Cyber Security Syllabus

Instructor

Marda Olson

Phone

605-864-1855

Email

Marda.Olson@k12.sd.us

Course Description

This Cyber Security course is based around a curriculum designed by Iowa State University that was funded by the Department of Justice and supplemented by other resources identified in the course.

This curriculum focuses on the first focus for cyber security… the user and on topics a user would face on a day-to-day basis. The curriculum works to strengthen the weakest link in cyber security, the user, by providing a concrete and applicable education about information technology. Students will relate the information they learn to real world situations Students will become familiar with security terms and mechanisms, security best practices, and identify security threats, sources and motivations.

The goals of this course are that students will:

- define computer security terms and mechanisms.
- describe fundamental security concepts.
- state computer security best practices.
- describe the strengths, weaknesses, and limitations of security mechanisms and concepts.
- give examples of common security threats, threat sources, and threat motivations.
- explain their role in protecting their own physical and non-physical computing assets.
- discuss current events topics and read security articles in the popular press.
- assess computing actions in the context of security.

Introduction

Students are in near constant contact with the Internet and as schools continue to incorporate more technology into curricula, students need to be aware of computer security issues and how to take steps towards mitigating the realistic security threats they may encounter. ~Tracy LaVan www.security-literacy.org

Course Materials

Content is contained and will be delivered through SD K-12 Blackboard Learn, referencing text, illustrations, videos, and activities. All assignments are contained within the Content section of Blackboard Learn.

Course of Study

Unit 1 – Introduction to Information Security

The goals and student objectives of this unit are that students will…

- be able to articulate the importance of information security.
- explain confidentiality, integrity and availability (CIA Triad) as the foundation of information security.
- identify vocabulary words presented in this chapter.
- identify basic online safety tips and advice

1.1 What is and why study cyber security?
1.2 CIA Triad
1.3 Cyber Security Terminology
1.4 Online Safety Habits – Tips & Advice

Unit 2 – Demystifying the Internet

The goals and student objectives of this unit are that students will…

- be able to summarize what the Internet is and how it works.
- be able to distinguish between the Internet and World Wide Web.
- be able to illustrate the hierarchical structure of the Internet.
- be able to explain how IP addresses are assigned to devices.
- be able to describe how information travels through the Internet.

2.1 The Internet – Protocol, IP, ISP
2.2 The Internet – Backbone, IP, Addressing
2.3 The Internet – DNS, Routing Tables, Web Pages

Unit 3 – What about Passwords

The goals and student objectives of this unit are that students will…

- be able to identify why passwords are important to us
- be able to explain how hash functions work to encrypt passwords
- be able to summarize and categorize common password threats – which ones they can defend themselves against and which ones they cannot
- be able to construct a strong password
- be able to differentiate between strong and weak passwords by analyzing existing passwords
- be able to revise existing passwords to make them stronger
- summarize and articulate information on passwords to others
- explain what a vulnerability is and how they impact cybersecurity,
- identify elements of their personal data which may be vulnerable to attack,

3.1 Cyber Insecurity
3.2 Personal Data – Simple Digital Footprint
3.3 Passwords / Hash Functions
3.4 Common Password Threats
3.5 Phishing
3.6 Strong Passwords
3.7 Password Management

Unit 4 – Social Engineering

The goals and student objectives of this unit are that students will…

- be able to describe the process an email takes when traveling from sender to recipient
- analyze and critique a company’s response to the public on an email hacking incident
- understand the premise of social engineering and it's role in cyber security
- differentiate between phishing, spear-phishing and whaling

4.1 Email Security
4.2 Social Engineering
4.3 Phishing, Spear Phishing & Whaling

Unit 5 – Malware

The goals and student objectives of this unit are that students will…

- be able to explain the difference between the various types of malware
- compare and contrast the different types of malware
- be able to identify and summarize the most common functions of malware
- be able to identify the effects of the different functions of malware
- be able to identify the eight most common sources of malware
- read an article, formulate an opinion, and develop a logical argument to defend their position on current cyber security events abroad
- be able to describe how to prevent or minimize malware attacks

5.1 Types of Malware
5.2 Functions of Malware
5.3 Malware – Sources / Solutions
5.4 Malware in the Real World

Unit 6 – The Web

The goals and student objectives of this unit are that students will…

- be able to describe the process a computer takes when interacting with a web browser
- learn to distinguish between good and bad hyperlinks by viewing source code on a webpage
- examine the tradeoff between security and convenience as it relates to web browser security
- evaluate and critique various internet security tools/technologies
- understand and evaluate the use web caching and cookies as it pertains to user experience and risk
- identify the practices for safe surfing

6.1 How the Web works, Cache, Cookies
6.2 Cookies
6.3 Secure Browsing

Unit 7 – Online Shopping & Wireless WiFi

The goals and student objectives of this unit are that students will…

- identify and list online shopping threats and how to diminish them
- analyze and critique an infographic about online shopping
- connect the information they know about online shopping and the infographic they analyzed to create their own infographic
- recognize how wireless internet connections function
- identify the security threats surrounding wireless internet connections
- distinguish behaviors that should be used and avoided on public Wi-Fi
- recognize steps they can take with their personal wireless routers at home to minimize threats

7.1 Online Shopping Safety Guidelines
7.2 Share the Knowledge
7.3 Wireless (WiFi) Connections
7.4 Security Dangers of Public WiFi
7.5 Safety Tips for Using Public WiFi

Unit 8 – Social Media and Privacy

The goals and student objectives of this unit are that students will…

- identify the types of social media
- explore how their social media content could have future consequences
- investigate how their sharing on social media can lead to them becoming targets of cyber criminals
- be able to define social engineering and explain four common threats associated with social engineering
- analyze a URL to determine where it leads and if it could be malicious
- analyze scenarios, formulate oppinions and present logical arguments of the effects of employment and social media privacy
- understand meta-tags and the role they play in vulnerability and cyber security

8.1 Social Media Explained
8.2 Sharing on Social Media
8.3 Metadata

Unit 9 – Cyber Good Guys

The goals and student objectives of this unit are that students will…

- understand the role of ethical hackers
- evaluate scenarios to classify hackers as black, white or gray hackers
- be introduced to skills required for ethical hacking
- be introduced to career opportunities in cyber security

9.1 Cyber Ethics
9.2 Ethical Hacking – Hacker / Cracker
9.3 Cyber Careers

Homework Policy

The course is self-paced with suggested unit completion dates equating to successful completion of the course. Students and facilitators will be invited to the online course gradebook using ThinkWave. Please check it often for assignment discrepancies and course progress.