www.cnn.com/2012/07/12/tech/web/yahoo-users-hacked

Appendix B. Who Are Hackers?



Lesson Plan **Grades 9-12**

Who are hackers?

Introduction

Despite its origins, the term “hacker” has come to evoke images of computer criminal sneaking across networks to cause damage, steal information, or for some personal gain. However, this this portrayal may not reflect reality. For example, the term “white hat hackers” is commonly applied to a non-criminal, professional hired to learn about systems to better protect them. To better protect ourselves, we may need a more nuanced understanding of “hackers.”

In the game *[d0x3d!]*, players act as hackers who attack a network to recover assets allegedly belonging to them. What type of hacker are these? What are their goals? What are the legal implications of their actions? This lesson, which may be taught playing the game, explores the idea of a hacker and their motivations. It is intended to be taught over four 50 minute class periods.

Summary

Students will learns who hackers are, the different types of hackers, and the legalities concerning hacking.

Objectives

1. Students will be able to define the terms *black-hat hacker, white-hat hacker, and gray-hat hacker.*
2. Students will be able to distinguish among types of hackers based on their motivations and actions.
3. Students will be able to discuss different perspectives related to a court case about hacking, and use evidence to defend a position.

Standards

CCSS.ELA-Literacy.CCRA.W.1 Write arguments to support claims in an analysis of substantive topics or texts using valid reasoning and relevant and sufficient evidence.

CCSS.ELA-Literacy.RI.9-10.1 Cite strong and thorough textual evidence to support analysis of what the text says explicitly as well as inferences drawn from the text

CCSS.ELA-Literacy.WHST.9-10.1a Introduce precise claim(s), distinguish the claim(s) from alternate or opposing claims, and create an organization that establishes clear relationships among the claim(s), counterclaims, reasons, and evidence.

CCSS.ELA-Literacy.RH.11-12.1 Cite specific textual evidence to support analysis of primary and secondary sources, connecting insights gained from specific details to an understanding of the text as a whole.

McREL Technology. Standard 3. (Grade 9-12): Understands the relationships among science, technology, society, and the individual.

McREL Technology. Standard 3. (Grade 9-12): Knows the role of technology in a variety of careers.

McREL Technology. Standard 3. (Grade 9-12): Understands the impact of the internet on society (e.g., addiction to and dependence on the internet; identity theft; access to unsuitable material)**.**

Assumed Student Prior Knowledge
This lesson assumes students have had prior experience with computer systems, the Internet and some awareness of the need for online safety and the threat of hackers.

Materials

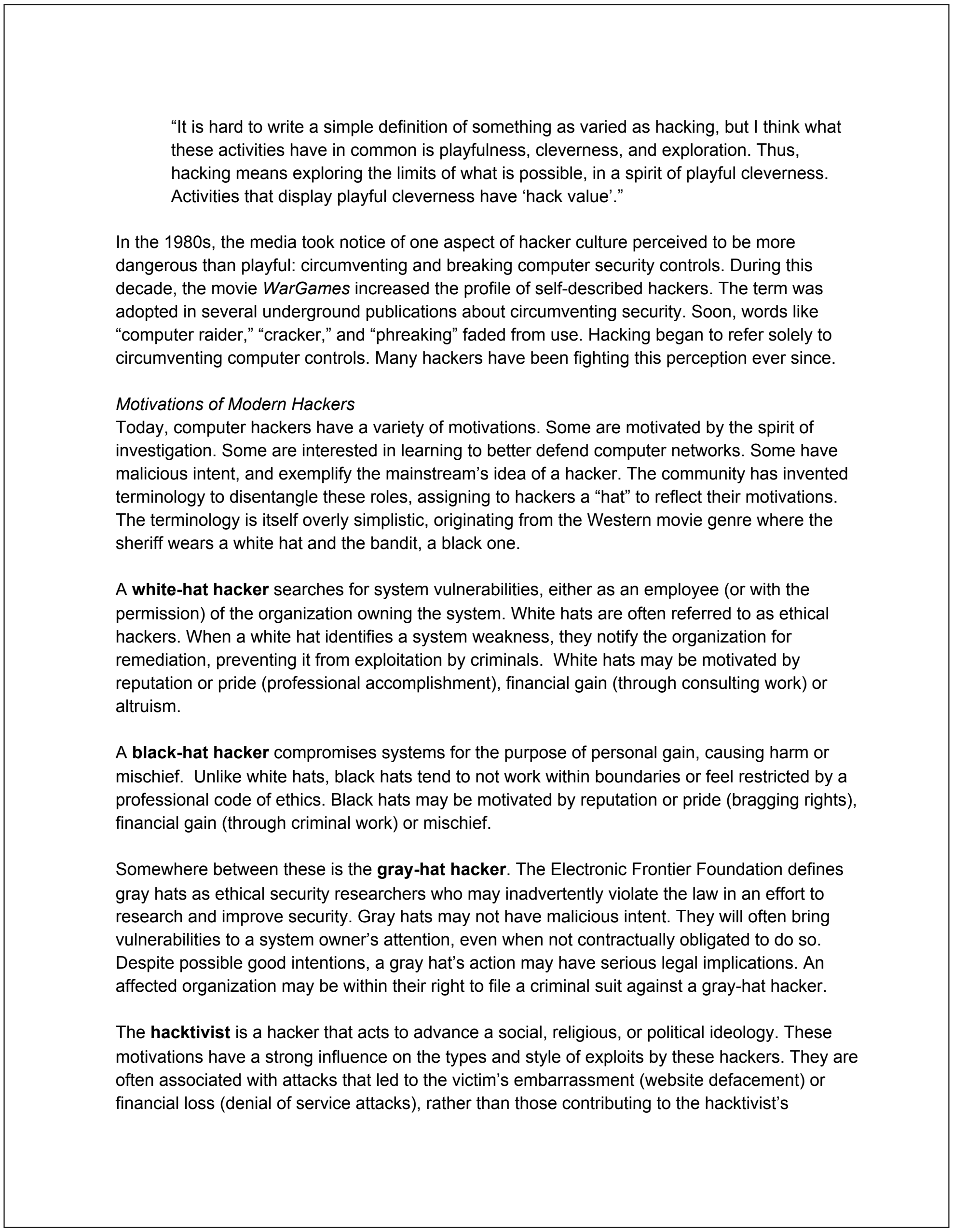
- The board game [d0x3d!]
- Computer with Internet access or home access to internet
- Chart paper/white board
- Articles referenced within the lesson .

Vocabulary

- Hacker
- White-hat hacking
- Black-hat hacking
- Gray-hat hacking
- Hacktivism

Background for Teacher
The term hacker began to take its modern connotations in the 1960s and 1970s among university students. Most notably, MIT is often credited as the birthplace of the “hacker culture,” at a student group called the Tech Model Railroad Club (TMRC). TMRC reflected its members’ love and curiosity for how objects worked. To understand or use these technologies in new ways, students would “hack” them. The club was diverse in its interests related to model trains: one group was interested in accurate replicas of historical trains, another wanted to run trains on strict schedules, and another (the Signals and Power Subcommittee) created the circuits that made the model trains run. This last group eventually expanded into the world of computers and programming. Over time, “hacking” became less about model trains and began to take on its modern connotations.

Even among experts, hacking is an ambiguous term. Richard Stallman, founder of the GNU project, reflects on what a definition might be, by writing:



> “It is hard to write a simple definition of something as varied as hacking, but I think what these activities have in common is playfulness, cleverness, and exploration. Thus, hacking means exploring the limits of what is possible, in a spirit of playful cleverness. Activities that display playful cleverness have ‘hack value’.”

In the 1980s, the media took notice of one aspect of hacker culture perceived to be more dangerous than playful: circumventing and breaking computer security controls. During this decade, the movie *WarGames* increased the profile of self-described hackers. The term was adopted in several underground publications about circumventing security. Soon, words like “computer raider,” “cracker,” and “phreaking” faded from use. Hacking began to refer solely to circumventing computer controls. Many hackers have been fighting this perception ever since.

Motivations of Modern Hackers

Today, computer hackers have a variety of motivations. Some are motivated by the spirit of investigation. Some are interested in learning to better defend computer networks. Some have malicious intent, and exemplify the mainstream’s idea of a hacker. The community has invented terminology to disentangle these roles, assigning to hackers a “hat” to reflect their motivations. The terminology is itself overly simplistic, originating from the Western movie genre where the sheriff wears a white hat and the bandit, a black one.

A **white-hat hacker** searches for system vulnerabilities, either as an employee (or with the permission) of the organization owning the system. White hats are often referred to as ethical hackers. When a white hat identifies a system weakness, they notify the organization for remediation, preventing it from exploitation by criminals. White hats may be motivated by reputation or pride (professional accomplishment), financial gain (through consulting work) or altruism.

A **black-hat hacker** compromises systems for the purpose of personal gain, causing harm or mischief. Unlike white hats, black hats tend to not work within boundaries or feel restricted by a professional code of ethics. Black hats may be motivated by reputation or pride (bragging rights), financial gain (through criminal work) or mischief.

Somewhere between these is the **gray-hat hacker**. The Electronic Frontier Foundation defines gray hats as ethical security researchers who may inadvertently violate the law in an effort to research and improve security. Gray hats may not have malicious intent. They will often bring vulnerabilities to a system owner’s attention, even when not contractually obligated to do so. Despite possible good intentions, a gray hat’s action may have serious legal implications. An affected organization may be within their right to file a criminal suit against a gray-hat hacker.

The **hacktivist** is a hacker that acts to advance a social, religious, or political ideology. These motivations have a strong influence on the types and style of exploits by these hackers. They are often associated with attacks that led to the victim’s embarrassment (website defacement) or financial loss (denial of service attacks), rather than those contributing to the hacktivist’s personal financial gain (money laundering, sending spam). The group Anonymous has become known for their politically-charged attacks on financial institutions, extreme religious organizations and government websites.

Legal Issues to Hacking
It is important to understand the legal consequences (any) hackers may face when exposing or exploiting a system's vulnerabilities. The legal landscape is broad and complex in this area. Here, we briefly describe two Acts that may provide a setting for relevant class discussion.

The Computer Fraud and Abuse Act of 1986 (CFAA) was intended to punish individuals that damaged government computer systems or stole information. In 1988, Robert Morris became the first person convicted under the Computer Fraud and Abuse Act after creating the Morris worm, a malicious program that replicates itself in order to spread across computers. Over time, the law was broadened by Congress. The CFAA now criminalizes "exceeding authorized access" to any computer system, not just those managed by the US government. Courts are still struggling to interpret the law in the context of an ever-changing technological landscape. For example, ambiguity in interpreting the CFAA has led to the criminal prosecution of Aaron Swartz and Andrew "weev" Auernheimer—two individuals whose actions don't neatly fit into either black hat or white hat categories.
(http://www.thelibertybeacon.com/2013/01/21/how-the-cfaa-can-effectively-mark-anyone-who-uses-the-internet-as-a-felon/).

The Digital Millennium Copyright Act (DMCA) contains similar language that prohibits the circumvention of access-control technology. The intention of the law was to criminalize the circumvention of anti-piracy technology (in particular, tools that circumvent those technologies intended to protect the interests of copyright holders). In 2007, John Stottlemire was sued by Coupons.com for posting code and instructions that helped shoppers circumvent protections on their downloadable coupons. This allowed people to print multiple coupons.
(http://www.wired.com/politics/onlinerights/news/2007/08/coupons).(http://arstechnica.com/tech-policy/2008/11/coupons-inc-drops-dmca-lawsuit-against-coupon-hacker/)

Engage

1. Introduce the court case *Massachusetts Bay Transportation Authority v. Anderson.*

    In 2008, while doing research for their final project in their MIT *Computer and Network Security* class, three students discovered a vulnerability in the electronic transportation magstripe card system. The value on the card was stored on the card itself, not in a secure database, which allowed the information on the card to be overwritten. The students submitted a presentation of their findings to the DEF CON Hacker Convention which demonstrated some of the vulnerabilities they discovered. The MBTA took legal action and filed a suit to prevent the students from presenting their work, claiming monetary damages and a threat to public safety. Furthermore, MBTA claimed that the students have a responsibility to notify them of the system flaw time before the presentation, so they could have ample time to correct the flaw.

Discussion: You may pose the following questions:
- From this provided information, who do you feel is at fault: the students or the MBTA? Defend your position.
- Should the students have notified the transportation authority before presenting their findings at the Hacker Convention? Why, or why not?
- Why might hackers feel it necessary to "go public" with their findings?

2. Present students with the below table, summarizing these hacker terms. Express that these terms are sometimes useful in discussions about hackers, but that not all individuals can be understood purely in these terms.

	Definition	**Motivation**	**Possible Consequences**
Black-hat hacker	Hacker who uses their skills in criminal or unethical ways.	Malicious intent. Bypass security illegally to compromise system. Steal data.	If caught, subject to relevant federal laws.
White-hat hacker	Hacker who is authorized to hack, and does so following some ethical guidelines.	Professional. Discover vulnerabilities, in order to prevent exploitation.	Legal, since hired by system owner.
Gray hat hacker	Hacker who enters computer systems and networks without authorization, may include vigilantes and hacktivists.	Reputation. To expose vulnerabilities, but make system owner aware of them. Political reasons.	Actions may be unappreciated, and face legal consequences.

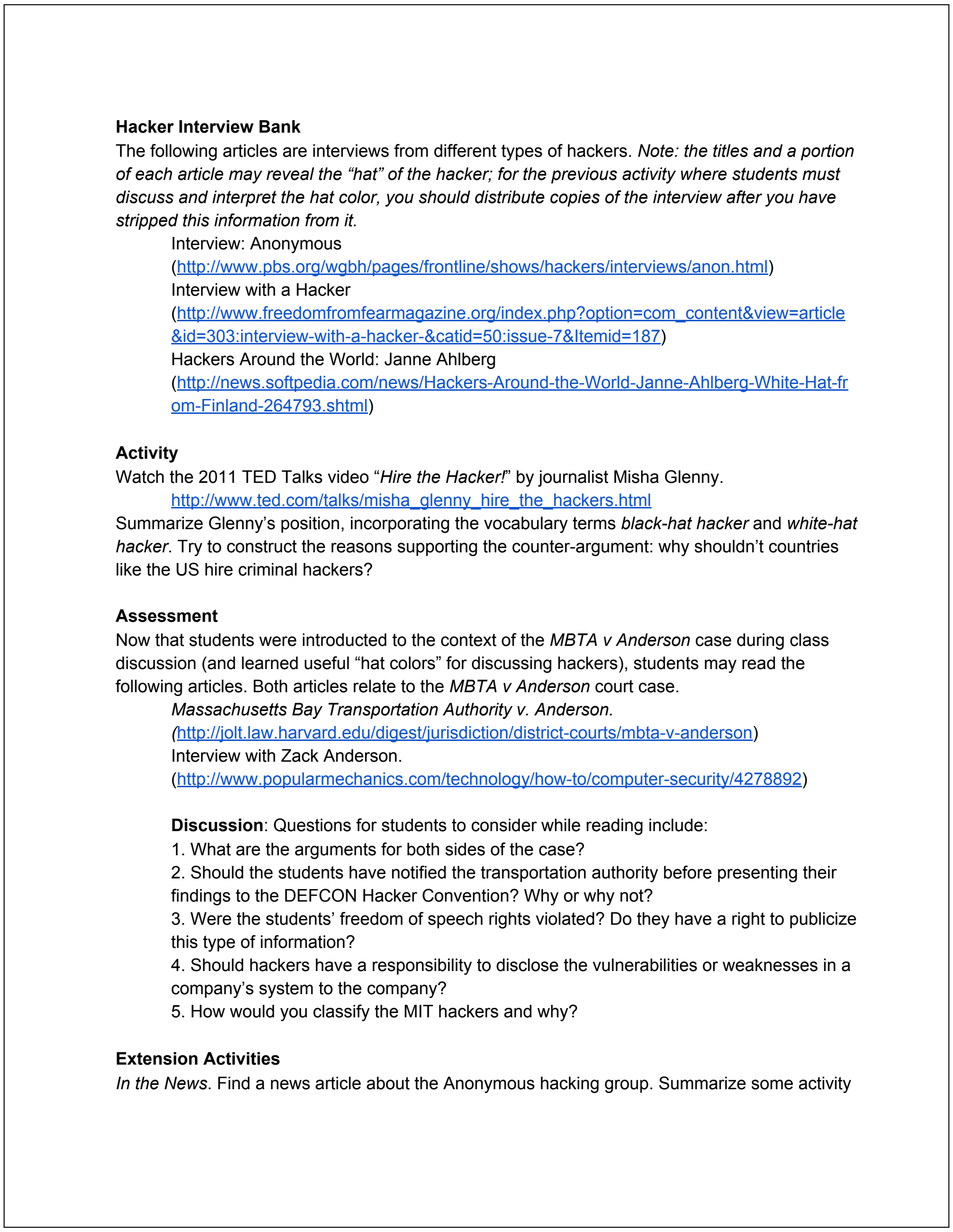
Check for Understanding

Divide students into groups of three, one for each type of hacker. Each student will

1. Read an assigned article from the **Hacker Interview Bank**.
2. Summarize the article to the members in their group.
3. Discuss which "hat" the hacker from the article wears (a black hat, white hat, or gray hat).

Follow Up Discussion to the Check for Understanding

Discuss the hackers from the game [d0x3d!]. Can you construct a story or context for the game where the players are white hats? Where they are black hats?



Hacker Interview Bank

The following articles are interviews from different types of hackers. *Note: the titles and a portion of each article may reveal the "hat" of the hacker; for the previous activity where students must discuss and interpret the hat color, you should distribute copies of the interview after you have stripped this information from it.*

Interview: Anonymous
(http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/anon.html)
Interview with a Hacker
(http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=303:interview-with-a-hacker-&catid=50:issue-7&Itemid=187)
Hackers Around the World: Janne Ahlberg
(http://news.softpedia.com/news/Hackers-Around-the-World-Janne-Ahlberg-White-Hat-from-Finland-264793.shtml)

Activity

Watch the 2011 TED Talks video "*Hire the Hacker!*" by journalist Misha Glenny.

http://www.ted.com/talks/misha_glenny_hire_the_hackers.html

Summarize Glenny's position, incorporating the vocabulary terms *black-hat hacker* and *white-hat hacker*. Try to construct the reasons supporting the counter-argument: why shouldn't countries like the US hire criminal hackers?

Assessment

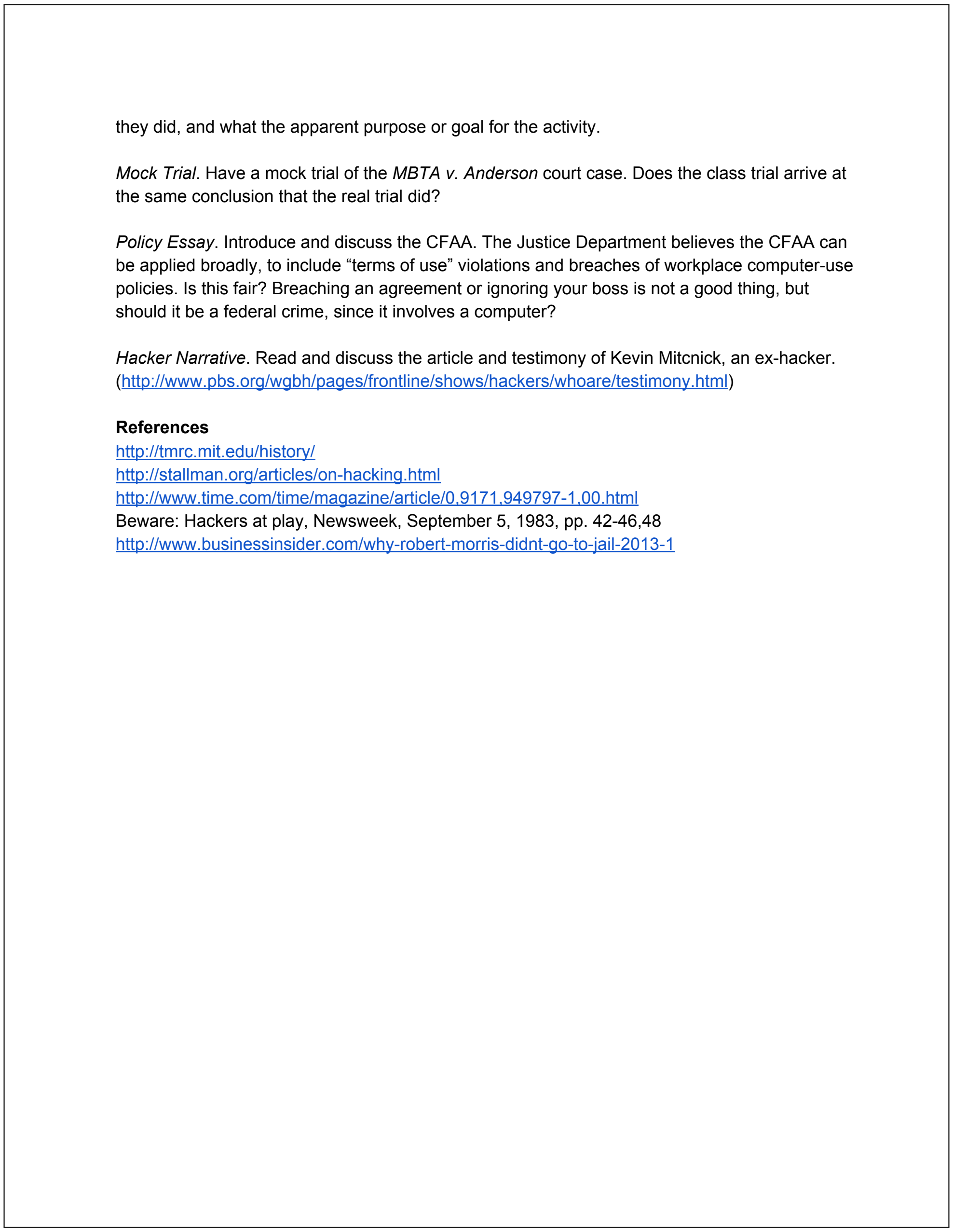
Now that students were introducted to the context of the *MBTA v Anderson* case during class discussion (and learned useful "hat colors" for discussing hackers), students may read the following articles. Both articles relate to the *MBTA v Anderson* court case.

Massachusetts Bay Transportation Authority v. Anderson.
*(*http://jolt.law.harvard.edu/digest/jurisdiction/district-courts/mbta-v-anderson)
Interview with Zack Anderson.
(http://www.popularmechanics.com/technology/how-to/computer-security/4278892)

Discussion: Questions for students to consider while reading include:
1. What are the arguments for both sides of the case?
2. Should the students have notified the transportation authority before presenting their findings to the DEFCON Hacker Convention? Why or why not?
3. Were the students' freedom of speech rights violated? Do they have a right to publicize this type of information?
4. Should hackers have a responsibility to disclose the vulnerabilities or weaknesses in a company's system to the company?
5. How would you classify the MIT hackers and why?

Extension Activities

In the News. Find a news article about the Anonymous hacking group. Summarize some activity



they did, and what the apparent purpose or goal for the activity.

Mock Trial. Have a mock trial of the *MBTA v. Anderson* court case. Does the class trial arrive at the same conclusion that the real trial did?

Policy Essay. Introduce and discuss the CFAA. The Justice Department believes the CFAA can be applied broadly, to include “terms of use” violations and breaches of workplace computer-use policies. Is this fair? Breaching an agreement or ignoring your boss is not a good thing, but should it be a federal crime, since it involves a computer?

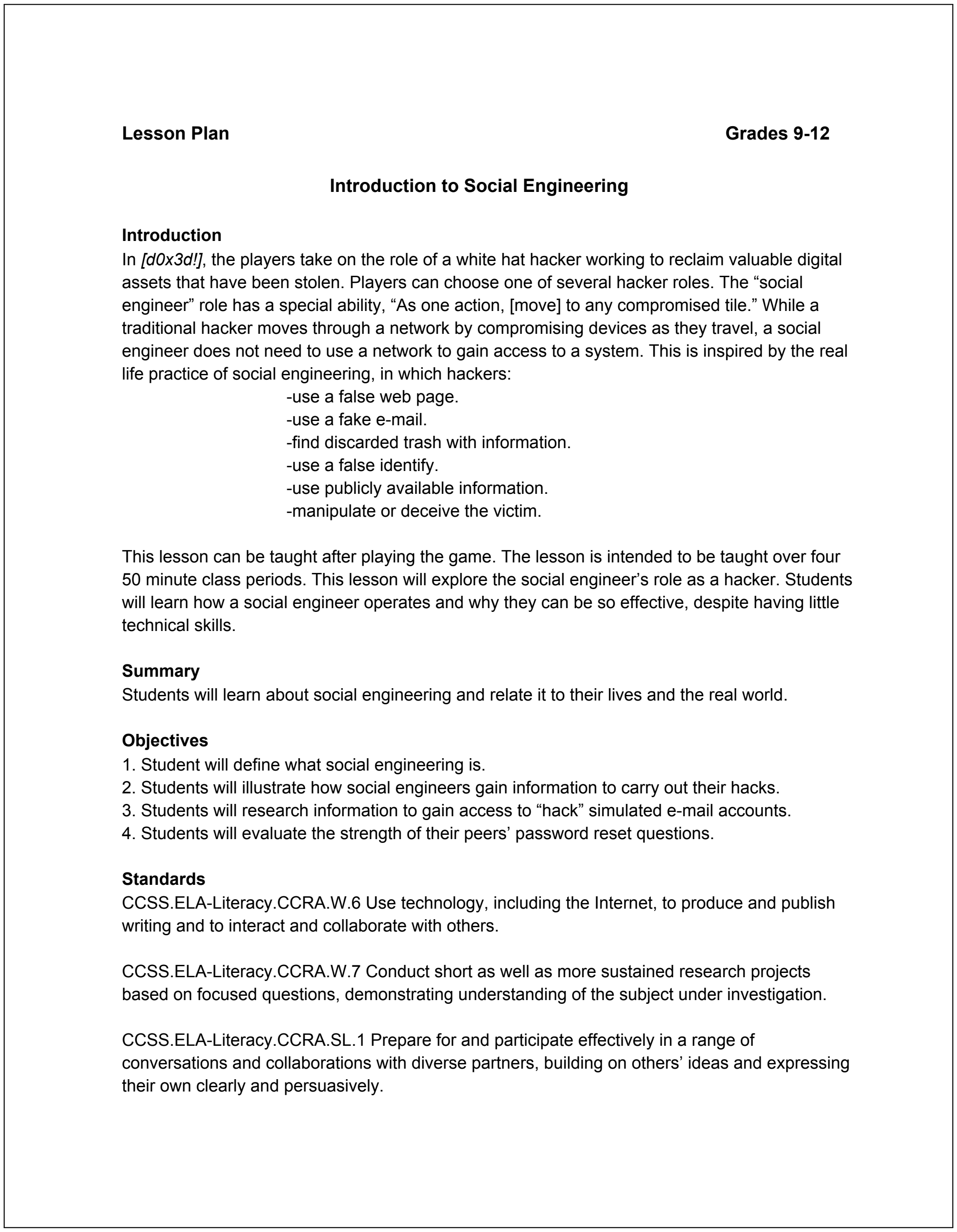
Hacker Narrative. Read and discuss the article and testimony of Kevin Mitcnick, an ex-hacker. (http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html)

References

http://tmrc.mit.edu/history/
http://stallman.org/articles/on-hacking.html
http://www.time.com/time/magazine/article/0,9171,949797-1,00.html
Beware: Hackers at play, Newsweek, September 5, 1983, pp. 42-46,48
http://www.businessinsider.com/why-robert-morris-didnt-go-to-jail-2013-1

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix C. Introduction to Social Engineering



Lesson Plan **Grades 9-12**

Introduction to Social Engineering

Introduction

In *[d0x3d!]*, the players take on the role of a white hat hacker working to reclaim valuable digital assets that have been stolen. Players can choose one of several hacker roles. The “social engineer” role has a special ability, “As one action, [move] to any compromised tile.” While a traditional hacker moves through a network by compromising devices as they travel, a social engineer does not need to use a network to gain access to a system. This is inspired by the real life practice of social engineering, in which hackers:

-use a false web page.
-use a fake e-mail.
-find discarded trash with information.
-use a false identify.
-use publicly available information.
-manipulate or deceive the victim.

This lesson can be taught after playing the game. The lesson is intended to be taught over four 50 minute class periods. This lesson will explore the social engineer’s role as a hacker. Students will learn how a social engineer operates and why they can be so effective, despite having little technical skills.

Summary

Students will learn about social engineering and relate it to their lives and the real world.

Objectives

1. Student will define what social engineering is.
2. Students will illustrate how social engineers gain information to carry out their hacks.
3. Students will research information to gain access to “hack” simulated e-mail accounts.
4. Students will evaluate the strength of their peers’ password reset questions.

Standards

CCSS.ELA-Literacy.CCRA.W.6 Use technology, including the Internet, to produce and publish writing and to interact and collaborate with others.

CCSS.ELA-Literacy.CCRA.W.7 Conduct short as well as more sustained research projects based on focused questions, demonstrating understanding of the subject under investigation.

CCSS.ELA-Literacy.CCRA.SL.1 Prepare for and participate effectively in a range of conversations and collaborations with diverse partners, building on others’ ideas and expressing their own clearly and persuasively.

CCSS.ELA-Literacy.RH.11-12.8 Evaluate an author's premises, claims, and evidence by corroborating or challenging them with other information.

McREL Technology. Standard 3. (Grade 9-12): Understands the relationships among science, technology, society, and the individual.

McREL Technology. Standard 3. (Grade 9-12):Understands the impact of the internet on society (e.g., addiction to and dependence on the internet; identity theft; access to unsuitable material)**.**

Assumed Student Prior Knowledge

This lesson assumes that students have experience using the Internet for personal and academic purposes, and have some experience or knowledge of authentication or password use online.

Materials

- [d0x3d!] board game
- Hacker role card
- Computer with Internet access or home access to internet
- Chart paper/white board

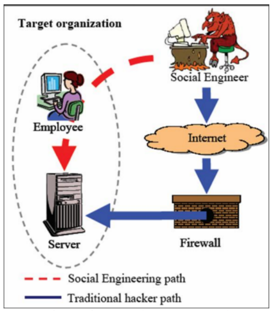
Vocabulary

Social Engineer
Digital Assets
Hacker
Dumpster diving

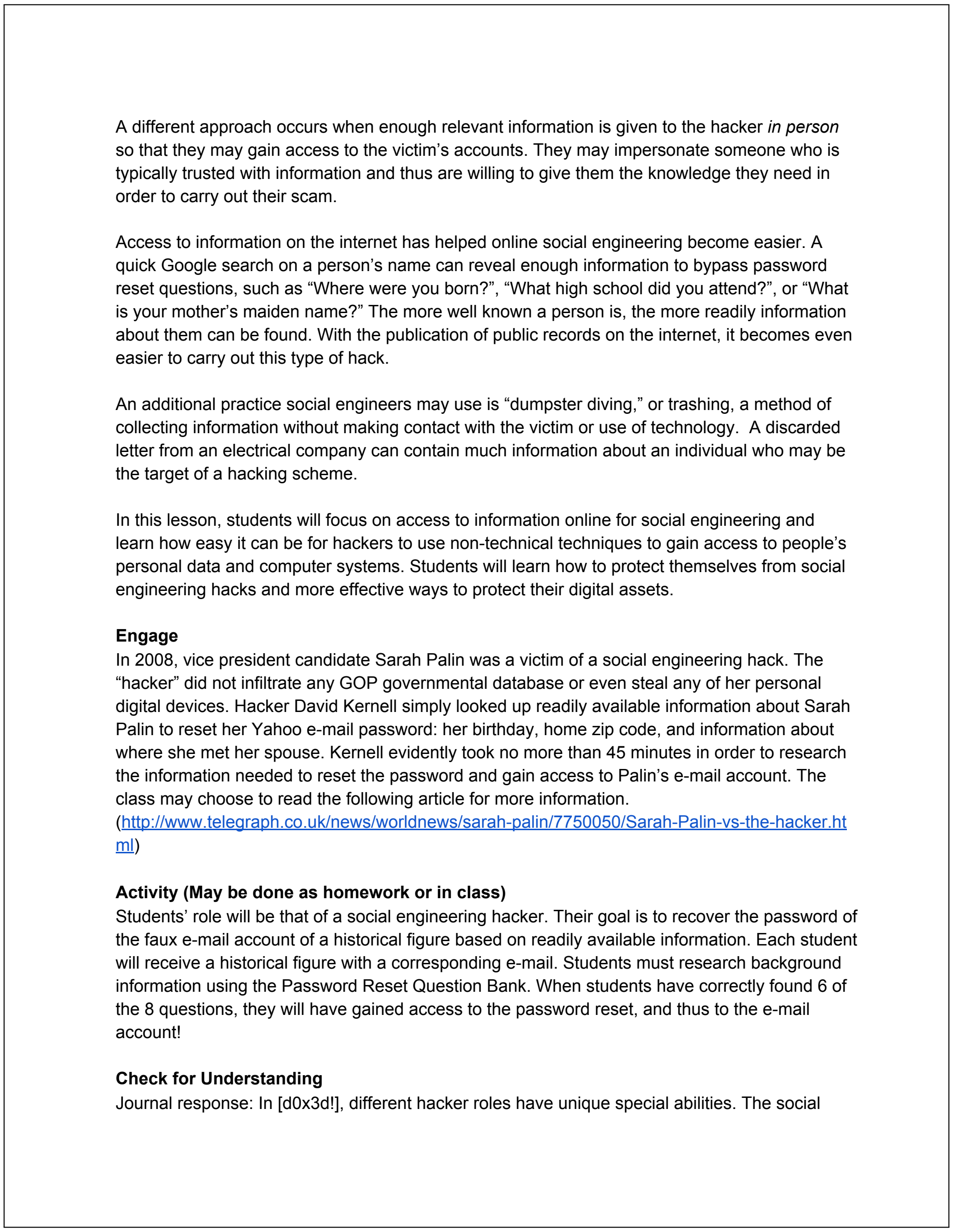
Background for Teacher

There has been an increase in news articles related to social engineering attacks. It's easy to see why: attackers know it is it easier to fool someone into giving information than to attempt to infiltrate a heavily guarded system in order to steal it.

Social engineers use a variety of different techniques. A user can be tricked into thinking they are interacting with a legitimate entity (person, company, etc.), and thus be willing to give up confidential information in a "phishing" attack. This may occur when a user receives an e-mail appearing to be from Facebook. In the e-mail, "Facebook" asks to confirm a friend request and includes a link that will lead to a fake Facebook login window. If credentials are entered, someone else now has their username and password!



Why Social Engineer (Hermansson, 2005)



A different approach occurs when enough relevant information is given to the hacker *in person* so that they may gain access to the victim's accounts. They may impersonate someone who is typically trusted with information and thus are willing to give them the knowledge they need in order to carry out their scam.

Access to information on the internet has helped online social engineering become easier. A quick Google search on a person's name can reveal enough information to bypass password reset questions, such as "Where were you born?", "What high school did you attend?", or "What is your mother's maiden name?" The more well known a person is, the more readily information about them can be found. With the publication of public records on the internet, it becomes even easier to carry out this type of hack.

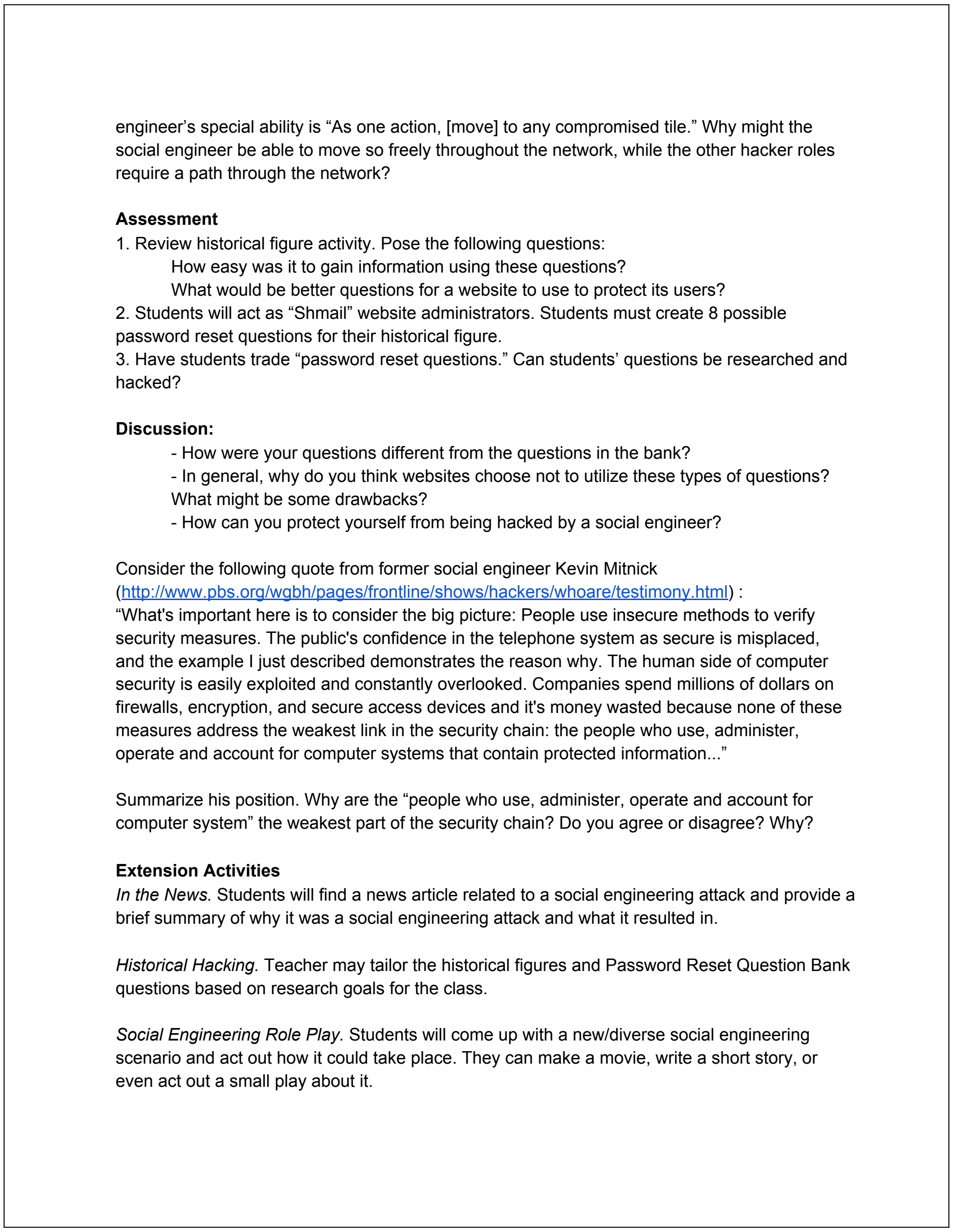
An additional practice social engineers may use is "dumpster diving," or trashing, a method of collecting information without making contact with the victim or use of technology. A discarded letter from an electrical company can contain much information about an individual who may be the target of a hacking scheme.

In this lesson, students will focus on access to information online for social engineering and learn how easy it can be for hackers to use non-technical techniques to gain access to people's personal data and computer systems. Students will learn how to protect themselves from social engineering hacks and more effective ways to protect their digital assets.

Engage
In 2008, vice president candidate Sarah Palin was a victim of a social engineering hack. The "hacker" did not infiltrate any GOP governmental database or even steal any of her personal digital devices. Hacker David Kernell simply looked up readily available information about Sarah Palin to reset her Yahoo e-mail password: her birthday, home zip code, and information about where she met her spouse. Kernell evidently took no more than 45 minutes in order to research the information needed to reset the password and gain access to Palin's e-mail account. The class may choose to read the following article for more information. (http://www.telegraph.co.uk/news/worldnews/sarah-palin/7750050/Sarah-Palin-vs-the-hacker.html)

Activity (May be done as homework or in class)
Students' role will be that of a social engineering hacker. Their goal is to recover the password of the faux e-mail account of a historical figure based on readily available information. Each student will receive a historical figure with a corresponding e-mail. Students must research background information using the Password Reset Question Bank. When students have correctly found 6 of the 8 questions, they will have gained access to the password reset, and thus to the e-mail account!

Check for Understanding
Journal response: In [d0x3d!], different hacker roles have unique special abilities. The social



engineer’s special ability is “As one action, [move] to any compromised tile.” Why might the social engineer be able to move so freely throughout the network, while the other hacker roles require a path through the network?

Assessment

1. Review historical figure activity. Pose the following questions:
    How easy was it to gain information using these questions?
    What would be better questions for a website to use to protect its users?
2. Students will act as “Shmail” website administrators. Students must create 8 possible password reset questions for their historical figure.
3. Have students trade “password reset questions.” Can students’ questions be researched and hacked?

Discussion:

- How were your questions different from the questions in the bank?
- In general, why do you think websites choose not to utilize these types of questions? What might be some drawbacks?
- How can you protect yourself from being hacked by a social engineer?

Consider the following quote from former social engineer Kevin Mitnick (http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html) :
“What's important here is to consider the big picture: People use insecure methods to verify security measures. The public's confidence in the telephone system as secure is misplaced, and the example I just described demonstrates the reason why. The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption, and secure access devices and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer, operate and account for computer systems that contain protected information...”

Summarize his position. Why are the “people who use, administer, operate and account for computer system” the weakest part of the security chain? Do you agree or disagree? Why?

Extension Activities

In the News. Students will find a news article related to a social engineering attack and provide a brief summary of why it was a social engineering attack and what it resulted in.

Historical Hacking. Teacher may tailor the historical figures and Password Reset Question Bank questions based on research goals for the class.

Social Engineering Role Play. Students will come up with a new/diverse social engineering scenario and act out how it could take place. They can make a movie, write a short story, or even act out a small play about it.

Handouts

Password Reset Question Bank

What is the name of your favorite pet?_______________

In what city were you born?_________________

What high school did you attend?_____________

What is the name of your spouse?_____________

What is your mother's maiden name?___________

When is your anniversary?________________

What is your father's middle name?____________

What is your zip code?_____________

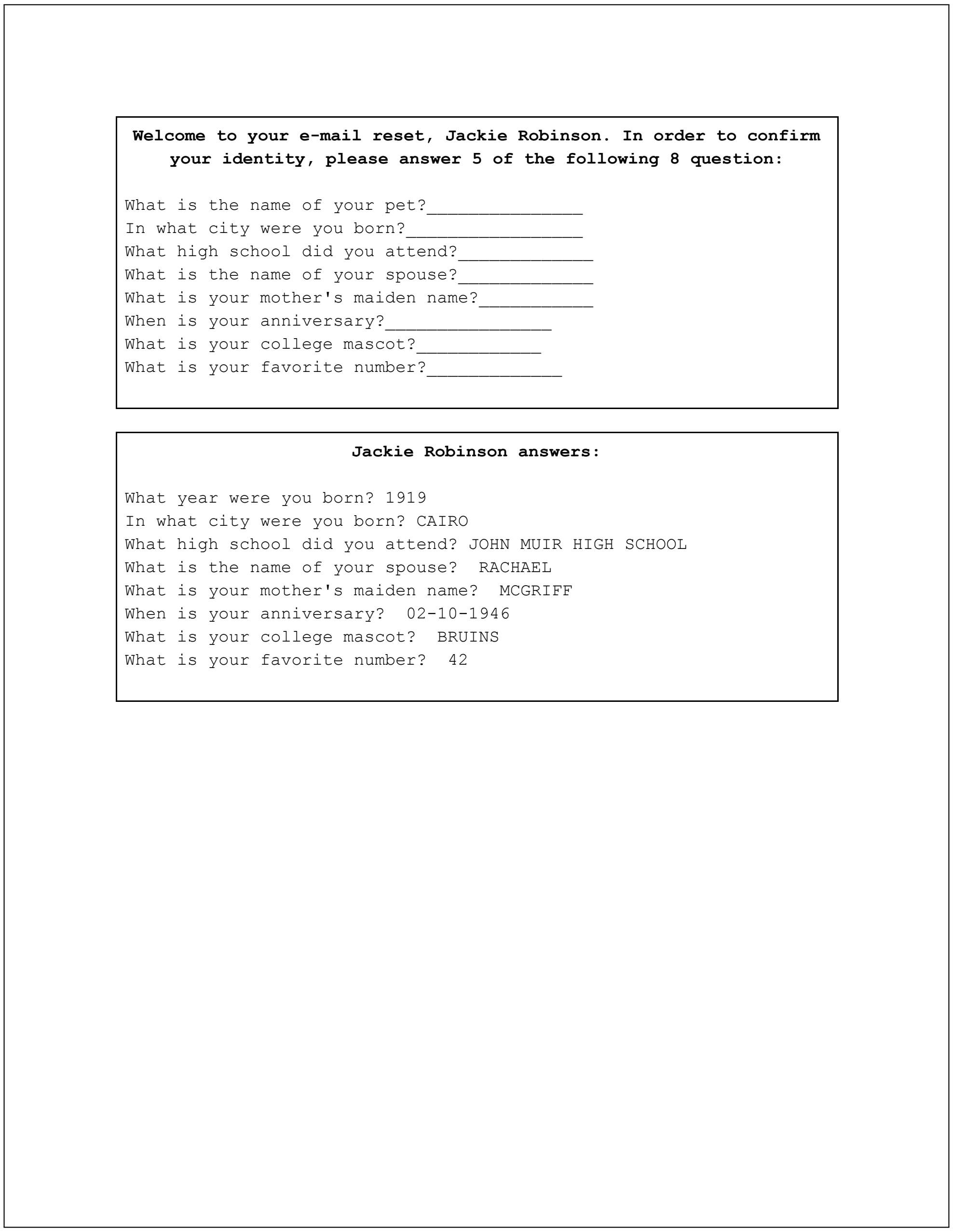
Examples:

```
   Welcome to your e-mail reset, Richard Nixon. In order to confirm
     your identity, please answer 5 of the following 8 question:

What is the name of your favorite pet?_______________
In what city were you born?_________________
What high school did you attend?_____________
What is the name of your spouse?_____________
What is your mother's maiden name?___________
When is your anniversary?________________
What is your father's middle name?____________
What is your zip code?_____________
```

```
                       Richard Nixon answers:

What is the name of your favorite pet? CHECKERS
In what city were you born? YORBA LINDA
What high school did you attend? FULLERTON UNION HIGH SCHOOL
What is the name of your spouse? PAT
What is your mother's maiden name? MILHOUS
When is your anniversary? 06-21-1940
What is your father's middle name? ANTHONY
What is your zip code? 20500
```



Welcome to your e-mail reset, Jackie Robinson. In order to confirm your identity, please answer 5 of the following 8 question:

What is the name of your pet?_______________
In what city were you born?_________________
What high school did you attend?_____________
What is the name of your spouse?_____________
What is your mother's maiden name?___________
When is your anniversary?________________
What is your college mascot?____________
What is your favorite number?_____________

Jackie Robinson answers:

What year were you born? 1919
In what city were you born? CAIRO
What high school did you attend? JOHN MUIR HIGH SCHOOL
What is the name of your spouse? RACHAEL
What is your mother's maiden name? MCGRIFF
When is your anniversary? 02-10-1946
What is your college mascot? BRUINS
What is your favorite number? 42

THIS PAGE INTENTIONALLY LEFT BLANK

REFERENCES

[1] Assessment Resources at HKU. "Bloom’s taxonomy". Accessed: 2013-07-01. [Online]. Available: http://ar.cetl.hku.hk/images/blooms.gif

[2] Frost *&* Sullivan. "The 2013 (ISC)2 global information security workforce study". Accessed: 2013-05-16. [Online]. Available: https://www.isc2.org/GISWSRSA2013/

[3] United Stated Department of Education. "The nation’s report card". Accessed: 2013-05-16. [Online]. Available: http://nces.ed.gov/nationsreportcard/pubs/studies/2011462.aspx

[4] The College Board. "AP exam volume changes (2002–2012)". Accessed: 2013-05-16. [Online]. Available: http://media.collegeboard.com/digitalServices/pdf/research/2012_exam_volume_change.pdf

[5] S. J. Cech. "College board intends to drop ap programs in four subjects". Accessed: 2013-05-16. [Online]. Available: http://www.edweek.org/ew/articles/2008/04/09/32ap.h27.html

[6] S. Zweben. "Computing research association Taulbee survey report 2009–2010". Accessed: 2013-05-16. [Online]. Available: http://cra.org/uploads/documents/resources/taulbee/CS_Degree_and_Enrollment_Trends_2010-11.pdf

[7] Bureau of Labor Statistics. "Occupational outlook handbook: Information security analysts, web developers, and computer network architects". Accessed: 2013-05-16. [Online]. Available: http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts-web-developers-and-computer-network-architects.htmf

[8] Microsoft. "A national talent strategy: Ideas for securing u.s. competitiveness and economic growth". Accessed: 2013-05-16. [Online]. Available: http://www.microsoft.com/en-us/news/download/presskits/citizenship/MSNTS.pdf

[9] S. Engle. "UCLA gets 2.5m to fund development program for computer science teachers". Accessed: 2013-05-16. [Online]. Available: http://newsroom.ucla.edu/portal/ucla/ucla-receives-2-5-million-grant-102576.aspx

[10] J. Cuny, “Transforming computer science education in high schools,” *Computer*, vol. 44, no. 6, pp. 107–109, 2011.

[11] [d0x3d!]. "[d0x3d!]:about". Accessed: 2013-05-16. [Online]. Available: http://d0x3d.com/d0x3d/about.html

[12] CyLab at Carnegie Mellon. "Anti-phishing phil". Accessed: 2013-05-16. [Online]. Available: http://cups.cs.cmu.edu/antiphishing_phil/

[13] C. E. Irvine, M. F. Thompson, and K. Allen, “Cyberciege: Gaming for information assurance,” *IEEE Security and Privacy*, vol. 3, no. 3, pp. 61–64, May 2005. [Online]. Available: http://dx.doi.org/10.1109/MSP.2005.64

[14] J. Hill, J. Surdu, S. Lathrop, G. Conti, and C. Carver, “MAADNET: Toward a web-distributed tool for teaching networks and information assurance,” in *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2003*, D. Lassner and C. McNaught, Eds. Honolulu, Hawaii, USA: AACE, 2003, pp. 773–776. [Online]. Available: http://www.editlib.org/p/13875

[15] Defense Information Systems Agency. "cyberprotect". Accessed: 2013-05-16. [Online]. Available: http://iase.disa.mil/eta/cyber-protect/launchpage.htm

[16] J. H. Saunders. "The case for modeling and simulation of information security". Accessed: 2013-05-16. [Online]. Available: http://www.johnsaunders.com/papers/securitysimulation.htm

[17] Microsoft. "The elevation of privilege (eop) card game". Accessed: 2013-05-16. [Online]. Available: http://www.microsoft.com/security/sdl/adopt/eop.aspx

[18] H. Hickey. "‘Control-alt-hack’ game lets players try their hand at computer security". Accessed: 2013-05-16. [Online]. Available: http://www.washington.edu/news/2012/07/24/control-alt-hack-game-lets-players-try-their-hand-at-computer-security/

[19] [d0x3d!]. "[d0x3d!]". Accessed: 2013-05-16. [Online]. Available: http://d0x3d.com

[20] Common Core State Standards Initiative. "In the states". Accessed: 2013-05-16. [Online]. Available: http://www.corestandards.org/in-the-states

[21] Mid-continent Research for Education and Learning. "Browse the online edition standards and benchmarks". Accessed: 2013-05-16. [Online]. Available: http://www2.mcrel.org/compendium/browse.asp

[22] The College Board. "AP computer science A course home page". Accessed: 2013-05-16. [Online]. Available: http://apcentral.collegeboard.com/apc/public/courses/teachers_corner/4483.html

[23] The College Board. "Important announcement about AP computer science AB". Accessed: 2013-05-16. [Online]. Available: http://apcentral.collegeboard.com/apc/public/courses/teachers_corner/195948.html

[24] The College Board. "Proposed new course and exam - ap computer science: Principles". Accessed: 2013-05-16. [Online]. Available: http://www.collegeboard.com/html/computerscience/

[25] Computer Science Unplugged. "Activities". Accessed: 2013-05-16. [Online]. Available: http://csunplugged.org/activities

[26] Y. Feaster, L. Segars, S. K. Wahba, and J. O. Hallstrom, "Teaching CS unplugged in the high school (with limited success)," in *Proceedings of the 16th annual joint conference on Innovation and technology in computer science education*, ser. ITiCSE '11. New York, NY, USA: ACM, 2011, pp. 248–252. [Online]. Available: http://doi.acm.org/10.1145/1999747.1999817

[27] Syracuse University. "SEED: Developing instructional laboratories for computer SEcurity EDucation". Accessed: 2013-05-16. [Online]. Available: http://www.cis.syr.edu/~wedu/seed/

[28] Towson University. "Security injections at towson university". Accessed: 2013-05-16. [Online]. Available: http://cis1.towson.edu/~cssecinj/

[29] DEF CON Communications. "DEF CON hacking conference - capture the flag archive". Accessed: 2013-05-16. [Online]. Available: http://www.defcon.org/html/links/dc-ctf.html

[30] University of California, Santa Barbara. "The UCSB iCTF". Accessed: 2013-05-16. [Online]. Available: http://ictf.cs.ucsb.edu/

[31] C. Irvine, "The value of capture-the-flag exercises in education: An interview with chris eagle," *IEEE Security & Privacy*, vol. 9, no. 6, pp. 58–60, 2011.

[32] Academic Games Leagues of America. "History". Accessed: 2013-05-16. [Online]. Available: http://agloa.org/history/

[33] Games for Thinkers. "Teacher resources". Accessed: 2013-05-16. [Online]. Available: http://gamesforthinkers.org/teacher-resources//

[34] Games in Education. "What is the games in education symposium?". Accessed: 2013-05-16. [Online]. Available: http://gamesineducation.org/about/

[35] M. Berland and V. R. Lee, "Collaborative strategic board games as a site for distributed computational thinking," *International Journal of Game-Based Learning*, vol. 1, no. 2, p. 65, 2011.

[36] I. Bezakova, J. E. Heliotis, and S. P. Strout, "Board game strategies in introductory computer science," in *Proceeding of the 44th ACM technical symposium on Computer science education*, ser. SIGCSE '13. New York, NY, USA: ACM, 2013, pp. 17–22. [Online]. Available: http://doi.acm.org/10.1145/2445196.2445210

[37] G. Wiggins, *Educative assessment: designing assessments to inform and improve student performance*, ser. Jossey-Bass education series. Jossey-Bass, 1998. [Online]. Available: http://books.google.com/books?id=LIHuAAAAMAAJ

[38] B. Grossen, "Overview: The story behind project follow through," *Effective School Practices*, vol. 15, no. 1, 1995.

[39] R. Slavin, *Cooperative learning*, ser. Research on teaching monograph series. Longman, 1983. [Online]. Available: http://books.google.com/books?id=5UAmAQAAIAAJ

[40] J. Bolen, E. Davis, and M. Rhodes, "Using a theory-based model for professional development: Implementing a national common core curriculum," *Southern Regional Council on Educational Administration Yearbook: Gateway to Leadership and Learning*, p. 15, 2012.

[41] J. Meltzer and E. T. Hamann, "Meeting the literacy development needs of adolescent english language learners through content-area learning-part two: Focus on classroom teaching and learning strategies," 2005.

[42] B. S. Bloom, M. B. Engelhart, E. J. Furst, W. H. Hill, and D. R. Krathwohl, *Taxonomy of educational objectives. The classification of educational goals. Handbook 1: Cognitive domain*. New York: Longmans Green, 1956.

[43] A. Abran, J. Moore, P. Bourque, R. DuPuis, and L. Tripp, "Guide to the software engineering body of knowledge 2004 version," *Guide to the Software Engineering Body of Knowledge, 2004. SWEBOK*, pp. –, 2004.

[44] G. A. Burgess, “Introduction to programming: blooming in america,” *J. Comput. Sci. Coll.*, vol. 21, no. 1, pp. 19–28, Oct. 2005. [Online]. Available: http://dl.acm.org/citation.cfm?id=1088791.1088796

[45] T. Scott, “Bloom’s taxonomy applied to testing in computer science classes,” *J. Comput. Sci. Coll.*, vol. 19, no. 1, pp. 267–274, Oct. 2003. [Online]. Available: http://dl.acm.org/citation.cfm?id=948737.948775

[46] R. A. Howard, C. A. Carver, and W. D. Lane, “Felder’s learning styles, bloom’s taxonomy, and the kolb learning cycle: tying it all together in the cs2 course,” *SIGCSE Bull.*, vol. 28, no. 1, pp. 227–231, Mar. 1996. [Online]. Available: http://doi.acm.org/10.1145/236462.236545

[47] I. Sanders and C. Mueller, “A fundamentals-based curriculum for first year computer science,” in *Proceedings of the thirty-first SIGCSE technical symposium on Computer science education*, ser. SIGCSE ’00. New York, NY, USA: ACM, 2000, pp. 227–231. [Online]. Available: http://doi.acm.org/10.1145/330908.331860

[48] D. Oliver, T. Dobele, M. Greber, and T. Roberts, “This course has a bloom rating of 3.9,” in *Proceedings of the Sixth Australasian Conference on Computing Education - Volume 30*, ser. ACE ’04. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2004, pp. 227–231. [Online]. Available: http://dl.acm.org/citation.cfm?id=979968.979998

[49] C. G. Johnson and U. Fuller, “Is bloom’s taxonomy appropriate for computer science?” in *Proceedings of the 6th Baltic Sea conference on Computing education research: Koli Calling 2006*, ser. Baltic Sea ’06. New York, NY, USA: ACM, 2006, pp. 120–123. [Online]. Available: http://doi.acm.org/10.1145/1315803.1315825

[50] B. Manaris and R. McCauley, “Incorporating hci into the undergraduate curriculum: Bloom’s taxonomy meets the cc’01 curricular guidelines,” in *Frontiers in Education, 2004. FIE 2004. 34th Annual*, 2004, pp. T2H/10–T2H/15 Vol. 1.

[51] C. W. Starr, B. Manaris, and R. H. Stalvey, “Bloom’s taxonomy revisited: specifying assessable learning objectives in computer science,” *SIGCSE Bull.*, vol. 40, no. 1, pp. 261–265, Mar. 2008. [Online]. Available: http://doi.acm.org/10.1145/1352322.1352227

[52] E. Thompson, A. Luxton-Reilly, J. L. Whalley, M. Hu, and P. Robbins, “Bloom’s taxonomy for cs assessment,” in *Proceedings of the tenth conference on Australasian*

computing education - Volume 78, ser. ACE '08. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2008, pp. 155–161. [Online]. Available: http://dl.acm.org/citation.cfm?id=1379249.1379265

[53] C. Tomlinson and J. McTighe, *Integrating Differentiated Instruction and Understanding by Design: Connecting Content and Kids*, ser. Connecting Content And Kids. Association for Supervision and Curriculum Development, 2006. [Online]. Available: http://books.google.com/books?id=OmiaaeNRCX4C

[54] R. Lister and J. Leaney, "Introductory programming, criterion-referencing, and bloom," *SIGCSE Bull.*, vol. 35, no. 1, pp. 143–147, Jan. 2003. [Online]. Available: http://doi.acm.org/10.1145/792548.611954

[55] A. M. Guillaume, *K-12 Classroom Teaching: A Primer for New Professionals*, 3rd ed. Pearson, 2008.

[56] National Aeronautics and Space Administration. "NASA - 5Es overview: "The 5E instructional model"". [Online]. Available: http://www.nasa.gov/audience/foreducators/nasaeclips/5eteachingmodels/index.html

[57] W. Baker, A. Hutton, C. D. Hylender, J. Pamula, C. Porter, and M. Spitler, "2011 data breach investigations report," http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf, Verizon Business, Tech. Rep., 2011.

[58] Technology, Entertainment, Design. "misha glenny: Hire the hackers!". Accessed: 2013-07-01. [Online]. Available: http://www.ted.com/talks/misha_glenny_hire_the_hackers.html

[59] Computing in the Core. "Issues and solutions". [Online]. Available: http://www.computinginthecore.org/issues-solutions

[60] Mid-continent Research for Education and Learning. "McREL: mid-continent research for education and learning, content knowledge standards and benchmark database". [Online]. Available: http://www2.mcrel.org/compendium/SubjectTopics.asp?SubjectID=19

[61] M. Hunter, *Enhancing teaching*. Macmillan College Publishing Company, 1994. [Online]. Available: http://books.google.com/books?id=5T-LQgAACAAJ

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudly Knox Library
   Naval Postgraduate School
   Monterey, California